

**QUESTION BANK
UNIT – I****PART – A****1. What is the fundamental principle of wireless communication ?**

The fundamental principle of wireless communication is electromagnetic wave transmission between a transmitter and a receiver.

2. Mention the categories of frequency spectrum.

The frequency spectrum can be divided into the following categories:

- very low frequency (VLF), low frequency (LF),
- medium frequency (MF), high frequency (HF),
- very high frequency (VHF), ultra-high frequency (UHF),
- super-high frequency (SHF), extremely high frequency (EHF), infrared,
- visible light, ultraviolet, X-ray, gamma-ray, and cosmic ray.

3. What is the difference between guided and unguided medium ?

- The guided medium carries **signals** or waves between a **transmitter and a receiver**, whereas the unguided medium typically carries **wireless signals** between an antenna and a receiver.

4. What are the dimensions of Multiplexing?

- Space, Frequency, Time, Code Division Multiplexing

5. What is multiplexing ? Mention the different ways of multiplexing.

Multiplexing is a collection of schemes that addresses the issue of transmitting multiple signals simultaneously in a wireless system to maximize the capacity of the system.

- Frequency-division multiplexing FDM: Subdivide the frequency without overlapping
- Time -division multiplexing TDM: Multiple digital signals can be carried on a single transmission path by interleaving portions of each signal in time
- Code Division Multiplexing CDM: Multiple users shares the same band at the same time, differentiated by code.

6. What limits the number of user in TDM & FDM compared to CDM?

The code space is huge compared to the frequency space and time space. Because of the limited time space and frequency space, the number of users in TDM & FDM are limited.

7. What is spread spectrum technique?

In order to avoid a jammer, the transmitter shifts the center frequency of the transmitted signal. If, move the center frequency randomly among 100 different frequencies than the required transmission bandwidth is 100 times more than the original transmission bandwidth. This is called spread spectrum because the spectrum is spread over a band that is 100 times larger than original traditional radio.

8. What are ways spectrum can be achieved?

- Direct sequence spread spectrum
- Frequency hopping spread spectrum.

9. What is FHSS?

- Frequency Hopping Spread spectrum.
- FHSS is a narrow band signal
- It uses frequency hopping system
- It uses 78 frequency in the 2.4 GHz

10. What are the main benefits of a spread spectrum?

The main benefit of spread spectrum is the resistance to narrow band interference. The spread spectrum converts the narrow band into a broad band signal. The energy needed to transmit the signal is the same, but it is now spread over a large frequency range. Thus the power level of the signal can be much lower than that of the original narrowband signal.

11. What is the frequency allocation of GSM?

- The GSM system has an allocation of 50 MHz (890-915 MHz and 935-960 MHz) bandwidth in the 900 MHz frequency band. GSM uses a combination of FDMA and TDMA.
- Using FDMA, this band is divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz. Using TDMA, each of these channels is then further divided into 8 time slots. (maximum of 992 channels),

12. Define HLR database.

The HLR is the most important Database in a GSM system as it stores all user-relevant information. This comprises static information, such as the mobile subscriber ISDN number (MSISDN). It contains Dynamic information like the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC.

13. What are the information stored in VLR database?

VLR is similar to a cache, whereas HLR is the persistent storage. The VLR contains selected administrative information borrowed from the HLR, necessary for call control and provisioning. When a MS enters the covering area of a new MSC, the VLR associated with this MSC will request information from its corresponding HLR in the home network. The VLR will then have enough information in order to assure the subscribed services without needing to refer to the HLR each time a communication is established

14. What are the databases used in OSS of GSM?

Authentication Centre (AuC) : is responsible for the authentication of a subscriber. This is a protected database and stores a copy of the secret key stored in each subscriber's SIM card. These data help to verify the user's identity.

Equipment identity register (EIR): The EIR is a database for all IMEIs, i.e., it stores all device identification registered for this network. The EIR has a blacklist of stolen (or locked) devices. The EIR also contains a list of malfunctioning devices

15. What are the Sequence of operations from speech to radio waves in call routing of GSM ?

Digitizer and source coding , Channel coding , Interleaving, Ciphering Burst formatting Modulation Multipath and equalization , Synchronization

16. What is the significance of digits in MSISDN?

The MSISDN categories follow the international ISDN (Integrated Systems Data Network) numbering plan as:

- Country Code (CC): 1 to 3 decimal digits of country code
- National Destination Code (NDC): Typically 2 to 3 decimal digits
- Subscriber Number (SN): maximum 10 decimal digits.

17. What is MSRN and TMSI?

Mobile Station Roaming Number (MSRN): When a subscriber is roaming in another network a temporary ISDN number is assigned to the subscriber. This ISDN number is assigned by the local VLR in charge of the mobile station. The MSRN has the same structure as the MSISDN.

Temporary Mobile Subscriber Identity (TMSI): This is a temporary identifier assigned by the serving VLR. in place of the IMSI for identification and addressing. TMSI is assigned in a VLR. The TMSI is never stored in the HLR. However, it is stored in the SIM card. Together with the current location area, a TMSI allows a subscriber to be identified uniquely. For an ongoing communication the IMSI is replaced by the 2-tuple LAI, TMSI code.

18. What are the security services provided in GSM?

Access Control and Authentication: It does Authentication of valid user for the SIM. The user need a secrete PIN to access the SIM. Subscriber authentication is based on challenge response scheme

- **Confidentiality** : User related data is encrypted. BTS and MS apply encryption to voice, data, and signaling. This confidentiality exists only between MS and BTS and not end-to-end
- **Anonymity** : To provide user anonymity, all data is encrypted before transmission, and user identifiers which would reveal an identity are not used over the air. GSM transmits a temporary identifier(TMSI),which is newly assigned by the VLR after each location update.

19. List out the strengths of SMS

- Omnibus nature of SMS: SMS uses SS7 signaling channel, which is available throughout the world
- Stateless SMS is session less and stateless. SMS is the best bearer for notifications, alerts and paging.
- Asynchronous: SMS is completely asynchronous., SMS can be used as message queues.
- Self-configurable and last mile problem resistant: SMS is self-configurable.
- Non-repudiation: SMS message carries the SC and the source MSISDN as a part of the message header. SMS can prove the origin of the SMS unlike IP.
- Always connected: SMS message is delivered to the MS without any interruption to the call

20.What are the two basic types of SMS ?

- SM MT is an incoming short message from the network side and is terminated in the MS. incoming message the path is from SC to the MS via HLR and the GMSC function of the home MSC
- SM MO is an outgoing message, originated in the user device (MS), and forwarded to the network for delivery. For outgoing message, the path is from MS to SC via the VLR and the IWMSC function of the serving MSC.

21. What is hand over? How it is different from roaming?

The user movements may make a user move away or closer to a tower. When the user moves away from a tower, the radio signal strength or the power of the signal keeps reducing. This can result in change of the channel or cell. This procedure of changing the resources is called handover/ `handoff`.

Handover relates to moving from one point of attachment to another point of attachment within the same network operator; when this movement happens between two different networks it is called roaming.

22.What are the different types of terminals-GPRS ?

- Class A terminal can make or receive calls on two services simultaneously. GPRS virtual circuits will be held or placed on busy rather than being cleared. SMS is supported in Class A terminal
- Class B terminal can monitor GSM and GPRS channels simultaneously, but can support only one of these services at any time. Therefore, a Class B terminal can support simultaneous attach, activation, and monitor but not simultaneous traffic. GPRS virtual circuits will be held or placed on busy rather than being cleared.
- Class C terminal supports only non-simultaneous attach. The user must select which service to connect to. Class C terminal can make or receive calls from only the manually selected network service. t support of SMS is optional for Class C terminals.

23.List out bearer services of GPRS

The bearer services of GPRS offer end-to-end packet switched data transfer. It supports: the point-to-point (PTP) service and the point-to-multipoint (PTM) service.

- SMS: It was originally designed for GSM . GPRS will continue to support SMS as a bearer.
- WAP: It is a data bearer service over HTTP protocol.

- **MMS:** MMS is Multimedia Messaging Service. This is the next generation messaging service.

24. List out GPRS-Specific Applications (any 5)

Chat : GPRS will offer ubiquitous chat by integrating Internet chat and wireless chat using SMS and WAP.

Multimedia Service: Multimedia objects like photographs, pictures, postcards, greet-ing cards and presentations, static web pages can be sent and received over the mobile network.

Virtual Private Network: GPRS network can be used to offer VPN services. Many banks are migrating from VSAT to GPRS-based networks because the transaction time reduced by 25%.

Personal Information Management: Personal diary, address book, appointments, engagements are kept in the phone some in the organizer and some in the Intranet.

Job Sheet Dispatch: GPRS can be used to assign and communicate job sheets from office-based staff to mobile field staff. It can be combined with vehicle positioning applications so that the nearest available suitable personnel can be deployed to serve a customer.

Unified Messaging: Unified messaging uses a single mailbox for all messages, including voice mail, fax, e-mail, SMS, MMS, and pager messages.

Vehicle Positioning: This application integrates GPS that tell people where they are. Vehicle-positioning applications can be used to deliver several services including remote vehicle diagnostics, ad hoc stolen vehicle tracking and new rental car fleet tariffs and services in logistics industry.

Location-based Services and Telematics: Location-based services provide the ability to link push or pull information services with a user's location. Examples include hotel and restaurant finders, roadside assistance, and city-specific news and information.

25. Mention the limitations of GPRS.

Limited Cell Capacity for All Users: There are only limited radio resources. Voice and GPRS calls use the same network resources. Use for one data precludes simultaneous use for voice.

Speed Lower in Reality: Achieving the theoretical maximum GPRS data speed of 172.2 kbps would require a single user taking over all eight time slots without any error protection. It is not common. The initial GPRS terminals are expected to be supporting only one, two or maximum three time slots.

GPRS Mobile Terminate Connection for a Mobile Server not supported: There are many services for which the server needs to be mobile. (e.g mobile healthcare center for rural population). Using GPRS network, such communication is not possible.

UNIT – II**1. List out IEEE 802.11 WLAN standards**

WLANs are flexible data communications systems implemented as an extension or as an alternative for wired LANs. WLANs transmit and receive data over the air using radio frequency (RF) technology. WLANs combine data connectivity with user mobility.

802.11a OFDM	High-speed physical layer in 5GHz band
802.11b DSSS Wi-Fi	Higher-speed phy layer extension in 2.4GHz
802.11d	Local and metropolitan area
802.11g OFDM > 20Mbps	wireless Broadband
802.11i	wireless Security
802.11n OFDM/ MIMO >100 Mbps	Wideband service

2. State applications of WLAN

- WLANs are deployed by Manufacturers for process and control applications.
- Retail applications have been expanded using wireless point of sale (WPOS).
- The health-care and education industry are also growing with WLANs.
- WLANs provide high-speed, reliable data communications in a campus as well as coverage in rural
- WLANs are more robust against disasters like, earthquakes

3. Compare: infrared vs. radio transmission technology for wireless communication

INFRARED	RADIO
Advantages simple, cheap, available in many mobiles No government regulations controlling Immunity to electro-magnetic (EM) and RF interference Disadvantages a short-range technology (30–50 ft) Signals cannot penetrate solid objects Signal affected by light, snow, ice, fog Used in : IrDA Devices	Advantages Longest range Low cost solution for large sites with medium data throughput Large radio and antennas increase wireless client size Disadvantages RF site license required for protected bands No multivendor interoperability Low throughput and interference potential Used in : WLAN , Bluetooth Devices

4. Define Spread Spectrum Technology and its types

Wideband RF technique uses the entire allotted spectrum in a shared fashion. Spectrum is spread over a band that is 100 times larger than original. The SS system spreads the transmission power over the entire usable spectrum.

Disadvantage: a less efficient use of the bandwidth than the narrowband approach.

Advantages: resistance to narrow band interference ,
 good trade off bandwidth efficiency for reliability, integrity, security and power needed.

Types : Direct sequence SS (DSSS) and frequency-hopping SS (FHSS).

5. State different WAN topologies WLAN Topologies

- **Peer-to-peer (ad hoc) topology** - client devices within a communication range can communicate directly to each other.
- **AP-based topology** - uses APs to bridge traffic onto a wired (Ethernet or Token Ring) or a wireless backbone. more commonly used topology.
- **Point-to-multipoint bridge topology**-Wireless bridges connect LANs in one building to LANs in another building even if the buildings are miles apart so that receive a clear line- of-sight between buildings.

6. Why CSMA/CD used in 802.3 cannot be used on a WLAN ?

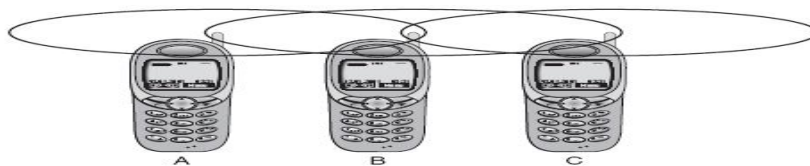
CSMA/CD used in 802.3 cannot be used on a WLAN for two reasons:

- Implementing a collision detection mechanism would require the implementation of a full duplex radio that increase the cost significantly.
- In a wireless environment a station that wants to transmit senses the medium as free does not necessarily mean that the medium is free around the receiver area- **hidden and exposed station problem**

7. What is Hidden station problem and exposed station problem ?

Hidden station problem:

- A sends to B, C cannot receive A
- C wants to send to B, C senses a “free” medium (CS fails)
- collision at B, A cannot receive the collision (CD fails)
- A is “hidden” for C



Exposed terminals

- B sends to A, C wants to send to another terminal (not A or B)
- C has to wait, CS signals a medium in use
- but A is outside the radio range of C, therefore waiting is not necessary
- C is “exposed” to B

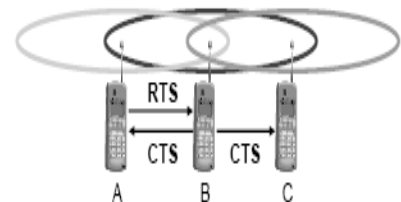
8. What is the use of RTS and CTS?

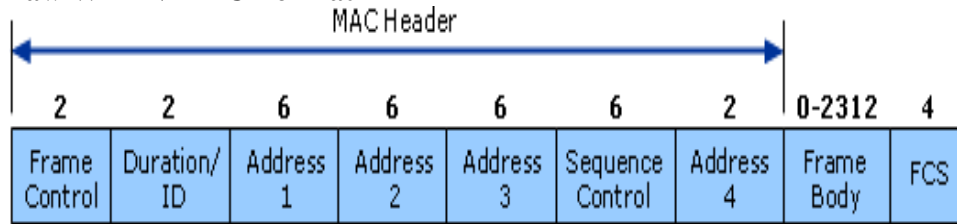
CSMA with CA uses short signaling (control) packets to eliminate hidden station and exposed station problem:

- **RTS** (request to send): a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
- **CTS** (clear to send): the receiver grants the right as soon as it is ready

Signaling packets contain:

- sender address ,receiver address
- packet size (from which the transmission time can be derived)

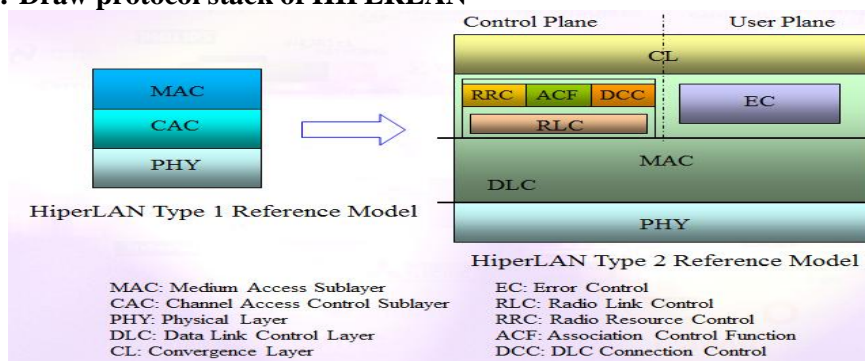


9. Draw WLAN MAC Format**10. Comparison of HIPERLAN/2 and IEEE 802.11.**

Characteristics	IEEE 802.11	HIPERLAN/2
Spectrum	2.4GHz	5GHz
Max. physical rate	2Mbps	54Mbps
Max. data rate, layer-3	1.2Mbps	32Mbps
Access scheme	DCF/PCF	Elimination yield non-preemptive priority multiple access
Connectivity	Connectionless	Connection-oriented
QoS support	PCF	ATM/802.1p/Resource reservation Protocol/
Frequency selection	FHSS or DSSS	Single carrier with dynamic frequency selection
Authentication		Network access identifier/IEEE address/X.509
Encryption	40-bit RC4	Data Encryption Standard (DES), triple DES
Handover support	No	No

11. What is the purpose of WAP/ applications of WAP?

- WAP is an open international standard for accessing web in wireless environment.
- The purpose of WAP is to facilitate browsing and use the wired Internet such that it is protocol independence.
- WAP provides a powerful framework for mobile applications to offer interactive data services and interactivity support Internet and Web.
- WAP defines an industry-wide specification for developing service applications.

12. Draw protocol stack of HIPERLAN**13. List High Performance Radio Local Area Networks Family of Standards.**

	Hiperlan 1	Hiperlan2	HiperAccess	HiperLink
Description	Wireless Ethernet	Wireless ATM	Wireless Local Loop	Wireless Point-to-Point
Freq. Range	5GHz	5GHz	5GHz	17GHz
PHY Bit Rate	23.5Mbps	6~54Mbps	~25Mbps (data rate)	~155Mbps (data rate)

14. What is the use of WAP Gateway?

- Gateway does protocol conversions between two ends—mobile client device and HTTP server.
- It has caches which is required due to frequent disconnections in the wireless environment.
- The gateway ensures security in wireless and wired networks.
- the gateway performs is iWML Script compilation and convert to CGI scripts for HTTP server

15. What is WBXML?

- WBXML is a specification in binary representation so that XML-based language can be transmitted in compact format. Here, a binary number can represent a tag in place of characters and an attribute in place of characters. Eg attribute ID that needs two characters can be represented by a single byte
- Hence, the binary format causes compact transmission. There is no change in contents, code-functionality and semantic information. WBXML keeps the element structure of XML intact.

16. Define WAP Protocols / Draw WAP protocol suite

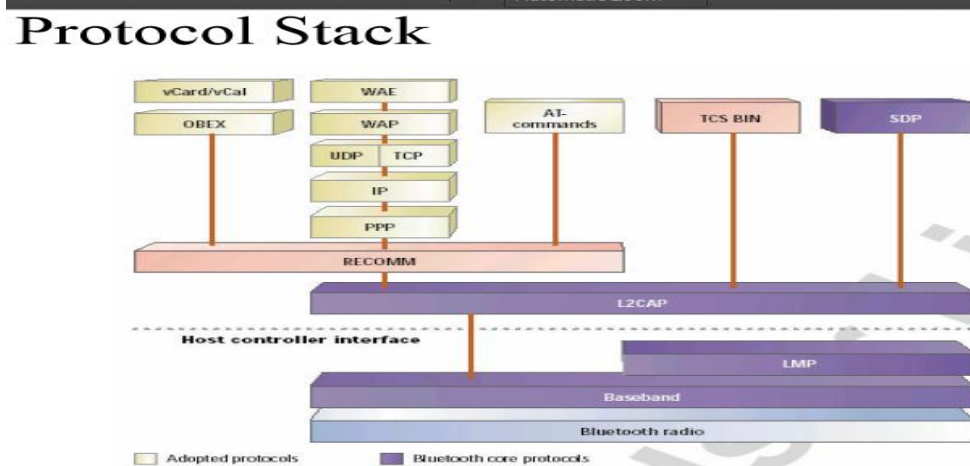
Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
Wireless Datagram Protocol (WDP)
*** Any Wireless Data Network ***

- WDP is used for transmitting and receiving the datagram over the network like UDP.
- WTLS, an optional layer, provides security mechanism similar to TLS.
- WTP provides transaction support (reliable request/response) adapted to the wireless world. and supports more effectively than TCP the problem of packet loss in wireless n/w
- WSP is as a compressed version of HTTP.
- Application layer includes Wireless Application Environment (WAE) which provides web services.

17. Difference between WAP 1.1 and WAP 2.0

WAP 1.1	WAP 2.0
Employs optimized protocols for relatively inexpensive terminals and low bandwidth wireless networks while sharing the tasks with WAP gateway	WAP2 assumes relatively high performance mobile terminals and employs a lot of Internet standards.
Enables mobile terminals to be simple, but secure connections must be severed by the WAP gateways to exchange WAP1 protocols with the Internet.	This enables WAP2 mobile terminals to interact with servers in the Internet directly and then to establish secure channels with them end-to-end.
WML is really simple and difficult to do any kind of text formatting or graphics with it. It uses tags, cards, decks	XHTML Mobile Profile (XHTML MP) is the markup language. Using XHTML MP and WAP CSS, it also possible to separate content and presentation . XHTML substitute for the <card> is the <body> tag.
Transmission protocol is WAP.	Transmission protocol is wTCP/IP.

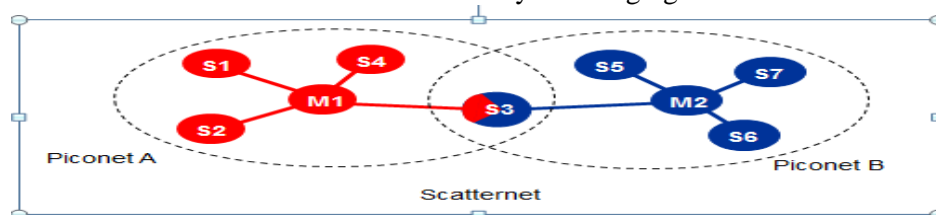
18. List the Bluetooth protocols



- Radio Layer Baseband (Link Controller) Link Manager Protocol (LMP)).
- Logical Link Control and Adaptation Protocol (L2CAP) : SDP (Service discovery protocol
- HCI (Host control interface RFCOMM TCS BIN OBEX

19. What is a piconet?

- Bluetooth devices form a network known as *piconet* with the devices within a distance of about 10 m.
- A piconet has master—slave architecture. The device which first establishes a piconet becomes the master. Other devices which discover the master become the slaves in that piconet. All devices in a Piconet have identical hopping sequences. In a piconet, there can be a maximum of eight devices including the master.
- Scatter net is an ad-hoc network formed by the bridging devices that connects two piconets.



20. Compare different Bluetooth versions

Version/ Features	Bluetooth1.v	Bluetooth2.v	Bluetooth3.v +SH	Bluetooth1.v
Data Rate	1 Mbps	1 to 3 Mbps	3 to 24 Mbps	24 Mbps
Features	No encryption	Simple pairing, Extended inquiry response, Less power consumption	unicast connectionless data, AES encryption.	low-energy technology, for small battery sensors
Setup delay	< 6s	< 6s	3s	3s
EDR	3 Mbps	2.1 Mbps	2.1 Mbps	2.1 Mbps

21.Compare Bluetooth and IrDA

Bluetooth	IrDA
Bluetooth is for wireless short range exchanges in mobile environment within 10 m network	IrDA is for exchanges within a range of one meter in the vicinity of line-of-sight. With respect to Bluetooth, it has small form factor in radiation pattern and has 30°
Network connection Latency-3 s for Bluetooth	Network connection Latency- few ms for IrDA
Bit rate-1 Mbps for Bluetooth 2.0	Bit rate- 1.152 Mbps to 4 Mbps for IrDA
Used for low power short range transmission	Used for low power short range transmission

22.Compare Bluetooth and Zigbee

Dissimilarities	<ul style="list-style-type: none"> Bluetooth used for wireless short range exchanges in mobile environment and ZigBee for big scale mesh-network-based automation and remote control Network connection latency-3s for Bluetooth and 20 ms for ZigBee Bit rate-1 Mbps for Bluetooth v 1.x and 250 kbps for ZigBee Protocol stack-250 kB for Bluetooth and 28 kB for ZigBee FHSS used for Bluetooth and DSSS for ZigBee.
Similarities	<ul style="list-style-type: none"> Both conform to IEEE 802.15 set of standards Use of spread spectrum modulation Use of 2.4 GHz Used for low power short range transmission

23.Difference among WiFi, Bluetooth and ZigBee protocols.

Property	WLAN(WiFi)	Bluetooth	ZigBee
IEEE Std	802.11z	802.15.1	802.15.4
Freq. band	Two 2.4 GHz physical layers	One 2.4 GHz physical layers	2.4 GHz for high data transfer
Data transfer rate	6 MHz to 54 MHz [OFDM]	1 MHz (v1.2) and 24 Mbps in higher versions.	250 kbps at 2.4 GHz, &40 kbps at other bands.
Application	A Wireless LAN interconnecting a set of computers communicating with each other.	A Short-range Wireless PAN using controlled-power for connecting a set of devices, within the personal area.	A wireless based low-power, Short-range WPAN for routing and forming a mesh network.
Application area	Network at high data transfer rates between computers ,devices	Networking using 2.4 GHz for a set of systems mobile phones, Printers, laptops, and smart sensors at short ranges of nearly 10m	Mesh networking for big scale automation and remote controls at short ranges at small data rates.

UNIT – III**1. Name the consequences & problems of using IP with the standard routing protocols & Name the requirements of mobile IP.**

- The standard routing protocols does not allow the mobility of a node. In standard routing protocols for mobile nodes, in the routing table corresponding entry to this node has to be updated. The routers are built for extremely fast forwarding and not for extremely fast updates of tables. **Requirements** Compatibility, Transparency, Scalability, efficiency, Security

2. Compare the different types of transmission errors that can occur in wireless and wired networks.

- Single error: Error in a single bit; Burst Error: Error in a group of bits.

3. Define COA.

- **Care-of-address:** The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are first delivered to the COA, not directly to the IP address of the MN.

4. What are the two types of COA?

- **Co-located COA:** The COA is called co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired services such as DHCP
- **Foreign agent COA** – The COA could be located at the FA, i.e., the COA is an IP address of the FA. Thus the FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

5. Define mobility agent.

- Mobile Internet Protocol (Mobile IP), a mobility agent is a router that facilitates Internet traffic forwarding for a mobile node when its location is changed to somewhere other than its home network. There are two different types of mobility agent: a home agent and a foreign agent.

6. Define Encapsulation.

- Encapsulation is an mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. Taking packet out of a data part of another packet is called encapsulation.

7. What are the three type's of encapsulations in Mobile IP?

- Encapsulation needed for the tunnel between HA and COA
 - IP in IP (Mandatory for Mobile IP),
 - Minimal (removes the redundant fields in IP-IP)
 - Generic routing (supports other network layer protocol in addition to IP)

8. Define tunneling.

- A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling: sending a packet through a tunnel, is achieved by using encapsulation.

9. What is triangular routing?

- A Japanese and a German meet at a conference on Hawaii. If the Japanese sends a packet to the German, his computer sends the data to the HA of the German, i.e., from Hawaii to Germany. The HA in Germany now encapsulates the packets and tunnels them to the COA of the German laptop on Hawaii.

- This means that although the computers might be only meters away, the packets have to travel around the world! This inefficient behavior of a non-optimized mobile IP routing is called triangular routing. The triangle is made of the three segments, CN to HA, HA to COA/MN, and MN back to CN.

10. What are reverse tunneling and its problem?

- Reverse tunneling creates a triangular routing problem in the reverse direction. All packets from an MN to a CN go through the HA. **Problems of reverse tunneling are** as follows:
- Firewalls – almost all companies and many other institutions secure their internal networks connected to the internet with the help of a firewall. Firewalls often filter packets coming from outside containing the source address from computers of the internal network.
- Multicast – while the nodes in the home network might participate in a multicast group, an MN in a foreign network cannot transmit multicast packets from its home network without a reverse tunnel.
- TTL – consider an MN sending packets with a certain TTL while still in its home network. The TTL might be low enough so that no packet is transmitted outside a certain region. If the MN now moves to a foreign network, this TTL might be too slow for the packets to reach the same nodes as before.

11. What is the basic purpose of DHCP in mobility? Name the entities of DHCP

- The Dynamic Host Configuration Protocol is mainly used for the simplification of installation computers in a network. If a new computer is connected to a network, DHCP can provide it with all necessary information for full integration to the network. DHCP is a major source of care-of-addresses needed for mobile IP. **Entities of DHCP :** DHCP server & DHCP client

12. How does a mobile node discover it has moved?

- For this purpose mobile IP describes two methods which are in fact router discovery methods plus extensions. i) Agent advertisement ii) Agent Solicitation.

13. When congestion occurs?

Congestion may appear from time to time. If the buffers of the router are filled and if the router cannot forward packets to output link, congestion occurs. As result of congestion, it drops packets.

14. What is the exponential growth of congestion window?

Suppose congestion window size = n , if a sender receives acknowledgement from this window, then it doubles the congestion window size as to $2n$, if the congestion window size $<$ congestion threshold. It is called exponential growth.

15. Difference between UDP and TCP

UDP	TCP
Connectionless	Connection-oriented
Does not guarantee reliable data delivery	Guarantee reliable data delivery
Out of order delivery	In order delivery

16. What is fast retransmitting?

A sender receives continuous acknowledgement for the same packet. It informs that the gap in packet stream is not due to severe congestion but a simple packet lost due to transmission error. The sender can now re-transmit the missing packet before the timer expires. This behavior is called fast retransmit.

17. What is fast recovery?

A sender receives continuous acknowledgement for the same packet. It informs that the gap in the packet stream is not due to severe congestion but a simple packet lost due to transmission error. The sender can continue with same window. The sender can now re-transmit the missing packet and now recover fast from the packet loss. This behavior is called fast recovery.

18. What is indirect TCP?

I-TCP segments a TCP connection into a fixed part and a wireless part. A good place for segmenting the connection between mobile host and correspondent host is at the foreign agent. If the correspondent host sends a packet, the foreign agent acknowledges this packet, then the foreign tries to forward the packet to the mobile host. If the mobile host receives the packet, it acknowledges the packet.

19. List the Advantages of I-TCP.

- I-TCP does not require in the TCP protocol
- Due to strict partitioning into two connections, transmission errors on the wireless link, i.e, lost packets, cannot propagate into the fixed network.
- The short delay between the mobile host and foreign agent can be determined. An optimized TCP can use precise time-outs to guarantee retransmission as fast as possible. Even standard TCP benefits from the short RTT, thus recovering faster from packet loss.
- Partitioning into two connections also allows the use different transport layer protocol between the foreign agent and the mobile host are the use of compressed header etc.

20. List the Disadvantages of I-TCP

- The loss of end-to-end semantics of TCP might cause problems if the foreign agent partitioning the TCP connection crashes. If a sender receives an acknowledgement, it assumes that the receiver got the packet. Receiving an acknowledgement now only means (for the mobile host and a correspondent host) that the foreign agent received the packet. The correspondent node does not know anything about the partitioning.
- Increased hand-over latency may be much more problematic.
- A foreign agent must be a trusted entity.

21. Define snooping TCP?

- The foreign agent buffers all packets with destination mobile host and additionally ‘snoops’ the packet flow in both directions to recognize acknowledgement. The reason for buffering packets toward the mobile node is to enable the foreign agent to perform a local retransmission in case of packet loss on the wireless link.

22. What are the advantages, Disadvantages of S TCP?**Advantages**

- The end-to-end TCP semantic is preserved and No matter at what time the foreign agent crashes most of the enhancements are in the foreign agent. Does not even require changes in the mobile host.
- As the mobile host moves to another foreign agent during, though data in the buffer is not transferred to the next foreign agent, it leads to a time-out at the correspondent host and CA does retransmission. If the next foreign agent is not using the enhancement the approach automatically falls back to the standard solution.

Disadvantages

- Snooping TCP does not isolate the behaviour of the wireless link as good as I-TCP.

- Using negative acknowledgement between the foreign agent and the mobile host assumes the additional mechanisms on the mobile host. Thus, this approach is no longer transparent for arbitrary mobile hosts.
- All efforts for snooping and buffering data may be useless, if certain encryptions are applied end-to-end between the correspondent host and mobile host.

23. What are the Advantages and Disadvantages of Mobile TCP?

- M-TCP maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MN.
- If the MN is disconnected, M-TCP avoids useless retransmissions, slow starts or breaking connections by simply shrinking the senders window to zero.
- Since M-TCP does not buffer data in the SH as I-TCP does, it does not necessary to forward buffers to a new SH. Lost packets will be automatically retransmitted to the new SH.

Disadvantages

- As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption.
- A modified TCP on the wireless link not only requires modifications to the MN protocol software but also new network elements like the bandwidth manager.

24. What is persistent mode in M-TCP? What is advantages and disadvantages of persistent TCP?

- The SH monitors all packets send to the MH and ACKs returned from the MH. If the SH does not receive an ACK for some time, it assumes that the MH is disconnected. It then chokes the sender by setting the sender's window size to zero. Setting the window size to zero forces the sender to go into persistent mode, i.e. the state of a sender will not change no matter how long the receiver is disconnected. This means that the sender will not try to retransmit data. As soon as the SH detects the connectivity again, it reopens the window of the sender to the old value. Thus the sender can continue sending at full speed.

25. What are the advantages of selective retransmission, disadvantages of selective retransmission?

Advantages

- a sender retransmits only the lost packets.
- This lowers bandwidth requirements and is extremely helpful in slow wireless links.
- Beneficial to wired, wireless networks.

Disadvantage

- more complex software on the receiver side to buffer necessary to re-sequence data Increase in memory sizes and CPU performance

26. What are the advantages & disadvantages of transaction-oriented TCP?

Advantage

- reduction in the overhead due to connection setup and connection release.

Disadvantages:

- it requires changes in the mobile host and all correspondent hosts
- no longer hides mobility
- Furthermore, T/TCP exhibits several security problems

UNIT –IV

1. What is a MANET?

- MANET is a **self-configuration wireless ad-hoc network** of mobile nodes.
- A **peer-to-peer wireless network** which transmits data packets from one computer to another **without the use of a central base station (access-point)**.
- Each node has a router or a switch connected by the wireless connection.

2. What is the difference between fixed infrastructure network and an Ad-hoc network ?

Fixed Infra structure Network	Ad-hoc network
<p>A fixed infrastructure network uses access-points, base stations, and gateways.</p> <p>Remote systems are networked using switches, hubs, and routers. The locations of these switches hubs, or routers are fixed.</p>	<p>An ad-hoc network is a network in which the locations of the switches, hubs, or routers can be mobile.</p> <p>The number of routers available at an instant can increase or decrease, and the available routing paths can vary in an ad-hoc network.</p>

3. What are the issues in fixed infrastructure network?

- The problem with fixed infrastructure network is when a wireless sensor or mobile device moves out of the range of access-point, base station, or gateway it is not possible for it to communicate with other devices through the network
- Fixed infrastructure network is not usable in operations like disaster relief.

4. What is the difference between multicast tree network and a mesh network?

- In multicast tree network provides only a single path between a sender and a receiver.
- A mesh provides multiple paths between the sender and receiver nodes.

5. What are the design issues in Ad-hoc routing?

Mobility: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes, hence an on-going session suffers frequent path breaks.

Bandwidth Constraint: In a wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer.

Error-Prone Shared Broadcast Radio Channel : The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless networks.

Hidden terminal problem : The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

Resource Constraints : Two essential and limited resources that form the major constraint for the nodes in an ad hoc wireless network are battery life and processing power.

6. What do you mean by route discovery ?

- A process in which a source seeking route information broadcasts the packets, each with a header. The source expects return acknowledgement from destination. The route information pertaining to a destination is cached from the packet header in reply to the source. Caching is done at the source as well as intermediate nodes.

7. Compare between proactive and reactive routing protocol.

- In **proactive or table-driven routing protocols**, every node maintains the network topology information in the form of **routing tables** by periodically exchanging routing information. Routing information is generally flooded in the whole network. Ex: CGSR, Flat Routing Table driven protocol

- A **reactive protocol** is one in which a routing node needs to maintain the routing addresses about the **active paths** only. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols **do not exchange routing information** periodically.

Ex: AODV , TORA

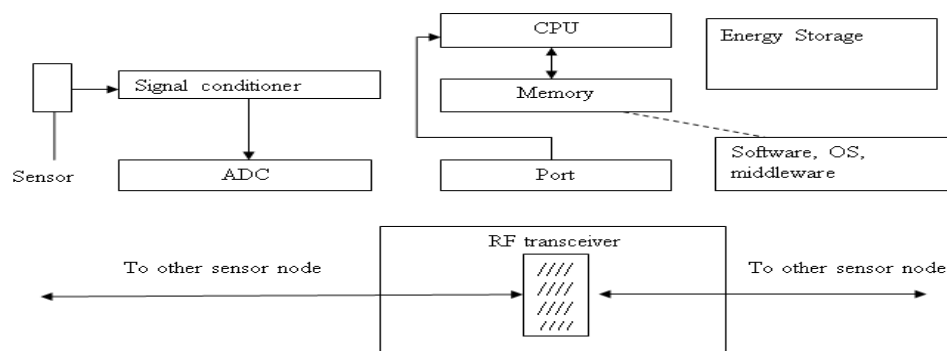
8. **Mention the security problems in ad-hoc mobile and wireless computing systems.**

SECURITY PROBLEMS	DESCRIPTION
Increased threat of eavesdropping	The probability that a MANET or sensor node transmits unsolicited messages while moving in the wireless region of two nodes is increased in ad-hoc networks. Each node attempts to identify itself with a new node moving in its vicinity and during that process eavesdropping occurs.
Unknown node caching the information	An unknown node can move into the network and thus rigorous authentication is required before the node is accepted as a part of MANET.
Denial of service attacks	A number of transmission requests can be flooded into the system by the attacking nodes. Since for each request, an authentication process is initiated, which require exchange of message, the flooding of the message-exchanges chokes the MANET and denies the required services to genuine nodes.
Authenticated node becoming hostile	A previously authenticated device can be used for security attacks.

9. **What is a sensor node /mote?**

- A sensor node / mote is a miniature node equipped with a microprocessor, memory, radio, and battery, combined with the functions of sensing, computing, and wireless communication.

10. **Draw the architecture of smart wireless sensor.**

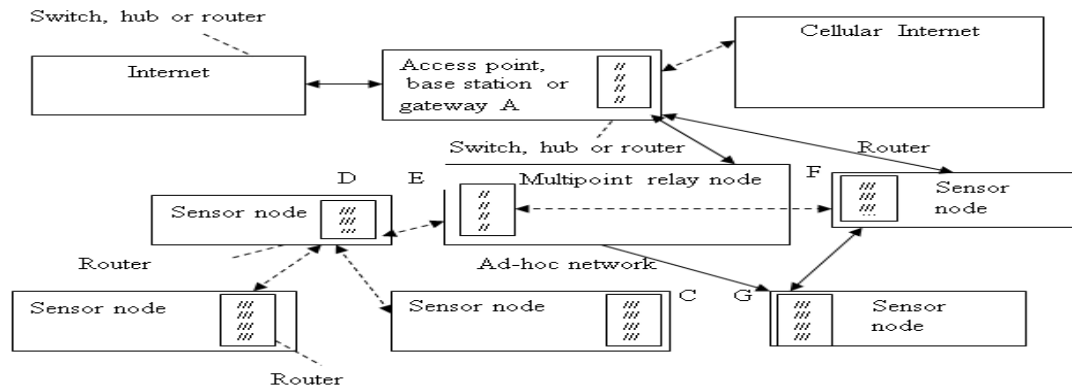


Sensor

- An RF transceiver for communication
- A microcontroller [CPU, memory, and ADC (analog-to-digital converter)]
- An energy source or a power supply. A charge pump in the sensor can trap the charge from the radiations and supply power for computations and communication
- Alternatively, an energy-harvesting module can be used to trap solar radiation and store the energy

11. **What is a wireless sensor network (WSN) ?**

A wireless sensor network is a MANET of smart sensors having computational communication and networking capabilities.



12. Mention few physical, chemical and biological entities that can be sensed and measured.

Few examples of physical, chemical, and biological entities that can be sensed and measured by a sensor are

- **Physical** — **Current**, voltage, magnetic, light, sound, frequency, temperature, pressure, acceleration, proximity to some object, rainfall, location shift, time stamps of GPS satellites, vibration, weather data, noise levels, traffic density of nearby passing vehicles and seismic activity
- **Chemical** — Chemical gas or liquid or material
- **Biological** — Protein or bacteria or virus

13. What are the requirements for WSN to be ad-hoc in nature ?

- The devices and the wireless links will not be laid out to achieve a planned topology.
- During the operation, it is impossible to access sensors hence their network needs to operate autonomously.
- Since sensors can't be replaced in case of failure due to battery drain, sensors should learn about each other and organize into a network on their own.
- Another crucial requirement is that since sensors may often be deployed randomly (e.g., simply strewn from an aircraft), in order to be useful, the devices need to determine their locations.

14. What do you mean by aggregation ?

- **Aggregation** refers to the process of joining together present and previously received data packets after removing redundant or duplicate data.

15. What is compaction?

- **Compacting** means making information short without changing the meaning or context, for example, transmitting only the incremental data so that information sent is short.

16. What is fusion?

- Fusion means formatting the information received in parts through various data packets and several types of data removing redundancy in the received data and presenting the formatted information created from the information parts in cases when the individual records are not required and not retrievable later.

17. What is the main difference between WSN and Mesh network ? / What are the characteristic features of WSN ?

- In a sensor network, there is usually a single, **global objective** to be achieved. For example, in a surveillance application, a sensor network may be deployed to detect intruders. The global objective here is intrusion detection.

- Another characteristic feature of sensor networks appears in the **packet scheduling algorithms** used. Sensor nodes are battery-powered and the batteries cannot be replaced. Hence, energy-aware packet scheduling is of crucial importance.
- In multi hop wireless mesh networks, where we have a collection of source – destination pairs, and each pair is interested in optimizing its individual performance metric.

18. What do you mean by coverage of a sensor ?

- Coverage is a measure of how well the network can observe or cover an event. Coverage depends upon the range and sensitivity of the sensing nodes, and the location and density of the sensing nodes in the given region.

19. Distinguish between communication coverage and sensing coverage of a sensor.

Each sensor can sense events within a certain radius of itself. All points within the disk of this radius are said to be covered by the sensor.

20. What is localization? Why is it needed ?

Localization is the process to determine the **physical coordinates** of a group of sensor nodes in a wireless sensor network (WSN).

Localization is needed for the following reasons :

- Use of GPS is unrealistic, therefore, sensors need to self-organize a coordinate system.
- To report data that is geographically meaningful
- Services such as routing rely on location information; geographic routing protocols; context-based routing protocols, location-aware services

21. What are anchors ?Specify their role in localization?

A group of sensors called anchors are aware of their own positions and transmit this information to others via beacons.

► Anchor Nodes:

- Nodes that know their coordinates a priori
- By use of GPS or manual placement
- For 2D three and 3D four anchor nodes are needed

In localization process, anchor nodes help the other non-anchor nodes to find their physical location

22. What are the types of routing in a wireless sensor networks ?

- Face routing - where the estimated node location information is used, and **attribute-based routing**, which does not depend on the knowledge of node locations. Directed Diffusion (DD) is a prominent example of attribute-based routing.

23. What do you mean by function computation ?

The maximum rate at which a particular type of function computation can be carried out is called function computation.

UNIT –V

1. What are the steps involved in Mobile Application Development workflow ?

The application development workflow consists of the following steps

- Application development using integrated development environment (IDE) or APIs it, a framework for a specific platform.
- Testing and debugging application executables on a simulator or emulator.
- Developing GUIs for the users of the device.
- Packaging applications for installation on the device for a service provider or application distributor

- Web-hosting of executables at an Application store or Mobile application distribution platform. (AppStore of Apple is an example of an application store.)
- The graphical user interfaces (GUIs) of the application are written using GUI development APIs.
- Applications are deployed on a device.

2. Mention the techniques/ approaches for composing mobile applications.

A mobile application can be developed through any one of the following approaches:

- *Application* (software for application) is written using a set of the statements, functions, methods, threads, objects, and classes. High-level language like C, Java, Visual Basic, Visual C++, Python or Brew native codes are used for that purpose.
- Applications are written using **APIs (Application Program Interfaces)** which are a set of functions, methods, routines, tools or protocols for building the *application*. API enables easier development of an Application. An API provides the blocks for Application building. These blocks are put together to write an *application*. All *applications* using a common API will have similar interfaces. This makes it easier for users to learn writing new programs.
- A **framework** like, NET or Qt is used for writing application software which use APIs
- Application is written using the APIs provided by a **development platform** (e.g., Operating Systems like Android or Symbian or Windows Phone 7).
- WAP (Wireless Application Protocol), XHTML-Mobile Profile, and Java ME (Micro Edition) are technologies for Web related applications which are used for mobile devices. HTML5 is a language used for web page development. Micro browsers are used for browsing on a mobile device.

3. What are the prerequisites for application development ?

A programming language and an IDE (IDE which includes a simulator, emulator and debugger) are the prerequisites for application development. An installer is used for packaging the application. A mobile application is installed in the mobile device or can be downloaded from Application Stores or an application distribution environment. Apple, BlackBerry, Nokia, and other companies provides these applications stores or distribution environments.

4. Mention few Android applications.

- An e-mail client compatible with Gmail but not limited to it
- An SMS management application
- A full PIM (personal information management) suite including a calendar and contacts list, both tightly integrated with Google's online services
- No licensing, distribution, or development fees
- Wi-Fi hardware access
- GSM, EDGE, and 3G networks for telephony or data transfer, allowing you to make or receive calls or SMS messages, or to send and retrieve data across mobile networks
- Comprehensive APIs for location-based services such as GPS
- Full multimedia hardware control including playback and recording using the camera and microphone
- APIs for accelerometer and compass hardware.
- IPC message passing.

5. What is android?

- Android is a stack of software for mobile devices which has Operating System, middleware and some key applications.
- The application executes within its own process and its own instance of Dalvik Virtual Machine. Many Virtual Machines run efficiently by a DVM device. DVM executes Java language byte code which later transforms into .dex format files.

- Android gives you a world-class platform for creating apps and games for Android users everywhere, as well as an open marketplace for distributing to them instantly.

6. What are the advantages of Android?

- Multitasking: With Android, you can quickly and seamlessly switch between apps and pick up whatever you were doing. Juggling multiple tasks at once on a mobile device has never been easier.
- It has simple and powerful SDK. Also allows multitasking. Licensing, Distribution or Development fee is not required. Easy to Import third party Java library. Supporting platforms are – Linux, Mac Os, Windows.
- Innovative products like the location-aware services, location of a nearby convenience store etc., are some of the additive facilities in Android.
- Components can be reused and replaced by the application framework. Optimized DVM for mobile devices.
- SQLite enables to store the data in a structured manner.
- Supports GSM telephone and Bluetooth, WiFi, 3G and EDGE technologies.
- The development is a combination of a device emulator, debugging tools, memory profiling and plug-in for Eclipse IDE.
- The customer will be benefited from wide range of mobile applications to choose, since the monopoly of wireless carriers like AT&T and Orange will be broken by Google Android.
- There's no other software quite like Android. Google engineered Android, and Google's own apps run best on it. And with millions of apps, games, songs, and videos on Google Play, Android is great for fun, and for getting things done.

7. What are the disadvantages of Android?

- Given that Android is an open-source platform, and the fact that different Android operating systems have been released on different mobile devices, there's no clear cut policy to how applications can adapt with various OS versions and upgrades.
- One app that runs on this particular version of Android OS may or may not run on another version. Another disadvantage is that since mobile devices such as phones and tabs come in different sizes and forms, it poses a challenge for developers to create apps that can adjust correctly to the right screen size and other varying features and specs.

8. What is Dalvik Virtual Machine?

- The name of Android's virtual machine. The Dalvik VM is an interpreter-only virtual machine that executes files in the Dalvik Executable (.dex) format, a format that is optimized for efficient storage and memory-mappable execution.
- The virtual machine is register-based, and it can run classes compiled by a Java language compiler that have been transformed into its native format using the included "dx" tool. The VM runs on top of Posix-compliant operating systems, which it relies on for underlying functionality (such as threading and low level memory management).
- The Dalvik core class library is intended to provide a familiar development base for those used to programming with Java Standard Edition, but it is geared specifically to the needs of a small mobile device.
- All Android hardware and system service access is managed using Dalvik as a middle tier. By using a VM to host application execution, developers have an abstraction layer that ensures they never have to worry about a particular hardware implementation.

9. Mention the types of android applications.

- Foreground Activity An application that's only useful when it's in the foreground and is effectively suspended when it's not visible. Games and map mash ups are common examples.
- Background Service An application with limited interaction that, apart from when being configured, spends most of its lifetime hidden. Examples of this include call screening applications or SMS auto-responders.

- Intermittent Activity Expects some interactivity but does most of its work in the background. Often these applications will be set up and then run silently, notifying users when appropriate. A common example would be a media player.

10. What are the six components of android application?

Activities, services, content providers, intents, broadcast receivers, notifications.

11. What are the requirements of android applications ?

Applications must be Fast Responsive Secure and Seamless.

12. What is activity?

- An activity is a single, focused thing that the user can do. Almost all activities interact with the user, so the Activity class takes care of creating a window for us in which we can place your UI.

13. Mention the different lifetimes associated with an activity in an android application.

The **full lifetime** of Activity occurs between the first call to onCreate and the final call to onDestroy.

An Activity's **visible lifetimes** are bound between calls to onStart and onStop. Between these calls, your Activity will be visible to the user, although it may not have focus and might be partially obscured.

The **active lifetime** starts with a call to onResume and ends with a corresponding call to onPause.

14. Mention the android activity classes.

MapActivity Encapsulates the resource handling required to support a MapView widget within an Activity.

ListActivity Wrapper class for Activities that feature a ListView bound to a data source as the primary UI metaphor, and exposing event handlers for list item selection

ExpandableListActivity Similar to the List Activity but supporting an ExpandableListView

ActivityGroup Allows us to embed multiple Activities within a single screen.

15. What are the exceptions in Android?

- **InflateException** : This exception is thrown by an inflater on error conditions.
- **Surface.OutOfResourceException**: When a surface is not created or re-sized, this exception is thrown.
- **SurfaceHolder.BadSurfaceTypeException**: This exception is thrown from the lockCanvas() method, when invoked on a Surface whose is SURFACE_TYPE_PUSH_BUFFERS
- **WindowManager.BadTokenException**: This exception is thrown at the time of trying to add view an invalid WindowManager.LayoutParams token.
-

16. What are the different methods of the Activity life cycle?

Here are Seven main methods:

- void onCreate()
- void onStart()
- void onRestart()
- void onResume()
- void onPause()
- void onStop()
- void onDestroy()

17. What dialog boxes are supported in android?

Android supports 4 dialog boxes:

- **AlertDialog**: An alert dialog box supports 0 to 3 buttons and a list of Selectable elements, including check boxes and radio buttons. Among the other dialog boxes, the most suggested dialog box is the alert dialog box.

- ProgressDialog: This dialog box displays a progress wheel or a progress bar. It is an extension of AlertDialog and supports adding buttons.
- DatePickerDialog: This dialog box is used for selecting a date by the user.
- TimePickerDialog: This dialog box is used for selecting time by the user.
-

18. What is the APK format? What is .apk extension?

- The APK file is compressed the AndroidManifest.xml file, application code (.dex files), resource files, and other files. A project is compiled into a single .apk file.
- The extension for an Android package file, which typically contains all of the files related to a single Android application. The file itself is a compressed collection of an AndroidManifest.xml file, application code (.dex files), resource files, and other files. A project is compiled into a single .apk file.

19. What is .dex extension?

- Android programs are compiled into .dex (Dalvik Executable) files, which are in turn zipped into a single .apk file on the device. .dex files can be created by automatically translating compiled applications written in the Java programming language.

20. What is a service?

- A Service is an application component representing either an application's desire to perform a longer- running operation while not interacting with the user or to supply functionality for other applications to use. Each service class must have a corresponding declaration in its package's AndroidManifest.xml.
- Services can be started with Context.startService() and Context.bindService().
- For example, a service might play background music as the user attends to other matters, or it might fetch data over the network or calculate something and provide the result to activities that need it. Each service extends the Service base class.

21. Describe a real time scenario where android can be used?

- Lets take a situation that you are in a country where no one understands the language you speak and you cannot read or write. However, you have mobile phone with you. With a mobile phone with android, the Google translator translates the data of one language into another language by using XMPP to transmit data. You can type the message in English and select the language which is understood by the citizens of the country in order to reach the message to the citizens.

22. What is intent?

- Intents are used as a **message-passing mechanism** that lets us declare our intention that an action be performed, usually with (or on) a particular piece of data.
- It is an abstract description of an operation to be performed. It can be used with startActivity to launch an Activity, broadcastIntent to send it to any interested BroadcastReceiver components, and startService to communicate with a background Service.
- It also provides a facility for performing late run time binding between the code in different applications. Its most significant use is in the launching of activities, where it can be thought of as the glue between activities.

23. What is an Implicit Intent?

- In an implicit intent, the main power of the android design, we just declare an intent and leave it to the platform to find an activity that can respond to the intent. Here, we do not declare the target component and hence is typically used for activating components of other applications seamlessly.

24. What is an Explicit Intent?

- In an explicit intent, we actually specify the activity that is required to respond to the intent. In other words, we explicitly specify the class to load. This is typically used for application internal messages.

25. What are the uses of intent?

- Intents can also be used to broadcast messages across the system. Any application can register a Broadcast Receiver to listen for, and react to, these broadcast Intents. Thus it lets to create event-driven applications based on internal, system, or third-party application events.
- Android uses broadcast Intents to announce system events, like changes in Internet connection status or battery charge levels. The native Android applications, such as the phone dialler and SMS manager, simply register components that listen for specific broadcast Intents such as “incoming phone call” or “SMS message received” and react accordingly.
- Using Intents to propagate actions even within the same application is a fundamental Android design principle. It encourages the decoupling of components, to allow the seamless replacement of application elements. It also provides the basis of a simple model for extending functionality.
- The most common use of Intents is to bind your application components. Intents are used to start, stop, and transition between the Activities within an application.

26. What is an Intent Filter?

- Activities and intent receivers include one or more filters in their manifest to describe what kinds of intents or messages they can handle or want to receive. An intent filter lists a set of requirements, such as data type, action requested, and URI format, that the Intent or message must fulfil.
- For Activities, Android searches for the Activity with the most closely matching valid match between the Intent and the activity filter. For messages, Android will forward a message to all receivers with matching intent filters.

27. What is an adaptor in an android ? Mention the two most useful adapters.

- Adapters are **bridging classes** that bind data to user-interface Views. The adapter is responsible for creating the child views used to represent each item and providing access to the underlying data.
- ArrayAdapter The ArrayAdapter is a generic class that binds Adapter Views to an array of objects. By default, the ArrayAdapter binds the toString value of each object to a TextView control defined within a layout.
- SimpleCursorAdapter The SimpleCursorAdapter binds Views to cursors returned from Content Provider queries. We can specify an XML layout definition and then bind the value within each column in the result set, to a View in that layout.

28. What's the difference between file, class and activity in android?

File – It is a block of arbitrary information, or resource for storing information. It can be of any type.

Class – Its a compiled form of .Java file . Android finally used this .class files to produce an executable apk

Activity – An activity is the equivalent of a Frame/Window in GUI toolkits. It is not a file or a file type it is just a class that can be extended in Android for loading UI elements on view.

29. What is an Android Manifest file?

- Every application must have an AndroidManifest.xml file (with precisely that name) in its root directory.
- The manifest presents essential information about the application to the Android system, information the system must have before it can run any of the application's code.

30. What are the functions included in a manifest file ?

- Among other things, the manifest does the following:
 - ❖ It names the Java package for the application and package name serves as a unique identifier for the application.
 - ❖ It describes the components of the application , the activities, services, broadcast receivers, and content providers that the application is composed of. It names the classes that implement each of the components and publishes their capabilities (for example, which Intent messages they can handle). These declarations let the Android system know what the components are and under what conditions they can be launched.
 - ❖ It determines which processes will host application components.
 - ❖ It declares which permissions the application must have in order to access protected parts of the API and interact with other applications.
 - ❖ It also declares the permissions that others are required to have in order to interact with the application's components.
 - ❖ It lists the Instrumentation classes that provide profiling and other information as the application is running. These declarations are present in the manifest only while the application is being developed and tested; they are removed before the application is published.
 - ❖ It declares the minimum level of the Android API that the application requires.
 - ❖ It lists the libraries that the application must be linked against.

31. What is context in android?

- Interface to global information about an application environment. This is an abstract class whose implementation is provided by the Android system. It allows access to application-specific resources and classes, as well as up-calls for application level operations such as launching activities, broadcasting and receiving intents, etc.

32. What is Notification in android?

- A class that represents how a persistent notification is to be presented to the user using the NotificationManager. TheNotification.Builder has been added to make it easier to construct Notifications.

33. What are the Android Database Design Considerations ?

There are several considerations specific to Android that you should consider when designing database:

- Files (such as bitmaps or audio files) are not usually stored within database tables. Instead, use a string to store a path to the file, preferably a fully qualified Content Provider URI.
- While not strictly a requirement, it's strongly recommended that all tables include an auto increment key field, to function as a unique index value for each row.

34. What is AsyncTask in android?

- AsyncTask enables proper and easy use of the UI thread. This class allows to perform background operations and publish results on the UI thread without having to manipulate threads and/or handlers. An asynchronous task is defined by a computation that runs on a background thread and whose result is published on the UI thread. An asynchronous task is defined by 3 generic types, called Params, Progress and Result, and 4 steps, called onPreExecute, doInBackground, onProgressUpdate and onPostExecute.

35. What is localization and how to achieve?

- Localization is a way of representing the products in different languages. Android is an operating system which runs in many regions, so to reach different users localization is a must. Localization in Android can be achieved by incorporating different languages in the application which you are using.
- To do this knowledge of Java, XML elements, Activity lifecycle and general principles of internationalization and localization are required.

36. What are the different Storage Methods in android?

- Android provides many options for storage of persistent data. It provides the solution according to our need. The storage's which have been provided in Android are as follows:
 - Shared Preferences: Store private primitive data in key value pairs
 - Internal Storage: Store private data on the device memory.
 - External Storage: Store public data on the shared external storage.
 - SQLite Databases: Store structured data in a private database.
 - Network Connection: Store data on the web with your own network server.

37. What is a Content Provider?

- Content Providers are the only way to share data across Android applications. They store and retrieve data thus making it accessible to all. Content Providers give a uniform interface to access the data. Android platform provides default implementations of content providers for data types like audio, video, images, contact information etc.
- Content providers manage access to a structured set of data. They encapsulate the data, and provide mechanisms for defining data security. Content providers are the standard interface that connects data in one process with code running in another process.

38. Mention few android content provider classes.

- **Browser** Use the browser Content Provider to read or modify bookmarks, browser history, or web searches.
- **CallLog** View or update the call history including both incoming and outgoing calls together with missed calls and call details, like caller ID and call durations.
- **Contacts** Use the Contacts provider to retrieve, modify, or store your contacts' details.
- **MediaStore** The Media Store provides centralized, managed access to the multimedia on our device, including audio, video, and images. You can store your own multimedia within the Media Store and make it globally available.
- **Settings** You can access the device's preferences using the Settings provider. Using it, we can view and modify Bluetooth settings, ring tones, and other device preferences.

39. What is the difference between Service and Thread?

- Service is like an Activity but has no interface. Probably if you want to fetch the weather for example you won't create a blank activity for it, for this you will use a Service. It is also known as Background Service because it performs tasks in background. A Thread is a concurrent unit of execution. You need to know that you cannot update UI from a Thread. You need to use a Handler for this.

PART B**UNIT- I****1. Explain in detail about the different types of multiplexing.**

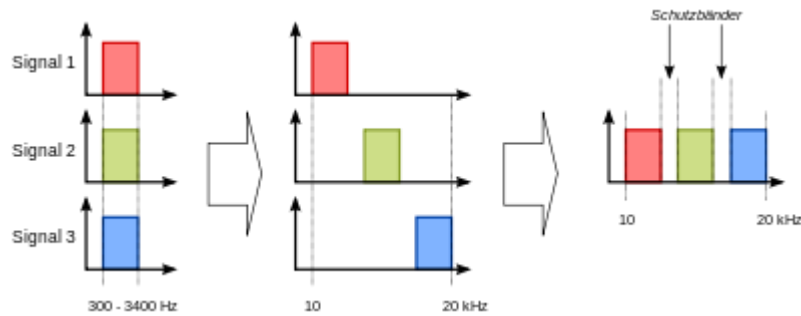
- Multiplexing technologies may be divided into several types, space-division multiplexing (SDM), frequency-division multiplexing (FDM), time-division multiplexing (TDM), and code division multiplexing (CDM).
- Variable bit rate digital bit streams may be transferred efficiently over a fixed bandwidth channel by means of statistical multiplexing, for example packet mode communication. Packet mode communication is an asynchronous mode time-domain multiplexing which resembles time-division multiplexing.
- Digital bit streams can be transferred over an analog channel by means of code-division multiplexing (CDM) techniques such as frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS).
- In wireless communications, multiplexing can also be accomplished through alternating polarization (horizontal/vertical or clockwise/counterclockwise) on each adjacent channel and satellite, or through phased multi-antenna array combined with a Multiple-input multiple-output communications (MIMO) scheme.

Space-division multiplexing

- In wired communication, space-division multiplexing simply implies different point-to-point wires for different channels. Examples include an analogue stereo audio cable, with one pair of wires for the left channel and another for the right channel, and a multipair telephone cable. Another example is a switched star network such as the analog telephone access network (although inside the telephone exchange or between the exchanges, other multiplexing techniques are typically employed) or a switched Ethernet network. A third example is a mesh network. Wired space-division multiplexing is typically not considered as multiplexing.
- In wireless communication, space-division multiplexing is achieved by multiple antenna elements forming a phased array antenna. Examples are multiple-input and multiple-output (MIMO), single-input and multiple-output (SIMO) and multiple-input and single-output (MISO) multiplexing. For example, a IEEE 802.11n wireless router with N antennas makes it possible to communicate with N multiplexed channels, each with a peak bit rate of 54 Mbit/s, thus increasing the total peak bit rate with a factor N. Different antennas would give different multi-path propagation (echo) signatures, making it possible for digital signal processing techniques to separate different signals from each other. These techniques may also be utilized for space diversity (improved robustness to fading) or beamforming (improved selectivity) rather than multiplexing.

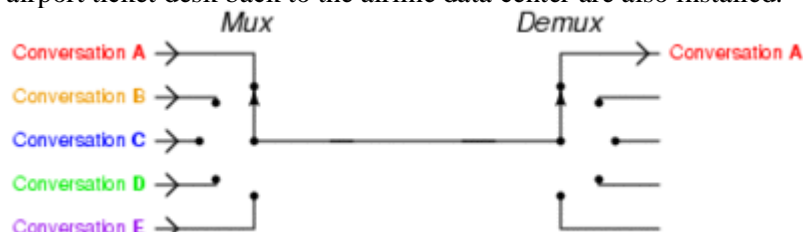
Frequency-division multiplexing

- Frequency-division multiplexing (FDM): The spectrums of each input signal are swiftd in several distinct frequency ranges.
- Frequency-division multiplexing (FDM) is inherently an analog technology. FDM achieves the combining of several digital signals into one medium by sending signals in several distinct frequency ranges over that medium.
- One of FDM's most common applications is cable television. Only one cable reaches a customer's home but the service provider can send multiple television channels or signals simultaneously over that cable to all subscribers. Receivers must tune to the appropriate frequency (channel) to access the desired signal.[1]
- A variant technology, called wavelength-division multiplexing (WDM) is used in optical communications.



Time-division multiplexing

- Time-division multiplexing (TDM) is a digital (or in rare cases, analog) technology. TDM involves sequencing groups of a few bits or bytes from each individual input stream, one after the other, and in such a way that they can be associated with the appropriate receiver.
- If done sufficiently and quickly, the receiving devices will not detect that some of the circuit time was used to serve another logical communication path.
- Consider an application requiring four terminals at an airport to reach a central computer. Each terminal communicated at 2400 bit/s, so rather than acquire four individual circuits to carry such a low-speed transmission; the airline has installed a pair of multiplexers.
- A pair of 9600 bit/s modems and one dedicated analog communications circuit from the airport ticket desk back to the airline data center are also installed.



Code-division multiplexing

- Code division multiplexing (CDM) or spread spectrum is a class of techniques where several channels simultaneously share the same frequency spectrum, and this spectral bandwidth is much higher than the bit rate or symbol rate. One form is frequency hopping, another is direct sequence spread spectrum.
- In the latter case, each channel transmits its bits as a coded channel-specific sequence of pulses called chips. Number of chips per bit, or chips per symbol, is the spreading factor. This coded transmission typically is accomplished by transmitting a unique time-dependent series of short pulses, which are placed within chip times within the larger bit time.
- All channels, each with a different code, can be transmitted on the same fiber or radio channel or other medium, and asynchronously demultiplexed. Advantages over conventional techniques are that variable bandwidth is possible (just as in statistical multiplexing), that the wide bandwidth allows poor signal-to-noise ratio according to Shannon-Hartley theorem, and that multi-path propagation in wireless communication can be combated by rake receivers.
- Code Division Multiplex techniques are used as an channel access scheme, namely Code Division Multiple Access (CDMA), e.g. for mobile phone service and in wireless networks, with the advantage of spreading intercell interference among many users. Confusingly, the generic term Code Division Multiple access sometimes refers to a specific CDMA based cellular system defined by Qualcomm.

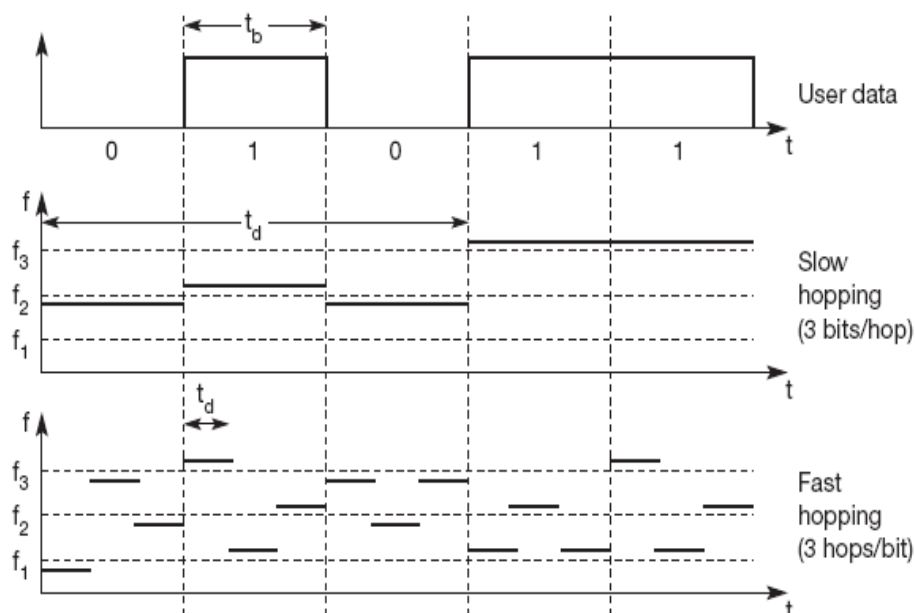
2. Explain in detail about DHSS, FHSS.

- Frequency hopping is one of two basic modulation techniques used in spread spectrum signal transmission. It is the repeated switching of frequencies during radio transmission, often to minimize the effectiveness of ISI. It also is known as frequency-hopping code division multiple accesses (FH-CDMA).

- Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal. The transmitter "spreads" the energy, originally concentrated in narrowband, across a number of frequency band channels on a wider electromagnetic spectrum. Benefits include improved privacy, decreased narrowband interference, and increased signal capacity.
- **Process 1 - Spreading code modulation** The frequency of the carrier is periodically modified (hopped) following a specific sequence of frequencies. In FHSS systems, the *spreading code* is this list of frequencies to be used for the carrier signal, also called as the "hopping sequence". The amount of time spent on each hop is known as dwell time and is typically in the range of 100 ms.
- **Process 2 - Message modulation** The message modulates the (hopping) carrier (FSK), thus generating a narrow band signal for the duration of each dwell, but generating a wide band signal, if the process is regarded over periods of time in the range of seconds. - Redundancy is achieved through the possibility to execute re-transmissions on different carrier frequencies (hops). There are two kinds of frequency hopping **Slow Frequency Hopping (SFH)**
- In this case one or more data bits are transmitted within one hop. An advantage is that coherent data detection is possible. Often, systems using slow hopping also employ (burst) error control coding to restore loss of (multiple) bits in one hop.

Fast Frequency Hopping (FFH)

- One data bit is divided over multiple hops. In fast hopping, coherent signal detection is difficult, and seldom used. Mostly, FSK or MFSK modulation is used. Slow frequency hopping is a popular technique for wireless LANs. In GSM telephony, slow frequency hopping can be used, at the discretion of the network control software.



3. i) Distinguish between GSM and CDMA. ii) Distinguish between 2G and 3G.

Feature	Global System for Mobile (GSM)/ General Packet Radio Service GPRS	Code-Division Multiple Access (CDMA)
Multiple access scheme	Time-division multiple access (TDMA)	CDMA
Duplexing frequency bands	Frequency-division duplex (FDD) 900, 1800, 1900 MHz	FDD 800, 1900 MHz
Channel bandwidth	200 KHz shared by eight time-slotted users	1250 KHz shared by 64 users (codes)
Data rate	Initially 9600 bps, now 38.4 Kbps or 115 Kbps shared by eight users	9.6–14.4 Kbps
Carrier RF spacing	1.25 MHz	200 KHz
Handoff	Hard handoff	Soft handoff
Speech encoding	Fixed rate codec	Variable rate codec
Power control	Open-loop and slow power control	Close-loop and faster power control
Identification	SIM card	Hardwired in the handset
3G	UMTS/WCDMA	cdma2000
Road to 4G	GPRS, EDGE, or HSCSD	cdma2000 1x (IS-95B)
Market	Europe, Asia, Australia, South America, North America, including some U.S. MNOs such as Cingular/AT&T wireless, and T-Mobile	Asia (South Korea and China), Canada, United States; mobile network operators (MNOs) such as Verizon Wireless and Sprint PCS

ii) Difference between 2G and 3G.

Differences between 2G and 3G Technology

- **Cost:** The license fee to be paid for 3G network is much higher as compared to 2G networks. The network construction and maintenance of 3G is much costlier than 2G networks. Also from the customers point of view the expenditure for 3G network will be excessively high if they make use of the various applications of 3G.
- **Data Transmission:** The main difference between 2G and 3G networks is seen by the mobile users who download data and browse the Internet on the mobile phones. They find much faster download speeds, faster access to the data and applications in 3G networks as compared to 2G networks. 2G networks are less compatible with the functions of smart phone. The speed of data transmission in 2G network is less than 50,000 bits per sec while in 3G it can be more than 4 million bits per sec.
- **Function:** The main function of 2G technology is the transmission of information via voice signals while that of 3G technologies is data transfer via video conferencing, MMS etc.
- **Features:** The features like mobile TV, video transfers and GPS systems are the additional features of 3G technology that are not available with 2G technologies.
- **Frequencies:** 2G technology uses a broad range of frequencies in both upper and lower bands, under which the transmission depends on conditions such as weather. A drawback of 3G is that it is simply not available in certain regions.
- **Implication:** 3G technology offers a high level of security as compared to 2G technology because 3G networks permit validation measures when communicating with other devices.
- **Making Calls:** Calls can be made easily on both 2G and 3G networks with no real noticeable differences except that in 3G network video calls can also be made. The transmission of text messages and photos is available in both the networks but 2G networks have data limit and the speed of the data transmission is also very slow as compared to 3G.
- **Speed:** The downloading and uploading speeds available in 2G technologies are up to 236 Kbps. While in 3G technology the downloading and uploading speeds are up to 21 Mbps and 5.7 Mbps respectively.

4. Explain in detail about two types of 2G mobile services.

Two types of 2G mobile services are i) WAP & imode ii) SMS

- WAP is an open-application layer protocol for mobile applications targeting cell phones and wireless terminals. It was developed by the WAP Forum, which has been consolidated into the Open Mobile Alliance (OMA).

- The current release is WAP 2.0. WAP is intended to be the World Wide Web for cell phones. It is independent of the underlying cellular networks in use. To a cell phone or PDA user, WAP is perceived as a small browser application that can be used to browse some specific websites, quite similar to the web browsing experience on a desktop computer but with significant constraints due to the form factor of the mobile terminal.
- A WAP system employs a **proxy-based architecture** to overcome the inherent limitations of mobile devices with respect to low link bandwidth and high latency. Below is a list of features that separate WAP from other application protocols:
 - ❖ Wireless markup language (WML), WML script, and supporting WAP application environment: Together, they are referred to as WAE. WML is an HTML-like markup language specifically devised for mobile terminals that have limited bandwidth, fairly small screen size, limited battery time, and constrained input methods.
 - ❖ WSL is a scaled-down scripting language supported by the WAP application environment. In addition, WAP 2.0 supports XHTML language, which allows developers to write applications for both desktop computers and mobile terminals.
 - ❖ WAP protocol stack: WAP Version 1.0 includes wireless session protocol (WSP), wireless transaction protocol (WTP), wireless transport layer security (WTLS), and wireless datagram protocol (WDP). Version 2.0 incorporates standard Internet protocols into its protocol stack, such as TCP, transport layer security (TLS), and Hyper Text Transport Protocol (HTTP). Both TCP and HTTP are optimized for wireless environments.
 - ❖ WAP services, such as push and traditional request/response, user agent profile, wireless telephony application, external functionality interface, persistent storage interface, data synchronization, and multimedia messaging service.
 - ❖ WAP 1.0 has proved to be a technological hype; it has been intensively promoted by wireless operators and content providers but has received little, if any, positive feedback from users.
 - ❖ Because of that, WAP has sometimes been referred to as “ **wait and pay.** ” Interestingly, it is not only the protocol but also the applications utilizing WAP that, as a whole, push users away because of application performance, input methods, and the GUI interface, among other reasons.
- Moving toward standard IP protocols rather than specialized wireless protocols, WAP 2.0 addresses most of the problems of the protocol stack and the application environment, thereby giving the technology a brighter future.
- **iMode is a successful wireless application service** provided by NTT DoCoMo. It is very similar to WAP in that it defines an architecture of web access on mobile terminals, primarily cell phones. Like WAP 2.0, iMode adopts standard Internet protocols as transport for applications, but iMode does not use any gateways. Instead, it utilizes overlay packet network on top of a cellular network for direct communication.
- The fundamental difference between WAP and iMode is that iMode requires mobile terminals to be designed to adapt to the services and applications of iMode, while WAP focuses on adapting itself to fit into general mobile terminals. Furthermore, NTT DoCoMo's effective WAP initiative has managed to attract many satisfied providers who can offer a wide array of services and applications to users .

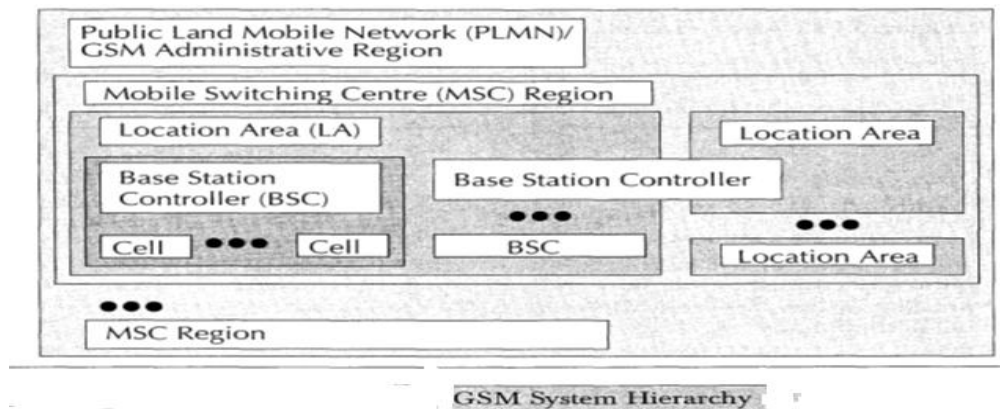
ii) Short Message Service

- SMS allows **two-way transmission of 160-character alphanumeric messages** between mobile subscribers and external computing systems such as e-mail systems and paging systems. Because of its increasing popularity, SMS has been extensively combined with many new types of information services in addition to traditional usage.
- For example, both Google and Yahoo offer Internet searching via SMS. SMS was initially designed to replace alphanumeric paging service with two-way guaranteed messaging and notification services.

- Two new types of SMS components have been added to the cellular network: **short message service center (SMSC) and signal transfer point (STP)**.
- An SMSC is a central controller of SMS services for the entire network. It interfaces with external message sources, such as voice-mail systems, e-mail systems, and the web. Messages sent from a mobile subscriber will also be stored and forwarded by the SMSC.
- An STP is a general network element connecting two separate portions of the network via SS7 signaling protocol. In the case of SMS, numerous STPs interface with the SMSC, each handling SMS transmission and delivery to and from a large number of mobile stations. No matter where the messages come from, the SMSC will guarantee delivery and inform the transmitter. For the SMSC to locate a mobile station for message delivery, it must utilize the cellular network, especially the HLR, VLR, and MSC of the mobile station.
- SMS has been enhanced with new capabilities to support enhanced message service (EMS) and multimedia message service (MMS). If you consider SMS to represent very early plaintext e-mails, you might think of EMS as the fancier HTML e-mails containing pictures, animations, embedded objects such as sound clips, and formatted text. MMS is the next generation messaging service that supports rich media such as video and audio clips.
- The wide use of picture messages sent from a camera cell phone is merely one example of MMS in action. MMS consumes more bandwidth so it requires a high data rate for the underlying network and considerable computing capability of the mobile handset. The multimedia service center (MMSC) performs similar tasks as the SMSC for SMS. The following list outlines the necessary steps of an MMS procedure:
 - ❖ The transmitter sends a message to the MMSC from a cell phone, PDA, or networked computer.
 - ❖ The MMSC replies to the transmitter with a confirmation of “ message sent. ” In fact, it is not sent to the receiver yet, as the message is stored at the MMSC.
 - ❖ The MMSC locates the receiver with the help of a number of cellular network elements, such as MSCs, HLRs, and VLRs. If the mobile station of the receiver is ON, the MMSC sends a notification of a new message to it, along with a URL to the new message. Otherwise, it waits and tries again later.
 - ❖ The receiver can choose to download the message right away or save the URL to download it later.
 - ❖ The MMSC will be notified by the receiver that the message has been downloaded and presumably read. Then the MMSC notifies the transmitter that the message has been delivered. MMS is the natural evolution of SMS, with EMS as an optional intermediate messaging service, but it is very unlikely that MMS will replace SMS completely as plain text messages are preferable in many cases.
 - ❖ Additionally, MMS does not require 3G; it can be done in 2.5G systems such as GPRS and EDGE. Problems that may hinder the widespread use of MMS include digital rights management of content being exchanged among many mobile subscribers, development of a user-friendly interface design, and sufficiently large bandwidth for message delivery.

5. Give the detail explanation of GSM ARCHITECTURE with neat diagram.

- It consists of minimum one administrative region assigned to one MSC (Mobile Switching Centre) known as PLMN (Public Land Mobile Network). Each administrative region is subdivided into one or many Location Area (LA).
- One LA consists of many cell groups. For each LA there will be at least one BSC. Cells are formed by the radio areas covered by a BTS (Base Transceiver Station). Several BTSs are controlled by one BSC.
- Traffic from the MS (Mobile Station) is routed through MSC. Calls originating / terminating in a fixed network or other mobile networks is handled by the GMSC (Gateway MSC).



- A GSM system consists of three subsystems, the radio sub system (RSS), the network and switching subsystem (NSS), and the operation subsystem (OSS). (GSM customer only notices MS, BTS).

1. Radio subsystem

- As the name implies, the radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS). The A interface is based on circuit-switched PCM whereas the O interface uses the signaling system no.7 (SS7) based on X.25 carrying management data to/from the RSS.
 - ❖ **Base transceiver station (BTS):** A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell.
 - ❖ **Base station controller (BSC):** The BSC basically manages the BTSs. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
 - ❖ **Mobile station (MS):** The MS comprises all user equipment and software needed for communication with a GSM network. It consists of user independent hard- and software and of the subscriber identity module (SIM).
 - ❖ SIM card contains many identifiers and tables such as card-type, serial number, a list of subscribed services, a personal identity number (PIN), a PIN unblocking key (PUK), an authentication key and the international mobile subscriber identity (IMSI).
 - ❖ The MS stores dynamic information while logged onto the GSM system, such as, eg., the cipher key and the location information consisting of a temporary mobile subscribers identity (TMSI) and the location area identification (LAI).
 - ❖ **Base station subsystem (BSS):** A GSM network comprises many BSSs, each controlled by a base station controller (BSC).

2. Network and switching subsystem

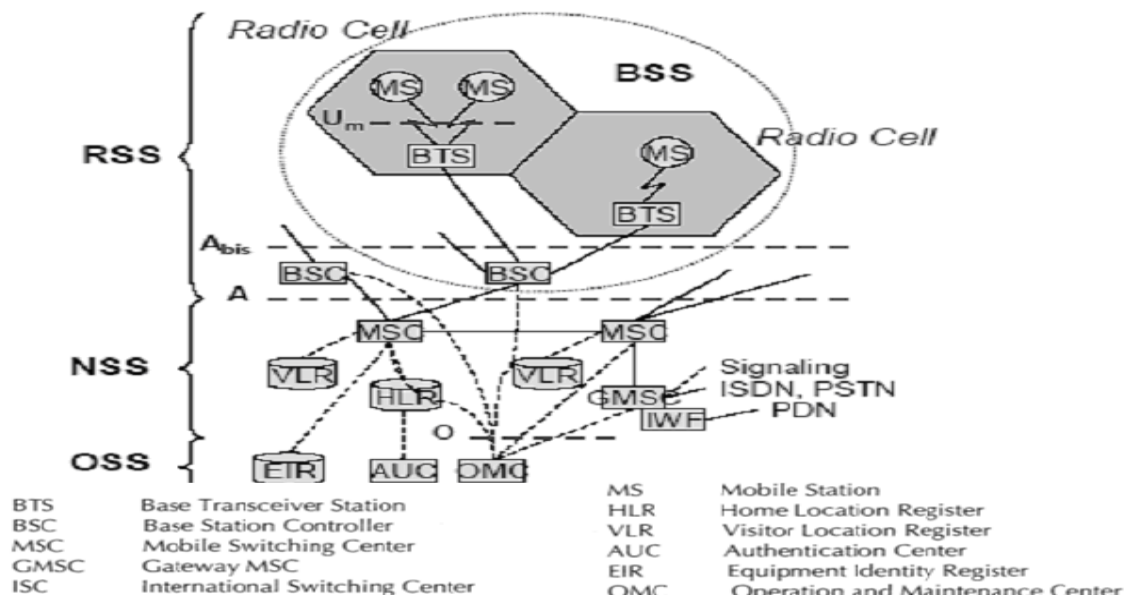
The main of the GSM system is formed by the Network and Switching Subsystem (NSS). The NSS consists of the following switches and database

- ❖ **Mobile services switches center (MSC):** MSCs are high-performance digital ISDN switches. Typically, an MSC manages several BSCs in a geographical region. MSC can also connect to public data network (PDN) such as X.25.
- ❖ **Gateway MSC (GMSC)** that is associated with the MSC. The GMSC is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user and vice versa. The GMSC is often implemented in the same node as the MSC.
- ❖ **Home location register (HLR):** The HLR is the most important Database in a GSM system as it stores all user-relevant information. This comprises static information, such as the mobile subscriber ISDN number (MSISDN). It contains Dynamic information like the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC.

- ❖ **Visitor location register (VLR):** VLR is similar to a cache, whereas HLR is the persistent storage. The VLR contains selected administrative information borrowed from the HLR, necessary for call control and provisioning. When a MS enters the covering area of a new MSC, the VLR associated with this MSC will request information from its corresponding HLR in the home network. The VLR will then have enough information in order to assure the subscribed services without needing to refer to the HLR each time a communication is established

3. Operation subsystem

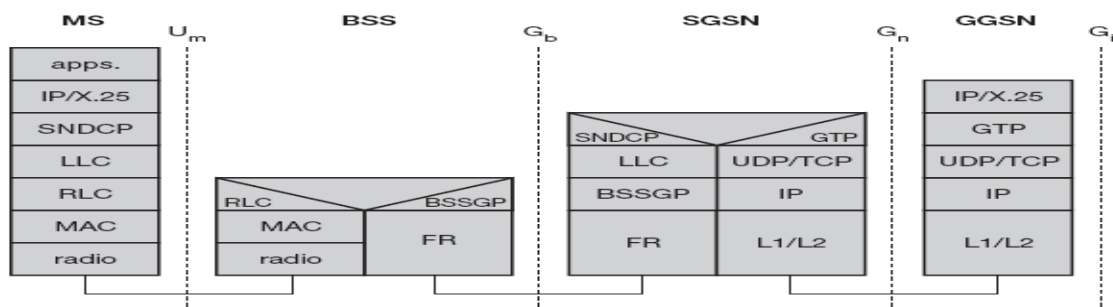
- ❖ The third part the operation subsystem (OSS), contains the necessary functions for network operation and maintenance. The OSS is connected to the different components of the NSS and to the BSC. It is also in charge of controlling the traffic load of the BSS.
- ❖ Operation and maintenance center (OMC) : The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). OMCs use the concept of telecommunication management network (TMN) as standardized by the ITU-T.
- ❖ Authentication centre (AuC) : is responsible for the authentication of a subscriber. This is a protected database and stores a copy of the secret key stored in each subscriber's SIM card. These data help to verify the user's identity.
- ❖ Equipment identity register (EIR): The EIR is a database for all IMEIs, i.e., it stores all device identification registered for this network. The EIR has a blacklist of stolen (or locked) devices. The EIR also contains a list of malfunctioning devices



6. Draw the Protocol stack of GSM and specify its functions?(Network aspects of GSM)

- Protocol Architecture of GSM consist of FIVE Layers. MS and MSC have five Protocol Layers whereas the BTS and BSC have only first three Layers
- **LAYER 1 (PHYSICAL LAYER) :-**It performs **Radio specific functions**, Modulations, Encryption / Decryption of Data, Channel Coding and Error Deduction / Correction, Voice Activity Deduction(VAD). Radio specific functions are **Creation of burst, Multiplexing** of burst into a TDMA frame, **synchronization** with the BTS.
 - ❖ **Synchronization** includes correction of individual path delay between an MS and the BTS. Difference in Round Trip Time is an issue. An MS close to the BTS have very short RTT. It requires Large Guard spaces. To reduce the Guard space adjustment is done via the variable **Timing Advance**
 - ❖ Physical layer at U_m uses (GMSK) Gaussian Minimum Shift Keying for Digital **Modulation**.
 - ❖ **Encryption** is performed between MS and BTS over the air interface.

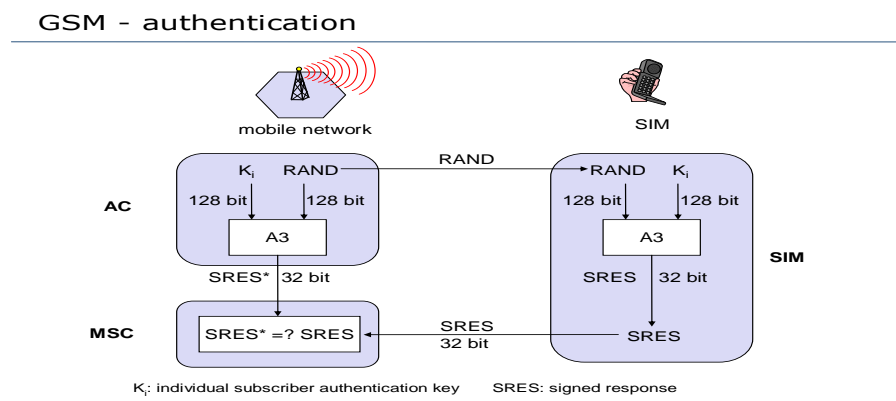
- ❖ **Channel Coding** make use of different Forward Error Correction Schemes(FEC) to add redundancy to the user data and to correct selected data.
- ❖ **Voice Activity Detection** transmits voice data only when there is a voice signal. During Periods of silence, the physical layer generates the **Comfort Noise** to fake a connection, but no actual transmission takes place.
- **LAYER 2: LAPDM**(Link Access procedure for D-channel) protocol has been defined at the Um interface for layer 2. It is the version of HDLC and it is a light weight LAPD as it does not need synchronization flags or checksum for error deduction. LAPDm has to obey the frame structure, recurrence pattern defined for Um interface. It provides Reliable data transfer over connection, Re-sequencing of data frames ,Flow control ‘Segmentation and reassembly of data ‘Acknowledged / Unacknowledged data transfer.
- **LAYER 3: NETWORK LAYER** : It Comprises many sub layers, lowest sub layer is **Radio Resource Management(Rr)**. The main task of RR include
 - Setup, Maintenance and Release of Radio channels
 - RR directly access the physical layer for Radio information
 - Offers a reliable connection to the next higher layer
- **RR’** : RR’ is a part of this layer that is implemented in the BTS, and the rest is in the BSC. The function of RR’ are supported by the BSC via the **BTS management (BTSM)** .



- **LAYER 4: MOBILITY MANAGEMENT(MM):** It contains functions for
 - Registration ,Authentication ,Identification
 - Location Updating and Provision of a **Temporary Mobile Subscriber**
 - a reliable connection to the next higher layer
 - **LAYER 5:CALL MANAGEMENT LAYER(CM)** CM layer consist of 3 entities
 - ❖ **Short Message Service** : SMS allows Message transfer using control channels **SDCCH** and **SACCH** .
 - ❖ **Call Control (CC)** : Call Control provides a point – point connection between two Terminals
 - ❖ CC is used by higher layers for Call Establishment, Call Clearing, Change of call parameter.CC layer provides functions to send in-band tones , called Dual Tone Multiple Frequency(DTMF) Supplementary Services(SS): These services offer various enhancement for the standard telephone services. Typical services are User Identification ,Call redirection, Forwarding of ongoing calls , Closed user groups and Multiparty Communication
- 7. Explain GSM SECURITY services Encryption & AUTHENTICATION in detail.**
- GSM offers several security services using confidential information stored in the AUC(Authentication Centre) and individual SIM(Subscriber Identity Module)
 - Important security services are

- ❖ **Access Control and Authentication:** It does Authentication of valid user for the SIM. The user need a secrete PIN to access the SIM. Subscriber authentication isbased on challenge response scheme
- ❖ **Confidentiality:** User related data is encrypted. BTS and MS apply encryption to voice, data, and signaling. This confidentiality exists only between MS and BTS and not end-to-end
- ❖ **Anonymity:** To provide user anonymity, all data is encrypted before transmission, and user identifiers which would reveal an identity are not used over the air. GSM transmits a temporary identifier (TMSI),which is newly assigned by the VLR after each location update.
- **ALGORITHMS USED**
 - ❖ **A3** : For Authentication
 - ❖ **A5** : For Encryption
 - ❖ **A8** : For Generation of a Cipher key
- **AUTHENTICATION:** Any subscriber must be authenticated before using service from GSM network. It is done at AUC
- ✓ Authentication is based on
 - SIM-which stores the individual authentication key K_i ,User identification IMSI and A3 – an algorithm used for authentication
- ✓ Authentication uses a **CHALLENGE – RESPONSE METHOD**
 - The access control AC generates a random number RAND as challenge
 - SIM with MS answer with SRES (signature response)as response
 - The AUC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR,
 - The current VLR requests the appropriate values for RAND, SRES, and Kc, from the HLR

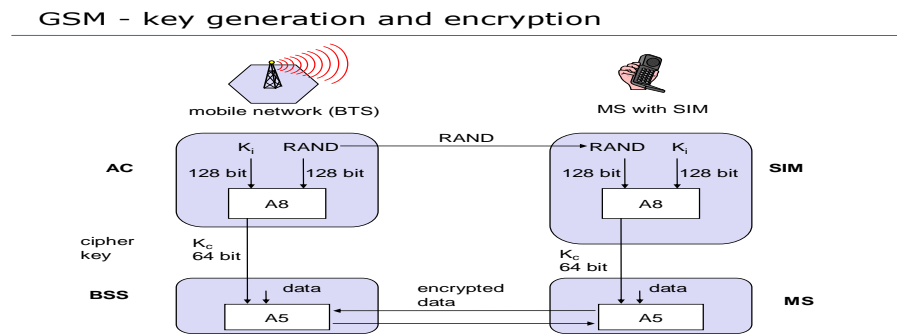
AUTHENTICATION



For Authentication the VLR sends the random values RAND to SIM

- ✓ Both sides, network and subscriber module ,perform the same operation with RAND and the key K_i called A3
- ✓ The MS sends back the SRES generated by the SIM, the VLR can now compare both values. If they are the same, the VLR accept the subscriber, otherwise the subscriber is rejected.
- **DATA ENCRYPTION**
 - ✓ Encryption is done to ensure privacy and is done by applying the cipher key Kc.Kc is generated using the individual key K_i and a random value by applying the algorithm A8.
 - ✓ The SIM in the MS and the network both calculate the same Kc, based on the random value RAND. The key Kc itself is not transmitted over the air interface.MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key Kc.

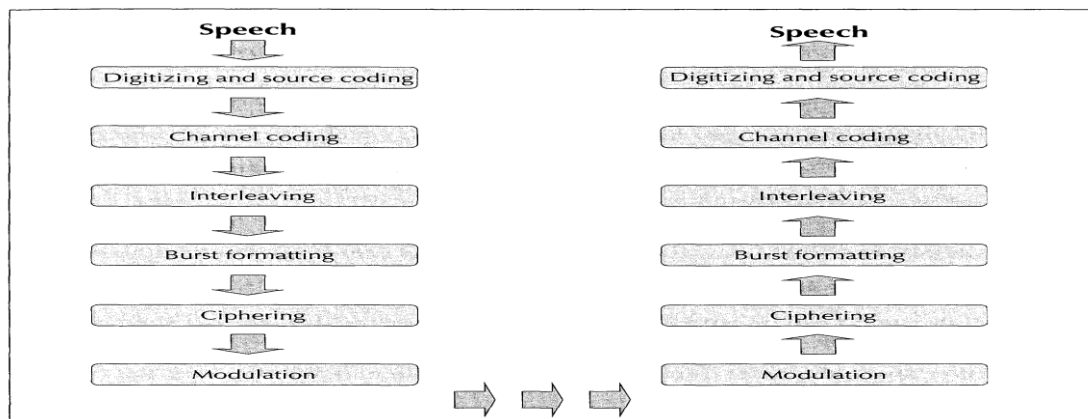
- ✓ **K_c** should be a 64 bits key which is not very strong but atleast a good protection against simple eavesdropping.



8. What are the sequence of operations in CALL ROUTING of GSM?

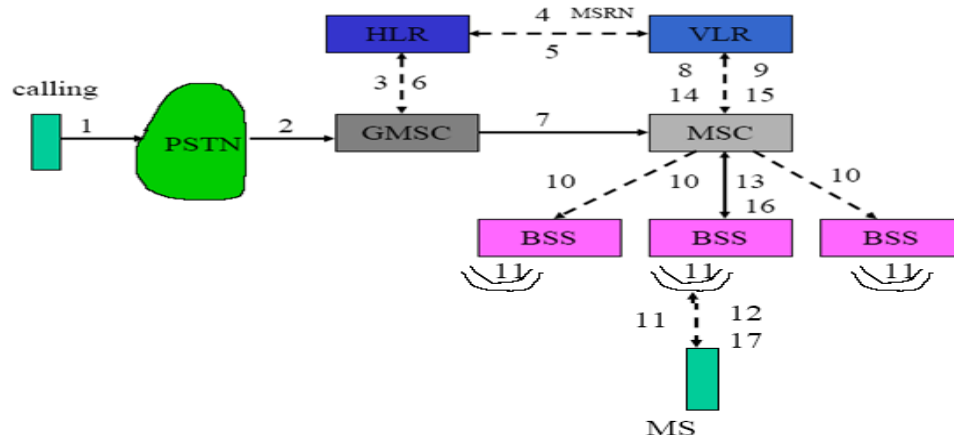
Explain it with an example.

- **Digitizer and source coding:** The user speech is digitized at 8 KHz sampling rate. Each sample is then represented in signed 13-bit linear PCM value. The encoder compresses these 160 samples into 260-bits GSM frames resulting in one second of speech compressed into 1625 bytes and achieving a rate of 13 Kbits/sec.
- **Channel coding:** This step introduces redundancy information into the data for error detection and possible error correction.
- **Interleaving:** This step rearranges a group of bits in a particular way. This is to improve the performance of the error-correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors.
- **Ciphering:** Encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS.
- **Burst formatting:** Adds some binary information to the ciphered block. This additional information is used for synchronization and equalization of the received data.
- **Modulation:** The modulation technique chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK). Using this technique the binary data is converted back into analog signal to fit the frequency and time requirements for the multiple access rules. This signal is then radiated as radio wave over the air.
- **Multipath and equalization:** At the GSM frequency bands, radio waves reflect from buildings, cars, hills, etc. So many reflected signals, which corrupt the information, with different phases are received. An equalizer is used to extract the 'right' signal from the received signal. In order to extract the 'right' signal, the received signal is passed through the inverse filter.
- **Synchronization:** Frequency synchronization is necessary so that transmitter and receiver frequency match (in FDMA). Time synchronization is necessary to identify the frame boundary and the bits within the frame (in TDMA). When a mobile station moves further away, the burst transmitted by this mobile may overlap with the timeslot of the adjacent timeslot. To avoid such collisions, the **Timing Advance** technique is used. In this technique, the frame is advanced in time so that this offsets the delay due to greater distance. Using this technique and the triangulation of the intersection cell sites, the location of a mobile station can be determined from within the network.

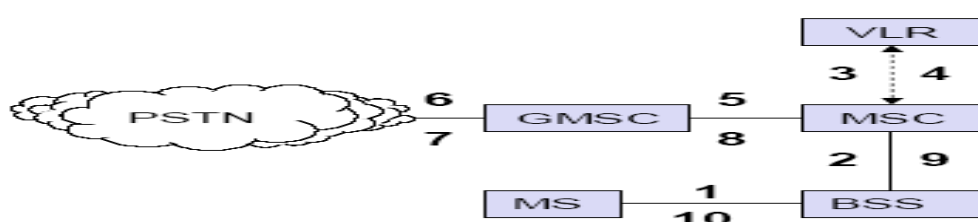


• **Example MOBILE TERMINATED CALL:**

- ❖ Consider the case the mobile terminated call (MTC), i.e. the situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station). The following figure shows the basic steps needed to connect the calling station with the mobile user.
- ❖ A user dials the phone number of a GSM subscriber(1).
- ❖ PSTN forward the call setup to the GMSC (of 2)
- ❖ GMSC identifies the HLR for the subscriber and signals the call setup to the HLR (3)
- ❖ HLR requests an MSRN mobile station roaming number from the current VLR (4).
- ❖ After receiving the MSRN(5) the HLR forwards the MSC responsible for the MS the GMSC (6).
- ❖ The GMSC can now forward the call setup request to the MSC indicated (7).
- From this point on, MSC is responsible for all further steps.
- ❖ MSC requests the current status of the MS from the VLR (8),reply (9)
- ❖ MSC initiates paging in all cells for location area, LA, 10
- ❖ All BTSs of all BSSs transmit this paging signal to the MSC (11).
- ❖ If the MS answers (12 & 13), the VLR has to perform the security check
- ❖ The VLR then signals to the MSC to setup a connection (15 – 17).



MOBILE ORIGINATED CALL:



Mobile Originated Call simpler than MTC

- The MS transmits the requests for a new connection (1).
- The BSS forwards the request to the MSC (2).
- The MSC then checks whether the user is allowed to setup a call with the requested service (3 & 4) and checks the availability of the resources through the GSM network and in to the PSTN.

9. Explain MOBILITY MANAGEMENT in GSM/Explain Handover and roaming?

- **Using Mobility management one can make and receive calls while in motion.** MM is in charge of all the aspects related to the mobility of the user, especially the roaming, the location management, and the authentication of the subscriber.
- **Paging:** MS is traced through the paging process
- **Location management** is concerned with the procedures that enable the system to know the current location of a powered-on mobile station so that the incoming call routing can be completed.
- When a mobile station is switched on in a new location area or the subscriber moves to a new location area or a different operator's PLMN, the subscriber must register with the new network to indicate its current location.
- **HANDOVER**
 - ❖ The user movements may make a user move away or closer to a tower. When the user moves away from a tower, the radio signal strength or the power of the signal keeps reducing. This can result in change of the channel or cell. This procedure of changing the resources is called **handover**. This procedure is called '**handoff**'.
 - ❖ Two reasons for Handover
 - ❖ The mobile station moves out of range of a BTS or a certain antenna of a BTS respectively. The received signal level decreases continuously. The error rate may grow due to interference,
 - ❖ The wired infrastructure (MSC, BSC) may decide to Handover may due to load balancing.

The following figure shows four possible handover scenarios in GSM:

Intra – cell Handover:

Within a cell, narrow – band interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency.

Inter-cell, intra – BSC handover:

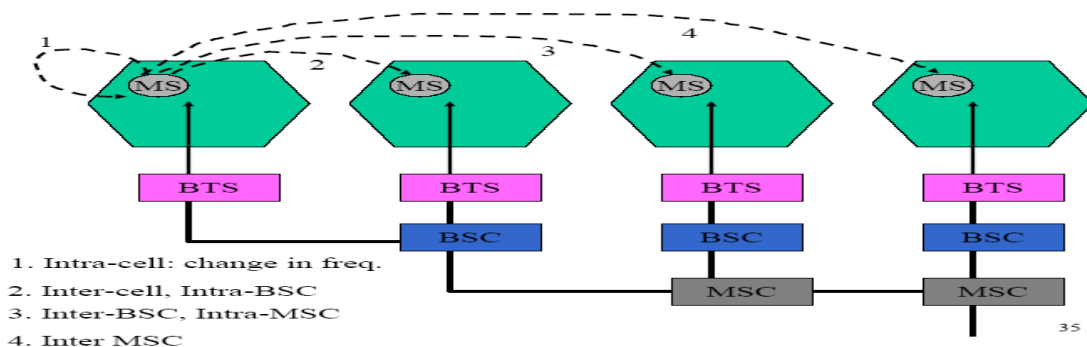
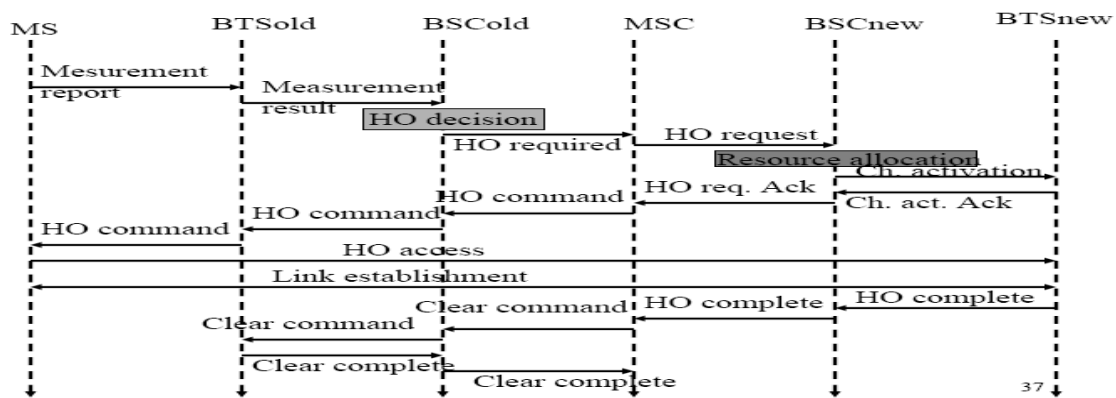
This is a typical handover scenario. The mobile station moves from one cell, to another but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one.

Inter – BSC, intra –MSC handover:

As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC.

Inter MSC Handover:

A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together.



ROAMING:

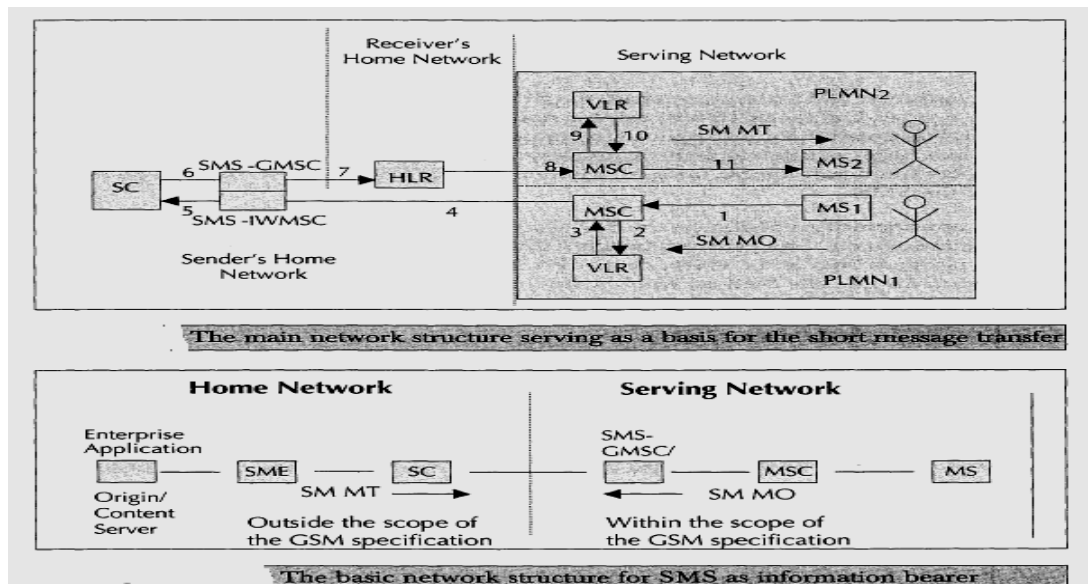
- Handover relates to moving from one point of attachment to another point of attachment within the same network operator; when this movement happens between two different networks it is called roaming.
- When a subscriber moves to a different operator's PLMN (Public Land Mobile Network), the subscriber must register with the new network to indicate its current location. The first location update procedure is called attach procedure. A location update message is sent to the new MSC / VLR, which records the location area information, and then sends the location information to the subscriber's HLR.
- If the mobile station is authenticated and authorized in the new MSC / VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR. A location update is also performed periodically.
- Roaming allows GSM users to seamlessly move around nationally and internationally and remain connected. A powered on mobile is informed of an incoming call by a paging message sent over the paging channel of the cells within the current location area. The location update procedures, and subsequent call routing, use the MSC and both HLR and the VLR. The information sent to the HLR is normally the SS7 address of the new VLR.
- An incoming mobile terminating call is directly to the Gateway MSC (GMSC) function. The GMSC is basically a switch, which is able to interrogate the subscriber's HLR to obtain routing information and thus contains a table linking MSISDNs to their corresponding HLR.
- MSRN is a temporary location-dependent MSISDN number. It is assigned by the serving VLR for each MS in its area. MSRNs are numbers reserved by a PLMN only for roaming use.

Roaming is of two types

- ❖ **Horizontal Roaming:** Horizontal Roaming is between two networks from same family. For example, GSM to GSM roaming or GSM to UMTS roaming.
- ❖ **Vertical Roaming:** Vertical Roaming is between two networks from different families. For example, GSM to CDMA roaming or GPRS to WiFi roaming. Seamless roaming is Vertical Roaming without disruption of session.

10.Explain SHORT MESSAGE SERVICES (SMS) architecture and features in detail.

- SMS is the most popular data bearer/service within GSM with an average of one billion SMS messages transacted every day around the world
- SMS uses the free capacity of the SS#7 signaling channel.
- **Unique characteristics of SMS**
 - ❖ **Omnibus nature of SMS:** SMS uses SS7 signaling channel, which is available throughout the world. **Stateless** SMS is session less and stateless. It is unidirectional and independent of any context. This makes SMS the best bearer for notifications, alerts and paging.
 - ❖ **Asynchronous:** SMS is completely asynchronous. SMS can be used as message queues.
 - ❖ **Self-configurable and last mile problem resistant:** SMS is self-configurable. While in a foreign network, one can access the SMS bearer without any change in the phone settings.
 - ❖ **Non-repudiation:** SMS message carries the SC and the source MSISDN as a part of the message header. **Always connected:** As SMS uses the SS7 signaling channel for its data traffic, it works always. When a phone is busy and a voice, data or FAX call is in progress, SMS message is delivered to the MS (Mobile Station) without any interruption to the call.
- **SMS Architecture**
SMS are basically of two types
SM MT (Short Message Mobile Terminated Point-to-Point),
SM MO (Short Message Mobile Originated Point-to-Point).
- SM MT is an incoming short message from the network side and is terminated in the MS. incoming message the path is from SC to the MS via HLR and the GMSC function of the home MSC.
- SM MO is an outgoing message, originated in the user device (MS), and forwarded to the network for delivery. For outgoing message, the path is from MS to SC via the VLR and the IWMSC function of the serving MSC,
- To use SMS as a bearer for Information exchange, the Origin server needs to be connected to the SC through a short message entity (SME). The SMS gateway interacts to the SC in one side, and the enterprise server on the other side. The SC is an independent computer in the network and works as a store and forward node. In SS7 terminology SC is a SCP (Service Control Point) within the SS7 cloud.
- Short Message Mobile Terminated (SM MT)
 - ❖ For a SM MT message, the message is sent from SC to the MS. This whole process is done in one transaction. For the delivery of MT or incoming SMS messages; the SC of the serving network is never used. This implies that a SMS message can be sent from any SC in any network to a GSM phone anywhere in the world. This makes any SM MT message mobile operator independent.
- Short Message Mobile Originated (SM MO)
 - ❖ SM MO is an outgoing message originated in the MS where generally the user types in a message and sends it to a MSISDN number. For a MO message, the MSC forwards the message to the home SC. MO message works in two asynchronous phases.
 - ❖ In the first phase, the message is sent from the MS to the home SC as a MO message. In the second phase, the message is sent from the home SC to the MS as a MT message.
 - ❖ It is possible to attempt to send a SMS message to an invalid MSISDN number. In such a case, the message will be sent successfully from the MS to the SC. However, it will fail during the SC to the MS transfer.



• VALUE ADDED SERVICES (VAS) THROUGH SMS

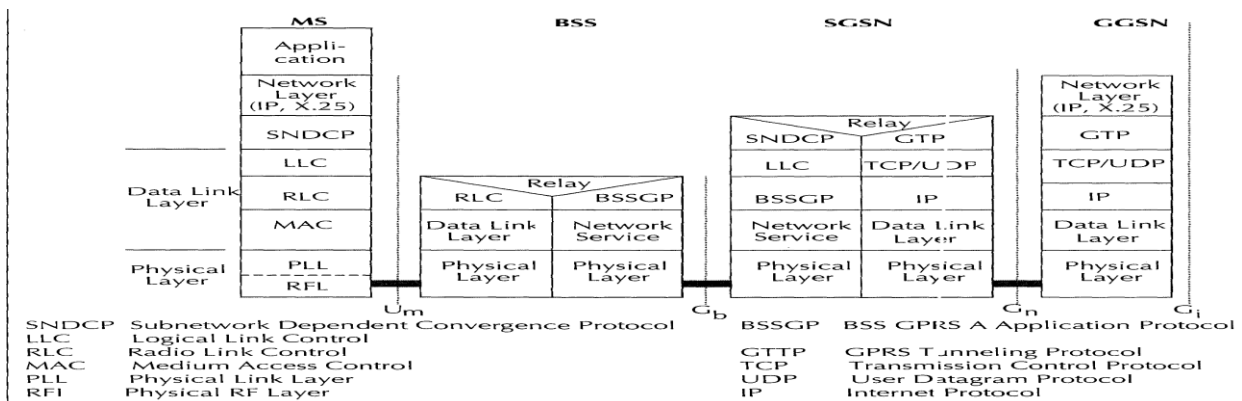
The most popular VAS over SMS are entertainment and information on demand. Information VAS Examples

- ❖ News/Stock Quotes Service: It gives the latest news or stock information. This will be a Short transaction.
- ❖ Session-based Chat Application: A chat service is essentially a session oriented transaction. Every SMS message carries the unique MSISDN number.
- ❖ Email through SMS is a transaction-oriented dialogue. message will be mailXXX@iitb.ac.in.
- ❖ Health Care Services; Health care applications need both Pull and Push.
- ❖ Micro-Payment Services : e.g a vending machine application
- ❖ Alert Services: These are proactive alert services.

11.Explain GPRS PROTOCOL ARCHITECTURE in detail.

Signaling Plane

- It comprises protocols for control and support of the functions like attach and detach, PDP context activation, control of routing paths, and allocation of network resources.
- Between SGSN and HLR, VLR, and EIR, it uses the same protocols as GSM but with extension. An enhanced MAP (Mobile Application Part) is employed. MAP is a mobile network-specific extension of the Signaling System SS#7 used in GSM. It transports the signaling information related to location updates, routing information and handovers. The exchange of MAP messages is accomplished over the transaction capabilities application part (TCAP) and the signaling connection control part (SCCP).
- The base station system application part (BSSAP+) is an enhancement of GSM's BSSAP. It is used to transfer signaling information between the SGSN and the VLR.



GPRS Backbone

- GTP protocol is used in between SGSN and GGSN within one PLMN & SGSN and GGSN of different PLMNs. GTP protocol tunnels the user data packets through the GPRS backbone with specific routing information. GTP packets carry the user's data packets from both IP and X.25 data networks.
- Below GTP, the standard protocols TCP or UDP are used. TCP is used for tunneling X.25 data. UDP is used for IP.
- Ethernet, ISDN, or ATM-based protocols may be used in the physical layer in the IP backbone. IP/X.25-over-GTP-over-UDP/TCP-over-IP transport architecture.

BSS-SGSN Interface

The BSS and SGSN interface is divided into the following layers:

Sub-Network Dependent Convergence Protocol (SNDSCP): It is used to transfer data packets between SGSN and MS. Its functionality includes:

Multiplexing of several connections of the network layer onto one virtual connection of LLC

Segmentation, compression, and decompression of user data.

Logical Link Control (LLC): a data link layer protocol for GPRS which functions similar to Link Access Procedure—D (LAPD).

Base Station System GPRS Protocol (BSSGP): The BSSGP delivers routing and QoS-related information between BSS and SGSN.

Network Service: This layer manages the convergence sublayer that operates between BSSGP and the Frame Relay Q922 Core by mapping.

Data Link Layer: The data link layer between the MS and the BSS is divided into three sublayers:

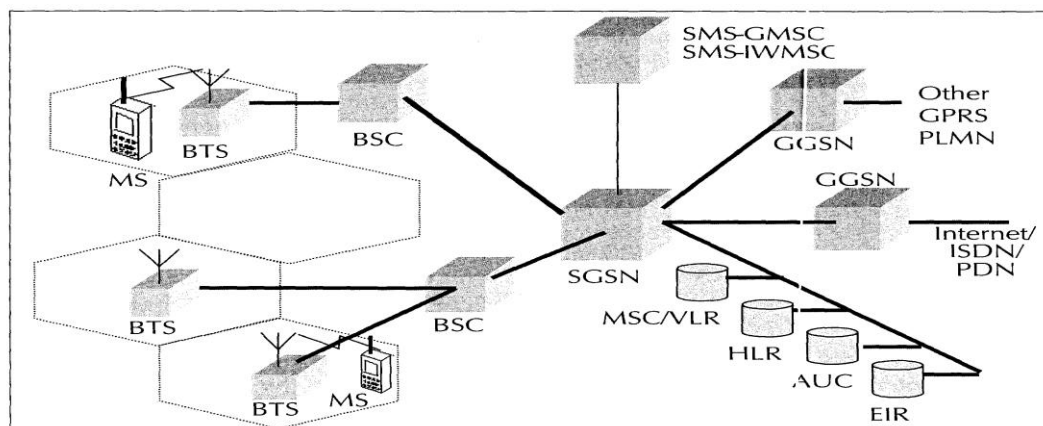
- **Logical Link Control (LLC):** It provides a reliable logical link between an MS and its assigned SGSN. Its functionality is based on HDLC protocol and includes sequence control, in-order delivery, flow control, detection of transmission errors, and retransmission ARQ. Encryption is used in this interface to ensure data confidentiality. Variable frame lengths are possible. Both acknowledged and unacknowledged data transmission modes are supported. This protocol is an improved version of the LAPDm protocol used in GSM.
- **Radio Link Control (RLC):** The main purpose is to establish a reliable link between the MS and the BSS. This includes the segmentation and reassembly of LLC frames into RLC data blocks and ARQ of uncorrectable data.
- **Medium Access Control (MAC):** It controls the access attempts of an MS on the radio channel shared by several VSSs. It employs algorithms for contention resolution, multiuser multiplexing on a packet data traffic channel (PDTCH), and scheduling and prioritizing based on the negotiated QoS.

Physical Layer: The physical layer between MS and BSS is divided into two sublayers: the physical link layer (PLL) and the physical RF Layer (RFL).

- **Physical Link Layer (PLL):** This layer provides services for information transfer over a physical channel between the MS and the network. These functions include data unit framing, data coding, and the detection and correction of physical medium transmission errors
- **Physical RF Layer (RFL):** This layer performs the modulation of the physical waveforms based on the sequence of bits received from the Physical Link layer above. The Physical RF layer also demodulates.

12. Explain the functions of various entities in GPRS ARCHITECTURE.

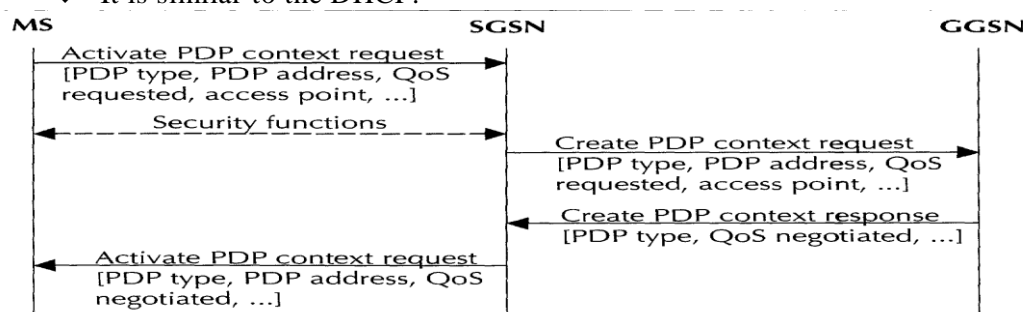
- GPRS uses the GSM architecture for voice. Its network nodes are called GPRS support nodes (GSN). GSNs are responsible for the delivery and routing of data packets between the mobile stations and PDN.
- **Serving GPRS Support Node (SGSN):** Serving GPRS support node (SGSN) is at the same hierarchical level as the MSC. SGSN's tasks include packet switching, routing and transfer, mobility management, logical link management, and authentication and charging. The location register of the SGSN stores location information (e.g., current cell, current VLR). SGSN sends queries to Home Location Register (HLR) to obtain profile data of GPRS subscribers. It is connected to the base station system with Frame Relay.
- **Gateway GPRS Support Node (GGSN):** GGSN acts as an interface between the GPRS backbone network and the external packet data networks. (Ill^r to that of a router in a LAN). GGSN maintains routing information to tunnel the PDUs to the SGSNs. It converts the GPRS packets coming from SGSN into appropriate packet data protocol (PDP) format. So, GGSN stores the current SGSN address of the user and his or her profile in its location register. It also does authentication and charging functions related to data transfer.



- **Some existing GSM network elements which are to be enhanced to support packet data:**
- **Base Station System (BSS):** BSS system needs enhancement to recognize and send packet data. This includes BTS upgrade to allow transportation of user data to the SGSN. Also, the BTS needs to be upgraded to support packet data transportation between the BTS and the MS (Mobile Station) over the radio.
- **HomeLocation Register (HLR):** It needs enhancement to register GPRS user profiles and respond to queries from GSNs regarding profiles.
- **Mobile Station (MS):** It is different from that of GSM.
- **SMS nodes:** SMS-GMSCs and SMS-IW/MSCs are upgraded 1.o support SMS transmission via the SGSN. Optionally, the MSC/VLR can be enhanced for more efficient co-ordination of GPRS and non-GPRS services and functionality.

13.Explain GPRS NETWORK OPERATIONS in detail.

- Once a GPRS mobile station is powered on, it 'introduces' itself to the network by sending a "GPRS attach" request. Network access can be achieved from either the network side or the MS side of the GPRS network.
- **Attachment and Detachment Procedure**
 - ❖ MS must **register** itself with an SGSN of the network. This is GPRS attach which is a logical link between the MS and the SGSN.
 - ❖ The network checks if the MS is authorized to use the services; if so, it copies the user profile from the HLR to the SGSN, and **assigns a Packet-TMSI** to the MS.
 - ❖ Then, MS must **apply for an address**. This address is called PDP (Packet Data Protocol) address. For each session, a PDP context is created. It contains the PDP type, the address assigned, the requested QoS, and the address of the GGSN (access point to the PDN). This context is stored in the MS, the SGSN and the GGSN. Now the MS is 'visible' to the external PDN.
 - ❖ User data is transferred through GTP encapsulation and tunneling. User data can be compressed and encrypted for efficiency and reliability. The allocation of the PDP address can be static or dynamic. Static address is assigned by the network operator. In dynamic case, a PDP address is assigned to the user upon activation of a PDP context. In dynamic PDP address assignment, the GGSN is responsible for the allocation and the activation/deactivation of the PDP addresses.
 - ❖ It is similar to the DHCP.

**PDP context activation procedure**

- 'activate PDP context request,' -MS informs the SGSN about the requested PDP context
- 'create PDP context request' – from SGSN to the GGSN if authentication is successful.
- The GGSN creates a new entry in its PDP context table to route data packets between the SGSN and the external PDN.
- 'create PDP context response' - GGSN returns confirmation to the SGSN with the PDP address
- 'activate PDP context accept' - SGSN updates its PDP table and confirms the activation to MS.
- The disconnection from the GPRS network is called **GPRS detach**. All the resources are released following a GPRS detach. Detach process can be initiated by the mobile station or by the network.

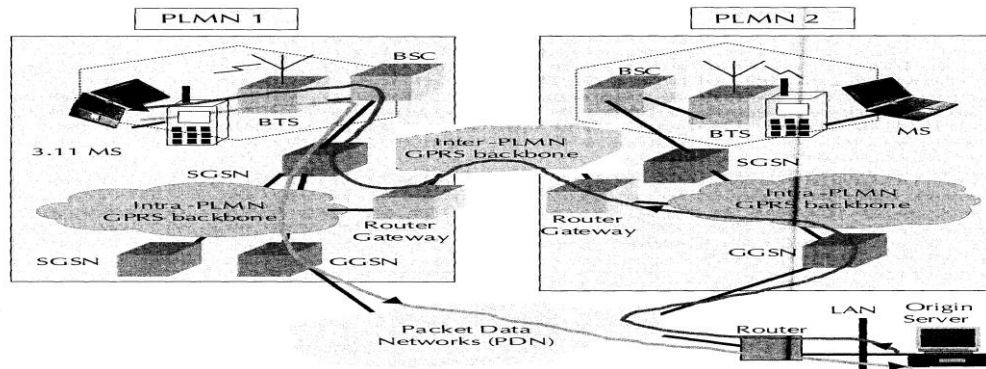
Mobility Management

- As a mobile station moves from one area to another, mobility management functions are used to track its location within each PLMN. SGSNs communicate with each other to update the MS's location in the relevant registers. The mobile station's profiles are preserved in the VLRs that are accessible to SGSNs via the local MSC. A logical link is established and maintained between the mobile station and the SGSN at each PLMN.

At the end of transmission the logical link is released and the resources associated with it can be reallocated.

Routing

- Consider two intra-PLMN backbone networks of different PLMNs. Intra-PLMN backbone networks connect GSNs of the same PLMN or the same network operator. These are private packet-based networks of the GPRS network provider; for example, Airtel GSNs in Bangalore connecting to Airtel GSNs in Delhi through a private data network.



- These intra-PLMN networks are connected with an inter-PLMN backbone. An inter-PLMN backbone network connects GSNs of different PLMNs and operators.
- The gateways between the PLMNs and the external inter-PLMN backbone are called border gateways. They perform security functions to protect against unauthorized users and attacks.

Scenario:

- We assume that the packet data network is an IP network. A GPRS mobile station located in PLMN1 sends IP packets to a host connected to the IP network, the SGSN that the mobile station is registered with encapsulates the IP packets coming from the mobile station, examines the PDP context and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN. The GGSN decapsulates the packets and sends them out on the IP network, where IP routing mechanisms are used to transfer the packets to the access router of the destination network.
- Let us assume the home-PLMN of the mobile station is PLMN2. An IP address has been assigned to the mobile by the GGSN of PLMN2. Thus, the MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2. The correspondent host is now sending IP packets to the MS. The packets are sent out onto the IP network and are routed to the GGSN of PLMN2 (the home-GGSN of the MS). The latter queries the HLR and obtains the information that the MS is currently located in PLMN1. It encapsulates the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1. The SGSN decapsulates the packets and delivers them to the MS.
- The SGSN informs the HLR about the current location of the MS. When the MS registers with a new SGSN, the HLR will send the user profile to the new SGSN. The signaling path between GGSN and HLR may be used by the GGSN to query a user's location and profile in order to update its location register.

14. Write short notes on (i) DATA SERVICES IN GPRS (ii) GPRS Applications.

i) DATA SERVICES IN GPRS

Two mode of services are **Application mode** or **Tunneling mode**.

Application mode: Users use GPRS mobile phone to access the applications running on the phone itself. The phone is the end user device. WAP browser allows browsing of WAP sites. This mode supports mobile execution environment. These devices support development of client application that can run on the device --- Symbian and J2ME.

Tunneling mode: This mode is for mobile computing where the user will use the GPRS interface as an access to the network. The end user device will be a large footprint device like laptop computer or small footprint device like PDAs. For these devices, access can be gained via a PC Card (PCMCIA) or via a serial cable to a GPRS-capable phone. These 'black-box' devices do not have display, keypad and voice accessories of a standard phone.

- **GPRS Handsets/ Terminals** A GPRS terminal can be one of three classes: A, B or C.
 - ❖ **Class A** terminal can make or receive calls on two services simultaneously. GPRS virtual circuits will be held or placed on busy rather than being cleared. SMS is supported in Class A terminal
 - ❖ **Class B** terminal can monitor GSM and GPRS channels simultaneously, but can support only one of these services at any time. Therefore, a Class B terminal can support simultaneous attach, activation, and monitor but not simultaneous traffic. GPRS virtual circuits will be held or placed on busy rather than being cleared.
 - ❖ **Class C** terminal supports only non-simultaneous attach. The user must select which service to connect to. Class C terminal can make or receive calls from only the manually selected network service. Support of SMS is optional for Class C terminals.
- **Device Types**
 - ❖ Each handset will have a unique form factor like a numeric keypad and a relatively small display. Other types of phones with different form factors, color displays, with cameras are common. Smart phones with built-in voice, non-voice and Web-browsing capabilities are also included.
- **Bearer Services in GPRS**

The bearer services of GPRS offer end-to-end packet switched data transfer. It supports: the point-to-point (PTP) service and the point-to-multipoint (PTM) service.

 - **SMS:** It was originally designed for GSM. GPRS will continue to support SMS as a bearer.
 - **WAP:** It is a data bearer service over HTTP protocol.
 - **MMS:** MMS is Multimedia Messaging Service. This is the next generation messaging service.

ii) APPLICATIONS of GPRS

- **Generic Applications :** Information services, Internet access, email, Web Browsing, mass market applications offering contents like sports scores, weather, flight information, news headlines, prayer reminders, lottery results, jokes, horoscopes, traffic information, Access to corporate net, Intranet Mobile commerce Banking over wireless

GPRS-Specific Applications

- **Chat** GPRS will offer ubiquitous chat by integrating Internet chat and wireless chat using SMS and WAP.
- **Multimedia Service:** Multimedia objects like photographs, pictures, postcards, greeting cards and presentations, static web pages can be sent and received over the mobile network.
- **Virtual Private Network:** GPRS network can be used to offer VPN services. Many banks are migrating from VSAT to GPRS-based networks. This is expected to reduce the transaction time by about 25%.
- **Personal Information Management:** Personal diary, address book, appointments, engagements are kept in the phone some in the organizer and some in the Intranet. Using GPRS, J2ME and WTAI the address book, the diary of the phone can be integrated with the diary at the home office.
- **Job Sheet Dispatch:** GPRS can be used to assign and communicate job sheets from office-based staff to mobile field staff. It can be combined with vehicle positioning applications so that the nearest available suitable personnel can be deployed to serve a customer.
- **Unified Messaging:** Unified messaging uses a single mailbox for all messages, including voice mail, fax, e-mail, SMS, MMS, and pager messages.

- **Vehicle Positioning:** This application integrates GPS that tell people where they are. Vehicle-positioning applications can be used to deliver several services including remote vehicle diagnostics, ad hoc stolen vehicle tracking and new rental car fleet tariffs and services in logistics industry.
- **Location-based Services and Telematics:** Location-based services provide the ability to link push or pull information services with a user's location. Examples include hotel and restaurant finders, roadside assistance, and city-specific news and information.

UNIT – II

Part -B

1. Explain about WLAN architecture and entities in detail

IEEE 802.11 WLAN

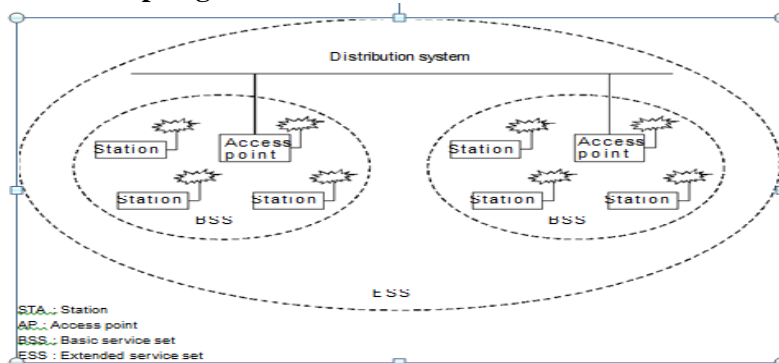
In 1997 the IEEE developed an international standard for WLANs: It focuses on the bottom two layers of the OSI model: the physical layer (PHY) and data link layer (DLL). The objective of the IEEE 802.11 standard was to define a medium access control (MAC) sublayer, MAC management protocols and services, and three PHYs for wireless connectivity of fixed, portable, and moving devices within a local area.

Architecture

The architecture of the IEEE 802.11 WLAN is designed to support a network where most decision-making is distributed to mobile stations. Two network architectures are defined in the IEEE 802.11 standard:

- *Infrastructure network:* It provides communication between wireless clients and wired network resources. The transition of data from the wireless to wired medium occurs via an AP. Together all the devices form a basic service set.
- *Point-to-point (ad hoc) network:* Typically, an ad hoc network is created spontaneously between wireless devices and does not support access to wired networks. An ad hoc network does not require an AP.

Three basic topologies for WLANs:



- The BSS is an ad hoc network/ a peer-to-peer network in which communicate directly with one another on an ad hoc\peer-to-peer basis. An IBSS is typically a short-lived network, with a small number of stations that is created for a particular purpose.
- The BSS configuration relies on an AP that acts as the logical server for a single WLAN cell or channel. All communications are through AP An AP performs a bridging function, connects multiple WLAN cells, and connects WLAN cells to a wired LAN.
- The ESS configuration consists of multiple BSS cells that can be linked by either wired or wireless backbones called a distributed system. To network the equipment outside of the ESS, the ESS and all of its mobile stations appear to be a single MAC-layer network where all stations are physically stationary. Thus, the ESS hides the mobility of the mobile stations from everything outside the ESS.

WLAN Equipment

- **LAN adapter :** They provide the interface between the network operating system and an antenna to create a transparent connection to the network.
- **AP :** The AP is the wireless equivalent of a LAN hub. It receives, buffers, and transmits data between the WLAN and the wired network
- **Outdoor LAN bridges :** Outdoor LAN bridges are used to connect LANs in different buildings.

2. How does 802.11 Medium Access Control protocol work?

WLANs implement a random access protocol, CSMA/CA with some modification, to deal with the *hidden node* problem.

IEEE 802.11 uses

distributed coordination function (DCF)

point coordination function (PCF)

DCF

DCF is a modified protocol known as *carrier-sense multiple-access with collision avoidance* (CSMA/CA). CSMA/CA attempts to avoid collisions by using *explicit packet acknowledgment* (ACK)

CSMA/CD used in 802.3 cannot be used on a WLAN for two reasons:

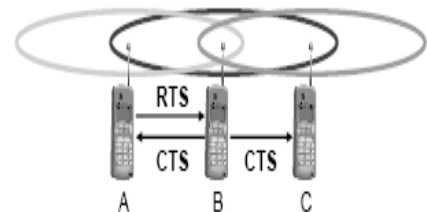
- Implementing a collision detection mechanism would require the implementation of a full duplex radio that increase the cost significantly.
- All stations cannot hear each other, and the fact that a station wants to transmit senses the medium. Free medium does not necessarily mean that the medium is free around the receiver area—(hidden and exposed station)

Hidden and Exposed Node Problems are specific to a WLAN. To avoid collisions DCF uses **MACA (Multiple Access with Collision Avoidance) [CSMA with CA] uses short signaling (control) packets**

- **RTS (request to send):** a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
- **CTS (clear to send):** the receiver grants the right as soon as it is ready

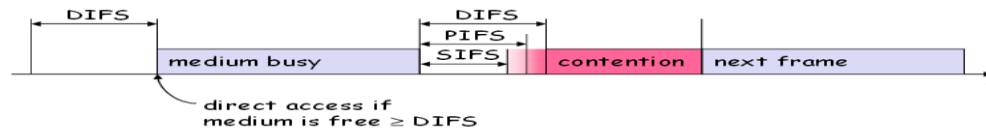
Signaling packets contain:

- sender address ,receiver address
- packet size (from which the transmission time can be derived)
- MACA avoids the problem of hidden stations
- A and later C want to send to B
- A sends RTS first
- B sends CTS to A and B
- C waits after receiving CTS from B



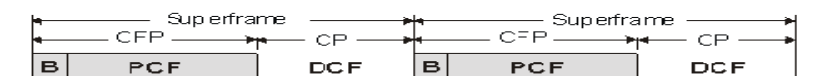
802.11 MAC uses a positive ACK, inter-frame space (IFS) & exponential back off algorithm.

- A station with a frame to transmit senses the medium. If the medium remains idle for a time equal to IFS (inter frame space- delay), then the station can transmit. If a medium is busy, the station defers transmission and continues to monitor the medium until transmission is over. Once the transmission is over, station delays another IFS. If the medium remains idle, then station senses the medium using exponential back off scheme.
- **Exponential Back off Algorithm**
 - ❖ It is used to resolve contention problems among different stations wishing to transmit data at the same time. When a station goes into the back off state, it waits an additional, randomly selected number of time slots
 - ❖ During the wait, the station continues sensing the medium. At the end of its contention window, if the medium is still free the station can send its frame. If another station begins transmitting data, the back off counter is frozen and counting down starts again when the channel returns to the idle state.
- **Inter frame space IFS:** It uses a delay is known as an inter frame space IFS. There are 3 different type of IFS.
 - SIFS (Short IFS) :** It is used for all immediate response action. (ACK, CTS)
 - PIFS (Point Coordination IFS) :** A middle length IFS, used by centralized controller in PCF scheme when issuing polls.
 - DIFS (Distributed Coordination IFS) :** A longest IFS used as a minimum delay for asynchronous frames .

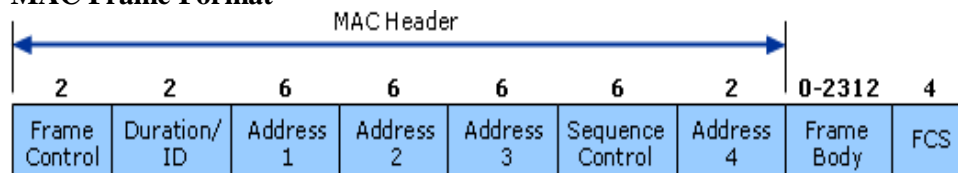


POINT COORDINATION FUNCTION : It provides contention free service. PCF is built on DCF. An alternative method implemented on top of PCF. Point coordinator makes use of PIFS when issuing polls. It seizes the medium and lockout all asynchronous traffic while it issues polls and receives responses.

Super Frame : At its beginning the point coordinator may optionally seize medium and issue polls for a given period of time. The responding stations send variable size frames. The remainder of super frame is available for contention based access. At the end of super frame it uses PIFS delay. If medium is idle, point coordinator gains immediate access and full super frame period follows. Suppose medium is busy, PCI must wait and it results in foreshortened super frame.



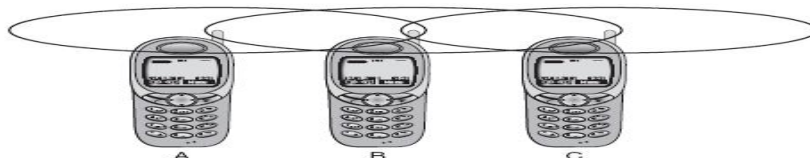
MAC Frame Format



3. (i) What is Hidden and Exposed Node Problem specific to a WLAN

Hidden station problem:

- A sends to B, C cannot receive A
- C wants to send to B, C senses a "free" medium (CS fails)
- collision at B, A cannot receive the collision (CD fails)
- A is "hidden" for C



Exposed terminals

- B sends to A, C wants to send to another terminal (not A or B)
- C has to wait, CS signals a medium in use
- but A is outside the radio range of C, therefore waiting is not necessary
- C is "exposed" to B

MACA (Multiple Access with Collision Avoidance) / CSMA with CA uses short signaling (control) packets for collision avoidance:

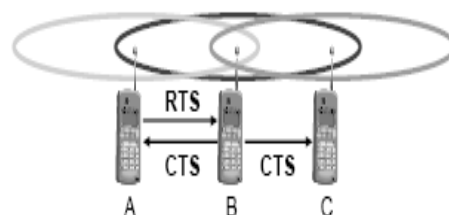
- **RTS** (request to send): a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
- **CTS** (clear to send): the receiver grants the right as soon as it is ready

Signaling packets contain:

- sender address, receiver address
- packet size (from which the transmission time can be derived)

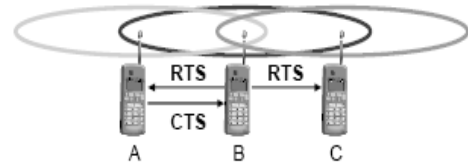
MACA avoids the problem of hidden stations

- A and later C want to send to B
- A sends RTS first
- B sends CTS to A and B
- C waits after receiving CTS from B



MACA avoids the problem of exposed stations

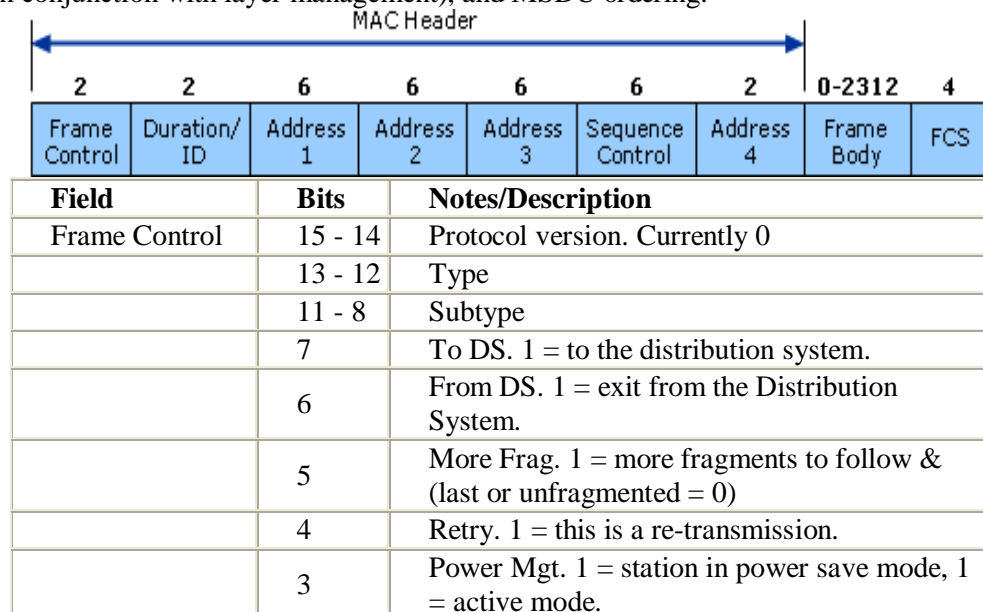
- B wants to send to A, C to another station
- now C does not have to wait because it cannot receive CTS from A

**(ii) Write short notes on IEEE 802.11n**

- Higher-performance WLANs is the task group 802.11n. The scope of this task group is to define modifications to the PHY and MAC layer to deliver a minimum of 100 Mbps throughput at the MAC service AP (SAP).
- 802.11n employs an evolutionary philosophy of reusing existing technologies like OFDM, FEC coding, interleaving, and QAM along with new technologies to provide effective performance improvements to meet the needs of evolving applications.
- **OFDM** implementation improves data rate than 802.11a/g standards. OFDM supports wider bandwidth and higher code rate to bring maximum data rate to 65Mbps.
- Multi-input, multi-output (**MIMO**) technology is used in 802.11n to evolve the existing OFDM using Space-division multiplexing (SDM): It splits a data stream into multiple parts through separate antennas. MIMO limits power consumption by utilizing multiple antennas only on as-needed basis.
- The MIMO power-save mode features:
- Beam-forming is a technique that focuses radio signals directly on the target antenna, thereby improving range and performance by limiting interference. Diversity exploits multiple antennas by combining the outputs of or selecting the best subset of a larger number of antennas than required to receive a number of spatial streams
- Effectively doubles data rates by **doubling channel width** from 20 to 40 MHz.
- Instead of sending a single frame, the client bundles several frames together. 40 MHz channels **Aggregation** Improves efficiency by allowing transmission bursts of multiple data packets between overhead communications.
- **Reduced interframe spacing** (RIFS) Designed to improve efficiency by providing a shorter delay between OFDM transmissions than in 802.11a or g.
- Greenfield mode improves efficiency by eliminating support for 802.11a/b/g devices in all 802.11n n/w.

4. Draw MAC Frame Format and explain the significance of fields?

In IEEE 802.11, the MAC sublayer is responsible for asynchronous data service [e.g., exchange of MAC service data units (MSDUs)], security service (confidentiality, authentication, access control in conjunction with layer management), and MSDU ordering.



	2	More Data. 1
	1	WEP. 1 = data processed with WEP algorithm. 0 = no WEP.
	0	Order. 1 = frames must be strictly ordered.
Duration ID	15 - 0	For data frames = duration of frame.
Address 1	47 - 0	Source address (6 bytes).
Address 2	47 - 0	Destination address (6 bytes).
Address 3	47 - 0	Receiving station address (destination wireless station)
Sequence Control	15 - 0	
Address 4	47 - 0	Transmitting wireless station.
Frame Body		0 - 2312 octets (bytes).
FCS	31 - 0	Frame Check Sequence (32 bit CRC). defined in P802.11.

Address : It uses 4 address fields

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

- **Destination Address (DA).** DA indicates the MAC address of the final destination to receive the frame.
- **Source Address (SA).** SA indicates the MAC address of the original source that initially created and transmitted the frame
- **Receiver Address (RA).** RA indicates the MAC address of the next immediate STA on the wireless medium to receive the frame.
- **Transmitter Address (TA).** TA indicates the MAC address of the STA that transmitted the frame onto the wireless medium

(ii) Write short notes on Power Management in 802.11

- Power management is necessary to minimize power requirements for battery-powered portable mobile units. The standard supports two power-utilization modes, called *continuous aware mode* and *power-save polling mode*. In the former, the radio is always ON and draws power, whereas in the latter, the radio is dozing with the AP and is queuing any data for it.
- A power-saver mode or sleep mode is defined when the station is not transmitting in order to save battery power. However, critical data transmissions cannot be missed. Therefore APs are required to have buffers to queue messages. Sleeping stations are required to periodically wake up and retrieve messages from the AP.
- Power management is more difficult for peer-to-peer IBSS configurations without central AP. In this case, all stations in the IBSS must be awakened when the periodic beacon is sent. Stations randomly handle the task of sending out the beacon. An announcement traffic information message window commences. During this period, any station can go to sleep if there is no announced activity for it during this short period.

5. Explain HIPERLAN family for short range wireless communication in detail?

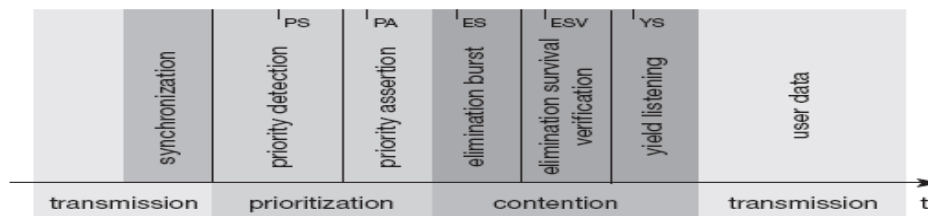
- **HiperLAN** (High Performance Radio LAN) is a Wireless LAN standard. It is a European alternative for the IEEE 802.11 standards (IEEE). It is defined by the European Telecommunications Standards Institute (ETSI). In ETSI the standards are defined by the

BRAN project (Broadband Radio Access Networks). The HiperLAN standard family has four different versions. It uses 5.15–5.25 GHz band.

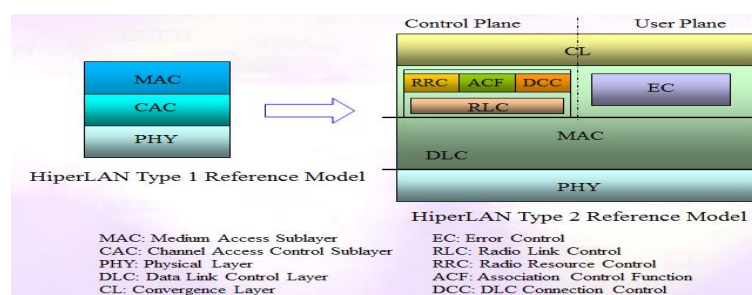
High Performance Radio Local Area Networks Family of Standards

	Hiperlan 1	Hiperlan2	HiperAccess	HiperLink
Description	Wireless Ethernet	Wireless ATM	Wireless Local Loop	Wireless Point-to-Point
Freq. Range	5GHz	5GHz	5GHz	17GHz
PHY Bit Rate	23.5Mbps	6~54Mbps	~25Mbps (data rate)	~155Mbps (data rate)

- HIPERLAN /1 is aligned with the IEEE 802 family of standards and is very much like a modern wireless Ethernet. DLL is further divided into two parts, the channel access control (CAC) sublayer and MAC sublayer.
- The CAC sublayer defines how a given channel access attempt will be made depending on whether the channel is busy or idle and at what priority level an attempt will be made.
- MAC layer defines the various protocols which provide the HIPERLAN/1 features of power conservation, security, and multihop routing as well as service to the upper layers of protocols.
- HIPERLAN/1 uses the same modulation technology that is used in GSM, GMSK. It has an over air data rate of 23.5 Mbps The range in a indoor environment is 35 to 50 m.
- Elimination-yield non-preemptive priority multiple access (EY-NPMA) divides the medium access of different competing nodes into three phases:
 - ❖ **Prioritization:** Determine the highest priority of a data packet ready to be sent by competing nodes.
 - ❖ **Contention:** Eliminate all but one of the contenders, if more than one sender has the highest current priority.
 - ❖ **Transmission:** Finally, transmit the packet of the remaining node.



- **HIPERLAN 2:**
Protocol stack of HIPERLAN/2.



HIPERLAN/2 has three basic layers: PHY, data link control layer (DLC), and convergence layer (CL)

The protocol stack is divided into a control plane and a user plane.

- The user plane includes functions for transmission of traffic over established connections

- The control plane performs functions of connection establishment, release, and supervision.
- A burst consists of a preamble part and a data part. The data part originates from each of the transport layers within DLC.
- A key feature of the PHY is to provide several modulation and coding schemes to meet the requirements for different PHY modes
- The DLC layer constitutes the logical link between an AP and mobile terminals (MTs). The DLC includes functions for medium access and transmission as well as terminal/user connection handling. The DLC layer consists of MAC, error control (EC), radio link control (RLC), DLC connection control (DCC), radio resource control (RRC), and association control function (ACF)
- HIPERLAN/2 is based on the time-division duplex/time-division multiple access (TDD/TDMA) and uses a MAC frame of 2 ms duration. HIPERLAN/2 operates as a connection-oriented wireless link.

The CL between the DLL and network layer provides QoS. CL is two-fold

- it maps the service requirements of the higher layer to the service offered by DLC
- converts packets received from the core n/w to the format expected by lower layers.

There are two types of CL. One is cell-based and the other is packet-based.

packet-based CL which can be further divided into a common part and a service-specific part (SSCS). SSCS is for switched Ethernet and IEEE 1394 Firewire. SSCS is dedicated to provide support to mobile IP.

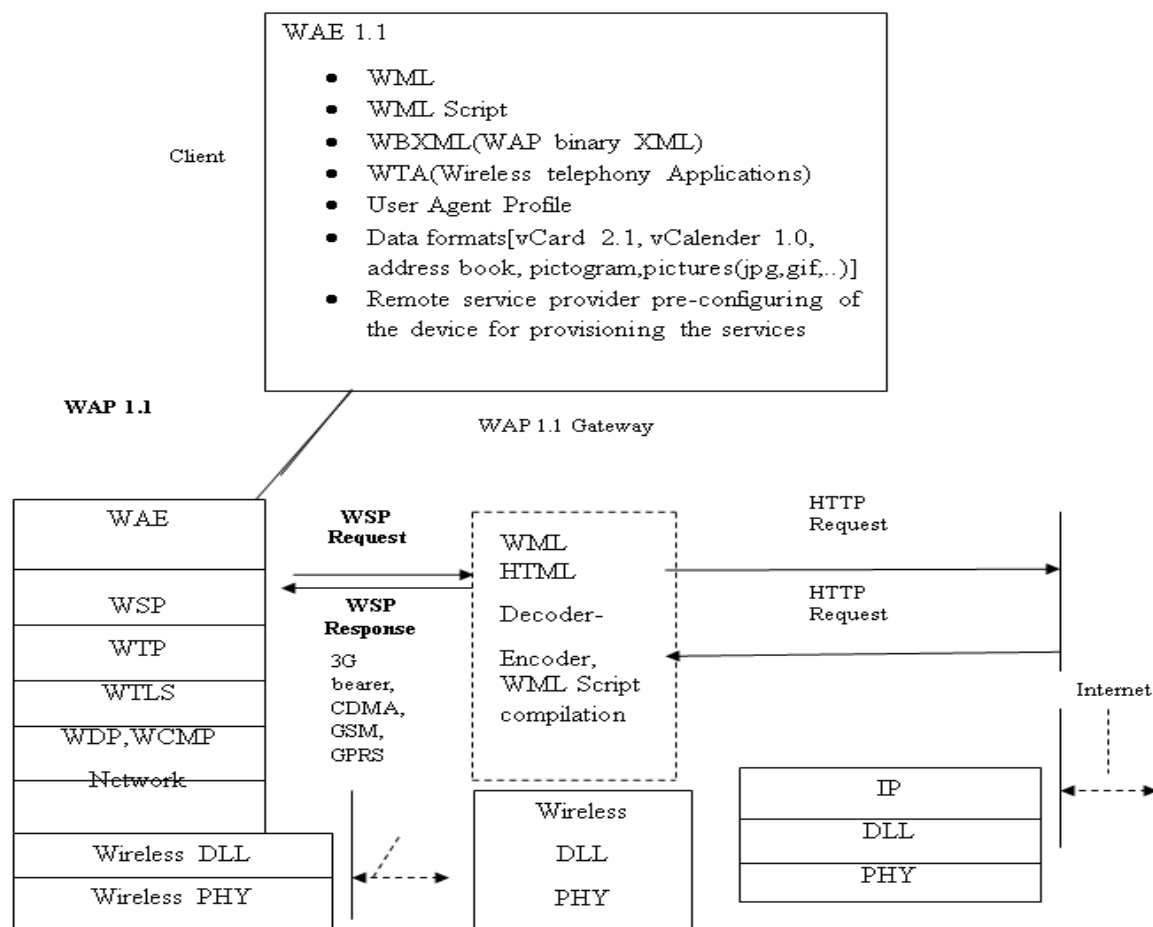
- **HIPERLAN /2 QoS schemes:** the best-effort scheme and priority scheme.
- By using IP QoS parameters, the CL establishes DLC connections in which IP QoS parameters are mapped into DLC connections for priority, radio bandwidth reservation, appropriate ARQ scheme, and handover strategy.
- The CL associates a specific link scheduling priority, discarding time and/or bandwidth reservation to each DLC queue. The CL segments IP traffic to fixed length packets. The segmentation and reassembly causes extra complexity in the CL but enables a better bandwidth reservation policy.

6. Draw WAP 1.1 Architecture (in comparison with HTTP) and explain about its components.

- WDP is used for transmitting and receiving the datagram over the network like UDP.
- WTLS, an optional layer, provides a public-key -based security mechanism similar to TLS.
- WTP provides transaction support adapted to the wireless world. **WTP** pulls the data from computing provisions for both push and pull
- Wireless Session Protocol (**WSP**) enables compressed binary encoding and does a number of tasks required for wireless environment sessions.
- Application layer includes Wireless Application Environment (WAE) which provides web services.

• WAP 1.1 gateway

- ❖ Gateway does **protocol conversions** between two ends—mobile client device and HTTP server. (i.e) The gateway converts WAE 1.1 data packets into the HTTP data packets and vice versa.
- ❖ It has **cache**s which is required due to frequent disconnections in the wireless environment.
- ❖ The gateway ensures security in wireless and wired networks.
- ❖ the gateway performs *iWML Script compilation*.
- ❖ WAP gateway does pull and push but HTTP can do only pull



WAP 1.1 Architecture

- **Wireless Datagram Protocol (WDP)**

- ❖ WDP sends the connectionless information in wireless environment, similar to UDP in TCP/ IP suite.
- ❖ **WDP offers port numbers used for multiplexing and demultiplexing of data respectively.** It is stateless.
- ❖ Figure shows the transfer of a WDP datagram.
- ❖ WDP header consists of a source port, a destination port (optional), source address (an identifier IP address or telephone number), destination address (optional), length of data, and checksum bytes for the header (to check erroneous receipt of header).
- ❖ An error-code is also reported to the upper layer, for example, in case the datagram could not reach its destination.
- ❖ **The wireless control message protocol (WCMP) provides error handling mechanisms for WDP.** WCMP (wireless control message protocol) is similar to ICMP for error reporting.
- ❖ WCMP employs a datagram with a WCMP header. WCMP is used for querying to find some n/w information, reporting errors, making route advertisement.
- ❖ WDP can be used for multicasting a datagram on the network.

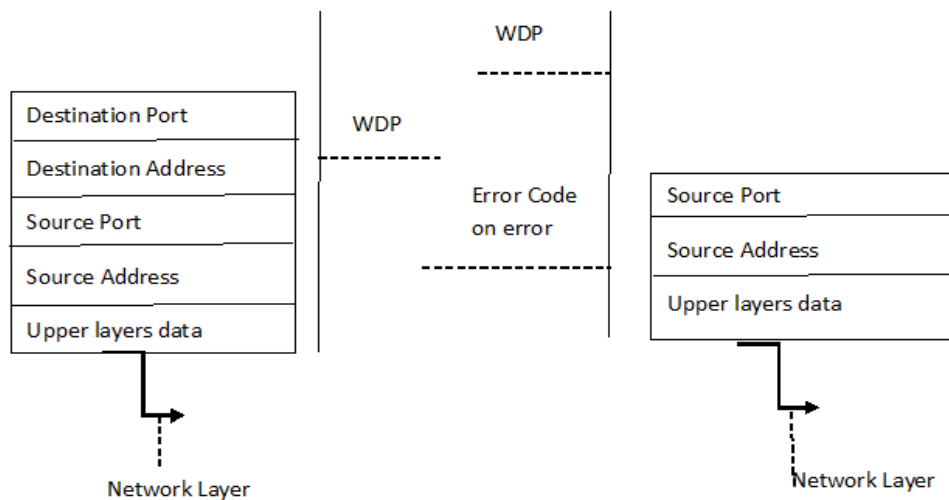


Fig : WDP protocol header over the upper layer data and return of error code as per the error

- **Wireless Transport Layer Security (WTLS)**

- ❖ TLS is an optional layer over wired Internet. TLS layer maps to SSL (secure socket layer) in HTTPS. It enables secured networking of data from the transport layer.

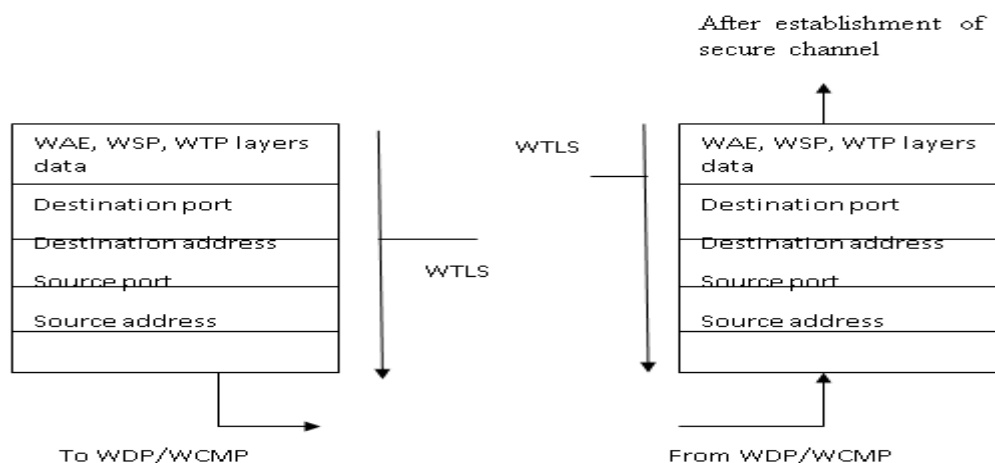


Figure WTLS protocol header over the upper layer data when requesting and WTLS protocol header from the lower layers when responding.

WTLS provisions for the following:

- assures integrity when data transaction occurs between a client device and a gateway
 - ensures privacy in transactions and device authentication
 - maps to SSL (secure socket layer) in HTTPS
 - supports TCP (transport layer protocols), WDP, and WCMP
 - serves as a layer above WDP when a secure is required for a datagram.
- sequence of peer-to-peer WTLS message exchanges** for establishing a secure session:
- Source device messages to create a secure channel as follows— source address and port, (ii) destination address and port, (iii) RSA(key exchange), (iv) IDEA or DES (ciphering the data), and (v) compression method.
 - Other end messages for confirmation of create process— (i)sequence number mode, (ii) how many times key is refreshed and exchanged again, (iii) identification of session, (iv) RSA or ECC (v) IDEA or DES and (vi) chosen compression
 - On request from the other end, source messages for authentication by a client certificate.
 - Source messages to commit request and Other end peer messages for commit confirmation

- **Wireless transaction protocol**

WTP transmits data to WTLS in case of secure transactions. It transmits directly to WDP or WCMP when optional WTLS is not used. WTP supports fusion of the messages and enables asynchronous transactions. WTP supports abortion of the transactions and success or failure of a transaction to the sender. WTP is an interface to ensure reliability of transactions.

There are three WTP service classes-0, 1, and 2.

- Class 0 Unreliable invoke messages with no result messages
- Class 1: Reliable invoke messages with no result messages- Reliability achieved by using unique transaction identifiers and just confirmation of invocation
- Class 2: Reliable invoke messages with exactly one reliable result message. -Reliability achieved by using unique transaction identifiers, acknowledgements, duplicate removal; and retransmissions.

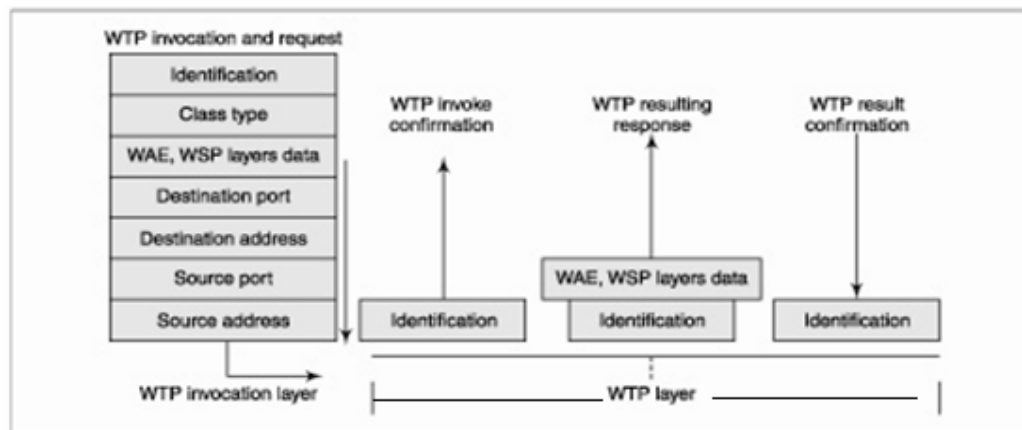


Fig : WTP headers when sending WTP invocation and request for results, confirmation of WTP invocation, resulting WTP response and confirmation of WTP transaction.

WIRELESS SESSION PROTOCOL

- It is responsible for establishing, maintaining and ending a session for wireless applications. The session consists of establishing a connection and receiving the resulting response headers.
- It provides two services:
 - Connection-oriented service to operate above WTP
 - Connectionless service above secure or non-secure datagram service WDP.

WSP supports stateless data transfers. SyncML codes bind with WSP for connectivity to the Internet. WSP can be thought as a compressed binary encoded version - extended version of HTTP.

WSP also supports asynchronous exchanges, multiple requests push and pull mechanisms of data dissemination, capability negotiation, content encoding, content type definitions, and WBXML (WAP binary XML).

There are three WSP service classes-0, 1, and 2.

- Class 0—for a source sending the unconfirmed push. It supports session suspension, resumption, and management. No response from the other end.
- Class 1—for a source sending the confirmed push.
- Class 2—for a source supporting session invocation, suspension, and resumption

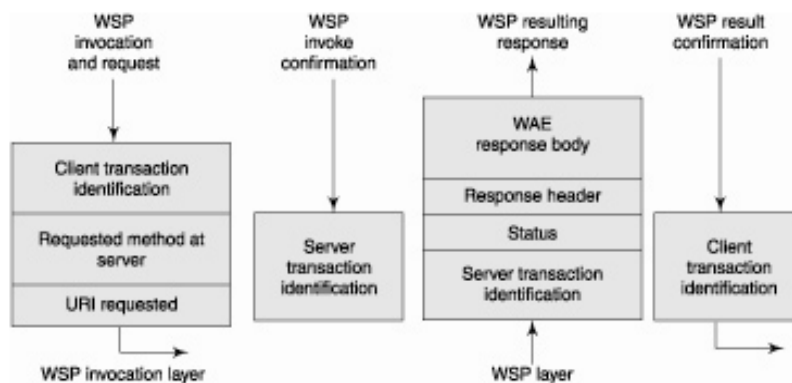


Fig : WSP headers when sending WSP invocation and request for results, confirmation of WSP invocation, resulting WSP response and confirmation of WSP transaction.

7. Describe the components of Wireless Application Environment in detail

WAE in WAP1.1 consists of the following components:

- WML (wireless markup language)
- WMLScript
- WBXML (WAP binary XML)
- WTA (wireless telephony application)
- Data formats [vCard 2.1, vCalendar 1.0, address book, pictures (jpg, gif, ..) etc].

WML

WML is web-page markup language for the wireless environment Internet which takes into account of mobile device constraints (small display, small keypad, state management, narrow bandwidth) while programming an application required for running on the device.

There are two versions of WML, namely WML 2.x and WML 1.x. WML 2.x includes XHTML-MP which includes XHTML. WML 1.x does not include XHTML.

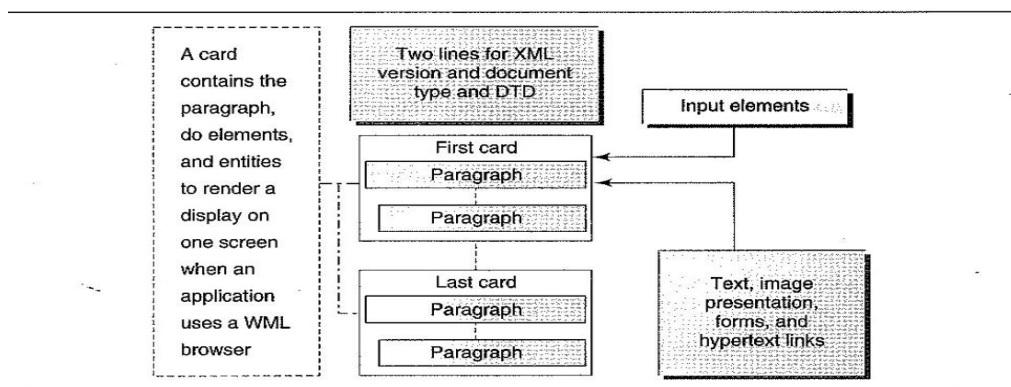


Figure Format of WML deck and WML card, and paragraph contents

All information in WML is a collection of decks and cards. Each deck can have number of cards. There is a navigational link from one card to another. WML provides for management of the navigation between cards and decks. Tags are used for markups before and after a text. A tag defines the specific function or action of the text. The information is taken from the text within a pair of start and end tags.

- WML card is used to create cards for mobile application (program, command, data, image)
- A card represents an interaction with the user (mobile) and the deck
- A set of procedural elements are used to control navigation between the cards.
- A WML parser parses the tags, the attributes, and the underlying text within the tags present within the deck or card.

Sample Code This code is an example of a WML deck which is saved in a file called *example12_3.wml*.

First line specifies the XML 1.0 version on which the WML card is based. Second line specifies the document type and DTD for the document. Third line has the tag `<wml>` to indicate the start of a WML document which will end at the tag `</wml>`. Fourth line specifies the start of a *card*.

One of the attributes of the card is an *id* which is defined here by *welcome*. Another attribute is *title* which is defined here by *First Card*. The card specifications are upto the line `</card>`. The paragraph tag is *p*. Another attribute called *mode* is defined here as *wrap* so that text wraps when displayed by browser. Text in the present example is WELCOME TO ABC MOBILE. The code for the deck is shown below:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//PHONE.COM/DTD WML 1.1//EN" "http://www.phone.com/dtd/wml13.dtd">
<wml>
<card id="welcome" title="First Card">
<p mode="wrap"> WELCOME TO ABC MOBILE </p>
</card>
</wml>
```

- A WML deck is saved in a file with extension WML. A WML card containing a client-request is transmitted and is decoded at the gateway to HTML and generates an HTML response is encoded in WML form at the gateway. The gateway transmits the WML response to mobile-device client which runs an application after parsing the WML.

WMLScript

WMLScript is a WAP 1.1 scripting language in WML and is used in wireless environment. WMLScript is analogous to CGI script in HTML. It is used for retrieving the application data after running the script codes at the server, (Script means the codes in text format that are interpreted when required- each code is converted to executable code-run when required)

Standard library functions

- *WMLBrowser* library - functions to control or to get information from the browser.
- *WMLDialogs* library - functions to display the input boxes to users, alert and confirmation messages.
- *WMLLang* library has the core WML functions (converting a data type)
- *WMLString* library - functions that help in concatenation, truncation, picking of select portions, and manipulation or finding the length of the strings.
- *WMLFloat* library - functions that help in performing floating-point arithmetic operations

WBXML

- WBXML is a specification in binary representation so that XML-based language can be transmitted in compact format. Here, a binary number can represent a tag in place of characters and an attribute in place of characters. E.g attribute ID that needs two characters can be represented by a single byte. Hence , the binary format causes compact transmission. There is no change in contents, code-functionality and semantic information. WBXML keeps the element structure of XML intact.

WTA

- The specific telephonic features are call set up, call accept, call forwarding, caller line ID, connected line ID,, call hold, call waiting, call charge advice, conferencing, ring tones, speed dial, telephone/fax, SMS up to 160 characters, emergency number, MMS, and videotext access. These features are defined by WATI (WTA interface).
- It provides the interfaces for the features using WML browser. A WTA URI can be `wtai://wap.mcard:` followed by a telephone number. This is identical to port number specifications provided in the URL.
- A WTA server can push the WML Script or deck contents. A WTA event handler can handle events. A persistent storage interface helps in storing the data on device when the content is modified. WTA also provides security interface.

User agent profile

- User agent is software used by the user to give input using VUI (voice user interface and GUI (graphic user interface) and to interact with mini browser (browser with limited screen

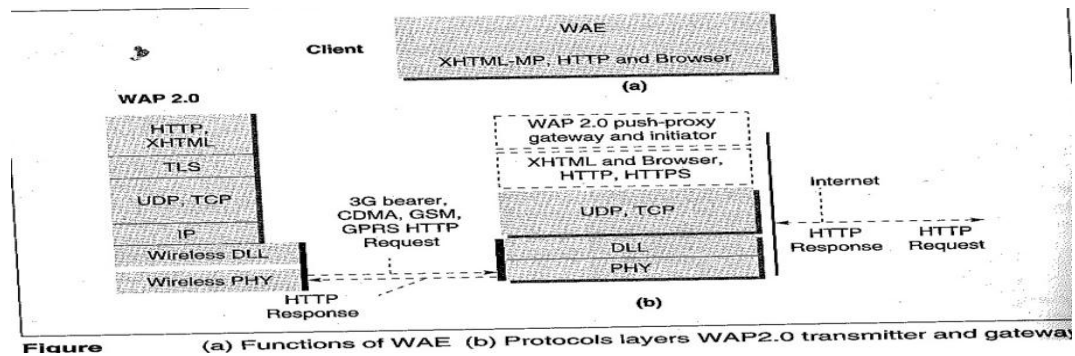
size). It executes the WMLScript at the client and displays the results. User agent displays the WML decks received as response from the server. User Agent Profile provides small screen device characteristics, font, and display capabilities.

Data formats

- The data displayed on a mobile device is in special data formats. vCard 2.1 is the format for visiting card. vCalendar 1.0 is the format for calendar. Also a mobile device provides pictogram which is a small picture of very low resolution that cannot be split and can be placed along with the text. A pictogram is used for displaying logo.

8. What is the significance of WIRELESS APPLICATION PROTOCOL - WAP 2.0

- A re-engineered 2.0 version was released in 2002. It uses a cut-down version of XHTML with end-to-end HTTP, dropping the gateway and custom protocol suite used to communicate with it. A WAP gateway can be used as a standard proxy server. The WAP gateway's role would then shift from one of translation to adding additional information to each request. This would include phone numbers, location, billing and handset information.
- WAP 2.0 uses XHTMLMP Extensible Hypertext Markup Language Mobile Profile in place of WML. Therefore encoding and compilation is not required and only a WAP 2.0 proxy suffices. It is a subset of XHTML and a superset of XHTML Basic. A version of cascading style sheets (CSS) called WAP CSS is supported by XHTML MP.



WAP Push-Proxy Gateway

- Mobile device applications require data dissemination by server in push mode, pull mode, and push-pull hybrid mode. A push-proxy gateway is used to exchange data packets between a mobile device through wired Internet and Web servers. The role of WAP 2.0 gateway is restricted to provisioning for push and pull mode services from the servers.

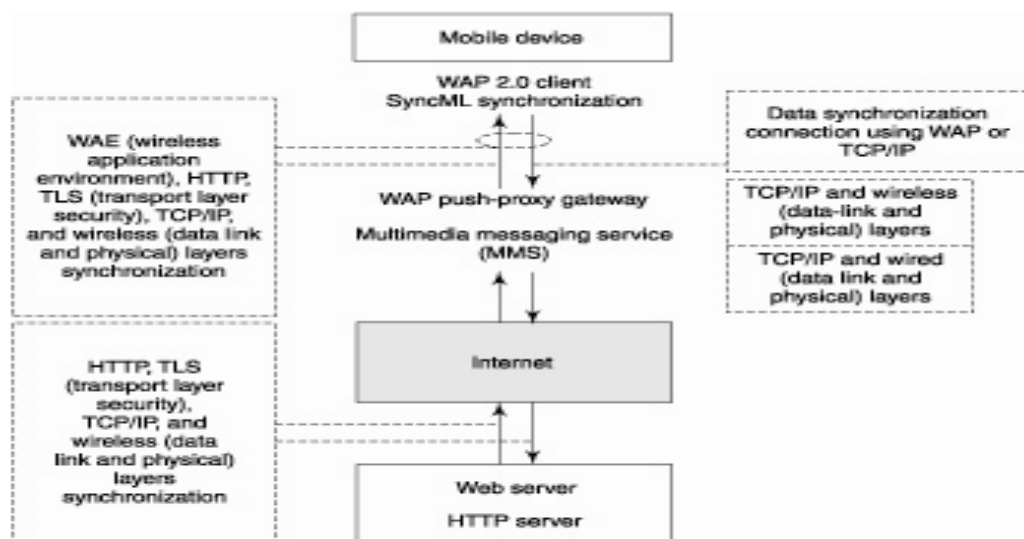


Fig : WAP 2.0 Client, gateway and web HTTP server architecture

- WAP 2.0 is wireless protocol for synchronization of WAP client computers and WAP /HTTP server. A WAP gateway connects WAP client to HTTP servers. HTTP server serves the websites on the Internet.
- WAP 2.0 has three important features over WAP 1.1—(a) SyncML synchronization, (b) WAP push service, and (c) MMS service.
- WAP 2.0 has backward compatibility and supports WAP 1.1 devices as well.

XHTML-MP (Extensible Hypertext Markup Language - Mobile Profile)& XHTML

- XHTML has two forms—XHTML basic and XHTML-MP.
- XHTML basic is HTML with strict syntax. XHTML-MP is for mobile devices and PDAs. An XHTML document can be parsed using a standard XML library and processed like any other standard XML document but using the same set of tags as in HTML.
- XHTML can be partitioned into modules and provides for navigation from one module to another. This feature is characteristic of XLINK. For example, WML deck is partitioned into cards and navigation from one card to another is permitted through hyperlinks .It supports tables but not the client-side style sheets since small devices are assumed to possess small computation resources. Frames are also not supported in basic XHTML.
- **XHTML 2.0** user agent parser is compatible with XHTML 1.1. HTML form will be replaced by XML-based user input specification and can be displayed as per user specifications and on the appropriate display devices. These are called XFORMs. XFrames have new features compared to HTML frames. The document object model (DOM) events are now XML Events and will use XML DOM.
- XHTML 2.0 has a number of modules. Examples are edit, presentation, meta information of a document, text, list, table, forms, structures, targets, bidirectional text, style-sheets, server-side image map, client-side image map, scripting, and link

9. What are the features of BLUETOOTH PROTOCOL :IEEE 802.15.1?

Property	Description
Frequency band	2.4 GHz with Bluetooth radio characteristics
Bluetooth protocol layers	<p>Radio Layer: specifies details of the air interface: Uses unlicensed ISM band, around 2.45GHz SS with frequency hopping- medium access is TDMA</p> <p>Baseband (Link Controller): connection establishment within a piconet, addressing, packet format, timing and power control.</p> <p>Link Manager Protocol (LMP): responsible for link setup and link management. Includes security aspects (encryption & authentication).</p> <p>Logical Link Control and Adaptation Protocol (L2CAP) : adapts upper layer protocols to the Baseband layer. Provides both connectionless and connection oriented services.</p> <p>SDP (Service discovery protocol): queries a device for device information, services and service characteristics.</p> <p>HCI (Host control interface): allows the implementation of lower Bluetooth functions on the Bluetooth device and higher protocol functions on a host machine.</p> <p>RFCOMM: a reliable transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol.</p> <p>TCS BIN (telephony control specification): bit oriented protocol that defines the call control signaling for the establishment of speech & data</p>

	calls between BD. OBEX : object exchange protocol. Provides functionality similar with HTTP. It provides a model for representing objects and operation Examples of formats transferred are vCard and vCalendar
Network characteristics	Connection-oriented communication Master-slave communication within same piconet Negligible interference between piconets as each used distinct channel-frequency hopping sequences Ad-hoc network peer-to-peer communication between two devices on two different piconets in a scatternet
Bluetooth features	Used for low power short range transmission Employed for wireless short range exchanges in 10 m network in master-slave mode and within 100 m in scatternet Network connection latency-between 3s and 6s Bit rate-less than 1 Mbps; 3.0 HS version 24 Mbps data transfer rate at 10 m range, 4.0 version 24 Mbps data transfer rate in 60m Code size-2% to 50% more compared to that for a Zigbee device Bluetooth radio-FHSS

10.i) Write short notes on IrDA PROTOCOLS ii) What are the features of ZIGBEE IEEE 802.15.4?

- Infrared (IR) rays are invisible radiations of wavelength higher than that of red. An LED or a solid-state laser emits IR rays when it is supplied with a 10-20 mA current from a low power battery or power source. Direct line-of-sight IR from an LED is detected at the receiver (photodetector) to get the data. The detector has 30° ($\pm 15^\circ$) window to detect the incoming radiation.
- IR rays are used for remote control of TV or IrDA (infrared data association) which is a protocol for personal communication area network deploying infrared rays.
- OBEX supports security by encryption and decryption at transmitter and receiver, respectively. It communicates and, exchanges binary data by establishing a client—server network between two IR devices.

Property	Description
Wavelength	900 nm
IrDA device levels of communication	Five levels of communication—minimum, access, index, sync, and SyncML (Levels 1-5). Levels specify a method of communication, from simple to SyncML-based.
IrDA data transfer rates	IrDA 1.0 protocol for data rates up to 115 kbps. IrDA 1.1 supports data rates of 1.152 Mbps to 4 Mbps (16 Mbps draft recommended).
Sessions, object exchange, and other IrDA protocols	(a) IrLAN (for Infrared LAN access) (b) IrBus (for access to serial bus by joysticks, keyboard, mice, and game ports) (c) IrMC (IrDA mobile communication and telephony protocol) (d) IrTran (IrDA transport protocol for image or file transfers) (e) IrComm [IrDA communication protocol by emulating serial or parallel port] (f) IrOBEX (for object exchange)

IrDA protocol layers	(a) Physical (b) Data link layer-IrLAP (link access protocol) & IrLMP (link management) (c) transport layer—tiny TP or IrLMIA (link management information access service protocol) (d) session—IrLAN, IrBus, IrMC, IrTran, IrComm, and IrOBEX (object exchange)
Network characteristics	Point to point communication from peer to peer
Application examples	<ul style="list-style-type: none"> • IR-based data transfer between a laptop (computer) and mobile handheld PocketPC when the two come in vicinity and line-of-sight of the IR receivers and detectors in each of them • Synchronization of PIM data between a PC and mobile device or a device at cradle and IR COM port.

ii)What are the features of ZIGBEE IEEE 802.15.4?

- Bluetooth operates by bridging the devices between remote networks and master-slave mode in a piconet. But Industrial applications in big-scale automation and remote control may require mesh networks. Bluetooth power requirement is larger due to the use of 2.4 GHz spectrum but industrial applications may have small payloads
- ZigBee is for low-power, short-range wireless personal area network. It is generally used for routing of messages. ZigBee devices form a mesh network and use reactive and proactive protocols for routing. It enables applications in big-scale automation and remote controls.
- ZigBee is a suite of high-level communication protocols. ZigBee devices conform to the IEEE 802.15.4
- It consists of three types of ZigBee devices which are as follows:
 - (a) ZigBee coordinator—root node at each ZigBee network tree. It can connect to other networks
 - (b) ZigBee router node—responsible for transfer of packets from source to nearby node (ZB, ZC, ZD).
 - (c) ZigBee end-device—receives packet from a source (ZE, ZF, ZG, ZH, and ZI).

A ZigBee network can be of two types:

- *Peer-to-peer*—For example, ZC—ZD—ZH network in which each node has path to neighbour.
- *Mesh*—For example, ZA—ZB—ZC network in which each node has a path to every other
- Assume three devices— set-top box, TV screen node, electric bulb node, each having ZigBee interfacing circuit. The ZigBee network also inter-network the Internet and WLAN

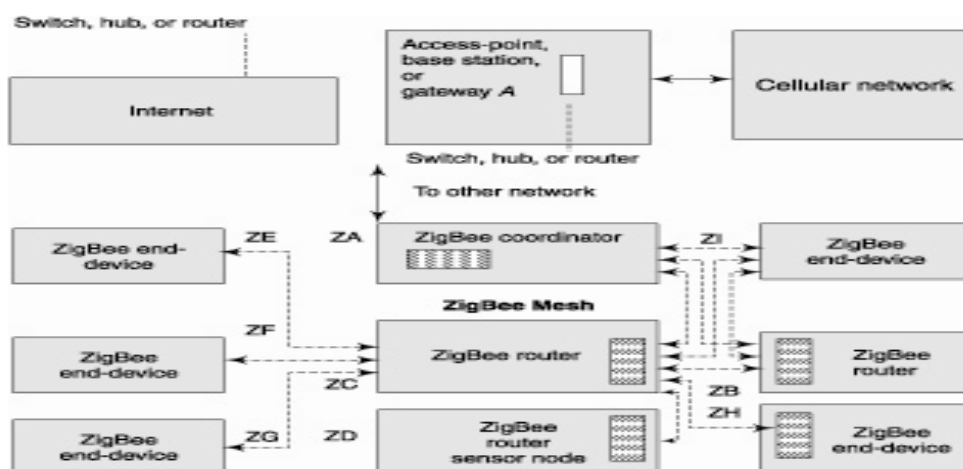


Fig : A network of Zigbee sensors, end devices and ZigBee router-devices connected to cellular network through an access point

A set of electric bulbs associates with the ZigBee routers ZB, ZC, and ZD forms a peer-to-peer connection network (ZE-ZD-ZC-ZB-ZA) with last one being ZigBee end-device (ZA).

A ZigBee coordinator (ZG) will connect this network with other ZigBee networks (e.g., of mobile hand-held devices ZE and ZF). The coordinator ZG also connects the access-point for WLAN and provides Internet connectivity to router ZJ for security system, to cellular phone network and set-up box device ZH,

Features	Description
Radio frequency	ISM bands-2.4 GHz orthogonal QPSK , 915 MHz (USA) and 868 MHz (USA)
ZigBee device channels	16 ZigBee channels 2.4 GHz,
ZigBee data transfer rates	250 kbps per channel, when using 915 MHz bands; thereafter n at 40 kbps per channel
Radio interface	DSSS
ZigBee protocol layers	Physical and a DLL (data link layer) part, called MAC (media access control)
Device types	Coordinator, router, and end-device types
Routing protocol	AODV
Protocol layers	<ul style="list-style-type: none"> Physical layer as provided in IEEE 802.15 MAC layer as provided in IEEE 802.15 Security and application software layers as specified by the ZigBee Alliance
Network characteristics	Self-organization, peer-to-peer, and mesh networks
Application examples	<ul style="list-style-type: none"> A ZigBee-enabled electric meter communicates electricity consumption data to the mobile meter reader A ZigBee-enabled home security system alerts the mobile user of any security breach at home

UNIT – III

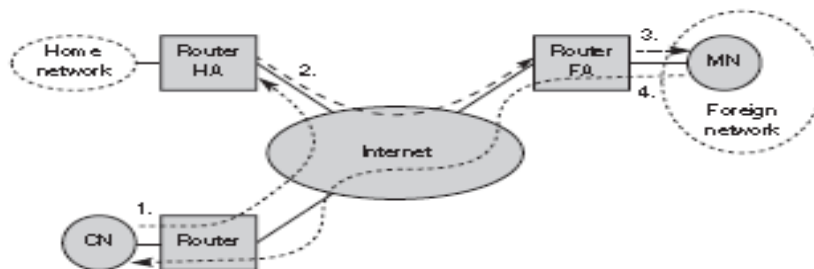
Part - B

1. Explain the various entities and terms needed to understand mobile IP & With neat diagram explain the packet delivery mechanism to and from MN

• **Various entities in Mobile IP**

- **Mobile node (MN):** A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP. The MN keeps its IP address and can continuously communicate with any other system in the internet
- **Correspondent node (CN):** At least one partner is needed for communication. CN represents this partner for the MN. The CN can be a fixed or mobile node.
- **Home network:** HN is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within the home network.
- **Foreign network:** FN is not the home network but the current subnet that the MN visits
- **Foreign agent (FA):** FA provides several services to the MN during its visit to the foreign network. Using CoA (care of Address) it works as conductor of channeling packet delivery to MN. It is default router for MN and provides security services
- **Care-of-address:** The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are first delivered to the COA, not directly to the IP address of the MN.
- **Co-located COA:** The COA is called co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired services such as DHCP
- **Foreign agent COA –** The COA could be located at the FA, i.e., the COA is an IP address of the FA. Thus the FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.
- **Home agent (HA):** HA provides several services for the MN and is located in the home network. The tunnel for packets toward the MN starts at the HA. The HA maintains a location registry (it is informed of the MN's location by the current COA). The HA can be a router at HN / on an arbitrary node in the subnet./ not necessary at all.

✓ **Packet delivery mechanism to and from MN.**



A CN wants to send packet to the MN. CN does not need to know anything about the MN's location.

Step 1 : CN sends the packet as usual to the IP address of MN . CN sends an IP packet with MN as a destination address and CN as a source address. The internet routes the packet to the router responsible for the home network of MN using the standard routing mechanisms.

Step 2: The HA now intercepts the packet knowing that MN is currently not in its home network. The packet is now encapsulated and tunneled to the COA. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet

Step 3: The FA now decapsulates the packet, i.e., removes the additional header and forwards the original packet with CN as source and MN as destination. MN receives the packet with the same sender and receiver address as it would have done in the home network.

Step 4: The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination. The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. If CN is a fixed node the remainder is as usual. If CN is also a mobile node in a foreign network, the same mechanisms as described in steps 1 through 3 would apply now in the other direction.

2. How does the mobile-network discover the foreign agent when it has moved?

MN after moving has to find a foreign agent. Methods to discover FA are

- i) Agent advertisement
- ii) Agent Solicitation.

After the process of either advertisement or agent solicitation, MN can receive a CoA. MN also knows its own location and the capabilities of the agent to which it needs to be connected

• Agent advertisement and discovery:

❖ FA and HA advertise their presence periodically using special **agent advertisement** messages. These advertisement messages are broadcasted as beacon into the subnet. ICMP messages (RFC 1256) are used with some mobility extensions for these advertisements. Routers in the fixed network implementing this standard also advertise their routing service periodically to the attached links.

❖ The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them.

❖ Advertisement Message : upper part - ICMP packet lower part - extension needed for mobility.

0	7	8	15	16	23	24	31
type		code		checksum			
#addresses		addr. size		lifetime			
router address 1							
preference level 1							
router address 2							
preference level 2							
...							
type = 16		length		sequence number			
registration lifetime				R	B	H	F
				M	G	r	T
				reserved			
COA 1							
COA 2							
...							

❖ The fields in the **ICMP part** are defined as follows.

- **type** is set to 9
- **code** can be 0, if the agent also routes traffic from non-mobile nodes,
16, if it does not route anything other than mobile traffic.
- **Checksum** is for validity of data
- **#addresses:** The number of addresses advertised with this packet
- **Lifetime** denotes the length of time this advertisement is valid.
- **addresses:** Addresses of router
- **Preference** levels help a node to choose the router that is the most eager to get a new node.

The **extension for mobility** has the following fields defined:

- **Type:** 16,
- **Length** depends on the number of COAs provided with the message.

- **Sequence number:** number of advertisements sent since initialization
- **Registration lifetime :** agent can specify the maximum lifetime in seconds during registration.
- **R, B, H, F, M, G, V:** characteristics of an agent in detail.
 - The **R** bit, if a registration with this agent is required
 - The **B** bit, If the agent is currently too busy.
 - The **H** bit, if the agent offers services as a home agent
 - the **F** bit, if the agent offers services as a foreign agent
 - Bits **M** and **G** specify the method of encapsulation used for the tunnel. **M** minimal encapsulation and **G** generic routing encapsulation.
 - **V** bit specifies the use of header compression
- **CoAs:** CoAs advertised.

ii) Agent Solicitation: If the MN has not received any advertisement or a CoA by some means, then MN must solicit by agent solicitations. Care must be taken to avoid flooding of router solicitations. Typically, a mobile node can send out three solicitations, one per second, as soon as it enters a new network.

In highly dynamic wireless networks with moving MNs and continuous packet streams even one second intervals between solicitation messages might be too long. Before an MN even gets a new address many packets will be lost.

If a node does not receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network until it reaches a maximum interval between solicitations (typically one minute). Solicitation is executed when the MN is disconnected. Even when it is connected it can solicit agents for better connection.

3. (i) Write down the requirements/Goal of mobile IP.

(ii) How does MN register with the HA, after received a COA?

(iii) Discuss the reverse Tunneling method in mobile IP.

The requirements/Goal of mobile IP.

- A new standard cannot introduce changes for applications or network protocols already in use. It is possible to enhance the capabilities to support mobility. Mobile IP has to remain compatible with all lower layers used for non-mobile, IP.
- Mobile IP must not require special media or MAC/LLC protocols, so it must use the same interfaces and mechanisms to access the lower layers as IP does. Finally, end-systems enhanced with a mobile IP implementation should still be able to communicate with fixed systems without mobile IP. Mobile IP has to ensure that users can still access the internet with same address format and routing mechanisms.

Transparency:

- Mobility should remain 'invisible' for many higher layer protocols and applications. Higher layers should continue to work even if MN has changed its point of attachment to the network. If the interruption is not too long, TCP connections can survive.
- Effects of mobility are higher delay and lower bandwidth. However, some applications like cost-based routing or video compression are to be 'mobility aware' Additional mechanisms are necessary to inform some applications about mobility.

Scalability and efficiency:

- Introducing a new mechanism should not reduce efficiency. Enhancing IP for mobility must not generate too many new messages flooding in network. So only some additional packets are necessary between a mobile system and a node in the network. Looking at the growth rates of mobile communication devices, it is necessary for a mobile IP to be scalable over a large number of internet participants.

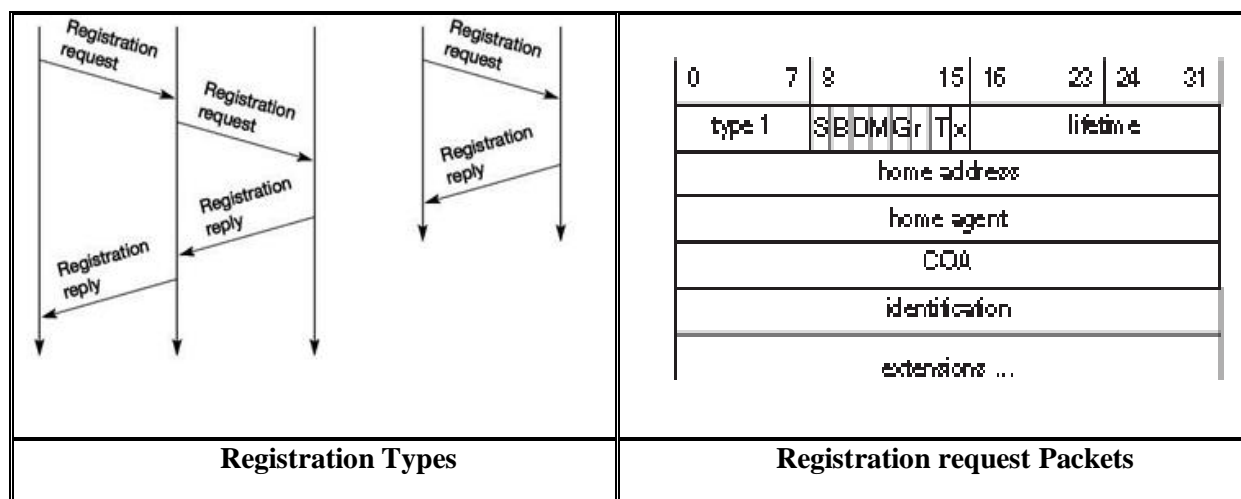
Security:

- Mobility poses many security problems. The minimum requirement is that of all the messages related to managing Mobile IP are authenticated. The IP layer must guarantee that if it forwards a

packet to a mobile host that this host receives the packet. There are no ways of preventing fake IP addresses or other attacks.

(ii) How does MN register with the HA, after received a COA?

- Having received a COA, the MN has to register with the HA. The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets.
 - ❖ **TYPE I Registration:** If the COA is at the FA, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now sets up a **mobility binding** containing the mobile node's home IP address and the current COA.
 - ❖ It also contains the lifetime of the registration which is negotiated during the registration process. After the lifetime the registration is deleted; so, an MN should reregister before expiration. After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN.
 - ❖ **TYPE II Registration :** If the COA is co-located, registration can be simpler. The MN may send the request directly to the HA and vice versa. This, by the way, is also the registration procedure for MNs returning to their home network
 - ❖ UDP packets are used for **registration requests** because of low overheads and better performance. The UDP destination port is set to 434. The fields are:
 1. **type** is set to 1 for a registration request.
 2. **S** bit -MN can specify if it wants the HA to retain prior mobility bindings.
 3. **B** bit indicates that an MN wants to receive the broadcast packets of home network.
 4. The **D** bit indicates the decapsulation at the tunnel endpoint.
 5. **M, G, V**, these indicate minimal, generic header compression respectively.
 6. **Lifetime:** Validity of registration (in seconds).
 7. **Home address:** fixed IP address of MN
 8. **Home agent:** IP address of MN
 9. **CoA:** Tunnel end point
 10. **Identification:** 64 bit -request ID generated by MN for matching with replies.



(iv) Discuss the reverse Tunneling method in mobile IP.

- MN can directly send its packets to the CN as in any other standard IP situation. The destination address in the packets is that of CN. But there are several severe problems associated with this simple solution.
- **Firewalls:** All data to and from the intranet must pass through the firewall to filter out malicious addresses. Quite often firewalls only allow packets with topologically correct addresses to pass.

However, MN still sends packets with its fixed IP address as source which is not topologically correct in a foreign network.

But, Firewalls filter packets coming from outside containing a source address from computers of the internal network. However, this also implies that an MN cannot send a packet to a computer residing in its home network. Use only some globally available addresses, to solve the problems arising when using NAT together with mobile IP.

- **Multi-cast:** Reverse tunnels are needed for the MN to participate in a multicast group. While the nodes in the home network might participate in a multi-cast group, an MN in a foreign network cannot transmit multi-cast packets in a way that they emanate from its home network without a reverse tunnel.

- **TTL:** Consider an MN sending packets with a certain TTL while still in its home network. The TTL might be low enough so that no packet is transmitted outside a certain region. If the MN now moves to a foreign network, this TTL might be too low for the packets to reach the same nodes as before.

Mobile IP is no longer transparent if a user has to adjust the TTL while moving. A reverse tunnel is needed that represents only one hop, no matter how many hops are really needed from the foreign to the home network.

Reverse tunneling now creates a triangular routing problem in the reverse direction. All packets from an MN to a CN go through the HA. RFCs not offer a solution for this reverse triangular routing, because

- it is not clear if the CN can decapsulate packets.
 - It is possible that mobile IP should work together with all traditional, non-mobile IP nodes.
- Therefore, one cannot assume that a CN is able to be a tunnel endpoint.

4. Discuss about Tunneling and Encapsulation mechanism.

- **Encapsulation** is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called **decapsulation**. Encapsulation and decapsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or vice versa.



- There are different ways of performing the encapsulation needed for the tunnel between HA and COA
- ❖ **IP-in-IP ENCAPSULATION:** For mobile IP, IP-in-IP encapsulation is mandatory. The new header is called the outer header and inner header is identical to the original header for IP-in-IP encapsulation.

ver.	HL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL	IP-in-IP		IP checksum	
IP address of HA				
Care-of address of COA				
ver.	HL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL	lay. 4 prot.		IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/... payload				

The field of the outer header are as follows:

- **ver:** 4 for IPvers 4.
- internet header length (**IHL**) denotes the length of the outer header in 32 bit words.
- **DS(TOS)** is just copied from the inner header,
- the **length** field covers the complete encapsulated packet.
- IPID, Flags and Fragments off-set: No significance in mobile IP
- **TTL** must be high enough so the packet can reach the tunnel endpoint. T
- **IP-in-IP**, is the type of the protocol used in the IP payload 4 for IPvers 4.
- **IP checksum** is calculated as usual.
- **IP address of the HA** the tunnel entry as source address
- **COA** the tunnel exit point as destination address.

If no options follow the outer header, the inner header starts. This header remains almost unchanged during encapsulation, thus showing the original sender CN and the receiver MN of the packet. The only change is TTL which is decremented by 1. This means that the whole tunnel is considered a single hop from the original packet's point of view. Finally, the payload follows the two headers.

❖ Minimal encapsulation:

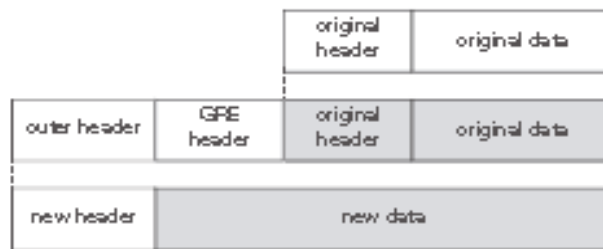
As seen with IP-in-IP encapsulation, several fields are redundant. **Minimal encapsulation** is an optional encapsulation method for mobile IP. The tunnel entry point and endpoint are specified. The type of the following protocol contains the value 55 for the minimal encapsulation protocol.

ver.	HL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL	min. encap		IP checksum	
IP address of HA				
care-of address of COA				
lay. 4 protoc.	S	reserved	IP checksum	
IP address of MN				
original sender IP address (if S=1)				
TCP/UDP/ ... payload				

The inner header is different for minimal encapsulation. The address of the MN is needed. If the **S** bit is set, the original sender address of the CN is included. There is no fragmentation offset in the inner header because minimal encapsulation does not work with already fragmented packets.

❖ Generic routing encapsulation:

While IP-in-IP and minimal encapsulation work only for IP, the following encapsulation scheme also supports other network layer protocols in addition to IP. **Generic routing encapsulation** (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.



The outer header is the standard IP header with HA as source address and COA as destination address. The protocol type used in this outer IP header is 47 for GRE. The other fields of the outer packet, such as TTL and TOS, may be copied from the original IP header. However, the TTL must be decremented by 1 when the packet is decapsulated to prevent indefinite forwarding.

ver.	HL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		GRE	IP checksum	
IP address of HA				
care-of address of COA				
C	R	K	S	rec. rev. ver. protocol
checksum (optional)			offset(optional)	
key(optional)				
sequence number (optional)				
routing (optional)				
ver.	HL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		lay. 4 prot.	IP checksum	
IP address of CH				
IP address of MH				
TCP/UDP/... payload				

The GRE header starts with several flags indicating if certain fields are present or not. A minimal GRE header uses only 4 bytes; nevertheless, GRE is flexible enough to include several mechanisms in its header.

- If **C** is set, the **checksum** field contains a valid IP checksum of the GRE header and the payload.
- **R** bit indicates if the offset and routing fields are present and contain valid information.
- **K** bit is set- **key** field which may be used for authentication.
- **S** Bit indicates whether the **sequence** number field is present, used by a decapsulator to restore order.
- **recursion control** field (rec.) represents a counter that shows the number of allowed recursive encapsulations.

If the field is not zero, additional encapsulation is allowed – the packet is encapsulated and the field decremented by one. Otherwise the packet will most likely be discarded.

This mechanism prevents indefinite recursive encapsulation which might happen with the other schemes if tunnels are set up improperly (e.g., several tunnels forming a loop). The default value of this field should be 0, thus allowing only one level of encapsulation.

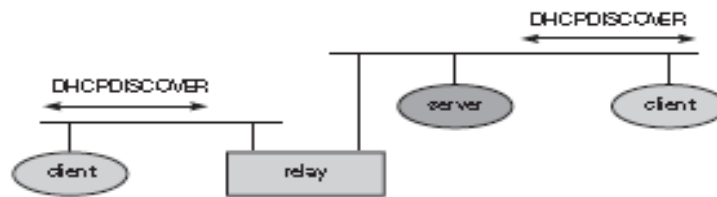
- **reserved** fields must be zero and are ignored on reception.
- **version** field contains 0 for the GRE version.
- **protocol** (2 byte) field represents the protocol of the packet following the GRE header.

e.g., 0×6558 for transparent Ethernet bridging using a GRE tunnel.

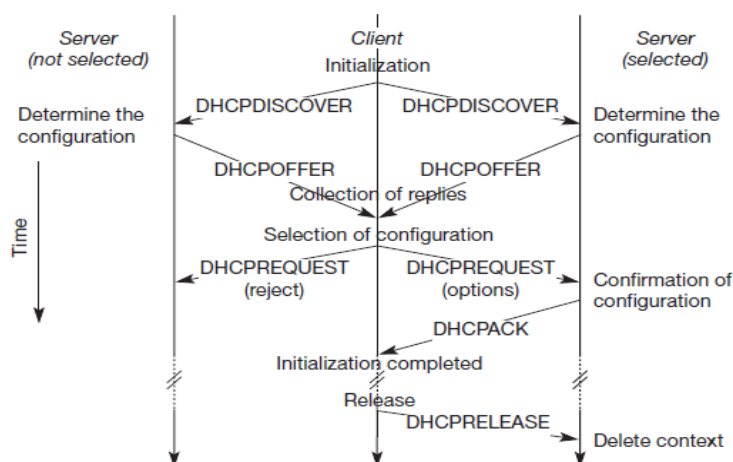
0×800 for mobile IP tunnel

5. How does Dynamic Host Configuration Protocol maintain a n/w?

- The dynamic host configuration protocol is mainly used to simplify the installation and maintenance of computers connected to a n/w.
- If a new computer is connected to a network, DHCP can provide it with all the Necessary following information for full system integration into the network, addresses of the default router & DNS servers the subnet mask the domain name IP address.
- Providing an IP address makes DHCP very attractive for mobile IP as a source of care-of-addresses.



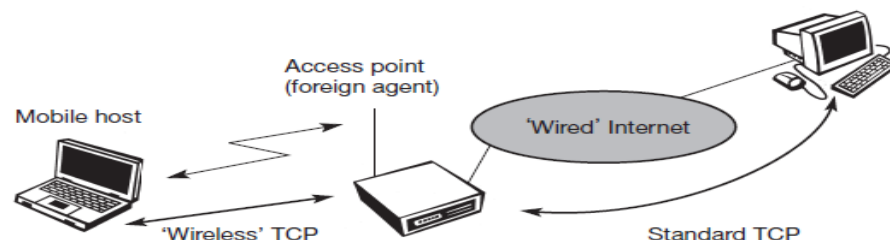
- DHCP is based on a client/server model. DHCP clients send a request to a server (**DHCPDISCOVER**) to. A client sends requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.
- **DHCP initialization with one client and two servers.**
 - ❖ The client broadcasts a **DHCPDISCOVER** into the subnet. There might be a relay to forward this broadcast. Two servers receive this broadcast and determine the configuration they can offer to the client.
 - ❖ This could be the checking of available IP addresses and choosing one for the client. Servers reply to the client request with **DHCPOFFER** - a list of configuration parameters offered. The client can now choose one of the configurations offered.
 - ❖ The client in turn replies to the servers, accepting one of the configurations and rejecting the others using **DHCPREQUEST**. If a server receives a **DHCPREQUEST** with a rejection, it can free the reserved configuration for other possible clients. The server with the configuration accepted by the client now confirms the configuration with **DHCPACK**. This completes the initialization phase.
 - ❖ If a client leaves a subnet, it should release the configuration received by the server using **DHCPRELEASE**. Now the server can free the context stored for the client and offer the configuration again.
 - ❖ The configuration a client gets from a server is only leased for a certain amount of time. It has to be reconfirmed from time to time. Otherwise the server will free the configuration. This timeout of configuration helps in the case of crashed nodes or nodes moved away without releasing the context.



- ❖ A DHCP server should be located in the subnet of the access point of the mobile node, or at least a DHCP relay should provide forwarding of the messages. RFC 3118 specifies authentication for DHCP messages

6. Explain about I-TCP working principle and performance in detail.

- I-TCP segments a TCP connection into a fixed part and a wireless part. A good place for segmenting the connection between mobile host and correspondent host is at the foreign agent of mobile IP. The foreign agent acts as a proxy and relays all data in both directions. The correspondent host in the fixed network does not notice the wireless link or the segmentation of the connection.
- **Standard TCP** is used between the fixed computer and the access point. Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy. (ie) the access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host.
- **A special TCP**, is adapted to wireless links, between the access point and the mobile host.
- If the correspondent host sends a packet, the foreign agent acknowledges this packet and tries to forward the packet to the mobile host. If the mobile host receives the packet, it acknowledges the packet. However, this acknowledgement is for the foreign agent. If a packet is lost on the wireless link due to a transmission error, the correspondent host would not notice this. In this case, the foreign agent tries to retransmit.
- Similarly, if the mobile host sends a packet, the foreign agent acknowledges this packet and tries to forward it to the correspondent host. If the packet is lost on the wireless link, the mobile host notices this much faster due to the lower round trip time and can directly retransmit the packet. Packet loss in the wired network is now handled by the foreign agent.
- **During Handover**
- I-TCP requires several actions as soon as a handover takes place. The access point acts as a proxy and buffer packets for retransmission. After the handover, the old proxy must forward buffered data to the new proxy because it has already acknowledged the data. Besides buffer content, the sockets of the proxy, too, must migrate to the new foreign agent located in the access point. The socket reflects the current state of the TCP connection, i.e., sequence number, addresses, ports etc.



Advantages of I-TCP

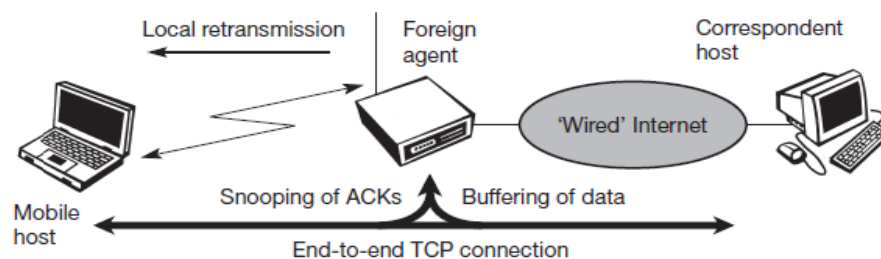
- I-TCP does not require any changes in the TCP protocol. All current optimizations for TCP still work between the foreign agent and the correspondent host
- Due to strict partitioning into two connections, transmission errors on the wireless link, i.e, lost packets, cannot propagate into the fixed network.
- Different solutions can be tested or used at the same time without jeopardizing the stability of the internet. Furthermore, optimizing of these new mechanisms is quite simple because they only cover one single hop
- The short delay between the mobile host and foreign agent can be determined and was independent of other traffic streams.. An optimized TCP can use precise time-outs to guarantee retransmission as fast as possible. Even standard TCP benefits from the short RTT, thus recovering faster from packet loss.
- Partitioning into two connections also allows the use different transport layer protocol between the foreign agent and the mobile host are the use of compressed header etc.

Disadvantages of I-TCP

- The loss of end-to-end semantics of TCP might cause problems if the foreign agent partitioning the TCP connection crashes. If a sender receives an acknowledgement, it assumes that the receiver got the packet. Receiving an acknowledgement only means (for the mobile host and a correspondent host) that the foreign agent received the packet. The correspondent node does not know anything about the partitioning.
- Increased hand-over latency may be much more problematic.
- A foreign agent must be a trusted entity.

7. Explain about Snooping TCP enhancement for mobile network in detail.

- Snooping- TCP enhancement works completely transparently and provides TCP end-to-end connection. The main function is to buffer data to perform fast local retransmission in case of packet loss in wireless link and 'snoops' the packet flow in both directions to recognize acknowledgements. It could be done at **the foreign agent**..



- **Data transfer from the correspondent host to mobile host:** The foreign agent buffers every packet until it receives an acknowledgement from the mobile host. If it does not receive an acknowledgement from the mobile host, now the foreign agent retransmits the packet directly from the buffer, performing a much faster retransmission compared to the correspondent host.
- The foreign agent must not acknowledge data to the correspondent host to remain transparent, However, the foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions.
- So even if the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission. The foreign agent may discard duplicates of packets and avoids unnecessary traffic on the wireless link.
- **Data transfer from the mobile host to correspondent host :** The foreign agent snoops into the packet stream to detect gaps in the sequence numbers of TCP. As soon as the foreign agent detects a missing packet, it returns a negative acknowledgement (NACK) to the mobile host. The mobile host can now retransmit the missing packet immediately.

Advantages:

- The end-to-end TCP semantic is preserved and No matter at what time the foreign agent crashes

- most of the enhancements are in the foreign agent. Does not even require changes in the mobile host.
- As the mobile host moves to another foreign agent during, though data in the buffer is not transferred to the next foreign agent, it leads to a time-out at the correspondent host and CA does retransmission.
- if the next foreign agent is not using the enhancement the approach automatically falls back to the standard solution.

Disadvantages:

- Snooping TCP does not isolate the behaviour of the wireless link as good as I-TCP. The problems on the wireless link are now also visible for the correspondent host and not fully isolated.
- Using negative acknowledgement between the foreign agent and the mobile host assumes the additional mechanisms on the mobile host. Thus, this approach is no longer transparent for arbitrary mobile hosts.
- All efforts for snooping and buffering data may be useless, if certain encryptions are applied end-to-end between the correspondent host and mobile host. Snooping on the sequence numbers will no longer work after encrypting TCP header.

8. Explain about mobile TCP enhancement ---mobile TCP in detail.

- M-TCP approach has the same goals as I-TCP and S-TCP: to prevent the sender window from shrinking if bit errors are disconnection but not congestion cause current problems.
- M-TCP improves overall throughput, to lower the delay, to maintain end-to-end semantics of TCP and to provide a more efficient handover. Additionally, M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections.
- M-TCP splits the TCP connection into two parts as I-TCP does. An unmodified TCP is used on the Correspondent Node CN-supervisory host (SH) connection, while an optimized TCP is used on the SH-MN connection. The supervisory host is responsible for exchanging data between both parts similar to the proxy in I-TCP
- The M-TCP approach assumes a relatively low bit error rate on the wireless link. SH does not perform caching/retransmission of data. If a packet is lost on the wireless link, it has to be retransmitted by the correspondent sender. This maintains the TCP end-to-end semantics.
- The SH monitors all packets sent to the MN and ACKs returned from the MH. If the SH does not receive an ACK for some time, it assumes that the MN is disconnected. It then chokes the sender by setting the sender's window size to 0 forces the sender to go into **persistent mode**. The sender will not try to retransmit data. As soon as the SH (either the old SH or a new SH) detects connectivity again, it reopens the window of the sender to the old value. This mechanism does not require changes to the sender's TCP.
- The wireless side uses an adapted TCP that can recover from packet loss much faster. It does not use slow start, thus, M-TCP needs a bandwidth manager to implement fair sharing over the wireless link.

Advantages

- M-TCP maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MN.
- If the MN is disconnected, M-TCP avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to zero.
- Since M-TCP does not buffer data in the SH as I-TCP does, it does not necessary to forward buffers to a new SH. Lost packets will be automatically retransmitted to the new SH.

Disadvantages

- As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender.
- M-TCP assumes low bit error rates, which is not always a valid assumption.
- A modified TCP on the wireless link not only requires modifications to the MH protocol software but also new n/w elements like bandwidth manager.

9. Short notes on Fast retransmit/fast recovery, Transmission/time-out freezing, Selective Retransmission and Transaction-oriented TCP.

Fast retransmit/fast recovery

- This TCP is to artificially force the fast retransmit behavior on the mobile host and correspondent host side. As soon as the mobile host registers at a new foreign agent using mobile IP, it starts sending duplicated acknowledgements to correspondent hosts. The proposal is to send three duplicates. These forces the corresponding host to go into fast retransmit mode and not to start slow start.

Advantages:

- It is simple.
- Only minor changes in the mobile host's software already result in a performance increase.
- No foreign agent or correspondent host has to be changed.

Disadvantages:

- insufficient isolation of packet losses.
- retransmitted packets still have to cross the whole network between correspondent host and mobile host.
- packet loss due to problems on the wireless link is not considered. requires more cooperation between the mobile IP and TCP layer making it harder to change one without influencing the other.

Transmission/time-out freezing

- It is designed for longer interruptions of transmission. Examples are the use of mobile hosts in a car driving into a tunnel, which loses its connection to. MAC layer knows the real reason for the interruption and does not assume congestion and can inform the TCP layer of an upcoming loss of connection not by congestion.
- TCP can now stop sending and 'freezes' the current state of its congestion window and further timers. If the MAC layer notices the upcoming interruption early enough, both the mobile and correspondent host can be informed. additional mechanisms in the access point are needed to inform the correspondent host of the reason for interruption.
- As soon as the MAC layer detects connectivity again, it signals TCP that it can resume operation at exactly the same point where it had been forced to stop. For TCP time simply does not advance, so no timers expire.

Advantages

- resume TCP connections even after longer interruptions of the connection.
- it can be used together with encrypted data.

Disadvantages

- Not only does the software on the mobile host have to be changed, but also correspondent host All mechanisms rely on the capability of the MAC layer to detect future interruptions.
- Freezing the state of TCP does not help in some encryption schemes like time-dependent random numbers.
- It needs resynchronization after interruption.

Selective retransmission

- Instead of retransmitting everything starting from the lost packet and wasting bandwidth, a selective retransmission of packets (ie) retransmitting the lost packets alone. The receiver can acknowledge single packets .

Advantages : A sender retransmits only the lost packets.

- This lowers bandwidth requirements and is extremely helpful in slow wireless links.
- Beneficial to wired, wireless networks.

Disadvantage : more complex software on the receiver side to buffer necessary to resequence data
Increase in memory sizes and CPU performance.

Transaction-oriented TCP

- TCP uses a three-way handshake to establish the connection. But in an example of only one data packet, TCP may need seven packets altogether. That is the overhead introduced by using TCP over GPRS in a web scenario.

- Web services are mostly based on HTTP. HTTP request can be transmitted the TCP connection has to be established. If GPRS is used as wide area transport system, one-way delays of 500 ms and more are quite common. The setup of a TCP connection already takes far more than a second.
- T/TCP can combine packets for connection establishment and connection release with user data packets. This can reduce the number of packets down to two instead of seven.

Advantage

- reduction in the overhead which standard TCP has for connection setup and connection release.

Disadvantages:

- it requires changes in the mobile host and all correspondent hosts.
- no longer hides mobility.
- Furthermore, T/TCP exhibits several security problems.

10. i) Explain in detail about Traditional TCP. ii) Compare all TCP enhancements for mobility.**i) Traditional TCP**

- **Congestion control:** Congestion may appear from time to time. If the buffers of the router are filled and if the router cannot forward packets to output link, congestion occurs. As result of congestion, it drop packets.
- **Exponential growth of congestion window** Suppose congestion window size = n , if a sender receives acknowledgement from this window, then it doubles the congestion window size as to n , if the congestion window size < congestion threshold, this is called exponential growth.
- **Slow start:** The sender always calculates a congestion window for a receiver. Initially, the congestion window is one. The sender sends one packet and waits for acknowledgement. If this acknowledgement arrives, the sender increases the congestion window by one, congestion window = 2. After arrival of the two corresponding acks, it increases the congestion window equal to 4. This exponential growth is used up to threshold (half of the current congestion window). As soon as the congestion window reaches the threshold, increase is only linear by adding 1 to the congestion window. When ACK is lost due to congestion, sender stats from sending one segment.
- **Fast retransmit** A sender receives continuous acknowledgement for the same packet. It informs that the gap in packet stream is not due to severe congestion but a simple packet lost due to transmission error. The sender can now re-transmit the missing packet before the timer expires. This behavior is called fast retransmit.
- **Fast recovery** A sender receives continuous acknowledgement for the same packet. It informs that the gap in the packet stream is not due to severe congestion but a simple packet lost due to transmission error. The sender can continue with same window. The sender can now re-transmit the missing packet and now recover fastly from the packet loss. This behavior is called fast recovery.

ii) Comparison of TCP enhancements :

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover, security problems
Snooping TCP	Snoops data and acknowledgements, local retransmission	Transparent for end-to-end connection, MAC integration possible	Insufficient isolation of wireless link, security problems
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management, security problems
Fast retransmit/ fast recovery	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
Transmission/ time-out freezing	Freezes TCP state at disconnection, resumes after reconnection	Independent of content, works for longer interruptions	Changes in TCP required, MAC dependent
Selective retransmission	Retransmits only lost data	Very efficient	Slightly more complex receiver software, more buffer space needed
Transaction-oriented TCP	Combines connection setup/release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent, security problems

UNIT- IV**Part - B****1. Briefly explain about the characteristics and applications of MANETs.**

- **MANET Characteristics :**

PROPERTY	DESCRIPTION
Flexibility	MANET enables fast establishment of networks. When a new network is to be established, the only requirement is to provide a new set of nodes with limited wireless communication range. A node has limited capability, that is, it can connect only to the nodes which are nearby. Hence it consumes limited power.
Direct communication through nearby node and neighbour discovery	A MANET node has the ability to discover a neighbouring node and service. A node discovers the service of a nearby node using a service discovery protocol. Then it communicates with a remote node.
Peer-to-peer connectivity	MANET nodes have peer-to-peer connectivity among themselves.
Computations decentralization	Each MANET node has independent computational, switching (or routing), and communication capabilities.
Limited wireless connectivity range.	MANETs require that a node should move in the vicinity of at least one nearby node within the wireless communication range, else the node should be provided with the access-point of wired communication. In other words, the wireless connectivity range in MANETs includes only nearest node connectivity.
Weak connectivity and remote server latency	Unreliable links to base station or gateway. The failure of an intermediate node results in greater latency in communicating with the remote server.
Resource constraints	Limited bandwidth available between two intermediate nodes becomes a constraint for the MANET. The node may have limited power and thus need energy-efficient computations.
No access-point requirement	There is no access-point requirement in MANET. Only selected access points (e.g., A and B in Fig. 11.1(b)) are provided for connection to other networks or other MANETs.
Requirement to solve exposed or hidden terminal problem	There is a requirement of a mechanism to solve exposed or hidden terminal problem.
Diversity	MANET nodes can be the iPods, handheld computers, Smartphones, PCs, smart labels, smart sensors, and automobile-embedded systems.
Protocol diversity	MANET nodes can use different protocols, for example, IrDA, Bluetooth, ZigBee, 802.11, GSM, and TCP/IP
Data caching, saving, and aggregation	MANET node performs data caching and saving. The nodes also perform data aggregation.
Seamless interaction and ubiquitous mobile	MANET mobile device nodes interact seamlessly when they move with the nearby wireless nodes, sensor nodes,

computing	and embedded devices in automobiles so that the seamless connectivity is maintained between the devices.
-----------	--

MANET Applications :

Content distribution and synchronization :

- In an enterprise, there are a number of Bluetooth-enabled mobile handheld devices, PCs, laptops, and Wi-Fi access points
- MANET used for content-distribution, personal information management (PIM), other information dissemination, information fusion, and file sharing in the enterprise.

Multicast Network

- MANET nodes in multicast tree topology disseminate data packets. Clusters of the nodes are used to provide a multicast tree topology. CGSR protocol will be explained later in the chapter.

Mesh network

- A mesh-based mobile network offers highly dynamic autonomous topology segments, The network enables robust IP-compliant data services. The network enables inexpensive alternatives or improvement to infrastructure-based cellular CDMA or GSM mobile service provider for the mobile wireless communication networks. Figure 11.2 shows a mesh network_ Protocol for unified multicasting through announcements (PUMA) is a protocol, that builds a mesh. The mesh connects the MANET nodes with each other.

Image acquisition, processing, and distribution using MANET

- Consider that there are a number of imaging devices forming a MANET—low cost digital still camera with a wireless network interface, a wireless webcam, a mobile device connected to a digital still camera, mobile phones, and pocket PCs equipped with an image acquisition sensor. Six applications to which such MANETs have been applied are as follows:
 - ❖ Remote viewfinder by security personnel in an office.
 - ❖ Remote processing on a computer for a video stream from wireless WebCam and other Devices.
 - ❖ Image file transfer.
 - ❖ Messaging and data transmission to remote devices using 802.11b.
 - ❖ Remote controlling.

IPv6 integration and Wireless sensor networks

- ❖ IPv6 is a new generation Internet and is used for Internet radio and real time video over the Internet. IPv6 can be integrated with MANET and wireless sensor networks.
- ❖ New generation Internet IPv6 addresses are of 128 bits ($2^{128} = 3.4 \times 10^{38}$ addresses). MANET consists of mobile devices as well as wireless sensor nodes..
- ❖ Therefore, integration of IPv6 with MANET enables assignment of IPv6 addresses to each sensor or device node. IPv6 deploys packet encryption and source authentication.
- ❖ It enables real-time traffic, peer-to-peer applications, and dissemination by push. Flow label defined in IPv6 provides the granular QoS support for multimedia real-time applications.
- ❖ Pervasive computing devices, MANET, and wireless sensors need large number of addresses and the above features.

2. Compare the reactive and proactive routing protocols. Describe DSR and AODV protocols. / Explain any two reactive routing protocols in MANETs.

Features	Proactive Routing protocol	Reactive / on-demand routing Protocol
Routing Table	In proactive or table-driven routing protocols , every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.	A reactive protocol is one in which a routing node needs to maintain the routing addresses about the active paths only.

Exchange of Routing Information	Routing information is generally flooded in the whole network.	Routing information is obtained by using a connection establishment process whenever needed. Hence these protocols do not exchange routing information periodically.
Average end-to-end delay	Remains constant in Proactive Protocol for a given Ad hoc network.	Variable in Reactive Protocols.
Delivery of packet	Less efficient than reactive Protocols	efficient in reactive Protocols
Performance	Slower in performance than Proactive protocols.	Much faster in performance than Proactive protocols.
Topology changes	Less Adaptive	More adaptive and work much better in different topographies than Proactive Protocols.

DSR - Dynamic Source Routing:

- DSR deploys source routing.
- Source routing means that each data packet includes the routing-node addresses also.

Reactive protocol feature of DSR

- Reacts to the changes and dynamically maintains only the routing addresses from source to destination, which are the active paths to a destination at a given instant.
- It Performs unicast routing. Unicast means routing packets to a single destined address.

DSR Nodes

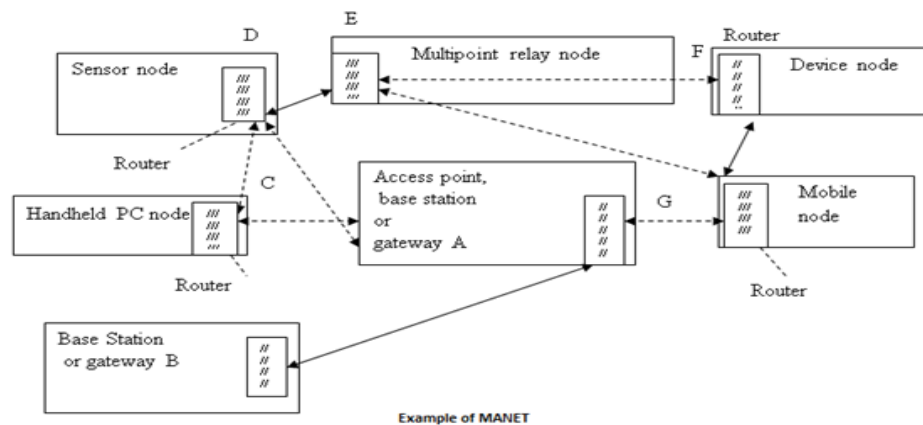
- Each node caches the specified route to destination during source routing of a packet through that node.
- This enables a node to provide route specification when a packet source routes from that node.
- Each node deletes the specified route to destination during routing of error packet in reverse path to the source in case of observing a disconnection during forward path to destination.
- The deletion of link shown in a table or cache is called **link reversal**.

Phase 1 in DSR Protocol

- Source node initiates a route discovery process. It broadcasts the packets, each with a header. It then expects return of acknowledgement from each destination.
- The packets are called route request (RREQ) packets. DSR uses flooding (sends multiple RREQs).
- A header for each route request packet has the i) unique request number and ii) source and iii) destination addresses.
- This enables identification of request at each intermediate node in the request and acknowledged packet(s).
- When the process starts, initially only the source address is given in the header. When the packet reaches a neighbour, that is, any intermediate node, the node adds its own address in the header if it is able to successfully send the packet to its next neighbor.
- When the packet reaches the destined address, its header therefore has all addresses of the nodes in the path.

Example

- Assume that node D is a source and G is a destination and the path D –E –F –G is not known. In such a case the path cannot be placed in the header.



Source Route Discovery Process

- Source node D - puts the sequence number q and source address D in the packet header and sends the packet to its next neighbour.
- When the packet reaches E, its header is (q, D).
- Assume that no route error packet bounced back from neighbour E. The packet is then transmitted to F.
- When the packet reaches F, its header is (q, D, E). Assume that no route error packet bounced back from neighbour F.
- The packet is transmitted from F to G. Assume that no route error packet bounced back from neighbour G. When the packet reaches G, its header is (q, D, E, F).

Domain Specific rules for consistency

- When packet reaches the destination, a route reply (RREP) for the sequence used in RREQ is generated.
- On return path, the route cache builds up at each intermediate node for deployment at a later instant of phase 2

Phase 2 in DSR

- When any source node desires to send a message, it first looks at its route cache.
- If the required route is available in cache, the source node puts all the addresses of the nodes for the path to destination in the header.

Source routing addresses in DSR

- Assuming that there is a message from a MANET node D in the network.

Node	Destination	Cached Path
D	A	D-C-A
D	B	D-C-A-B
D	F	D-E-F
D	G	D-E-F-G

Ad-hoc On-demand Distance Vector Routing protocol (AODV) :

- AODV is a reactive protocol. Reacts to the changes and maintains only the active routes in the caches or tables for a pre-specified expiration time. Routes that are found are available at a given instant.
- It Performs unicast routing. Distance vector means a set of distant nodes, which defines the path to destination. D-E-F-G is a distance vector for source-destination pair D and G

- In AODV, a distance vector is provided on demand during forwarding of a packet to destination by a node in the path and not by the route cache providing path through the header in the source data packet [phase 2]
- Every node keeps a **next-hop routing table**, which contains the destinations to which it currently has a route. A routing table entry expires if it has not been used or reactivated for a pre specified expiration time
- AODV adopts the destination sequence number technique. Does not deploy flooding (multiple RREQs)
- Stores the next hop routing information of the active routes in the routing caches (tables) at each node. Therefore, packet has small header size and thus reduces the network traffic overhead.

Phase – I of AODV

- A node uses hello messages to notify its existence to its neighbours. Therefore, the link status to the next hop in an active route is continuously monitored.
- When any node discovers a link disconnection, it broadcasts a route error (RERR) packet to its neighbors, who in turn propagate the RERR packet towards those nodes whose routes may be affected by the disconnected link. Then, the affected source can be informed.

Phase – II of AODV

- Source node initiates a route discovery process if no route is available in the routing table. It broadcasts the demand through the RREQ packets. Each **RREQ has an ID and the addresses of the source and destination in its header**.
- It expects return acknowledgement from destination. A node identifies the last observed sequence number of the destination from the ID.
- Each RREQ starts with a small TTL (time to live) value [Number of attempts] If the destination is not found during the TTL, the TTL is increased in subsequent RREQ packets.
- The node also identifies sequence number of source node. Sequence numbers ensure loop-free and up-to-date routes.
- Loop-free means free from bouncing of a packet to a node after intermediate hops.
- Each node rejects the RREQ which it had observed before. This reduces flooding which means it reduces too many RREQs present in the network at a given instant.

Route Table in AODV

- Keep entries for a specified period and each node maintains a cache. The cache saves the received RREQs.
- Only the RREQ of highest sequence numbers are accepted and previous ones are discarded.
- The cache also saves the return path for each RREQ source.
- When a node having a route to the destination or the destined node receives the RREQ, it checks the destination sequence number it currently knows and the one specified in the RREQ.
- RREP packet is created and forwarded back to the source only if the destination sequence number is equal to or greater than the one specified in RREQ. It guarantees the updation of routing cache information.

Advantage:

- The main advantage of this protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to destination. The connection setup delay is less.

Disadvantage:

- One disadvantage is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple Route Request packets in response to a single Route Request packet can lead to heavy control overhead.

DSR	AODV
DSR uses source routing in which a data packet carries the complete path to be traversed.	In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission.

Less routing overhead.	More routing overhead.
Has less frequent route discovery process.	Route discovery process is frequently needed.
DSR doesn't perform well in higher-mobility scenarios.	Has better performance in higher-mobility scenarios.

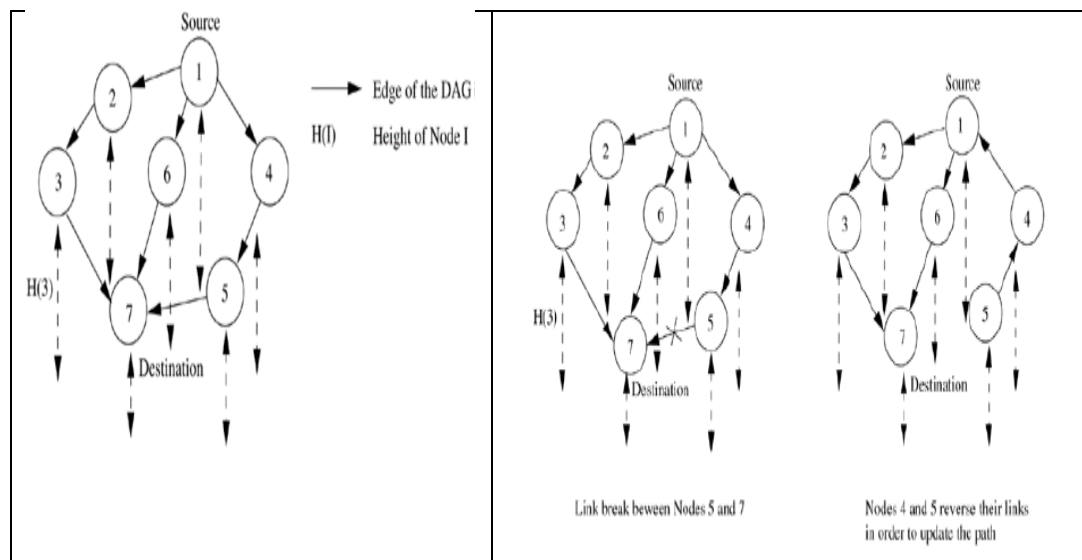
3. Describe TORA. Compare the features of TORA with the DSR and AODV protocols.

Temporally ordered routing Algorithm (TORA)

- Temporally ordered routing algorithm (TORA) is a **source-initiated on demand routing protocol (reactive)** which uses a link reversal algorithm and provides loop-free multipath routes to a destination node.
- In TORA, each node maintains its **one-hop local topology information** and also has the capability to detect partitions.
- TORA has the unique property of limiting the control packets to a small region during the reconfiguration process initiated by a path break.
- Employed for highly dynamic MANETs and provides an improved partial link reversal process. Discovers the network portions showing the link reversal(s).
- Assumes addresses of the routers in the path and of source and destination for one set of input route. Each node provides only one set of subsequent route addresses.
- It Possesses network capacity such that many nodes can send packets to a given destination.
- **Links between routers** conceptually viewed as a **“height”**.
- Link is directed from the higher router to the lower router. Height adjustments occur when topology changes.

Phase I:

- The route establishment function is performed only when a node requires a path to a destination but does not have any directed link.
- This process establishes a **destination-oriented directed acyclic graph (DAG)** using a **Query/Update mechanism**. Consider the network topology shown in the following Figure.

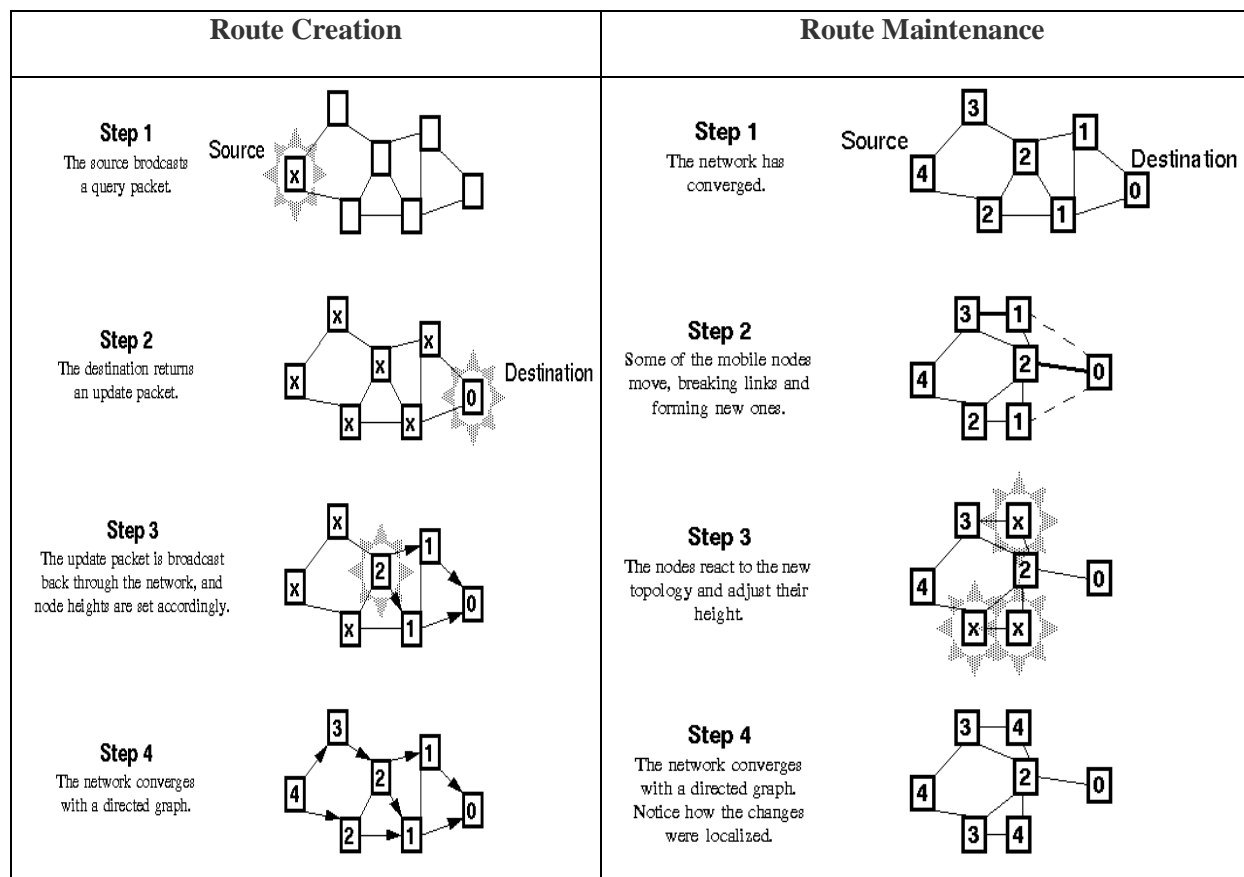


- In this example **source node is 1** and the destination node is 7. Source node sends a **Query packet** with the **destination address** included in it.
- This **Query** packet is forwarded by intermediate nodes 2, 3, 4, 5, and 6, and reaches the destination node 7, or any other node which has a route to the destination.
- In this example, the destination node 7 originates an **Update packet** containing its **distance** from the destination which is zero.

- Each node that receives the *Update* packet sets its distance to a value higher than the distance of the sender of the *Update* packet.
- By doing this, a set of directed links from the node which originated the *Query* to the destination node 7 is created.
Thus $H(7) = 0$: $H(3) = H(5) = H(6) = 1$: $H(2) = H(4) = 2$: $H(1) = 3$
- Once a path to the destination is obtained, it is considered to exist as long as the path is available, irrespective of the path length changes due to the reconfigurations that may take place during the course of the data transfer session.

Phase II:

- When an intermediate node (say, node 5) discovers that the route to the destination node is invalid, as illustrated in the following Figure, it changes its distance value to a higher value than its neighbors and originates an *Update* packet.
- The neighboring node 4 that receives the *Update* packet reverses the link between 1 and 4 and forwards the *Update* packet. This is done to update the DAG corresponding to destination node 7. This results in a change in the DAG.
- If the source node has no other neighbor that has a path to the destination, it initiates a fresh *Query/Update* procedure. Assume that the link between nodes 1 and 4 breaks. Node 4 reverses the path between itself and node 5, and sends an update message to node 5.
- Since this conflicts with the earlier reversal, a partition in the network can be inferred. If the node detects a **partition**, it **originates a Clear message**, which erases the existing path information in that partition related to the destination.



Advantages & Disadvantages :

- By limiting the control packets for route reconfigurations to a small region, TORA incurs less control overhead.
- Concurrent detection of partitions and subsequent deletion of routes could result in temporary oscillations and transient loops.
- The local reconfiguration of paths results in non-optimal routes.

DSR	AODV	TORA
Flooding is used for route discovery.	Flooding is used for route discovery.	Flooding is used for route discovery.
DSR exploits source routing and routing information caching.	Stores the next hop routing information in the routing tables at nodes along active routes.	It is a source-initiated on demand routing protocol (reactive) which uses a link reversal algorithm and provides loop-free multipath routes to a destination node.
Supports unidirectional link as well as provide multiple paths.	Doesn't Support unidirectional link.	Supports unidirectional link as well as provide multiple paths.
It does not exchange hello messages.	It exchanges hello messages periodically to listen to disconnected links.	It does not exchange hello messages periodically to listen to disconnected links.
In DSR, a node notifies the source to re-initiate a new route discovery operation when a routing path disconnection is detected.	In AODV, a node notifies the source to re-initiate a new route discovery operation when a routing path disconnection is detected.	In TORA, a node re-constructs DAG when it lost all downstream links.
Uses flooding to inform nodes that are affected by a link failure.	Uses flooding to inform nodes that are affected by a link failure	TORA localizes the effect in a set of node near the occurrence of the link failure.
Loop can be avoided by checking addresses in route record field of data packets.	AODV uses sequence numbers to avoid formation of route loops.	In TORA, each node in an active route has a unique height and packets are forwarded from a node with higher height to a lower.

**4. Describe an application of defining the cluster of nodes and features of CGSR protocol.
/ Explain in detail about any two proactive routing protocols.**

i) Cluster-head Gateway Switch Routing (CGSR) :

- A hierarchical routing protocol. proactive protocol
- When a source routes the packets to destination, the routing tables are already available at the nodes
- A cluster higher in hierarchy sends the packets to the cluster lower in hierarchy. Each cluster can have several daughters and forms a tree-like structure in CGSR.
- The nodes aggregate into clusters using an appropriate algorithm. The different clusters can be assigned to different band of frequencies in FDMA or different spreading CDMA codes.

CGSR Algorithm :

- Defines a cluster-head, the node used for connection to other clusters. Also defines a gateway node which provides switching (communication) between two or more cluster-heads.
- Three types of nodes in CGSR
 - i) Internal nodes in a cluster which transmit and receive the messages and packets through a cluster-head.
 - ii) Cluster-head in each cluster such that there is a cluster-head which dynamically schedules the

route paths. It controls a group of ad-hoc hosts, monitors broadcasting within the cluster, and forwards the messages to another cluster-head.

- iii) Gateway node to carry out transmission and reception of messages and packets between cluster-heads of two clusters

Cluster structure

- A higher performance of the routing protocol as compared to other protocols because it provides gateway switch-type traffic redirections and clusters provide an effective membership of nodes for connectivity.

Phases 1, 2, and 3 of CGSR

- Routing path discovery and caching, maintaining update, and distribution, respectively
- The basic processes of CGSR are cluster definitions and selection of clusters for routing
- Algorithms are used for both the processes.

Phase 1: Routing path discovery and caching :

- Each node maintains a routing table that determines the next hop to reach other clusters. An algorithm that can be used in this phase is the destination-sequenced distance vector (DSDV) algorithm.
- It means that it finds the next hop to the distant destinations. With the help of the algorithm, cluster member table is created using the sequence numbers in RREQ packets which are broadcast periodically.

Phase 2: Maintaining routing information :

- A clustering algorithm used for maintenance of routing information is least cluster change (LCC). A cluster-head changes only when one of the nodes moves out of the range of all the cluster-heads in the cluster or two cluster-heads come within one cluster.
- A token-based algorithm can be used to control the transmission within a cluster. A cluster-head should get more chance to transmit as it is in charge of broadcasting within the cluster and of forwarding packets between nodes.
- The cluster-heads are given priority such that route path utilization is maximized and packets are transmitted with minimum delay. Another algorithm is the priority token scheduling (PTS). It gives higher priority to the neighbouring nodes from which a packet was received recently.
- Each node dynamically maintains a cluster member table. An algorithm is such that a node will periodically change the entries in its cluster member table when a new sequence number entry is received from the neighbour after successful RREP.
- The table rows map each node to its own cluster-head. A node transmits its cluster member table periodically. After receiving broadcasts from other nodes, a node uses the DSDV algorithm to update its own cluster member table. Following example explains the meaning of hierarchical clustering.

ii) Flat Routing Table Driven Protocol

- Routing cache table used earlier was a routing table which builds by caching the RERP and RERR packets
- Flat routing table driven protocol is a proactive protocol. • This means that routing table will be available in advance at a node
- In the proactive protocol, the routing table is available at each node shows available routes from itself to target destination node, is dynamically modified to show available routes, and has rows for all destined targets irrespective of whether they will eventually be needed or not.
- The packet does not specify route in the header and the routes need not be discovered after the demand is raised

iii) Optimized Link State Routing Protocol (OLSR)

- The optimized link state routing (OLSR) protocol is a **proactive routing protocol** that employs an efficient link state packet forwarding mechanism called **multipoint relaying**. This protocol optimizes the pure link state routing protocol.
- Optimizations are done in two ways: by **reducing the size of the control packets and by reducing the number of links** that are used for forwarding the link state packets.

- The reduction in the size of link state packets is made by declaring only a subset of the links in the link state updates.
- This subset of links or neighbors that are designated for link state updates and are assigned the responsibility of packet forwarding are called **multipoint relays**.

Multipoint relays - MPRset

- The set consisting of nodes that are *multipoint relays* is referred to as *MPRset*. Each node (say, *P*) in the network selects an *MPRset* that processes and forwards every link state packet that node *P* originates.
- The neighbor nodes that do not belong to the *MPRset* process the link state packets originated by node *P* but do not forward them.
- Similarly, each node maintains a subset of neighbors called **MPR selectors**, which is nothing but the set of neighbors that have selected the node as a *multipoint relay*.
- A node forwards packets that are received from nodes belonging to its *MPRSelector* set. The members of both *MPRset* and *MPRSelectors* keep changing over time. The members of the *MPRset* of a node are selected in such a manner that every node in the node's two-hop neighborhood has a bidirectional link with the node.

MPR Selector

- Every node periodically broadcasts its *MPRSelector* set to nodes in its immediate neighborhood.
- In order to decide on the membership of the nodes in the *MPRset*, a node periodically sends *Hello* messages that contain the list of neighbors with which the node has bidirectional links and the list of neighbors whose transmissions were received in the recent past but with whom bidirectional links have not yet been confirmed.
- The nodes that receive this *Hello* packet update their own two-hop topology tables. The selection of multipoint relays is also indicated in the *Hello* packet.

Neighbor table :

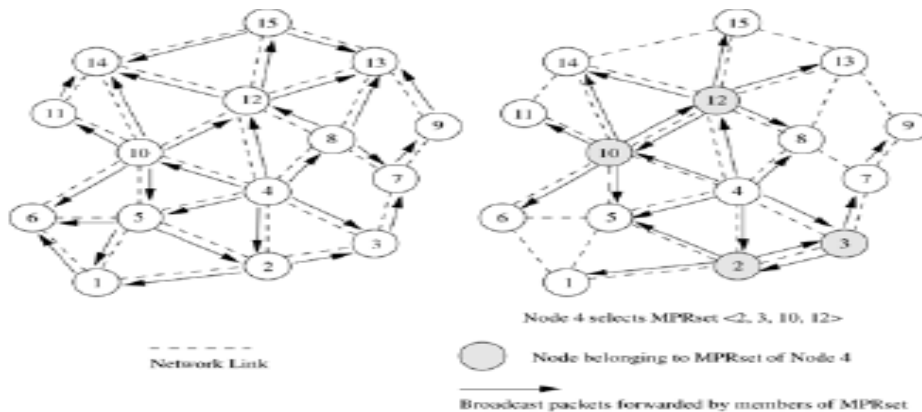
- A data structure called neighbor table is used to store the list of neighbors, the two-hop neighbors, and the status of neighbor nodes.
- The neighbor nodes can be in one of the three possible link status states, that is, unidirectional, bidirectional, and multipoint relay.
- In order to remove the stale entries from the neighbor table, every entry has an associated timeout value, which, when expired, removes the table entry. Similarly a sequence number is attached with the *MPRset* which gets incremented with every new *MPRset*.
- Every node periodically originates *topology control* (TC) packets that contain topology information with which the routing table is updated.
- These TC packets contain the *MPRSelector* set of every node and are flooded throughout the network using the *multipoint relaying* mechanism.
- Every node in the network receives several such TC packets from different nodes, and by using the information contained in the TC packets, the *topology table* is built.
- A TC message may be originated by a node earlier than its regular period if there is a change in the *MPRSelector* set after the previous transmission and a minimal time has elapsed after that.
- An entry in the *topology table* contains a destination node which is the *MPRSelector* and a last-hop node to that destination, which is the node that originates the TC packet. Hence, the routing table maintains routes for all other nodes in the network.

Selection of Multipoint Relay Nodes

- The following figure shows the forwarding of TC packets using the *MPRset* of node 4. In this example, node 4 selects the nodes 2, 3, 10, and 12 as members of its *MPRset*. Forwarding by these nodes makes the TC packets reach all nodes within the transmitting node's two-hop local topology.

MPR set construction :

- The MPRset need not be optimal, and during initialization of the network it may be same as the neighbor set. The smaller the number of nodes in the MPRset, the higher the efficiency of protocol compared to link state routing.
-



The notations used in this heuristic are as follows: $Ni(x)$ node x .

1. $MPR(x) \leftarrow \emptyset$ /* Initializing empty MPRset */
2. $MPR(x) \leftarrow \{ \text{Those nodes that belong to } N1(x) \text{ and which are the only neighbors of nodes in } N2(x) \}$
3. While there exists some node in $N2(x)$ which is not covered by $MPR(x)$
 1. For each node in $N1(x)$, which is not in $MPR(x)$, compute the maximum number of nodes that it covers among the uncovered nodes in the set $N2(x)$.
 2. Add to $MPR(x)$ the node belonging to $N1(x)$, for which this number is maximum.

Advantages and Disadvantages

- OLSR has several advantages that make it a better choice over other table driven protocols.
- It reduces the routing overhead associated with table-driven routing, in addition to reducing the number of broadcasts done. Hence OLSR has the advantages of low connection setup time and reduced control overhead.

5. What are the security threats to a MANET? Why a MANET faces greater security threats than a fixed infrastructure network?

SECURITY PROBLEMS	DESCRIPTION
Increased threat of eavesdropping	The probability that a MANET or sensor node transmits unsolicited messages while moving in the wireless region of two nodes is increased in ad-hoc networks. Each node attempts to identify itself with a new node moving in its vicinity and during that process eavesdropping occurs.
Unknown node caching the information	An unknown node can move into the network and thus rigorous authentication is required before the node is accepted as a part of MANET.
Denial of service attacks	A number of transmission requests can be flooded into the system by the attacking nodes. Since for each request, an authentication process is initiated, which require exchange of message, the flooding of the message-exchanges chokes the MANET and denies the required services to genuine nodes.
Authenticated node becoming hostile	A previously authenticated device can be used for security attacks.

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user identity before allowing data access. MANET is more vulnerable than wired network. Some of the **security threats and vulnerabilities of the MANETs** can be classified as follows:

- **Lack of centralized management:** MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.
- **Cooperation:** Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.
- **Dynamism of Topology:** The nodes of MANET are randomly, frequently and unpredictably mobile within the network. These nodes may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes.
- **Lack of fixed infrastructure:** The absence of a fixed or central infrastructure is a key feature of MANET. This eliminates the possibility to establish a centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.
- **Resource constraints:** MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth, etc. by default. So, in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring. Although the security requirements (availability, confidentiality, integrity, authentication, nonrepudiation) remain the same whether be it the fixed networks or MANETs, the MANETs are more susceptible to security attacks than the fixed networks due their inherent characteristics .
- **Scalability:** Due to mobility of nodes, scale of ad-hoc network changes all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as smaller ones.
- **Adversary inside the Network:** The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behaviour of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called **compromised nodes**.

6. Describe wireless sensor networks and its applications. Explain the similarities in MANET and wireless sensor networks.

Some applications of wireless sensor networks and MANETs are described below.

- **Street lighting with local as well as remote central control of a cluster of lights.**
- **Industrial plant wireless sensor networks** Industrial plants use a large number of sensors in instruments and controllers. Wireless sensor network proves to be powerful for an industrial plant.
- **Pervasive computing networks** Mobile pervasive computing means a set of computing devices, sensors, or systems or a network having the characteristics of transparency, application-aware adaptation, and environment sensing. Wireless sensor networks and MANETs are therefore an important element of pervasive computing.
- **Traffic monitoring using traffic density wireless sensor networks** Traffic can be monitored at different points in a city and traffic density information can be aggregated at a central server. The server relays this information to motorists on wireless Internet.
- **A traffic control server sends the traffic reports on Internet.** The automobile owner can subscribe to a traffic control service provider which provides SMS messages about traffic slowdowns and blockades at various city points.
- **It enables a driver to select the roads with the least hurdles.** TTS (text to speech)

converters can also give voice messages to the drivers.

- Medical applications of wireless sensor networks Patients can be monitored by the sensors attached to them. When a patient moves, the sensors form a MANET.
- Military applications of wireless sensor networks The voice of a person can be sensed by a wireless sensor network deployed in remote border areas. This monitors the enemy troop and machines movements.
- Smart labels and RFID-based wireless sensor network It is used worldwide for monitoring movement of goods, movement of books in library, and supply chain management systems.
- Environmental monitoring wireless sensor network Environmental parameters like temperature, pressure, light, rainfall, and seismic activity are sensed and communicated over a wireless network.
- Home automation Home automation including security is possible using a wireless sensor network.

	WSN	MANET
Similarity	Wireless	Multi-hop networking
Security	Symmetric Key Cryptography	Public Key Cryptography
Routing	Support specialized traffic pattern. Cannot afford to have too many node states and packet overhead	Support any node pairs Some source routing and distance vector protocol incur heavy control traffic
Resource	Tighter resources (power, processor speed, bandwidth)	Not as tight.

7. Describe about distributed network and its characteristics in sensor networks.

- A wireless sensor network can be considered as a MANET of autonomous devices, which are spatially distributed. Sensor devices cooperate with each other to disseminate the sensed or other data in the network.

Distributed Network and Characteristics

- The characteristics are energy constraints, probability of node failure, mobile network topology, and nodes using heterogeneous protocols with no maintenance during their operation it is known as full copy replication.

Clustering of Nodes

- All sensor nodes in a set can route the sensed data through the cluster coordinator or cluster head. A wireless sensor node (WSN) has low power transceivers.
- Each WSN has a limited range of communication. Therefore a set of WSNs can be clustered. Each WSN communicates with the wireless cluster coordinator (WCC), also called the cluster head.
- WCC is a multifunctional unit.
 - (i) Each WCC collects the sensed data from the WSNs.
 - (ii) A WCC detects the faulty node and the events.
 - (iii) WCC also performs the aggregation, compaction, and fusion of data.
 - (iv) WCC has limited control and maintenance processing.

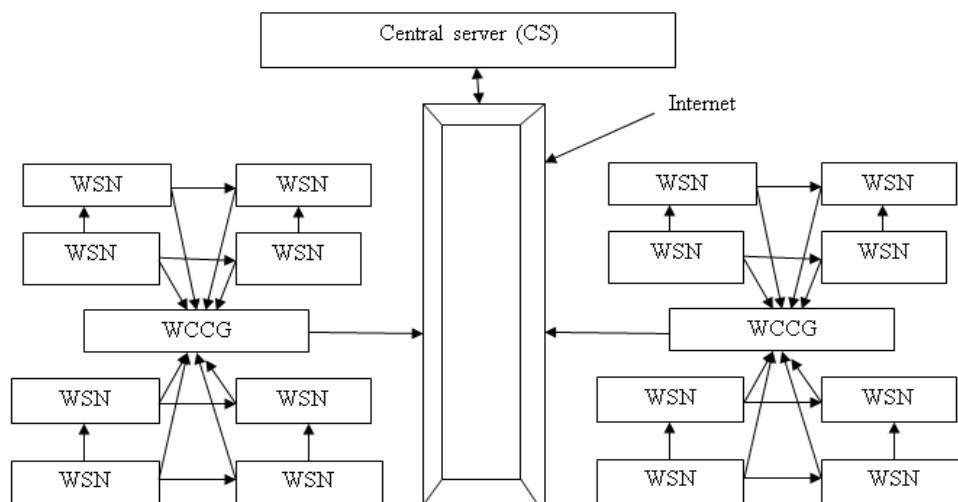
A WCC can also provide gateway to the Internet. WCC has greater data computing capability than the WSN. A hierarchy of WCC can also be arranged with the root server.

Coordination of Nodes

- Coordinating node is centralized computing system and provides communication between the clusters of the wireless sensor nodes (WSNs). A coordination node is a part of a piconet (short range network). A coordination algorithm for the WSNs can be designed for effective coordination.
- There may be a network of WCCs connected to a wireless cluster coordinator gateway (WCCG). Similarly we may have a network of WCCGs connected to a central server (CS).

Wireless Sensor Network - Example

- Networks can have hierarchical tree-like structures, for example, CS at level 1, WCCG at level 2, WCC at level 3, and WSN at level 4.
- The next example shows the clustering of wireless sensor networks of WSNs, WCCs, WCCGs, and CS for street-lighting control and maintenance, both locally and remotely.



Two WSNs in two clusters of a wireless sensor network deploying the WCCG and connected to a central

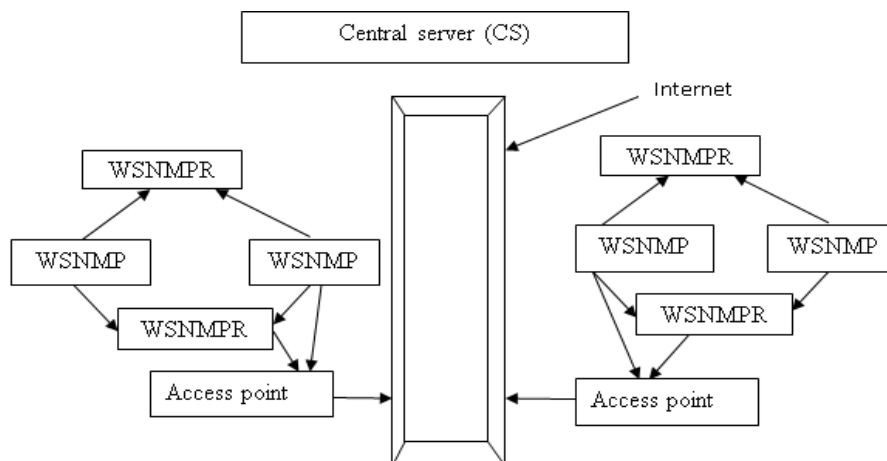
- A WSN node has a sensor for sensing environmental light conditions. Each WSN in a set of nodes transmits the data to the WCCG. Each WSN has three paths to a WCCG. Each WSN has a multipoint relay. A central server connects through internet to the WCCG to control and program the firmware of WCCG.
- In the figure, two WSNs for street-lighting and WCCG. The gateway connects to the CS. The WCCG is a multifunctional unit which does the following:
 - i) Collects the sensed light from the WSNs
 - ii) Senses the ambient conditions which are present near the WCCG.
 - iii) Detects the faulty node.
 - iv) Performs the aggregation, compaction and fusion of data.
 - v) Has firmware for the control and maintenance locally and
 - vi) Provides Gateway to the internet.

Distributed Networks – Example :

To enable remote traffic control and monitoring :

- The figure shows a WSN for distributed network of traffic signaling and control system using wireless sensor node with multipoint relays (WSNMPRs). A WSNMPR is a multifunctional distributed computing unit.
 - i) It senses vehicular noise among multiple paths to a road junction.

- ii) It computes the traffic density. The interval for which traffic lights should be green along one of the multiple paths at a road-crossing is function of traffic density.
- iii) Each WSNMPR computes the sensed traffic density data along a particular vehicular path.
- iv) Each WSNMPR senses the event in real time.
- v) It senses ambient conditions which are present near the WSNMPR.
- vi) Each WSNMPR performs data aggregation , compaction and fusion.
- vii) WCCG provides Gateway to the internet.



- A central server controls the functions remotely. The server programs the firmware in WSNMPRs.
- The central server collects data from distributed nodes and monitors the synchronization between different traffic lights at different road junctions. Monitoring is central with traffic density is computed locally.

The application layer consists of:

1. sensor management protocol
2. sensor query and data dissemination protocol
3. task assignment and data advertisement
4. application specific protocols.
 - Data link layer provides MAC (medium access control) protocol. It also deploys protocols for power saving and error control.

Standard protocols for wireless sensor networks are as follows:

1. IEEE 802.15.4-2003 ZigBee (a set of communication protocols used by small-sized low power digital radio embedded in the sensors and home devices)

• A Standard protocol for wireless sensor networks

• ZigBee — a set of communication protocols used by small-sized low power digital radio embedded in the sensors and home devices

6lowpan Protocol

• 6lowpan (IPv6 over low power wireless personal area network which permits communication of IPv6 packets in sensor network)

Software

• Software once embedded into the sensor node is for lifetime

• Should be robust, fault tolerant, and should provide maximum features and middleware

• Software should have features of security, self-healing, and self configuration

Few specific operating systems

• tinyOS and CORMOS (communication oriented runtime system for sensor networks)

Router

Sensor networks deploy special routing protocols such as CGSR, DSR, or AODV.

TinyOS

- TinyOS is an OS with components. It is installed at the sensor node. The components enable the application to run on the sensor hardware as well as facilitate packet communication and routing. That enables networking of the nodes and the nodes function in distributed environment. Only the required components are embedded and installed in the firmware of a wireless sensor node.
- The components for the packet communication, routing, sensing, actuation, and storage can be embedded. TinyOS provides interfaces. It considers multiple tasks (threads), which are run in first-in first-out (FIFO) order. Each task is assumed to be of identical priority.
- A language for sensor networks is nesC and it uses C programming language for memory optimization and cooperating tasks and processes. Supplementary tools can be in Java and Shell Script.
- State machine programming is a concept in which a program is said to change the states from one state to another. TinyOS enables state machine programming.

8. Brief about communication coverage and sensing coverage in wireless sensor networks.

Communication Coverage :

- If two nodes can hear each other *in the absence of interference from other nodes*, then there will be an edge between the corresponding vertices. Essentially, this corresponds to the receiver being within the **decode region of the transmitter**.
- In this graph model, which is obtained when only the decode regions are considered, it is desirable that each vertex have a path to the vertex corresponding to the sink. This assures us that there is a way for a sensor node i to communicate its measurements to the sink. This is because one can think of a strategy in which i is the *only* node that transmits in a time slot, thereby passing its information to a neighbor within its decode region.
- Similarly, in the next slot, the neighbor is the only node that transmits. This naive strategy, albeit inefficient, will succeed in transferring information from i to the sink, over several time slots, *if* there is a path in the graph model from i to the sink. Let us enlarge the requirement slightly and ask that there be a path between *any* pair of nodes.

What is the minimum power at which the nodes should transmit so that the graph obtained is *connected* ?

- In passing, we recall that *not all* the edges in a path from a vertex to the sink can be active *simultaneously*. In this section, we will consider only the question of connectivity of the graph obtained by considering just the decode regions.
- Now for a random placement of nodes, the right question to ask is: What is the minimum power at which the nodes should transmit so that the graph is connected *with a given high probability* ? For a given number of nodes N , this question is hard to answer. Rather, answers have been found in the asymptotic regime where N tends to ∞ .
- Suppose that N sensors are deployed in a square region of unit area. Each sensor is located independently of any other, and the location is chosen by sampling the uniform distribution.
- Further, let $r_c(N)$ be the *range* of each of the nodes, i.e., if nodes i and j are separated by a distance less than or equal to $r_c(N)$, then they can decode each other's transmission. We note that $r_c(N)$ is being regarded as a function of the total number of nodes N ; this suggests that the range changes as N varies. In fact, we would be interested in understanding how to set $r_c(N)$ for a given N , so that the sensor network remains connected.
- As N increases, it is expected that the range required to maintain connectivity decreases; $r_c(N)$ is a decreasing function of N . Suppose we consider a range such that

$$\pi r_c^2(N) = \frac{\ln N + c(N)}{N}$$

- where $c(N)$ is some function of N that we will discuss later. Note that this range assignment essentially means that a disk of area $\ln N + c(N)/N$ is within reach of a node.
- Let $P_d(N, r_c(N))$ be the probability that, with this $r_c(N)$, the graph $G(N, r_c(N))$ is disconnected.

$$\liminf_{N \rightarrow \infty} P_d(N, r_c(N)) \geq e^{-c} (1 - e^{-c})$$

where $c = \limsup_{N \rightarrow \infty} c(N)$. Also,

$$\limsup_{N \rightarrow \infty} P_d(N, r_c(N)) \leq 2e^{-c}$$

Sensing Coverage :

- Given an area to be monitored and given a sensing disk around each sensor, how many sensors are required? Now as the node deployment process is random, as a first step, we assume that the nodes are deployed as a two-dimensional spatial Poisson process of intensity λ points per unit area.
- The significance of the Poisson assumption is that in two non-overlapping areas, the numbers of sensors are independent random variables. Further, in an area A , the number of sensors is Poisson-distributed with parameter λA , where A is the area of A .
- This question must be refined as follows: What is the minimum intensity λ such that the probability that every point in the monitoring region is covered by at least k nodes is close to 1?
- Let r_s denote the *sensing radius* of each disk. Let us choose the unit of area such that each sensor covers unit area: $\pi r_s^2 = 1$.
- Let us define V_k to be the total area that is *not* k -covered. This means that each point in the area V_k is at most $(k-1)$ -covered. V_k is referred to as the *k-vacancy value*.
- Clearly, V_k is a nonnegative random variable that depends on the particular instance of the Poisson deployment process.
- First, it can be shown that no finite λ , no matter how large, can ensure that each point in the monitoring area is covered by at least k nodes. To see this, let $I_k(x)$ denote the indicator function corresponding to k -vacancy at location x . That is,

$$I_k(x) = \begin{cases} 1 & \text{if at most } k-1 \text{ nodes cover point } x \\ 0 & \text{else} \end{cases}$$

- If the point x is covered by at most $(k-1)$ sensors, then it is within the sensing distance r_s from at most that many sensors. Equivalently, if we draw a circle of radius r_s centered at x , then there are at most $(k-1)$ sensors within it. Recalling that the deployment process is Poisson with intensity λ and that r_s has been chosen such that the area of a circle with radius r_s is unity, we have

$$\Pr(I_k(x) = 1) = e^{-\lambda} \sum_{i=0}^{k-1} \frac{\lambda^i}{i!}$$

Now V_k can be written as

$$V_k = \int_A I_k(x) dx$$

Then

$$\begin{aligned} \mathbf{E}(V_k) &= \int_A \mathbf{E}(I_k(x)) dx \\ &= A \Pr(I_k(x) = 1) \\ &= a^2 e^{-\lambda} \sum_{i=0}^{k-1} \frac{\lambda^i}{i!} \\ &> 0 \end{aligned}$$

- where we have assumed that A is a square region with each side of length a . In arriving at the second line, we have used the fact that $\Pr(I_k(x) = 1)$ does not depend on x .
- We note that $\mathbf{E}(V_k) > 0$ for any finite λ , no matter how large it is. But $\mathbf{E}(V_k) > 0$ implies that $\Pr(V_k = 0)$ cannot be 1.
- Thus, for any finite λ no matter how large, we see that $\Pr(V_k > 0) > 0$; we cannot ensure that each point in the area is covered by at least k nodes.

9. How is localization achieved in wireless sensor networks ?

Localization:

Methods that allow the nodes in a network to determine their geographic positions

- ❑ Use of current GPS systems not feasible:
 - o Cost
 - o Power consumption
 - o Form factor

- o Do not work indoors or under dense foliage
- In many situations of practical interest, sensor nodes are strewn randomly over the deployment area. Consequently, the position of each sensor node is not known a priori. Position information, however, is crucial in many situations; e.g., to report *where* an event has occurred.
- Moreover, knowledge of node positions can be exploited in routing also, as in *geographic routing* . Hence, localization is an important problem in sensor networks.
- Let us consider several sensors distributed over an area. A small fraction of these are **anchor devices** that know their own positions.
- They could be GPS-enabled, or they could have been placed precisely at particular positions, with the position information being programmed into them. The problem is to localize the other sensors with help from these anchors.
- A crude idea of the distance from an anchor node can be obtained by noting the strength of the signal received from the anchor and the transmit power of the anchor.
- The quality of a distance estimate obtained in this way depends on the accuracy of the model of signal attenuation used. Further, the transmit power used by an anchor may not be easily available to a sensor. For this reason, let us consider “ range-free ” localization, where we do not calculate distances from anchors based on the received signal strength.
- Suppose each anchor sends out messages including its own position and including a hop count parameter. The anchor initializes the hop count to 1.
- A sensor (i.e., nonanchor node) receiving the message notes down the anchor’s position and the hop count contained in the packet. Next, it increments the hop count value and broadcasts the packet again.
- In this way, a wave of packets originates from an anchor and spreads outward. If a sensor receives a packet with a hop count value that is greater than the one stored locally, it ignores the received packet.
- The hop count from the i -th anchor, stored at a sensor, is a crude measure of its distance from the anchor. As the density of sensor deployment increases, the distance estimate indicated by the hop count becomes more reliable.
- As the density increases, sensors at the same hop count from an anchor tend to form concentric rings, of annular width approximately r_c , where r_c is the communication range of a sensor. Thus, if h_i is the hop count from anchor i , then the sensor is at a distance approximately $h_i r_c$ from anchor i . After obtaining several node – anchor distance estimates as before, nodes follow the **multilateration technique**. Suppose a node has heard from M anchors, and the anchors ’ positions are, respectively, (x_i, y_i) , $1 \leq i \leq M$. The sensor node j is located at position (x_j, y_j) , and this information is not available to it. The actual distance between node j and anchor i is given by

$$d_{j,i} = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}$$

which, of course, is unknown in j . The estimate of this distance that is available to j is $\hat{d}_{j,i} := h_{ir} r_c$. Then, a natural criterion that can be used to determine the unknown (x_j, y_j) is the total *localization error* E_j , defined as

$$\begin{aligned} E_j &= \sum_{i=1}^M (d_{j,i} - \hat{d}_{j,i})^2 \\ &= \sum_{i=1}^M \left(\sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} - \hat{d}_{j,i} \right)^2 \end{aligned}$$

10. Explain in detail about any two routing techniques in WSN.

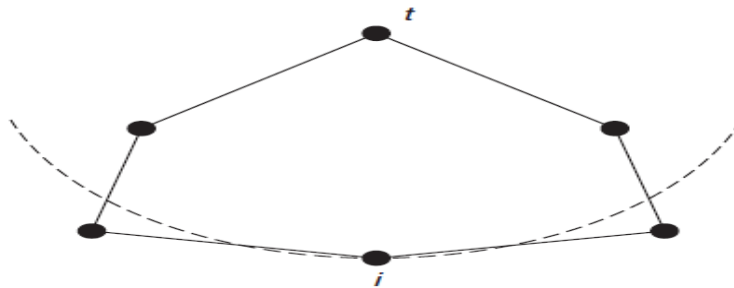
- Standard table-driven routing approaches are often not attractive in the sensor network context. Route discovery and route maintenance are periodic and energy-intensive tasks, and typical sensor nodes are severely constrained in energy, memory, and computing power.
- In WSN, there are two types of routing approaches:
 - 1) Routing strategy that depend on nodes’ positions.
 - 2) Routing strategy that based on attributes

1) Routing strategy that depend on nodes’ positions.

- Consider routing ideas referred to as geographic or geometric or position-based routing. Its characteristic features are: (1) every node knows its own position and the positions of its neighbors;

(2) the source knows the position of the destination; (3) there are no routing tables stored in the nodes; (4) the additional information stored in a packet is bounded above by a constant times the number of nodes in the graph; the additional information is $O(|V|)$, where V is the vertex set of the graph $G(V,E)$ representing the sensor network.

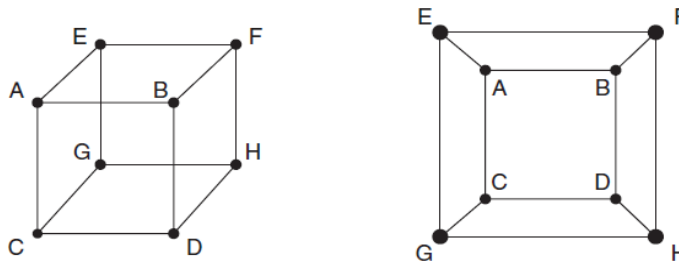
- The simplest approach is for a source node s to forward data to a neighbor who is closer to t . Basically, this is a **greedy approach** — a packet is passed to a neighbor who is closest to the destination.
- For simplicity, we will assume that all nodes transmit at the same power, so that the communication radius r_c is the same for all nodes. This means that any two nodes at a distance less than or equal to r_c can communicate directly with each other. If r_c is defined as the unit of distance, then we have what is called a **Unit Disk Graph (UDG)**.
- In a dense network, it is clear that a UDG will give rise to numerous edges. Typically, in a graph with a large number of edges, significant computational effort is required to find routes between pairs of nodes.
- This suggests that removing some edges from the UDG, while retaining graph connectivity, is an option worth exploring.



Scenario where greedy routing fails. Neither of the neighbors of i is closer to the destination t than i itself.

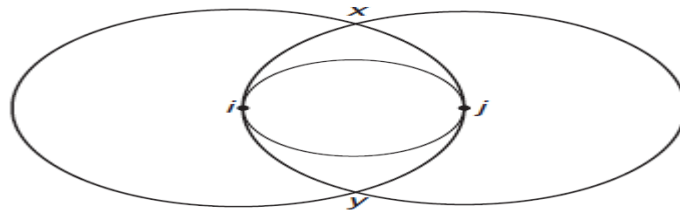
To obtain a planar graph from UDG

- A planar graph is one that can be drawn such that no edges intersect on the plane. When it is drawn in such a way, what we get is a plane graph. Planar graphs are of interest because they are usually sparse. Example for planar graph as shown below.
- One possibility is to start with the node positions of the original UDG, eliminate all edges in the UDG, and then reintroduce some edges appropriately. Several standard geometric constructions are used to get planar graphs in this way.
- The basic idea is to introduce an edge between nodes i and j , say $i \rightarrow j$, if a suitable region around $i \rightarrow j$ (called the *witness region*) is free of other nodes.



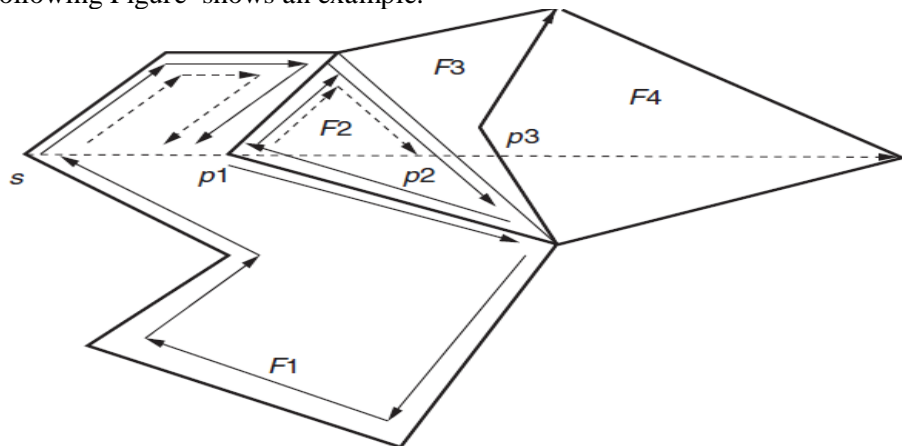
Relative Neighborhood Graph

- Let $d(i, j)$ be the geometric or Euclidean distance between nodes i and j . Consider two circles of radius $d(i, j)$ centered around the nodes i and j (see Figure 8.7). The intersection of the two circles is called the *lune*.
- Suppose we introduce the edge $i \rightarrow j$ if the lune is free of other nodes. If we do this for every pair of nodes, we get the *Relative Neighborhood Graph (RNG)*.



Obtaining the Relative Neighborhood Graph (RNG) and the Gabriel Graph (GG) from the node positions. To get the RNG, we introduce edge $i \rightarrow j$ if the lune $ixjy$ is free of other nodes. To get the GG, we introduce edge $i \rightarrow j$ if the circle of diameter $d(i, j)$ within the lune is free of other nodes.

- On the other hand, suppose we introduce the edge $i \rightarrow j$ if the circle of diameter $d(i, j)$ within the lune is free of other nodes. Doing this for every pair of nodes gives us the **Gabriel Graph (GG)**. For the RNG, the witness region is the lune; for the GG, the witness region is the circle within the lune.
- It is known that both the RNG and the GG are planar graphs. Further, it is also evident that the RNG is a subgraph of the GG. It turns out that both of these planar graphs can be computed using local algorithms, involving exchange of information among a node and its neighbors only.
- To get around the problem encountered with greedy routing, consider a strategy that routes along the boundaries of the faces that are crossed by the straight line between the source and the destination. The following Figure shows an example.



- we see four faces, F_1 , F_2 , F_3 , and F_4 , in the planar graph. The source s and the destination t are also marked. F_1 is the face that contains s and the line s, t intersects F_1 . To begin with, say the boundary of F_1 is explored, in the clockwise direction.
 - This is indicated by the thin solid arrows in Figure 8.8. As the boundary is traversed, the algorithm notes all points where the line s, t intersects the boundary, and the point closest to t is stored for future use.
 - In Figure, there is only one such point, viz., p_1 . After traversing the whole boundary and reaching s again, a second traversal (along the dashed line) is started. This time, when p_1 is reached, the face F_2 is explored in a similar manner. We may refer to the point p_1 as a switch point.
 - Essentially, the idea is to show that in the course of the **execution of the face routing algorithm**, each edge is traversed *at most* a constant number of times. Then, a theorem about planar graphs is applied; this theorem says that the number of edges $|E|$ in a connected plane graph with at least three vertices satisfies $|E| \leq 3|V| - 6$.
 - This relation is significant, because it indicates that planar graphs are basically sparse graphs.
- 2) Routing strategy based on attributes : - Directed Diffusion (DD)**
- Here we consider a routing strategy that doesn't need nodes' positions and even addresses. In fact, the routing scheme to be discussed here does not even attempt to reach a specific node from another; it uses a completely different philosophy.

- In a deployed sensor network, a specific type of event may be of interest. For example, in a sensor network used for environment monitoring, observations of a particular type of animal may be of interest.

Strategy :

- The strategy in *attribute-based* routing schemes is to launch a query that *describes the data of interest*.
- As this query propagates through the network, it encounters nodes that have observed the event of interest. Such nodes now provide replies that move back toward the original node issuing the query. Thus, attribute-based routing provides a way for **information seekers and information gatherers** to “meet,” *without* knowing one another beforehand.
- Data are described by *attribute-value* pairs that characterize the information that is of interest. For example, a query can be expressed as a *record* consisting of multiple attribute-value pairs:
 type = animal
 instance = leopard
 rectangle = [0, 400, 0, 400]
- In the first line, “type” is the attribute and “animal” is the value; similarly, “instance” is the attribute and “leopard” is the value. The third line specifies an area (in some coordinate system) within which the observation is sought; a rectangle of size 400 _ 400 is shown here, with the ranges along the *x* and *y* axes specified.

Directed Diffusion (DD)

- A prominent example of attribute-based routing is provided by a scheme known as *Directed Diffusion* (DD). In DD terminology, the node issuing the query is called a *sink*, while the nodes providing the observation are called *sources*.
- The query itself is referred to as the *interest*. To begin with, the sink broadcasts the interest. As shown in the previous example, the **interest is a collection of several attribute-value pairs**, among which are the attributes ***duration*, *interval*, and *update***.
- The duration attribute specifies the period of time for which the interest is valid. The interval attribute specifies the intervals at which the observation is to be reported.
- Implicit in this attribute is the characteristic of DD that *repeated observations* of the event of interest are important.
- Further, the duration attribute indicates that the interest persists for some time. Both attributes suggest that the sink is not satisfied with just one observation of the event; rather observations extended over time are important. This allows DD to amortize the cost of finding paths between sources and sinks over the duration of the communication.

Interest generation & interest cache

- The interest generated originally by the sink passes through nodes in the network.
- A node that receives the interest checks if it has any event record that matches the interest.
 - ❖ If it does, then it becomes a source and proceeds to relay the information back to the sink;
 - ❖ If it does not, then it forwards the received interest to its neighbors.
- Each node maintains an *interest cache*, where valid interests are stored. Along with each interest, the node notes down the neighbor from which the interest was received. It is noteworthy that this is strictly *local information*; the sink that generated the interest in the first place is not tracked.
- A particular interest may be received at a node from a number of neighbors because, initially, the interest is flooded through the network and may arrive at the node via multiple paths. All such neighbors are stored in the interest cache.
- The repetition of sending the report is determined by the *update* attribute of the interest received from that neighbor.
- The smaller the value of update, the more frequently the neighbor receives a report. In fact, the update attribute determines what is called a *gradient* toward a neighbor, where gradient is defined as the reciprocal of the update value.

- In this way, utilizing neighbors and the gradient toward each neighbor, an observed event record makes its way back toward the sink.
- As in the forward pass when the interest was making its way into the network, the requested information may arrive back at the sink over multiple paths. In the DD scheme, the update attribute is now used in a clever way to reinforce good quality paths.
- To do this, the sink observes the returned reports received from various neighbors. The neighbor from which the *first* report was received is likely to lie on the least-delay path from the source to the sink.
- The sink now resends the interest to *this* particular neighbor, with a smaller update attribute. This leads to higher gradients being set up all along the backward path from the source to the sink.
- In this way, DD provides a way of adaptively selecting preferred paths. Similarly, the update interval toward a nonpreferred neighbor can be increased, so that ultimately, that particular path from source to sink is suppressed.
- It is worth noting that DD is inherently robust to node failures, because if the currently preferred path becomes unavailable (due to node failure, say), then an alternate path (which was currently not preferred) may be picked up and reinforced by update attribute manipulation.

11. Explain in detail about any two scheduling algorithms in WSN.

Need for scheduling Algorithm :

- Sensor nodes share the wireless medium. Therefore, they need a MAC protocol to coordinate access. However, in a sensor network, energy efficient MACs are extremely important, and this forces us to look at MAC protocols closely.
- The notable point here is that a sensor spends the same order of energy in simply listening on the medium as in actually receiving a packet. Since saving energy is so important, we need to understand **how energy can be wasted**.

The following causes can be recognized – (Four sources of energy inefficiency)

- *Idle Listening*: If the medium is idle and yet a sensor node's radio transceiver is ON, then it is spending energy unnecessarily.
- *Collision*: If transmissions collide, then all packets involved are garbled, leading to waste of energy all around.
- *Overhearing*: Overhearing occurs when a node receives a packet that is not addressed to it.
- *Control Packet Overhead*: From an application's point of view, energy spent in carrying information bits is energy usefully spent. It is desirable that the energy spent on control path activities, like channel reservation, acknowledgment, and route discovery, be as small as possible.

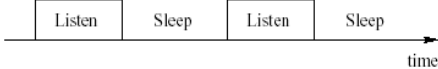

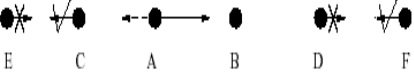
IEEE 802.11 Vs Sensor MAC

- A good sensor MAC protocol leads to savings on all four of these fronts.
- Sensor MAC protocols are significantly different from other wireless MAC protocols (like IEEE 802.11) because they can put the sensors into the *sleep state*. In this state, the radio transceiver is turned OFF completely.
- Nodes wake up periodically, listen on the medium for a short while, and then go back to sleep. This reduces idle listening drastically, and is a major reason for energy savings.

Sensor - MAC (S-MAC)

- The protocol sensor-MAC (S-MAC) is one of the first to use the notion of sleep – wake duty cycles heavily. It aims to ensure a low duty cycle operation on the network.
- It introduces the notion of **coordinated sleeping**, in which clusters of nodes synchronize their sleep schedules so that all of them sleep together.
- Tries to reduce wastage of energy from all four sources of energy inefficiency
 - ❖ Collision – by using RTS and CTS

- ❖ Overhearing – by switching the radio off when the transmission is not meant for that node
- ❖ Control overhead – by message passing
- ❖ Idle listening – by periodic listen and sleep

Idle listening - Periodic Listen and Sleep	<ul style="list-style-type: none"> • If no sensing event happens, nodes are idle for a long time. • So it is not necessary to keep the nodes listening all the time. • Each node go into periodic sleep mode during which it switches the radio off and sets a timer to awake later. • When the timer expires it wakes up and listens to see if any other node wants to talk to it.  <p>Fig. 1. Periodic listen and sleep.</p>  <p>Fig. 2. Neighboring nodes A and B have different schedules. They synchronize with nodes C and D respectively.</p>
Collision Avoidance –by using RTS and CTS	<ul style="list-style-type: none"> • Perform carrier sense before initiating a transmission • If a node fails to get the medium, it goes to sleep and wakes up when the receiver is free and listening again • Broadcast packets are sent without RTS/CTS • Unicast packets follow the sequence of RTS/CTS/DATA/ACK between the sender and receiver
Overhearing Avoidance	<ul style="list-style-type: none"> • Duration field in each transmitted packet indicates how long the remaining transmission will be. • So if a node receives a packet destined to another node, it knows how long it has to keep silent. • The node records this value in network allocation vector (NAV) and set a timer. • When a node has data to send, it first looks at NAV. • If NAV is not zero, then medium is busy (virtual carrier sense).  <p>Fig. 4. Who should sleep when node A is transmitting to B?</p> <ul style="list-style-type: none"> • All immediate neighbors of both the sender and receiver should sleep after they hear RTS or CTS packet until the current transmission is over.
Control Overhead-Message passing	<ul style="list-style-type: none"> • A message is a collection of meaningful, interrelated units of data. • Transmitting a long message as a packet is disadvantageous as the re-transmission cost is high. • Fragmentation into small packets will lead to high control overhead as each packet should contend using RTS/CTS. • Fragment message in to small packets and transmit them as a burst.

- S-MAC forms a flat, peer-to-peer topology. Thus, unlike clustering protocols, there is no cluster-head to coordinate channel access.

Exchange of schedules – SYNC Packet

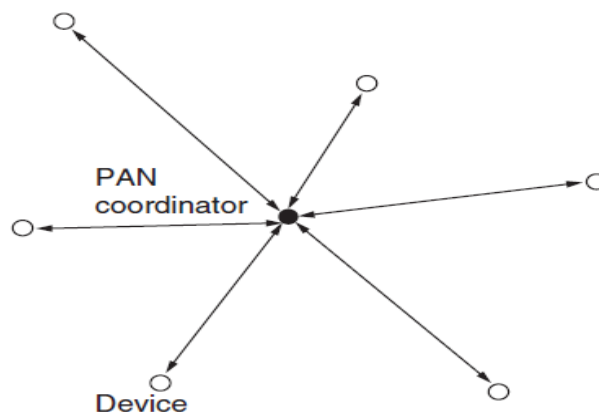
- Because coordinated sleeping is so important in S-MAC, nodes need to exchange schedules before data transfer can begin.
- The *SYNC* packet is used for this purpose. The transmission time for a SYNC packet is called the *synchronization period*.

Schedule table

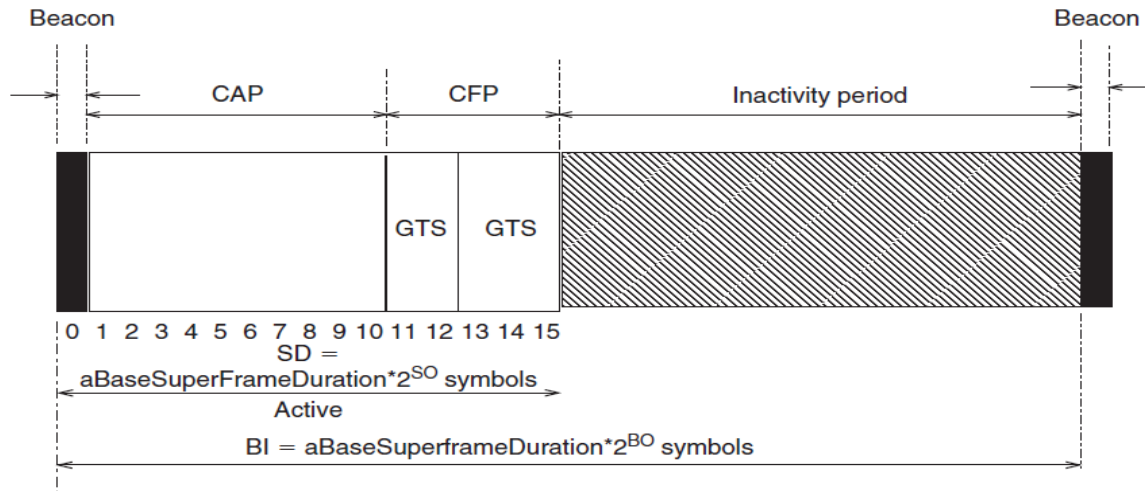
- Each node maintains a *schedule table* that stores the schedules of all its neighbors. To choose a schedule, a node first listens for at least the synchronization period.
- If no SYNC packet is heard within this time, then the node chooses its own schedule and starts to follow it. It also broadcasts its schedule by transmitting its own SYNC packet.
- If the node does receive a SYNC packet within the initial listen interval, then it sets its own schedule to the received one. Thus, synchronization with a neighbor is achieved. As before, it announces its schedule by transmitting its own SYNC packet later.
- However, the following can also happen: After a node chooses and announces its own schedule, it receives a new and different schedule. What it does now depends on how many neighbors it heard from. If the node had no neighbors, then it discards its original schedule and switches to the new schedule just received. If the node had one or more neighbors, it adopts *both* schedules, by waking up at the listen times of both. Such behavior typically is found among nodes that are located at the borders of two virtual clusters and facilitates communication between the two.

IEEE 802.15.4 (Zigbee)

- The other sensor MAC protocol that has received wide attention is the IEEE 802.15.4 MAC. The protocol was introduced first in the context of Low-Rate Wireless Personal Area Networks (LR-WPANs).
- The physical (PHY) and MAC layers in LR-WPANs are defined by the IEEE 802.15.4 group, whereas the higher layers are defined by the Zigbee alliance.
- IEEE 802.15.4 defines two types of devices: a *Full Function Device* (FFD) and a *Reduced Function Device* (RFD).
- The FFDs are capable of playing the role of a *network coordinator*, but RFDs are not. FFDs can talk to any other device, while RFDs can only talk to an FFD.
- Thus, one mode of operation of the IEEE 802.15.4 MAC is based on a hierarchy of nodes, with one FFD and several RFDs connected in a *star* topology as shown in following figure.



- The FFD at the hub, which is a network coordinator, plays the role of a cluster-head, and all communication is controlled by it. In the *peer-to-peer* topology, however, all nodes are equally capable; all are FFDs.



The Zigbee MAC superframe structure. CAP and CFP stand for Contention Access Period and Contention Free Period, respectively. GTS means Guaranteed Time Slot.

- The above Figure shows the super frame structure defined for IEEE 802.15.4. The super frame begins with a beacon.
- Nodes hearing the beacon can set their local clocks appropriately, so that they go to sleep and wake up at the same time. This means *synchronized operation*.
- The superframe is divided into an *active* and an *inactive* period. During the inactive period, nodes sleep.
- The active period consists of at most three parts — beacon transmission interval, the *Contention Access Period* (CAP) and an optional *Contention Free Period* (CFP).
- During the CAP, nodes contend using slotted CSMA/CA, as in IEEE 802.11. In the CFP, a node can be allotted *Guaranteed Time Slots* (GTSs) by the network coordinator.
- Nodes request for GTS allocation by sending explicit GTS allocation *requests*. Transmitted frames are always followed by *Inter-Frame Spacings*.

12. Briefly explain about function computation in MANETs.

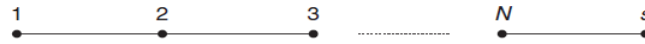
- Let us imagine a situation where N sensors have been distributed uniformly and independently in a square area A .
- These sensors have self-organized to form a network. In particular, the transmission range of each has been set to a value $r_c(N)$ such that the network $G(N, r_c(N))$ is connected asymptotically; the probability that $G(N, r_c(N))$ is connected goes to 1 as N goes to infinity. As we have seen before, this will happen when

$$r_c(N) = \sqrt{\frac{\ln N + c(N)}{\pi N}} \quad \text{with } \limsup_{N \rightarrow \infty} c(N) = \infty.$$

- The sensors make periodic measurements. There is a single sink in the network where some function of the sensors' measurements is to be computed. The function, in general, would depend on the inference problem that the sensor network has been designed to solve. For example, in an event-detection application, the function could be the conditional probability of the sensor output being in a certain range, given that there has been no event (the null hypothesis). In statistics, such a function is referred to as a likelihood function, and it is extensively used in event detection.
- One naive way to compute the function is to forward all the measured data to the sink, which then computes the function. This is a centralized model of computation. However, this fails to

take advantage of the processing capability of the sensors. An alternative approach is in network processing, where the sensors compute intermediate results and forward these to the sink. This aggregation helps in reducing the amount of data to be forwarded to the sink, and thus helps in easing congestion as well as prolonging battery life.

- For example, consider a linear network of $(N + 1)$ sensors as shown in Figure, with s denoting the sink. Suppose that each sensor measures the temperature in its neighborhood and the objective is to compute the maximum temperature. If all measurements are simply forwarded to the sink, then the communication effort is $O(N^2)$; sensor 1 data requires N hops to reach the sink, sensor 2 data requires $(N - 1)$ hops, and so on. On the other hand, an alternate strategy is one in which node i compares received data with its own measurement and forwards the maximum of the two. In this strategy, in-network processing is being done, and the communication effort drops to just $O(N)$.



A linear network of $(N + 1)$ sensors is shown. Each sensor makes measurements, and the maximum of all measurements is desired at the sink s .

- Suppose that the N sensors make periodic measurements. Let each sensor reading belong to a discrete set χ . Let time be slotted. $\mathbf{X}(t)$ denotes the vector of N sensor readings at discrete time slot t . Let us also assume that readings over a period $t = 1, 2, \dots, T$ are available with each sensor; here T is the block length over which measurements have been collected. The $N \times T$ matrix \mathbf{X} represents the complete data set, across sensors as well as across the block length, that is available. \mathbf{X}_i , the i -th row of the matrix, represents the readings of the i -th sensor over the block. Correspondingly, the t -th column $\mathbf{X}(t)$ represents the readings across the sensors at time t . The objective is to compute the function $f(\mathbf{X}(t))$, for every $t \in \{1, 2, \dots, T\}$.
- Generally, if C is a subset of sensors, then $f(\mathbf{X}(t))_C$ is the function computed by taking the readings of sensors in the set C at time t .
- We have tacitly assumed that the function to be computed admits distributed computation in a divide-and-conquer fashion, in which the result of a partial computation by some sensors is forwarded to others, which then repeat the process. To formally state the property that we assumed, we introduce the notion of *divisible functions*.
- Let C be a subset of $\{1, 2, \dots, N\}$, and let $\pi := \{C_1, C_2, \dots, C_s\}$ be a *partition* of C . The function $f(\cdot)$ is said to be divisible, if for any $C \subset \{1, 2, \dots, N\}$ and any partition $\pi = \{C_1, C_2, \dots, C_s\}$ of C , there exists a function $g(\pi)(\cdot)$ such that

$$f(\mathbf{X}_C^{(t)}) = g^{(\pi)}(f(\mathbf{X}_{C_1}^{(t)}), f(\mathbf{X}_{C_2}^{(t)}), \dots, f(\mathbf{X}_{C_s}^{(t)}))$$

- This says that if we know the values of the function $f(\cdot)$ evaluated over the sets in any partition π of C , then we can combine these values, using the function $g(\pi)(\cdot)$, to obtain $f(\cdot)$ evaluated over C . Thus, it is possible to compute $f(\mathbf{X}(t))_C$ in a divide-and-conquer fashion.

UNIT – V

Part - B

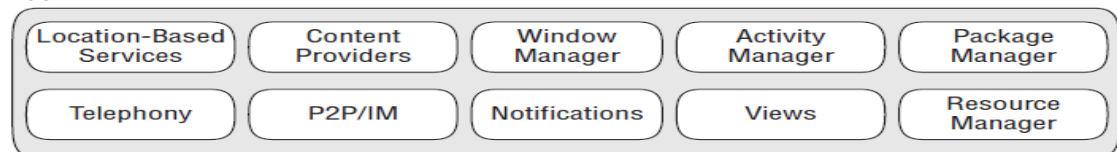
1. Explain in detail about Android software stack with a neat diagram.

- The Android software stack is composed of the elements shown in Figure 1-1 and described in further detail below it. Put simply, a Linux kernel and a collection of C/C++ libraries are exposed through an application framework that provides services for, and management of, the run time and applications.

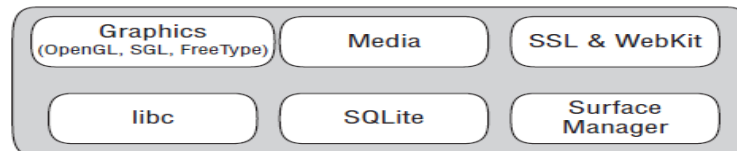
Application Layer



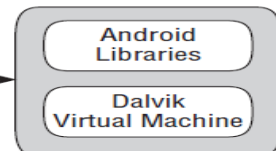
Application Framework



Libraries



Android Runtime



Linux Kernel

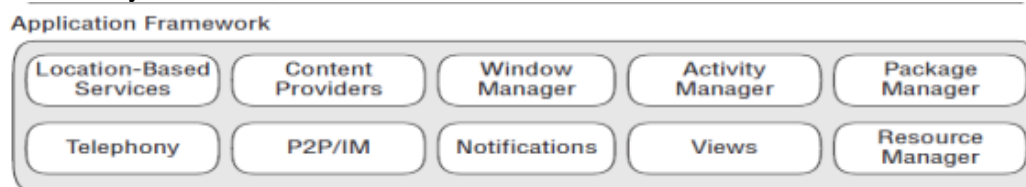


- Linux Kernel Core services (including hardware drivers, process and memory management, security, network, and power management) are handled by a Linux 2.6 kernel. The kernel also provides an abstraction layer between the hardware and the remainder of the stack.
- Libraries Running on top of the kernel, Android includes various C/C++ core libraries such as libc and SSL, as well as:
 - ❖ A media library for playback of audio and video media
 - ❖ A Surface manager to provide display management
 - ❖ Graphics libraries that include SGL and OpenGL for 2D and 3D graphics
 - ❖ SQLite for native database support
 - ❖ SSL and WebKit for integrated web browser and Internet security
- Android Run Time What makes an Android phone an Android phone rather than a mobile Linux implementation is the Android run time. Including the core libraries and the Dalvik virtual machine, the Android run time is the engine that powers your applications and, along with the libraries, forms the basis for the application framework.
 - ❖ Core Libraries While Android development is done in Java, Dalvik is not a Java VM. The core Android libraries provide most of the functionality available in the core Java libraries as well as the Android-specific libraries.
 - ❖ Dalvik Virtual Machine Dalvik is a register-based virtual machine that's been optimized to ensure that a device can run multiple instances efficiently. It relies on the Linux kernel for threading and low-level memory management.
- Application Framework The application framework provides the classes used to create Android applications. It also provides a generic abstraction for hardware access and manages the user interface and application resources.
- Application Layer All applications, both native and third party, are built on the application layer using the same API libraries. The application layer runs within the Android run time using the classes and services made available from the application framework.
- The Dalvik Virtual Machine

- ❖ One of the key elements of Android is the Dalvik virtual machine. Rather than use a traditional Java virtual machine (VM) such as Java ME (Java Mobile Edition), Android uses its own custom VM designed to ensure that multiple instances run efficiently on a single device.
- ❖ The Dalvik VM uses the device's underlying Linux kernel to handle low-level functionality including security, threading, and process and memory management. It's also possible to write C/C++ applications that run directly on the underlying Linux OS.
- ❖ All Android hardware and system service access is managed using Dalvik as a middle tier. By using a VM to host application execution, developers have an abstraction layer that ensures they never have to worry about a particular hardware implementation.
- ❖ The Dalvik VM executes Dalvik executable files, a format optimized to ensure minimal memory footprint. The .dex executables are created by transforming Java language compiled classes using the tools supplied within the SDK.

2. Explain in detail about Android application architecture.

- Android's architecture encourages the concept of component reuse, allowing us to publish and share activities, services, and data with other applications with access managed by the security restrictions you put in place.
- The same mechanism that lets us to produce a replacement contact manager or phone dialer for exposing our application components to let other developers create new UI front ends and functionality extensions, or otherwise build on them.

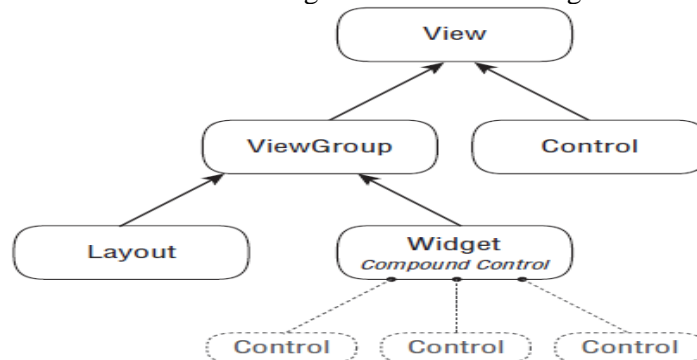


- The following application services are the architectural cornerstones of all Android applications, providing the framework.
 - ❖ **Activity Manager** Controls the life cycle of our activities, including management of the activity stack.

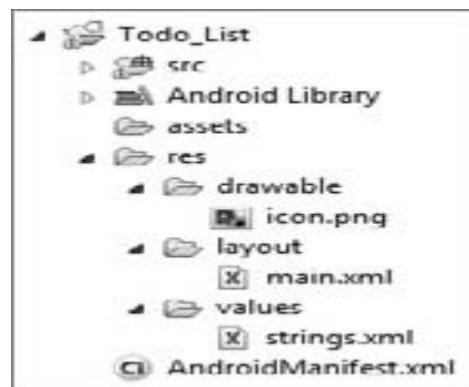
Functions of Activity Manager :

- Interact with the overall activities running in the system.
- The state of each Activity is determined by its position on the Activity stack, a last-in–first-out collection of all the currently running Activities.
- Android applications do not control their own process lifetimes; the **Android run time** manages the process of each application, and by extension that of each Activity within it. While the run time handles the termination and management of an Activity's process, the Activity's state helps determine the priority of its parent application.
- The application priority, in turn, influences the likelihood that the run time will terminate it and the Activities running within it.
- ❖ **Views** are used to construct the user interfaces for our activities.
 - This class represents the basic building block for user interface components. A View occupies a rectangular area on the screen and is responsible for drawing and event handling.
 - View is the base class for *widgets*, which are used to create interactive UI components (buttons, text fields, etc.).
 - The ViewGroup subclass is the base class for *layouts*, which are invisible containers that hold other Views (or other ViewGroups) and define their layout properties.
 - All of the views in a window are arranged in a single tree.

- By convention, a control usually refers to an extension of Views that implements relatively simple functionality, while a widget generally refers to both compound controls and more complex extensions of Views.
- The conventional naming model is shown in Figure



- ❖ **Notification Manager** Provides a consistent and non-intrusive mechanism for signaling our users.
 - Notifications represent a more robust mechanism for alerting users. For many users, when they're not actively using their mobile phones, they sit silent and unwatched in a pocket or on a desk until it rings, vibrates, or flashes.
 - Should a user miss these alerts, status bar icons are used to indicate that an event has occurred. All of these attention-grabbing antics are available within Android as Notifications.
- ❖ **Content Providers** Lets our applications share data between applications.
 - Content Providers are a generic interface mechanism that lets you share data between applications. By abstracting away the underlying data source, Content Providers let you decouple your application layer from the data layer, making our applications data-source agnostic.
 - Content Providers feature full permission control and are accessed using a simple URI model. Shared content can be queried for results as well as supporting write access. As a result, any application with the appropriate permissions can add, remove, and update data from any other applications — including some native Android databases.
 - Many of the native databases have been made available as Content Providers, accessible by third-party applications. This means that your applications can have access to the phone's Contact Manager, media player, and other native database once they've been granted permission.
 - By publishing our own data sources as Content Providers, we make it possible for us (and other developers) to incorporate and extend our data in new applications.
- ❖ **Resource Manager** Supports non-code resources like strings and graphics to be externalized.
 - Application resources are stored under the res/ folder of your project hierarchy. In this folder, each of the available resource types can have a subfolder containing its resources.
 - If we start a project using the ADT wizard, it will create a res folder that contains subfolders for the values, drawable, and layout resources that contain the default layout, application icon, and string resource definitions, respectively, as shown in Figure .



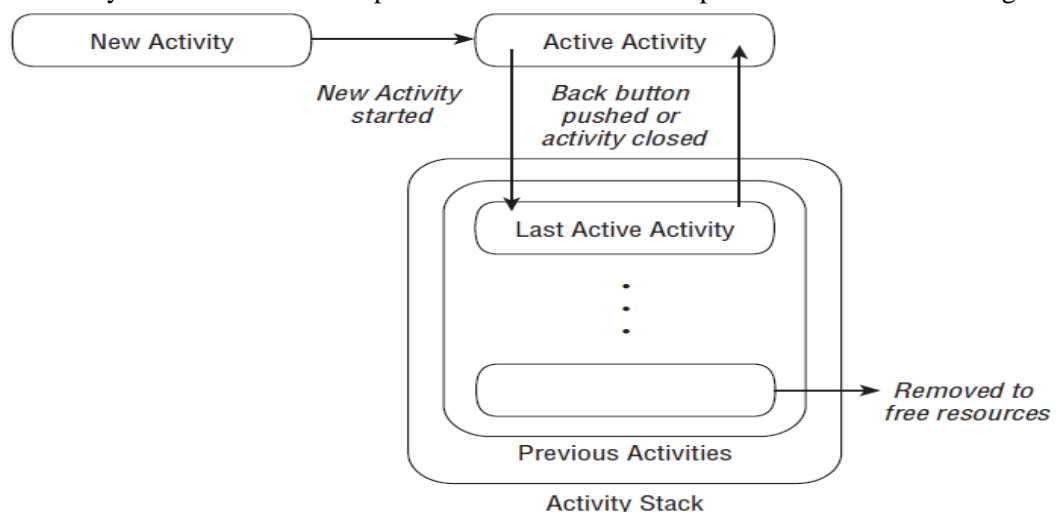
- There are seven primary resource types that have different folders: simple values, drawables, layouts, animations, XML, styles, and raw resources.
 - When our application is built, these resources will be compiled as efficiently as possible and included in our application package.
 - This process also creates an R class file that contains references to each of the resources we include in our project.
- ❖ **Location-based services (LBS)** is an umbrella term used to describe the different technologies used to find the device's current location. The two main LBS elements are:
- **LocationManager** Provides hooks to the location-based services.
 - **LocationProviders** Each of which represents a different location-finding technology used to determine the device's current location.

3. Explain in detail about activity life cycle in android .

- Android applications do not control their own process lifetimes; the **Android run time** manages the process of each application, and by extension that of each Activity within it. While the run time handles the termination and management of an Activity's process, the Activity's state helps determine the priority of its parent application.
- The application priority, in turn, influences the likelihood that the run time will terminate it and the Activities running within it.

Activity Stacks

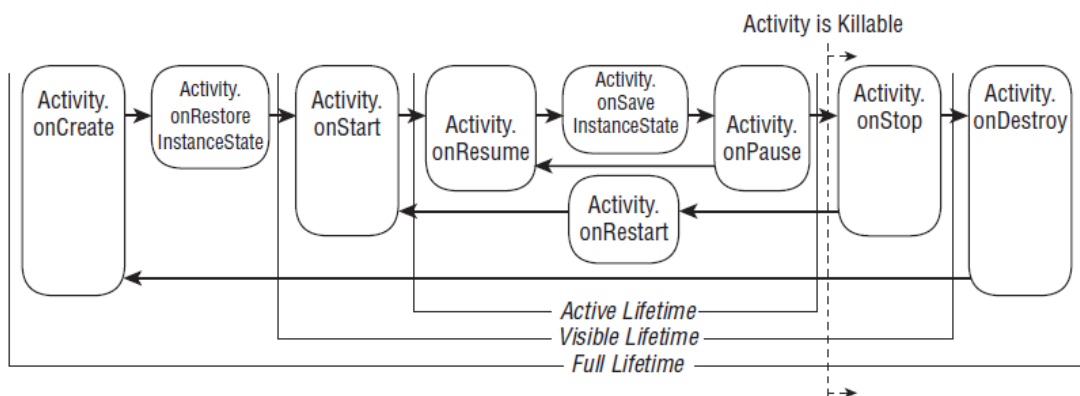
- The state of each Activity is determined by its position on the Activity stack, a last-in–first-out collection of all the currently running Activities. When a new Activity starts, the current foreground screen is moved to the top of the stack.
- If the user navigates back using the Back button, or the foreground Activity is closed, the next Activity on the stack moves up and becomes active. This process is illustrated in Figure.



- An application's priority is influenced by its highest-priority Activity. The Android memory manager uses this stack to determine the priority of applications based on their Activities when deciding which application to terminate to free resources.
 - ❖ **Active** : When an Activity is at the top of the stack, it is the visible, focused, foreground activity that is receiving user input. Android will attempt to keep it alive at all costs, killing Activities further down the stack as needed, to ensure that it has the resources it needs. When another activity becomes active, this one will be paused.
 - ❖ **Paused** : In some cases, your Activity will be visible but will not have focus; at this point, it's paused. This state is reached if a transparent or non-full-screen Activity is active in front of it. When paused, an Activity is treated as if it were active; however, it doesn't receive user input events. In extreme cases, Android will kill a paused Activity to recover resources for the active Activity. When an Activity becomes totally obscured, it becomes stopped.
 - ❖ **Stopped** : When an Activity isn't visible, it "stops." The Activity will remain in memory retaining all state and member information; however, it is now a prime candidate for execution when the system requires memory elsewhere. When an Activity is stopped, it's important to save data and the current UI state. Once an Activity has exited or closed, it becomes inactive.
 - ❖ **Inactive** : After an Activity has been killed, and before it's been launched, it's inactive. Inactive Activities have been removed from the Activity stack and need to be restarted before they can be displayed and used.
- State transitions are nondeterministic and are handled entirely by the **Android memory manager**. Android will start by closing applications that contain inactive Activities, followed by those that are stopped, and in extreme cases, it will remove those that are paused.

Monitoring State Changes

To ensure that Activities can react to state changes, Android provides a series of event handlers that are fired when an Activity transitions through its full, visible, and active lifetimes. The following figure summarizes these lifetimes in terms of the Activity states described above.



- Within an Activity's full lifetime, between creation and destruction, it will go through one or more iterations of the active and visible lifetimes. Each transition will trigger the method handlers.
- onCreate(Bundle)** – called when the Activity is created; using the method argument you can restore the Activity state that has been saved from a previous session; once the Activity has been created is going to be started (`onStart()`);
- onStart()** – called when the Activity is going to be displayed; from this point the Activity can come to the foreground (`onResume()`) or stay hidden (`onStop()`);
- onRestoreInstanceState(Bundle)** – called when the Activity is initialized with data from a previous saved state; by default, the system restores the state of the user interface;
- onResume()** – called when the Activity is visible and the user can interact with it; from this state, the Activity can go in the background becoming paused (`onPause()`);

- **onRestart()** – called when the Activity is going back to the foreground from a stopped state; after that, the Activity is started (*onStart()*) once again;
- **onPause()** – called when the system is bringing into the foreground another Activity; the current Activity is set into the background and later it may be stopped (*onStop()*) or resumed and displayed (*onResume()*); this is a good moment to save application data to a persistent storage (files, database)
- **onSaveInstanceState(Bundle)** – called to save the Activity state; by default, the system saves the state of the user interface;
- **onStop()** – called when the Activity is not longer used and not visible as another Activity is interacting with the user; from this point, the Activity can be restarted (*onRestart()*) or destroyed (*onDestroy()*);
- **onDestroy()** – called when the Activity is deleted and its memory released; this can happen if the system requires more memory or if the programmer terminates it by calling the Activity *finish()* method;

Activity Lifetimes

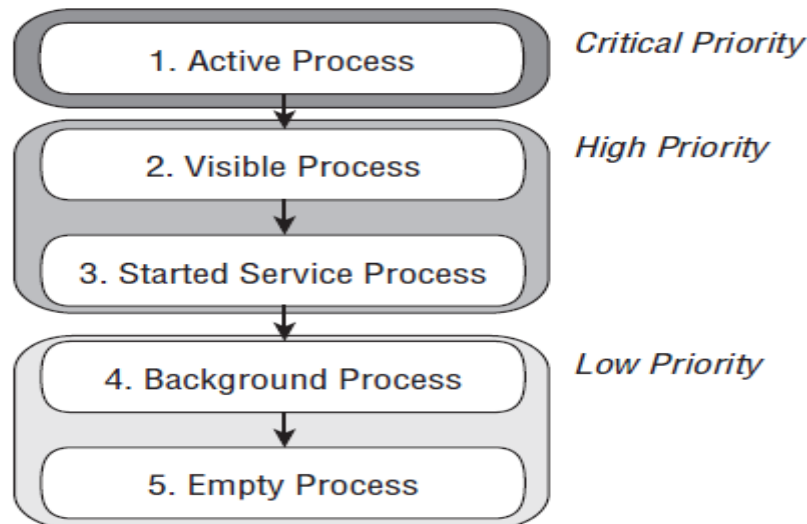
- **The full lifetime** of our Activity occurs between the first call to *onCreate* and the final call to *onDestroy*. It's possible, in some cases, for an Activity's process to be terminated without the *onDestroy* method being called.
- **An Activity's visible lifetimes** are bound between calls to *onStart* and *onStop*. Between these calls, our Activity will be visible to the user, although it may not have focus and might be partially obscured. Activities are likely to go through several visible lifetimes during their full lifetime, as they move between the foreground and background.
- **The active lifetime** starts with a call to *onResume* and ends with a corresponding call to *onPause*. An active Activity is in the foreground and is receiving user input events. our Activity is likely to go through several active lifetimes before it's destroyed

4. Explain in detail about Android application life cycle.

- Android applications have no control over their own life cycles. Instead, application components must listen for changes in the application state and react accordingly, taking particular care to be prepared for untimely termination.
- By default, each Android application is run in its own process that's running a separate instance of Dalvik. Memory and process management of each application is handled exclusively by the run time.

Application Priority and Process States

- The order in which processes are killed to reclaim resources is determined by the priority of the hosted applications. An application's priority is equal to its highest-priority component.
- Where two applications have the same priority, the process that has been at a lower priority longest will be killed first. Process priority is also affected by inter process dependencies; if an application has a dependency on a Service or Content Provider supplied by a second application, the secondary application will have at least as high a priority as the application it supports.
- All Android applications will remain running and in memory until the system needs its resources for other applications.



- **Active Processes** :Active (foreground) processes are those hosting applications with components currently interacting with the user. These are the processes Android is trying to keep responsive by reclaiming resources. There are generally very few of these processes, and they will be killed only as a last resort.
 - ❖ Active processes include:
 - ❖ Activities in an “active” state; that is, they are in the foreground and responding to user events.
 - ❖ Activities, Services, or Broadcast Receivers that are currently executing an onReceive event handler.
 - ❖ Services that are executing an onStart, onCreate, or onDestroy event handler.
 - **Visible Processes** Visible, but inactive processes are those hosting “visible” Activities. As the name suggests, visible Activities are visible, but they aren’t in the foreground or responding to user events. This happens when an Activity is only partially obscured (by a non-full-screen or transparent Activity). There are generally very few visible processes, and they’ll only be killed in extreme circumstances to allow active processes to continue.
 - **Started Service Processes** : Processes hosting Services that have been started. Services support ongoing processing that should continue without a visible interface. Because Services don’t interact directly with the user, they receive a slightly lower priority than visible Activities. They are still considered to be foreground processes and won’t be killed unless resources are needed for active or visible processes.
 - **Background Processes** : Processes hosting Activities that aren’t visible and that don’t have any Services that have been started are considered background processes. There will generally be a large number of background processes that Android will kill using a last-seen-first-killed pattern to obtain resources for foreground processes.
 - **Empty Processes** To improve overall system performance, Android often retains applications in memory after they have reached the end of their lifetimes. Android maintains this cache to improve the start-up time of applications when they’re re-launched. These processes are routinely killed as required.
5. Develop a mobile application for a small game.
 6. Develop a mobile application for a clock.
 7. Develop a mobile application for a calendar.
 8. Develop a mobile application for a convertor.
 9. Develop a mobile application for a phone book.
 10. Develop a mobile application for a Text Editor.