Unit I Part-A

1. What is mobile computing?

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

2. Distinguish between mobile computing and wireless networking

Mobile computing	Wireless networking
Mobile computing refers to computing devices that are not restricted to a desktop. A mobile device may be a PDA, a smart phone or a web phone, a laptop computer, or any one of numerous other devices that allow the user to complete tasks without being tethered, or connected, to a network. Accessing information and remote computational service while on the move.	Wireless refers to the method of transferring information between a computing device, and a data source, such as an agency database server, without a physical connection

3. What are the different characteristics of mobile computing?

- Ubiquity
- Location awareness:
- Adaptation
- Broadcast
- Personalization

4. Define ubiquity

In the context of mobile computing, ubiquity means the ability of a user to perform computations from anywhere and at anytime.

5. What is meant by Adaptation?

Adaptation in the context of mobile computing implies the ability of a system to adjust to bandwidth fluctuation without inconveniencing the user.

6. What is personalization?

Services in a mobile environment can be easily personalized according to a users profile. This is required to let the users easily avail information with their hand-held devices.

7. Give different types of mobile computing applications

- Presentation (Tier-1): It is a user inferface. It includes web browsers and customizes client program for dissimination of information and for collection of data from the user.
- Application(Tier-2):vital responsibility of making logical decisios and performing calculations
- Data(Tier-3):Basic facilites of data storage,access and manipulation

8. What is meant by MAC Protocols?

When an IP packet reaches its destination (sub)network, the destination IP address (a layer 3 or network layer concept) is resolved with the Address Resolution Protocol for IPv4, or by Neighbor Discovery Protocol (IPv6) into the MAC address (a layer 2 concept) of the destination host.

9. What are the different features of MAC Protocols

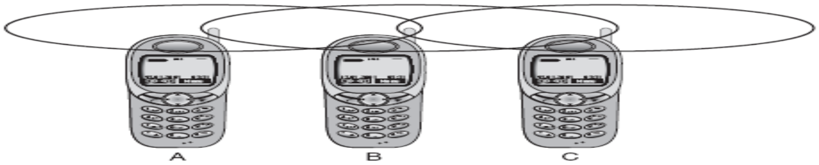
- It should implement some rules that help to enforce discipline when multiple nodes contend for a shared channel.
- It should help maximize the utilization of the channel
- Channel allocation needs to be fair.
- It should be capable of supporting several types of traffic having different maximum and average bit rates.

10. What is Hidden 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

11. Write the three types of MAC protocol

Fixed assignment scheme: resource required for a call are assigned for the entire duration of the call

Random assignment scheme: reservation schemes are called packet switched scheme. No reservations are made. ALOHA, Slotted ALOHA, CSMA, CSMA/CD, CSMA/CA

Reservation based scheme: a node makes explicit reservation of the channel for an entire call before transmitting

12. What are the categories of Fixed assignment Mac protocols (Nov 2013)

- Frequency Division Multiple Access(FDMA)
- Time Division Multiple Access(TDMA)
- Code division Multiple Access(CDMA)

13. What is ALOHA?

Aloha, also called the Aloha method, refers to a simple communications scheme in which each source (transmitter) in a network sends data whenever there is a frame to send. If the frame successfully reaches the destination (receiver), the next frame is sent. If the frame fails to be received at the destination, it is sent again.

14. How performance is improved in CSMA/CD protocol compared to CSMA protocol?

In CSMA scheme, a station monitors the channel before sending a packet. Whenever a collision is detected, it does not stop transmission leading to some wastage of time. On the other hand, in CSMA/CD scheme, whenever a station detects a collision, it sends a jamming signal by which other station comes to know that a collision occurs. Wastage of time is reduced leading to improvement in performance.

15. What is meant by FDMA?

FDMA is a channel access method used in multiple-access protocols as a channelization protocol. FDMA gives users an individual allocation of one or several frequency bands, or channels. It is particularly commonplace in satellite communication.

16. Define TDMA

Time division multiple access (TDMA) is a channel access method for shared medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots. The users transmit in rapid succession, one after the other, each using its own time slot.

17. What is CDMA? (Nov 2013)

Code Division Multiple Access (CDMA) is a channel access method used by various radio communication technologies. CDMA is an example of multiple access, where several transmitters can send information simultaneously over a single communication channel.

18. What is the difference between Infrastructure and Adhoc Modes?

- Infrastructure mode- Devices on the network all communicate through a single access point, which is generally the wireless router.
- Ad-hoc mode –It is also known as “peer-to-peer” mode. Ad-hoc networks don’t require a centralized access point. Instead, devices on the wireless network connect directly to each other.

19. What is reservation based scheme

It is by RTS/CTS scheme. A sender transmits an RTS(Ready to send) packet to the receiver before the actual data transmission. On receiving this, the receiver sends CTS (Clear to send) packet and the actual data transfer commence only after that**.**

20. What is meant by MACA?

Multiple Accesses with Collision Avoidance (MACA) is a slotted media access control protocol used in wireless LAN data transmission to avoid collisions caused by the hidden station problem and to simplify exposed station problem.

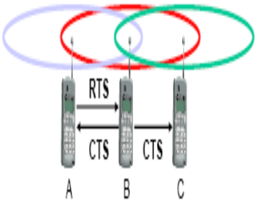
21. What is the use of RTS and CTS?

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



22. How exposed terminal problem is solved in MACA

Assume B needs to transmit to A. B has to transmit RTS. The RTS would contain the names of the receiver (A) and the sender(B) . C does not act in response to this message as it is not the receiver. But A responds with a CTS. C does not receive this CTS and conclude that A is outside the detection range.. Thus C can start its transmission assuming that no collision would occur at A.

Part B UNIT I

What is mobile computing? Mention the characteristics and applications of mobile computing

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

characteristics of mobile computing

- Ubiquity
- Location awareness:
- Adaptation
- Broadcast
- Personalization

Applications

In many fields of work, the ability to keep on the move is vital in order to utilise time efficiently. The importance of Mobile Computers has been highlighted in many fields of which a few are described below:

1. **Vehicles:** Music, news, road conditions, weather reports, and other broadcast information are received via digital audio broadcasting (DAB) with 1.5 Mbit/s. For personal communication, a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity with 384 kbit/s. The current position of the car is determined via the global positioning system (GPS). Cars driving in the same area build a local ad-hoc network for the fast exchange of information in emergency situations or to help each other keep a safe distance. In case of an accident, not only will the airbag be triggered, but the police and ambulance service will be informed via an emergency call to a service provider. Buses, trucks,

   and trains are already transmitting maintenance and logistic information to their home base, which helps to improve organization (fleet management), and saves time and money.
2. **Emergencies**: An ambulance with a high-quality wireless connection to a hospital can

carry vital information about injured persons to the hospital from the scene of the accident. All the necessary steps for this particular type of accident can be prepared and specialists can be consulted for an early diagnosis. Wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquakes. In the worst cases, only decentralized, wireless ad-hoc networks survive.

3. **Business**: Managers can use mobile computers say, critical presentations to major customers. They can access the latest market share information. At a small recess, they can revise the presentation to take advantage of this information. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can leverage competitive advantages. A travelling salesman today needs instant access to the company's database: to ensure that files on his or her laptop reflect the current situation, to enable the company to keep track of all activities of their travelling employees, to keep databases consistent etc. With wireless access, the laptop can be turned into a true mobile office, but efficient and powerful synchronization mechanisms are needed to ensure data consistency.

4. **Credit Card Verification**: At Point of Sale (POS) terminals in shops and Supermarkets, when customers use credit cards for transactions, the intercommunication required between the bank central computer and the POS terminal, in order to effect verification of the card usage, can take place quickly and securely over cellular channels using a mobile computer unit. This can speed up the transaction process and relieve congestion at the POS terminals.

5. **Replacement of Wired Networks**: wireless networks can also be used to replace wired networks, e.g., remote sensors, for tradeshows, or in historic buildings. Due to economic reasons, it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information. Wireless connections, e.g., via satellite, can help in this situation. Other examples for wireless networks are computers, sensors, or information displays in historical buildings, where excess cabling may destroy valuable walls or floors.

6. **Infotainment**: wireless networks can provide up-to-date information at any appropriate location. The travel guide might tell you something about the history of a building (knowing via GPS, contact to a local base station, or triangulation where you are) downloading information about a concert in the building at the same evening via a local wireless network. Another growing field of wireless network applications lies in entertainment and games to enable, e.g., ad-hoc gaming networks as soon as people meet to play together.

2. **Distinguish between mobile computing and wireless networking explain briefly?**

Mobile is a word that is commonly used to describe portable devices. A mobile device is one that is made to be taken anywhere. Therefore, it needs an internal battery for power, and must be connected to a modern mobile network that can help it to send and receive data without attaching to a hardware infrastructure.

Wireless, on the other hand, does not mean mobile. Traditional computers or other non-mobile devices can access wireless networks. One very common example is the use of a localized browser product in a local area network (LAN), where the router takes what used to be a cabled interaction and makes it wireless. Other kinds of wireless networks called wide area networks (WAN) can even use components of 3G or 4G wireless systems made specifically for mobile devices, but that doesn't mean that the devices on these networks are mobile. They may still be plugged in or require proximity to a router or network node.

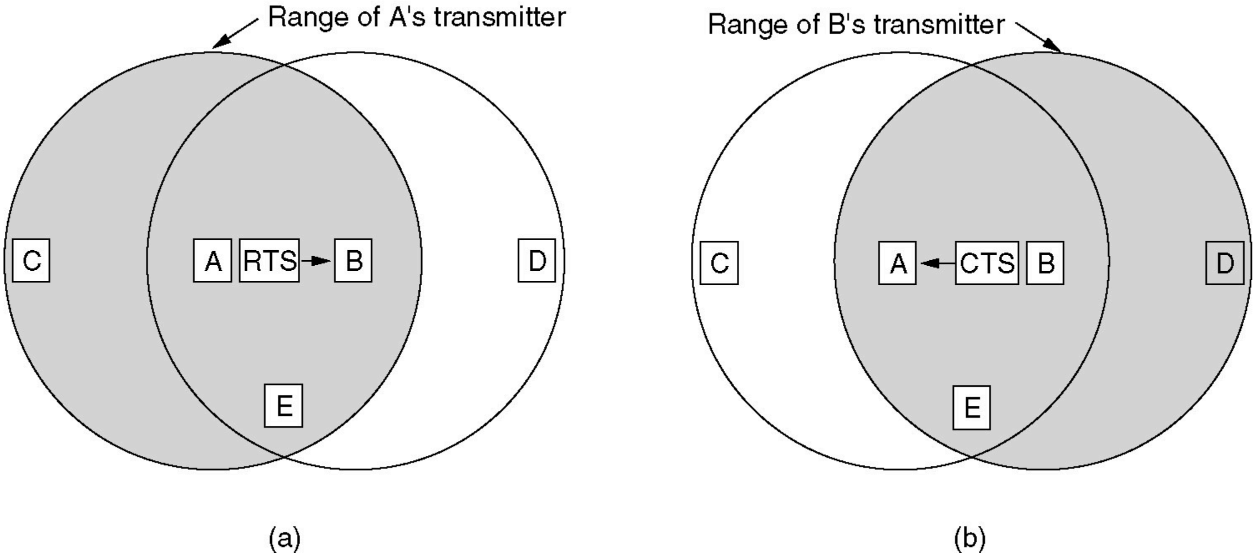
Mobile and wireless systems really accomplish two very different things. While a wireless system provides a fixed or portable endpoint with access to a distributed network, a mobile system offers all of the resources of that distributed network to something that can go anywhere, barring any issues with local reception or technical area coverage.

For another example of the difference between mobile and wireless, think of businesses that offer Wi-Fi hotspots. A Wi-Fi hotspot is typically a resource for someone who has a relatively fixed device, such as a laptop computer that doesn't have its own internal Internet access built in. By contrast, mobile devices already have inherent access to the Internet or other wireless systems through those cell tower networks that ISPs and telecom companies built specifically for them. So mobile devices don't need Wi-Fi - they already have their connections.

- **Wireless links**: unique channel characteristics
  - High, time-varying bit-error rate
  - Broadcast where some nodes can't hear each other
- **Mobile hosts**: addressing and routing challenges
  - Keeping track of the host's changing attachment point
  - Maintaining a data transfer as the host moves
  - Two specific technologies
  - Wireless: 802.11 wireless LAN (aka "WiFi")
  - Mobility: Mobile IP

3. **Explain the working of a contention based MAC protocol. Give two examples of contention based MAC Protocols.**

- Contention-based protocols with scheduling mechanisms
  - Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.
  - Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.
  - Some scheduling schemes also consider battery characteristics.
- MACAW: A Media Access Protocol for Wireless LANs is based on MACA (Multiple Access Collision Avoidance) Protocol
- **MACA**
  - When a node wants to transmit a data packet, it first transmit a **RTS** (**Request To Send)** frame.
  - The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a **CTS (Clear to Send)** packet.
  - Once the sender receives the CTS packet without any error, it starts transmitting the data packet.
  - If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying.
- The binary exponential back-off mechanism used in MACA might starves flows sometimes. The problem is solved by MACAW.



The MACA protocol. (a) A sending an RTS to B. (b) B responding with

- Variants of this method can be found in IEEE 802.11 as DFWMAC (Distributed Foundation Wireless MAC),
- **MACAW (MACA for Wireless) is a revision of MACA**.
  - The sender senses the carrier to see and transmits a **RTS** (**Request To Send)** frame if no nearby station transmits a RTS.
  - The receiver replies with a **CTS** (**Clear To Send**) frame.
  - Neighbors
    - see CTS, then keep quiet.
    - see RTS but not CTS, then keep quiet until the CTS is back to the sender.
  - The receiver sends an ACK when receiving an frame.
    - Neighbors keep silent until see ACK.
  - Collisions
    - There is no collision detection.
    - The senders know collision when they don't receive CTS.
    - They each wait for the exponential backoff time.
- **Floor acquisition Multiple Access Protocols (FAMA)**
  - Based on a channel access discipline which consists of a carrier-sensing operation and a collision-avoidance dialog between the sender and the intended receiver of a packet.
  - Floor acquisition refers to the process of gaining control of the channel. At any time only one node is assigned to use the channel.
  - Carrier-sensing by the sender, followed by the RTS-CTS control packet exchange, enables the protocol to perform as efficiently as MACA.
  - Two variations of FAMA
    - RTS-CTS exchange with no carrier-sensing uses the ALOHA protocol for transmitting RTS packets.
    - RTS-CTS exchange with non-persistent carrier-sensing uses non-persistent CSMA for the same purpose.
- **Busy Tone Multiple Access Protocols (BTMA)**
  - The transmission channel is split into two:
    - a data channel for data packet transmissions

  - a control channel used to transmit the busy tone signal
- When a node is ready for transmission, it senses the channel to check whether the busy tone is active.
  - If not, it turns on the busy tone signal and starts data transmissions
  - Otherwise, it reschedules the packet for transmission after some random rescheduling delay.
  - Any other node which senses the carrier on the incoming data channel also transmits the busy tone signal on the control channel, thus, prevent two neighboring nodes from transmitting at the same time.

- **Dual Busy Tone Multiple Access Protocol (DBTMAP)** is an extension of the BTMA scheme.
  - a data channel for data packet transmissions
  - a control channel used for control packet transmissions (RTS and CTS packets) and also for transmitting the busy tones.
- **Receiver-Initiated Busy Tone Multiple Access Protocol (RI-BTMA)**
  - The transmission channel is split into two:
    - a data channel for data packet transmissions
    - a control channel used for transmitting the busy tone signal
  - A node can transmit on the data channel only if it finds the busy tone to be absent on the control channel.
  - The data packet is divided into two portions: a preamble and the actual data packet.
- **MACA-By Invitation (MACA-BI)** is a receiver-initiated MAC protocol.
  - By eliminating the need for the RTS packet it reduces the number of control packets used in the MACA protocol which uses the three-way handshake mechanism.

Media Access with Reduced Handshake (MARCH) is a receiver-initiated protocol.

4. **Name one MAC protocol that is used in mobile adhoc networks. Briefly explain its working** (April 2014)

5. **What is FDMA? Briefly explain its working and its important applications**

- FDMA (Frequency Division Multiple Access)
  - assign a certain frequency to a transmission channel between a sender and a receiver
  - permanent (e.g., radio broadcast), slow hopping (e.g., GSM), fast hopping (FHSS, Frequency Hopping Spread Spectrum)
  - It deals with allocating frequencies to transmission channels according to the Frequency Division Multiplexing (FDM).
  - Allocation can be either, Fixed, or Dynamic (demand driven)

Techniques of FDMA

(i) **Pure FDMA:** Channels assigned to the **same frequency** at all times.

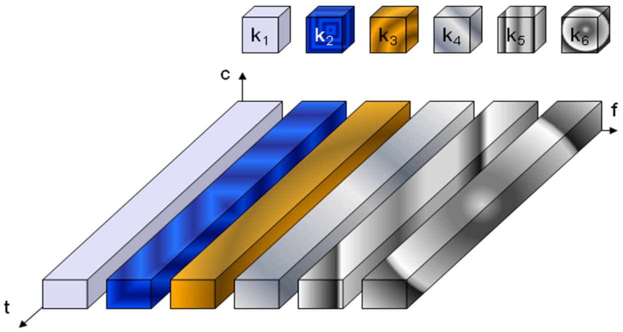
(ii) **FDMA / TDMA:** Assigning **different frequencies** according to a certain pattern.

Frequency hopping:

- Narrow band interference at certain frequencies known **as frequency hopping.**

  - Sender and receiver must agree on a hopping pattern

1.15.3. Diagram

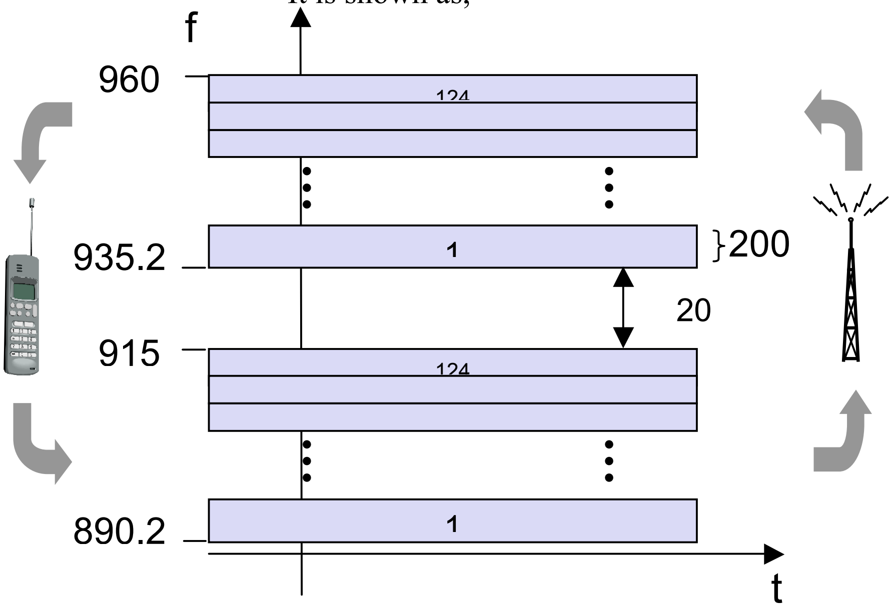


t-time,c-code,f-frequency,ki-channel

Assigning individual channel to each users.

1.15.4.Description

- FDM is generally used for simultaneous access to the medium by base station and mobile station in cellular networks.
- It is shown as,



FDD/FDMA - general scheme, example GSM

- The two partners establish **duplex channel, i.e.,** the simultaneous transmission in both directions.

❖ **FDD:**

  - If separate frequency is used for transmission from mobile station to base station and from base station to mobile station is said to be **Frequency Division Duplex (FDD).**
  - These two frequencies are termed as
    - **Uplink:** From mobile to base station, and
    - **Downlink:** From base to mobile station.

- Generally, up and down link have a fixed relation.
    - If uplink frequency is f_u = 890MHz + 0.2(n)MHz downlink frequency is f_d=f_u+45MHz.

- **Advantages:**
    - FDMA is more simpler than TDMA.
    - The bandwidths of channels are narrow.
- **Disadvantages:**
    - Cell site cost is higher.
    - Adjacent Channel Interference (ACI) is high.

6**. What is TDMA? Briefly explain its working and its important applications**

TDMA (Time Division Multiple Access)

- assign the fixed sending frequency to a transmission channel between a sender and a receiver for a certain amount of time

Features of TDMA

(i) Handoff process is very simple in TDMA.

(ii) TDMA shares a single carrier frequency

Various TDMA Techniques

The various TDMA Techniques are,

- Fixed TDM
- Classical ALOHA
- Slotted ALOHA
- CSMA
- DAMA
- PRMA
- Reservation TDMA
- MACA
- Polling
- ISMA

Fixed TDM

The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern. Fixed access patterns (at least fixed for some period in time) fit perfectly well for connections with a fixed bandwidth.

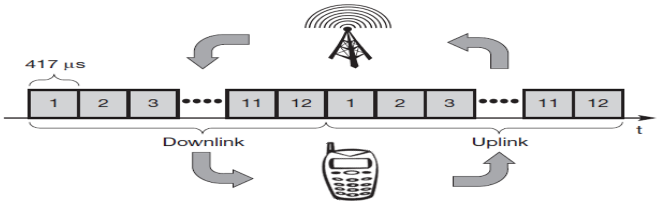
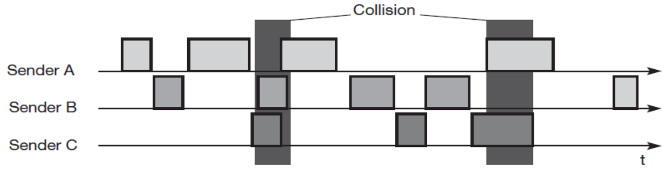


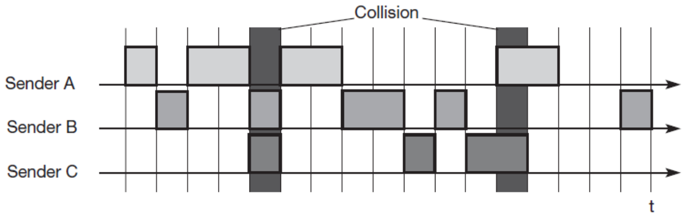
Figure shows how these fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station. Assigning different slots for uplink and downlink using the same frequency is called **time division duplex (TDD)**.Up to 12 different mobile stations can use the same frequency.The pattern is repeated every 10 ms, each slot has a duration of 417 µs

Classical Aloha

- Aloha: Each station can access the medium at any time - random, distributed (no central arbiter), time-multiplex
- Slotted Aloha additionally uses time-slots, sending must always start at slot boundaries



Slotted Aloha



Carrier sense multiple access

Channel efficiency only 18% for Aloha, 36% for Slotted Aloha (assuming Poisson distribution for packet arrival and packet length)

Protocols in which stations listen for a carrier (i.e. transmission) and act accordingly are called carrier sense protocols.

Non-persistent CSMA:

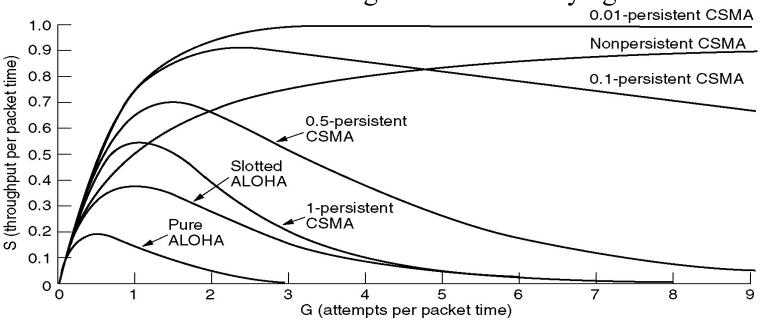
- Channel Busy - Wait for a random length of time and sense again.
- Channel Idle - Transmit.
- Collision - Wait for a random length of time and try again.

p-persistent CSMA:

- Channel Busy - Continue sensing until free (same as idle).
- Channel Idle - Transmit with probability p, and defer transmitting to the next slot with probability q = 1-p.
- Collision - Wait for a random length of time and try again.

1-persistent CSMA

- Channel Busy - Continue sensing until free and then grab.
- Channel Idle - Transmit with probability 1.
- Collision - Wait for a random length of time and try again.



Demand assigned multiple accessDAMA

Reservation can increase efficiency to 80%

- a sender reserves a future time-slot
- sending within this reserved time-slot is possible without collision
- reservation also causes higher delays under a light load but allow higher throughput
- typical scheme for satellite links

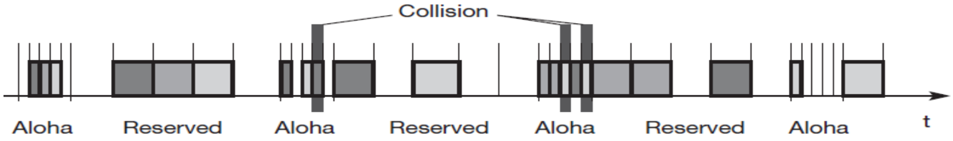
Examples for reservation algorithms:

- Explicit Reservation (Reservation-ALOHA)
- Implicit Reservation (PRMA)
- Reservation-TDMA

Explicit Reservation (Reservation Aloha):

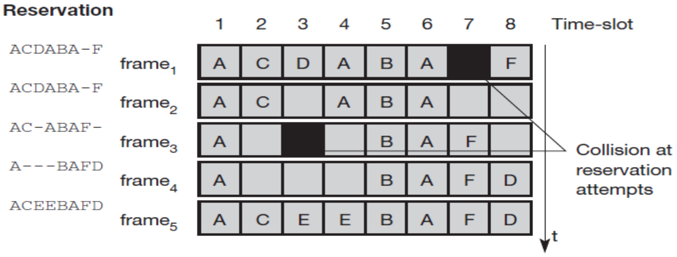
- two modes:

  - ✓ ALOHA mode for reservation:competition for small reservation slots, collisions possible
  - ✓ reserved mode for data transmission within successful reserved slots (no collisions possible)
- ❑ it is important for all stations to keep the reservation list consistent at any point in time and, therefore, all stations have to synchronize from time to time



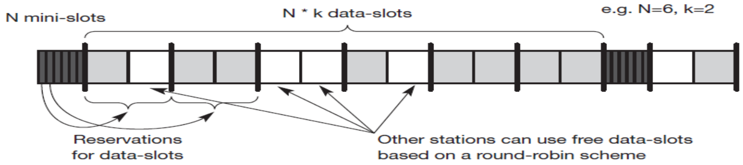
Implicit reservation (PRMA - Packet Reservation MA):

- ❑ a certain number of slots form a frame, frames are repeated
- ❑ stations compete for empty slots according to the slotted aloha principle
- ❑ once a station reserves a slot successfully, this slot is automatically assigned to this station in all following frames as long as the station has data to send
- ❑ competition for this slots starts again as soon as the slot was empty in the last frame



Reservation Time Division Multiple Access

- ❑ every frame consists of N mini-slots and x data-slots
- ❑ every station has its own mini-slot and can reserve up to k data-slots using this mini-slot (i.e. x = N * k).
- ❑ other stations can send data in unused data-slots according to a round-robin sending scheme (best-effort traffic)

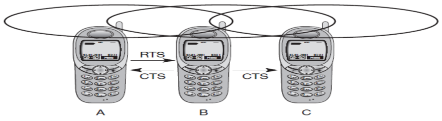

N mini-slots
N * k data-slots
e.g. N=6, k=2
Reservations for data-slots
Other stations can use free data-slots based on a round-robin scheme

MACA (Multiple Access with Collision Avoidance) uses short signaling 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 to send as soon as it is ready to receive

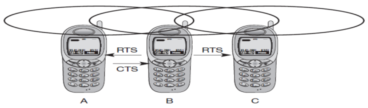
Signaling packets contain

- ❑ sender address
- ❑ receiver address
- ❑ packet size



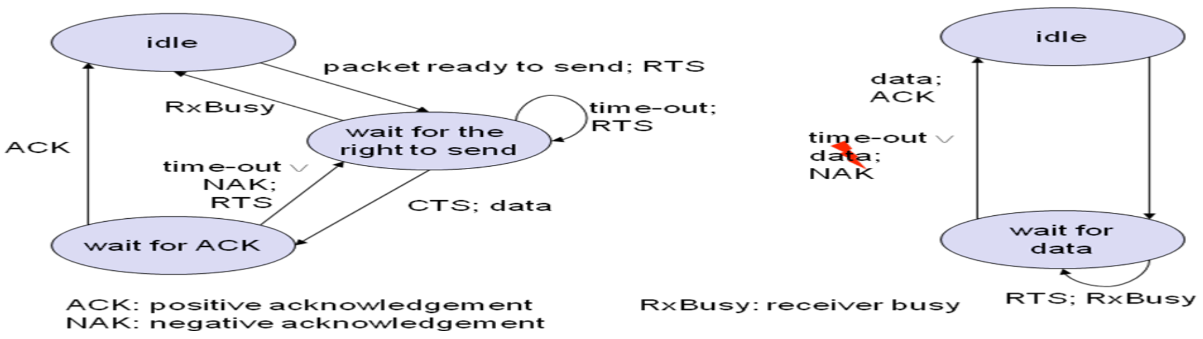
MACA avoids the problem of hidden terminals

- ❑ A and C want to send to B
- ❑ A sends RTS first
- ❑ C waits until it receives CTS from B



MACA avoids the problem of exposed terminals

- ❑ B wants to send to A, C
  to another terminal now C does not have to wait for it.it cannot receive CTS from A.



Polling

- When one station is to heard by all others, **Polling** scheme can be applied.
- The concept of polling is used in mainframe and terminals.
- Carried out by one master station over many slave stations.
- Many polling schemes are there such as Round-robin, Random and as per reservation patterns.

Inhibit sense multiple access

Another combination of different schemes is represented by **inhibit sense multiple access (ISMA)**. This scheme, which is used for the packet data transmission service. Cellular Digital Packet Data (CDPD) in the AMPS mobile phone system, is also known as **digital sense multiple access (DSMA)**. Here, the base station only signals a busy medium via a busy tone on the downlink .After the busy tone stops, accessing the uplink is not coordinated any further.

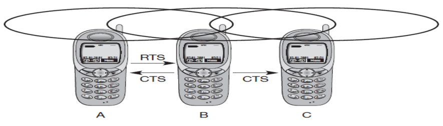
7. **What is MACA protocol? In which environment is it suitable? Briefly explain**

MACA (Multiple Access with Collision Avoidance) uses short signaling 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 to send as soon as it is ready to receive

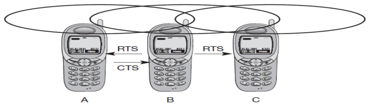
Signaling packets contain

- sender address
- receiver address
- packet size



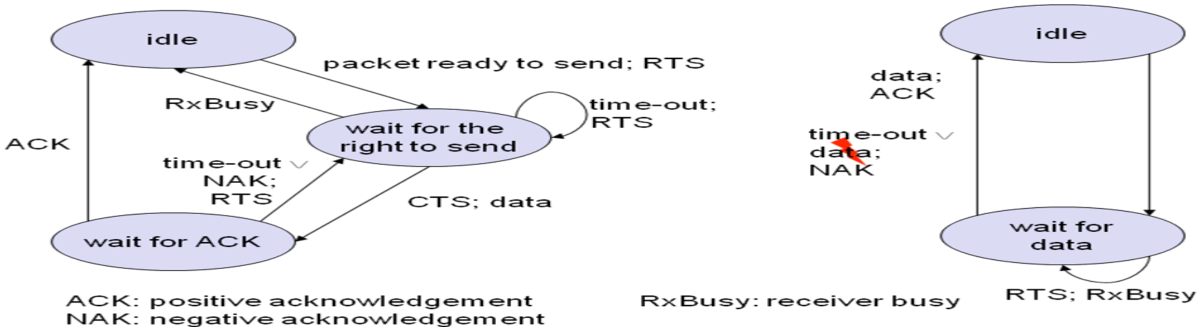
MACA avoids the problem of hidden terminals

- A and C want to send to B
- A sends RTS first
- C waits until it receives CTS from B



MACA avoids the problem of exposed terminals

- B wants to send to A, C to another terminal now C does not have to wait for it.it cannot receive CTS from A.



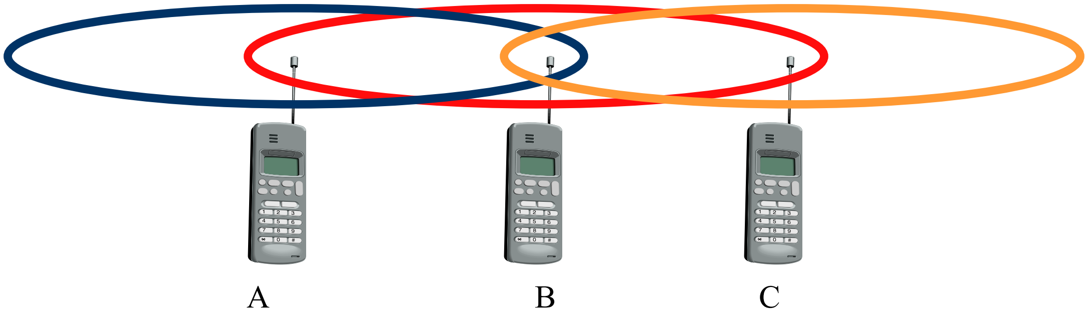
8. **What is hidden terminal? What problem does it create during wireless communications?(April 2012)**

- **Hidden and exposed station problem:**

  Let three mobiles A, B, C

  (i) Transmission range of A reaches B, not C and
  (ii) Transmission range of C reaches B, not A
  (iii) Transmission range of B reaches both A and C

- It is shown as



- **Problem definition of hidden stations:**
  - A starts sending to B, and C now wants to transmit data to B thereby senses the medium, it seems to be free and starts transmission.
  - Since, B already commits with A, C's transmission leads to **collision.**
- **Problem definition of exposed stations:**
  - This won't cause collision, but results in **delay.**
  - If B communicates with A, now, C wants to transmit to some other station D, before transmission starts, C will sense medium, it finds it to be busy and wait for the channel to be idle, it is an unnecessary delay, because only B communicates with A not to D.

9. **Explain the basic schemes of the CDMA protocol. What is the role of a pseudo random sequence generator in the working of the CDMA protocol?**

Codes with certain characteristics can be applied to the transmission to enable the use of **code division multiplexing (CDM)**. **Code division multiple access (CDMA)** systems use exactly these codes to separate different users in code space and to enable access to a shared medium without interference. The main problem is how to find "good" codes and how to separate the signal from noise generated by other signals and the environment.

By using CDMA Each code is supposed to have

❑ Good auto co-relation(the value of the inner product should be large)
❑ Orthogonal to other codes(the value of the inner product is zero)

Consider how CDMA works:

Sender A

- sends $A_d = 1$, key $A_k = 010011$ (assign: „0“= -1, „1“= +1)
- sending signal $A_s = A_d * A_k = (-1, +1, -1, -1, +1, +1)$

Sender B

- sends $B_d = 0$, key $B_k = 110101$ (assign: „0“= -1, „1“= +1)
- sending signal $B_s = B_d * B_k = (-1, -1, +1, -1, +1, -1)$

Both signals superimpose in space

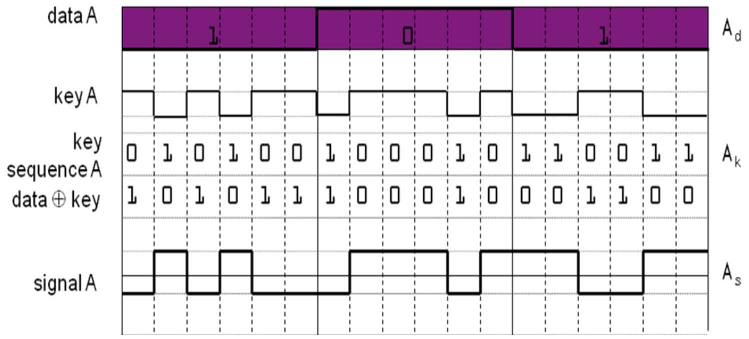
- interference neglected (noise etc.)
- $A_s + B_s = (-2, 0, 0, -2, +2, 0)$

Receiver wants to receive signal from sender A

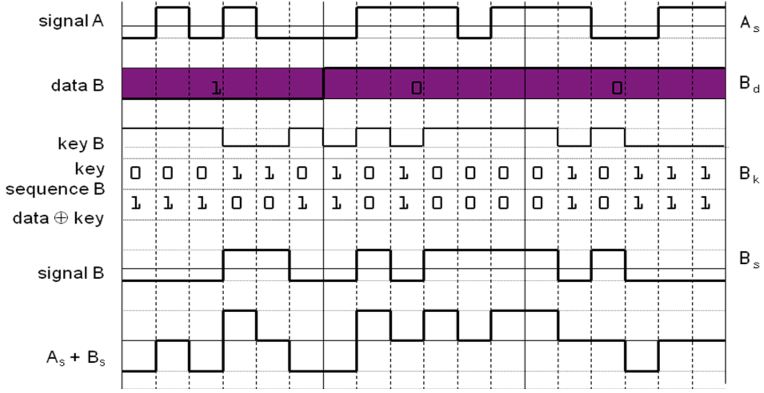
- apply key A_k bitwise (inner product)
  - $A_e = (-2, 0, 0, -2, +2, 0) \cdot A_k = 2 + 0 + 0 + 2 + 2 + 0 = 6$
  - result greater than 0, therefore, original bit was „1“
- receiving B
  - $B_e = (-2, 0, 0, -2, +2, 0) \cdot B_k = -2 + 0 + 0 - 2 - 2 + 0 = -6$, i.e. „0“

Result less than 0, therefore original bit was 0

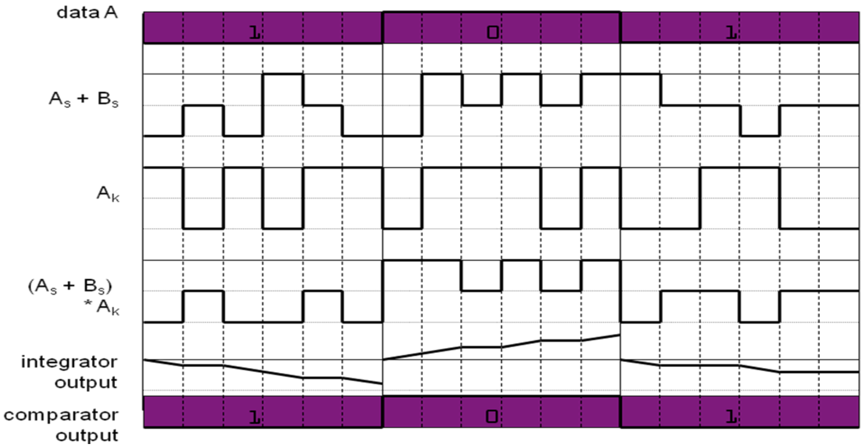
CDMA on signal level I



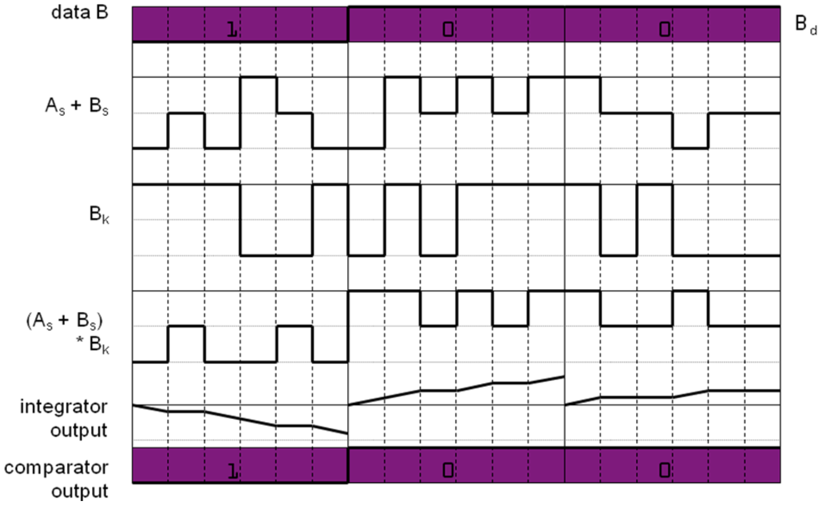
CDMA on signal level II



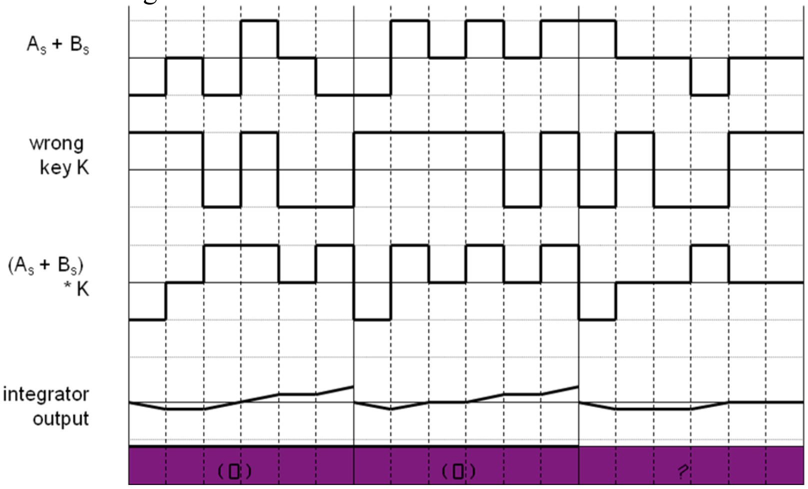
CDMA on signal level III



CDMA on signal level IV

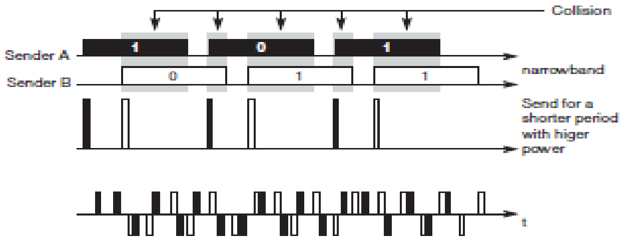


CDMA on signal level V



- Spread Aloha Multiple Access.

It combine CDMA spreading with aloha medium access.
Fig shows that each transmitter uses the same PN sequence for spreading(110.101)
A and B access the medium at the same time(collision occurs)
To resolve collision by transmitting short burst of high power



10. **Explain about spread aloha multiple accesses in CDMA. (Nov 2014)**

Advantage to using a single code for all transmitters in a CDMA network, esp. for small cell sizes and multiple access satellite apps • Choice of a multiple-access protocol depends on traffic characteristics and state of the technology at deployment time: • DAMA (demand assigned multiple access): users request on a separate control channel; request protocol introduces delay and just moves the multiple-access problem to the (lower-bandwidth) request channel • DAMA w/random access: e.g. INMARSAT uses pure ALOHA for request channel. OK since allocation tends to be long-lived; no good if transmissions are bursty or short-lived • Multiple access protocols • Slotted or pure ALOHA. Efficiency (r): eff. channel capacity divided by capacity of a continuous channel with same power & bandwidth. For ALOHA, r=.18, asymptotically optimal for the special case of small values of throughput and S/N ratio. • Spread spectrum: max channel capacity in bits per Nyquist sample: C = .5 log (1+P/N) based on Shannon & Nyquist relations. "Spread spectrum" means C << 1. • CDMA. Multiply channel signals by orthogonal set of spreading signals; multiply by cx conjugate at receiver. Requires multiple receivers at CDMA BS to demodulate received signal. • Qualcomm CDMA (IS-95 std). Spreading code is dynamically assigned via separate ALOHA channel when call request is made. Up to 64 codes can be active at once. • We can choose same spreading code for all CDMA users and the channel will still have multiple-access capability (spread ALOHA): • Each sub channel's bits will be offset by a constant amount g from the previous sub channel's bits within the frame • With k sub channels, prob. that 2 bits will not overlap is (1-1/g)^k; then total traffic G = k/g. • Get the noise-immunity of spread-spectrum with the nice queuing properties of slotted ALOHA. • Previous studies: no compelling evidence that there is a clear advantage for multiple-code CDMA systems, despite their complexity

.

UNIT II Part -A

1. What is meant by mobile IP?

Mobile IP communication protocol refers to the forwarding of Internet traffic with a fixed IP address even outside the home network. It allows users having wireless or mobile devices to use the Internet remotely.

2. List out the features of Mobile IP? (Nov 2014, Nov 2011)

- Transparency : Mobile end system should continue to keep its IP address
- Compatibility : It should be compatible with existing internet protocol
- Scalability : It should be scalable to support billions of moving host worldwide.
- Security : provide users with secure communication over the internet

3. Mention 3- types of address assignment policies used in DHCP. (May 2014, May 2013)

- **Manual configuration** – manager can configure a specific address for a specific computer.
- **Automatic configuration** – DHCP server assigns permanent address when a computer first attaches to the network.
- **Dynamic configuration** – server loans an address to a computer for a limited time.

4. What are the different terminologies of mobile IP?

- Home Network

- Home address
- Foreign agent
- Foreign Network
- Mobile IP

5. What is meant by care of address and its types?

It is the address that is used to identify the present location of a foreign agent

- Foreign agent care of address
- Co-located care of address

6. What is agent advertisement?

Foreign and the home agents advertise their presence through periodic agent advertisement messages. An agent advertisement message, lists one or more care of address and a flag indicating whether it is a home agent or a foreign agent.

7. What are the key mechanisms in mobile IP?

- Discovering the care of address
- registering the care of address
- Tunneling to the care of address.

8. What are the Features provided by FTP?

- Interactive Access
- Format (representation) Specification.
- Authentication Control.

9. Mention the service of TCP/IP

TCP/IP services into two groups:

- Services provided to other protocols and services provided to end users directly.
- Services provided to other protocols: at the network layer, IP provides functions such as addressing, delivery, and datagram packaging, fragmentation and reassembly. At the transport layer, TCP and UDP are concerned with encapsulating user data and managing connections between devices.

10. What is SMTP?

SMTP is used to transfer electronic mail messages from one machine to another. Simple Mail Transfer Protocol specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

11. What is MIME?

MIME – Multipurpose Internet Mail Extensions.

A standard used to encode data such as images as printable ASCII text for transmission through e-mail. MIME is the shortened form of the complete term i.e. Multipurpose Internet Mail Extensions. It is particular description used to format the non-ASCII messages in order to send them over the Internet. Nowadays a number of e-mail clients are supporting MIME that enabled them to received ad send the graphics, MIME also supports the messaging in the character set in addition to ASCII.

12. What is HTTP?

Hyper Text Transfer Protocol (HTTP) used to transfer web documents from a server to a browser. Hyper text Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.

13. Define DNS.

It is the on-line distributed database system used to map human-readable machine names into IP addresses. DNS servers implement a hierarchical namespace that allows sites to assign names and addresses. The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses.

14. What is the purpose of IGMP?

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. It is also used by connected routers to discover these group members.

15. Define Routers

Router is responsible for routing the packets that is receives to their destinations based on their ip addresses, possibly via other routers.

16. What are the different layers of TCP/IP?

- Application layer
- Transport layer
- Internet layer
- Network access layer

17. What are all the various flavours of TCP available? Explain them in detail? **(**Nov 2013)

- Indirect TCP- I-TCP segments a TCP connection into a fixed part and a wireless part.
- Snooping TCP- Here the foreign agent buffers all packets with destination mobile host and additionally snoops the packet flow in both directions to recognize acknowledgements.
- Mobile TCP- M-TCP wants to improve overall throughput,to lower the delay,to maintain end to end semantics of TCP,and to provide a more efficient handover.
- Fast Transmit/Fast Recovery
- Transmission/Time-out freezing
- Selective retransmission
- Transaction-oriented TCP.

18. What is the goal of M-TCP? (Nov 2011)

- The goal of M-TCP is to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems. It wants
- To provide overall throughput
- To lower the delay
- To maintain end-to-end semantics of TCP
- To provide a more efficient handover.

19. What led to the development of Indirect TCP? (Nov 2012, May 2012)

TCP performs poorly together with wireless links

TCP within the fixed network cannot be changed.

This led to the development of I-TCP which segments a TCP connection into a fixed part and a wireless part.

20 List the disadvantages of I-TCP **(**April 2015)

It does not maintain the semantics of TCP as the FH gets the acknowledgement before the packet is delivered at MH.I Tcp does not maintain the end –end semantic of TCp and assumes that application layer would ensure reliability

21. What is BOOTP?

BOOTP protocol is used for Booting (starting) a diskless computer over a network. Since a diskless computer does not store the operating system program in its permanent memory, BOOTP protocol helps to download and boot over a network using the operating system files stored on a server located in the network.

22. Define Agent solicitation

Mobile node does not receive any COA,then the MN should send an agent solicitation message. But it is important to monitor that these agent solicitation message do not flood the network.

23. What is the different operation of mobile IP?

- The remote client sends a datagram to the MN using its home address it reaches the home agent a usual.
- The home agent encapsulates the datagram in a new packet and sends it to the foreign agent.

24. Define Home agent

It is located in home network and it provides several services for the Mobile Network (MN).Home agent maintains a location registry. The location registry keeps track of the node locations using the current care of address of the mobile network.

Part-B UNIT II

1. List the requirements for Mobile IP. (Nov 2014, Nov 2011)

Compatibility:

The installed base of Internet computers, i.e., computers running TCP/IP and connected to the internet, is huge. A new standard cannot introduce changes for applications or network protocols already in use. People still want to use their favorite browser for www and do not want to change applications just for mobility, the same holds for operating systems. Mobile IP has to be integrated into existing operating systems or at least work with them (today it is available for many platforms). Routers within the internet should not necessarily require other software. While it is possible to enhance the capabilities of some routers to support mobility, it is almost impossible to change all of them. Mobile IP has to remain compatible with all lower layers used for the standard, 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 all the other servers and systems in the internet. But that implies using the same address format and routing mechanisms.

Transparency:

Mobility should remain 'invisible' for many higher layer protocols and applications. Besides maybe noticing a lower bandwidth and some interruption in service, higher layers should continue to work even if the mobile computer has changed its point of attachment to the network. For TCP this means that the computer must keep its IP address as explained above. If the interruption of the connectivity does not take too long, TCP\ connections survive the change of the attachment point. Problems related to the performance of TCP are discussed in chapter 9. Clearly, many of today's applications have not been designed for use in mobile environments, so the only effects of mobility should be a higher delay and lower bandwidth. However, there are some applications for which it is better to be 'mobility aware'. Examples are cost-based routing or video compression. Knowing that it is currently possible to use different networks, the software could choose the cheapest one. Or if a video application knows that only a low bandwidth connection is currently available, it could use a different compression scheme. Additional mechanisms are necessary to inform these applications about mobility (Brewer, 1998).

Scalability and efficiency:

Introducing a new mechanism to the internet must not jeopardize its efficiency. Enhancing IP for mobility must not generate too many new messages flooding the whole network. Special care has to be taken considering the lower bandwidth of wireless links. Many mobile systems will have a wireless link to an attachment point, so only some additional packets should be necessary between a mobile system and a node in the network. Looking at the number of computers connected to the internet and at the growth rates of mobile communication, it is clear that myriad devices will participate in the internet as mobile components. Just 306 Mobile communications think of cars, trucks, mobile phones, every seat in every plane around the world etc. – many of them will have some IP implementation inside and move between different networks and require mobile IP. It is crucial for a mobile IP to be scalable over a large number of participants in the whole internet, worldwide.

Security:

Mobility poses many security problems. The minimum requirement is that of all the messages related to the management of Mobile IP are authenticated. The IP layer must be sure that if it forwards a packet to a mobile host that this host receives the packet. The IP layer can only guarantee that the IP address of the receiver is correct. There are no ways of preventing fake IP addresses or other attacks. According to Internet philosophy, this is left to higher layers (keep the core of the internet simple, push more complex services to the edge).

The goal of a mobile IP can be summarized as: 'supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols.

2. Explain in detail about overview of the operation and features of mobile IP

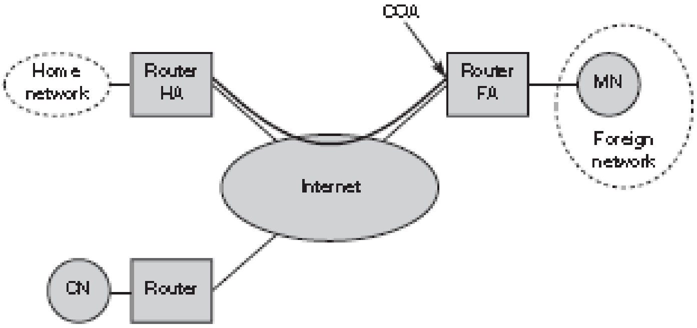


Fig : Mobile IP example network

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 as long as link-layer connectivity is given. Mobile nodes are not necessarily small devices such as laptops with antennas or mobile phones; a router onboard an aircraft can be a powerful mobile node.

Correspondent node (CN):

At least one partner is needed for communication. In the following the CN represents this partner for the MN. The CN can be a fixed or mobile node.

Home network:

The home network 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:

The foreign network is not the home network but the current subnet that the MN visits

Foreign agent (FA):

The FA can provide several services to the MN during its visit to the foreign network. Using CoA(care of Address) it works as conductor of channeling packet delibery to MN. it is default router for MN and provides security services

Care-of address (COA):

The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, Packet delivery to MN is done using a tunnel

. There are two different possibilities for the location of the COA:

Foreign agent COA:

The COA could be located at the FA, i.e., the COA is an IP address of the FA. 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.

Co-located COA:

The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. Co-located addresses can be acquired using services such as DHCP One problem associated with this approach is the need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

Home agent (HA):

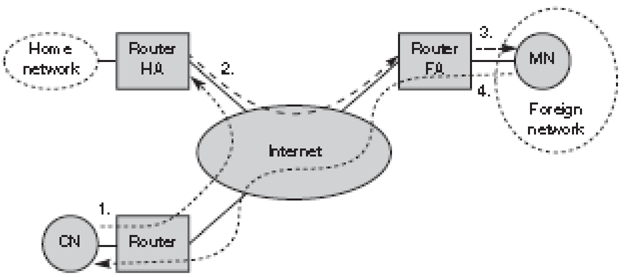
The HA provides several services for the MN and is located in the home network. The tunnel for packets toward the MN starts at the HA. The HA maintains a location registry, i.e., it is informed of the MN’s location by the current COA. Three alternatives for the implementation of an HA exist.

● The HA can be implemented on a router at the home network.

● HA can be implemented on an arbitrary node in the subnet.

Home network is not necessary at all. The HA could be again on the ‘router’ but this time only acting as a manager

3. Discuss in detail about three mechanisms in mobile IP



1.

Fig : Packet delivery to and from the mobile node

A correspondent node CN wants to send an IP packet to the MN. One of the requirements of mobile IP was to support hiding the mobility of the MN. CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN (step 1). This means that CN sends an IP packet with MN as a destination address and CN as a source address. The internet, not having information on the current location of MN routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet. The HA now intercepts the packet knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but 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 2). 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 to the MN (step 3). Again, for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network.

At first glance, sending packets from the MN to the CN is much simpler. The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination (step 4). 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. As long as CN is a fixed node the remainder is in the fixed internet as usual. If CN were also a mobile node residing in a foreign network, the same mechanisms as described in steps 1 through 3 would apply now in the other direction.

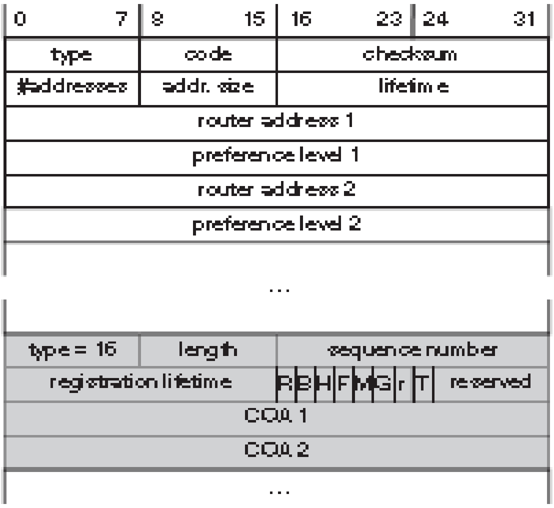
For the whole operations to take place as explained above some of the requirements are:

- Additional mechanisms.
- Enhancements to the protocol
- Some techniques to take care of efficiency and security problems

2.

Agent advertisement and discovery:

One initial problem of an MN after moving is how to find a foreign agent. For the first method, foreign agents and home agents advertise their presence periodically using special **agent advertisement** messages. These advertisement messages can be seen as a beacon broadcast into the subnet. For these advertisements Internet control message protocol (ICMP) messages according to RFC 1256 are used with some mobility extensions. Routers in the fixed network implementing this standard also advertise their routing service periodically to the attached links. The agent advertisement packet according to RFC 1256 with the extension for mobility is shown in Figure 8.3. The upper part represents the ICMP packet while the lower part is the extension needed for mobility. The fields necessary on lower layers for the agent advertisement are not shown in this figure. Clearly, mobile nodes must be reached with the appropriate link layer address. The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them. The IP destination address according to standard router advertisements can be either set to 224.0.0.1, which is the multicast address for all systems on a link , or to the broadcast address 255.255.255.255.



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			
…			

Agent advertisement packet (RFC 1256+Mobility extension)

The fields in the ICMP part are defined as follows.

- The **type** is set to 9,
- The **code** can be 0, if the agent also routes traffic from non-mobile nodes, or 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
- **addresses:** Addresses of router
- **Lifetime** denotes the length of time this advertisement is valid.
- **Preference** levels for each address help a node to choose the router that is the most eager one 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** the agent can specify the maximum lifetime in seconds a node can request 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. While IP-in-IP encapsulation is the mandatory standard, **M** can specify minimal encapsulation and **G** generic routing encapsulation.
    - ❖ **V** bit specifies the use of header compression
- **CoAs**: CoAs advertised.

Mobile node must be in apposition to receive an advertisement from either a home agent or a foreign agent depending on its current physical location. If the MN has not received any advertisement or a CoA by some means, then MN must solicit by; means of agent solicitations. Care must be taken to avoid flooding of router solicitations. Agent discovery need not be limited to the time when the MN is disconnected. Even when it is connected it can solicit agents for better connection. After the process of either advertisement or agent discovery, MN can receive a CoA. MN also knows its own location and the capabilities of the agent to which it needs to be connected. Next step is the registration of MN to tis HA through a foreign agent if is currently located in a foreign network.

RFC1256 most be the standard for router advertisements. While the norm of three seconds interval between advertisements is sufficient in wired networks, at times such interval may not be sufficient in wireless networks.

3.

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 from a lower to a higher layer respectively. Here these functions are used within the same layer.

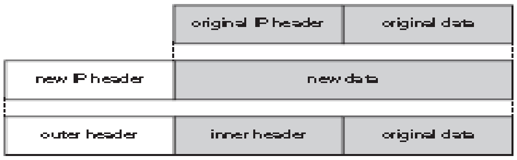


Fig: IP Encapsulation

This mechanism is shown in Figure 4.5 and describes exactly what the HA at the tunnel entry does. The HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sets the new IP header in such a way that the packet is routed to the COA. The new header is also called the **outer header** for obvious reasons. Additionally, there is an **inner header** which can be identical to the original header as this is the case for IP-in-IP encapsulation.

IP-in-IP ENCAPSULATION:

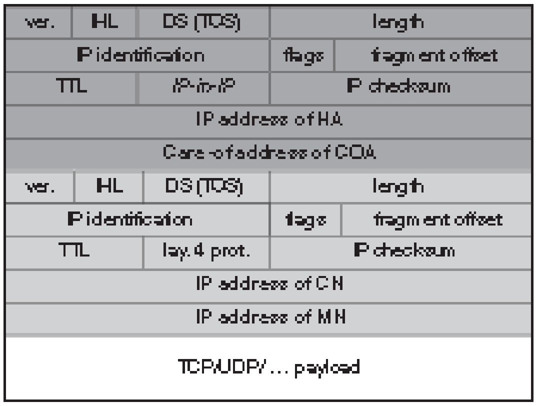


Fig IP-in-IP ENCAPSULATION

Whenever there is tunnel between HA and CoA, encapsulation is required. For mobile IP, IP-in-IP encapsulation is mandatory. There are two parts in the packet. There is an outer header, inner header and actual data. The field sof the meter header are as follows:

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

4. Write short notes on:

a)Telnet b)FTP c)SMTP d)TCP/IP vs ISO/OSI protocol model

a)Telnet

Telnet is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards.

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a configuration (including systems based on Windows NT).[clarification needed] However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

The term telnet is also used to refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. Telnet is also used as a verb. To telnet means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface. For example, a common directive might be: "To change your password, telnet to the server, log in and run the passwd command." Most often, a user will be telnetting to a Unix-like server system or a network device (such as a router) and obtaining a login prompt to a command line text interface or a character-based full-screen manager.

b)FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network.

FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as Web page editors.

c)SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with the Extended SMTP additions by RFC 5321—which is the protocol in widespread use today.

SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as SMTPS, default to port 465 (nonstandard, but sometimes used for legacy reasons).

Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either POP3 or IMAP.

Although proprietary systems (such as Microsoft Exchange and IBM Notes) and webmail systems (such as Outlook.com, Gmail and Yahoo! Mail) use their own non-standard protocols to access mail box accounts on their own mail servers, all use SMTP when sending or receiving email from outside their own systems.

d)TCP/IP vs ISO/OSI protocol model

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)

1. OSI provides layer functioning and also defines functions of all the layers.
2. In OSI model the transport layer guarantees the delivery of packets
3. Follows horizontal approach
4. OSI model has a separate presentation layer
5. OSI is a general model.
6. Network layer of OSI model provide both connection oriented and connectionless service.

OSI model has a problem of fitting the protocols in the model

8. Protocols are hidden in OSI model and are easily replaced as the technology changes
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.

10.It has 7 layers

TCP/IP(Transmission Control Protocol / Internet Protocol)

TCP/IP model is more based on protocols and protocols are not flexible with other layers.

2. In TCP/IP model the transport layer does not guarantees delivery of packets.

3.Follows vertical approach.

. 4. TCP/IP does not have a separate presentation layer

5. TCP/IP model cannot be used in any other application.
6. The Network layer in TCP/IP model provides connectionless service.
7. TCP/IP model does not fit any protocol
8. In TCP/IP replacing protocol is not easy.

9.. In TCP/IP it is not clearly separated its services, interfaces and protocols.

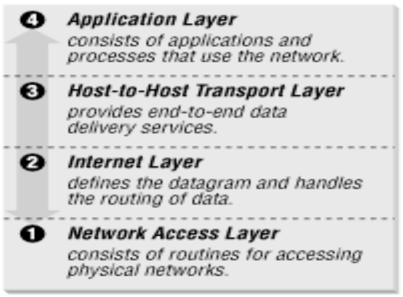
10It has 4 layers

5. Write short notes on Architecture of TCP/IP

TCP/IP Protocol Architecture

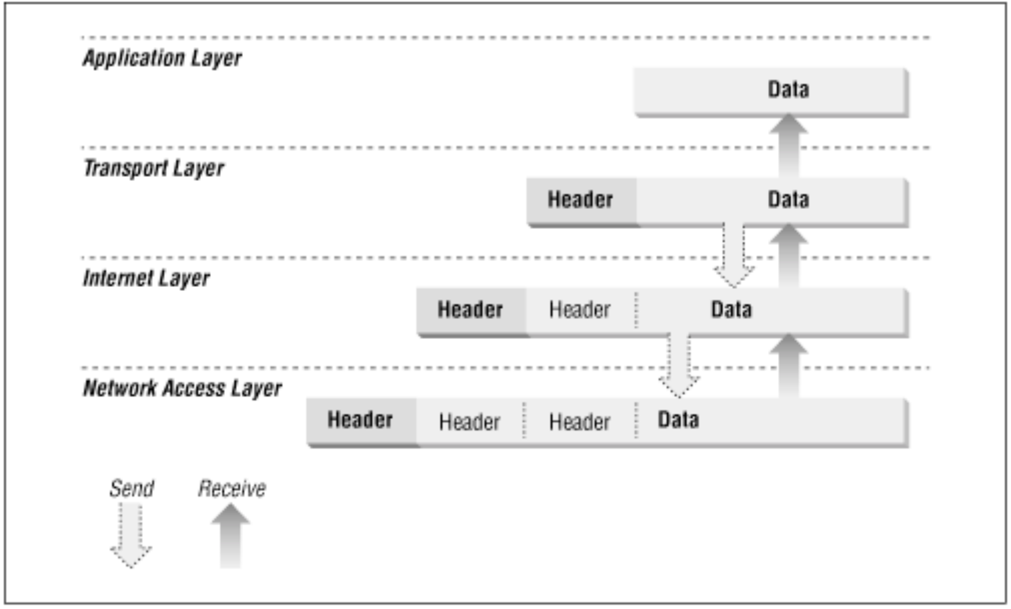
While there is no universal agreement about how to describe TCP/IP with a layered model, it is generally viewed as being composed of fewer layers than the seven used in the OSI model. Most descriptions of TCP/IP define three to five functional levels in the protocol architecture. The four-level model illustrated in Figure based on the three layers (Application, Host-to-Host, and Network Access) shown in the DOD Protocol Model in the *DDN Protocol Handbook - Volume 1* , with the addition of a separate Internet layer. This model provides a reasonable pictorial representation of the layers in the TCP/IP protocol hierarchy.

Figure 1.2: Layers in the TCP/IP protocol architecture


4 Application Layer
consists of applications and processes that use the network.
3 Host-to-Host Transport Layer
provides end-to-end data delivery services.
2 Internet Layer
defines the datagram and handles the routing of data.
1 Network Access Layer
consists of routines for accessing physical networks.

As in the OSI model, data is passed down the stack when it is being sent to the network, and up the stack when it is being received from the network. The four-layered structure of TCP/IP is seen in the way data is handled as it passes down the protocol stack from the Application Layer to the underlying physical network. Each layer in the stack adds control information to ensure proper delivery. This control information is called a *header* because it is placed in front of the data to be transmitted. Each layer treats all of the information it receives from the layer above as data and places its own header in front of that information. The addition of delivery information at every layer is called *encapsulation* . (SeeFigure for an illustration of this.) When data is received, the opposite happens. Each layer strips off its header before passing the data on to the layer above. As information flows back up the stack, information received from a lower layer is interpreted as both a header and data.

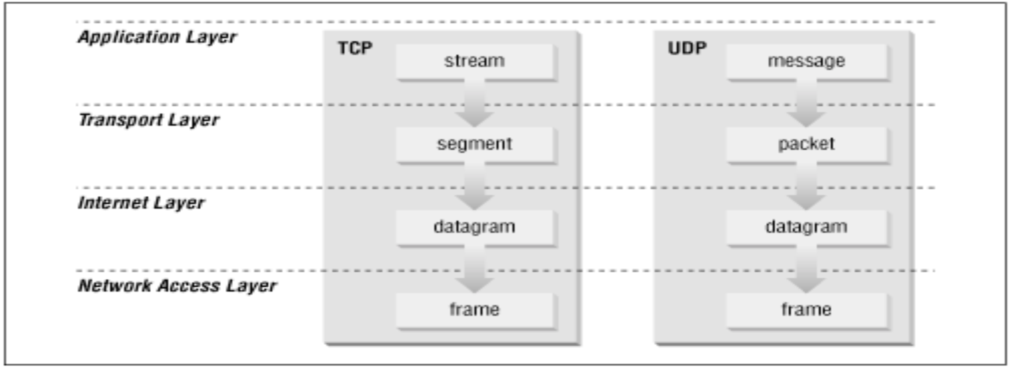
Figure 1.3: Data encapsulation



Each layer has its own independent data structures. Conceptually, a layer is unaware of the data structures used by the layers above and below it. In reality, the data structures of a layer are designed to be compatible with the structures used by the surrounding layers for the sake of more efficient data transmission. Still, each layer has its own data structure and its own terminology to describe that structure.

Figure shows the terms used by different layers of TCP/IP to refer to the data being transmitted. Applications using TCP refer to data as a *stream* , while applications using the User Datagram Protocol (UDP) refer to data as a *message* . TCP calls data a *segment* , and UDP calls its data structure a *packet* . The Internet layer views all data as blocks called *datagrams* .TCP/IP uses many different types of underlying networks, each of which may have a different terminology for the data it transmits. Most networks refer to transmitted data as *packets* or*frames* . In figure we show a network that transmits pieces of data it calls *frames* .

Figure 1.4: Data structures



1.4 Network Access Layer

The *Network Access Layer* is the lowest layer of the TCP/IP protocol hierarchy. The protocols in this layer provide the means for the system to deliver data to the other devices on a directly attached network. It defines how to use the network to transmit an IP datagram. Unlike higher-level protocols, Network Access Layer protocols must know the details of the underlying network (its packet structure, addressing, etc.) to correctly format the data being transmitted to comply with the network constraints. The TCP/IP Network Access Layer can encompass the functions of all three lower layers of the OSI reference Model (Network, Data Link, and Physical).

The Network Access Layer is often ignored by users. The design of TCP/IP hides the function of the lower layers, and the better known protocols (IP, TCP, UDP, etc.) are all higher-level protocols. As new hardware technologies appear, new Network Access protocols must be developed so that TCP/IP networks can use the new hardware. Consequently, there are many access protocols - one for each physical network standard.

Functions performed at this level include encapsulation of IP datagrams into the frames transmitted by the network, and mapping of IP addresses to the physical addresses used by the network. One of TCP/IP's strengths is its universal addressing scheme. The IP address must be converted into an address that is appropriate for the physical network over which the datagram is transmitted.

.5 Internet Layer

The layer above the Network Access Layer in the protocol hierarchy is the *Internet Layer* . The Internet Protocol, RFC 791, is the heart of TCP/IP and the most important protocol in the Internet Layer. IP provides the basic packet delivery service on which TCP/IP networks are built. All protocols, in the layers above and below IP, use the Internet Protocol to deliver data. All TCP/IP data flows through IP, incoming and outgoing, regardless of its final destination.

1.5.1 Internet Protocol

The Internet Protocol is the building block of the Internet. Its functions include:

- Defining the datagram, which is the basic unit of transmission in the Internet
- Defining the Internet addressing scheme
- Moving data between the Network Access Layer and the Host-to-Host Transport Layer
- Routing datagrams to remote hosts
- Performing fragmentation and re-assembly of datagrams

Before describing these functions in more detail, let's look at some of IP's characteristics. First, IP is a *connectionless protocol* . This means that IP does not exchange control information (called a "handshake") to establish an end-to-end connection before transmitting data. In contrast, a *connection-oriented protocol* exchanges control information with the remote system to verify that it is ready to receive data before any data is sent. When the handshaking is successful, the systems are said to have established a *connection* . Internet Protocol relies on protocols in other layers to establish the connection if they require connection-oriented service.

IP also relies on protocols in the other layers to provide error detection and error recovery. The Internet Protocol is sometimes called an *unreliable protocol* because it contains no error detection and recovery code. This is not to say that the protocol cannot be relied on - quite the contrary. IP can be relied upon to accurately deliver your data to the connected network, but it doesn't check whether that data was correctly received. Protocols in other layers of the TCP/IP architecture provide this checking when it is required.

1.6 Transport Layer

The protocol layer just above the Internet Layer is the *Host-to-Host Transport Layer* . This name is usually shortened to *Transport Layer* . The two most important protocols in the Transport Layer are *Transmission Control Protocol* (TCP) and *User Datagram Protocol*(UDP). TCP provides reliable data delivery service with end-to-end error detection and correction. UDP provides low-overhead, connectionless datagram delivery service. Both protocols deliver data between the Application Layer and the Internet Layer. Applications programmers can choose whichever service is more appropriate for their specific applications.

1.6.1 User Datagram Protocol

The User Datagram Protocol gives application programs direct access to a datagram delivery service, like the delivery service that IP provides. This allows applications to exchange messages over the network with a minimum of protocol overhead.

UDP is an unreliable, connectionless datagram protocol. As noted previously, "unreliable" merely means that there are no techniques in the protocol for verifying that the data reached the other end of the network correctly. Within your computer, UDP will deliver data correctly. UDP uses 16-bit *Source Port* and *Destination Port* numbers in word 1 of the message header, to deliver data to the correct applications process.

Why do applications programmers choose UDP as a data transport service? There are a number of good reasons. If the amount of data being transmitted is small, the overhead of creating connections and ensuring reliable delivery may be greater than the work of re-transmitting the entire data set. In this case, UDP is the most efficient choice for a Transport Layer protocol. Applications that fit a *query-response* model are also excellent candidates for using UDP. The response can be used as a positive acknowledgment to the query. If a response isn't received within a certain time period, the application just sends another query. Still other applications provide their own techniques for reliable data delivery, and don't require that service from the transport layer protocol. Imposing another layer of acknowledgment on any of these types of applications is inefficient.

1.6.2 Transmission Control Protocol

Applications that require the transport protocol to provide reliable data delivery use TCP because it verifies that data is delivered across the network accurately and in the proper sequence. TCP is a *reliable* , *connection-oriented* , *byte-stream* protocol. Let's look at each of the terms - reliable, connection-oriented, and byte-stream - in more detail.

TCP provides reliability with a mechanism called *Positive Acknowledgment with Re-transmission* (PAR). Simply stated, a system using PAR sends the data again, unless it hears from the remote system that the data arrived okay. The unit of data exchanged between cooperating TCP modules is called a *segment* . Each segment contains a checksum that the recipient uses to verify that the data is undamaged. If the data segment is received undamaged, the receiver sends a *positive acknowledgment* back to the sender. If the data segment is damaged, the receiver discards it. After an appropriate time-out period, the sending TCP module re-transmits any segment for which no positive acknowledgment has been received.

1.7 Application Layer

At the top of the TCP/IP protocol architecture is the *Application Layer* . This layer includes all processes that use the Transport Layer protocols to deliver data. There are many applications protocols. Most provide user services, and new services are always being added to this layer.

6. Discuss in detail about terminologies of TCP/IP

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:

TCP's reaction to a missing ack is quite drastic, but it is necessary to get rid of congestion quickly. The behavior TCP shows after the detection of congestion is called slow start.

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

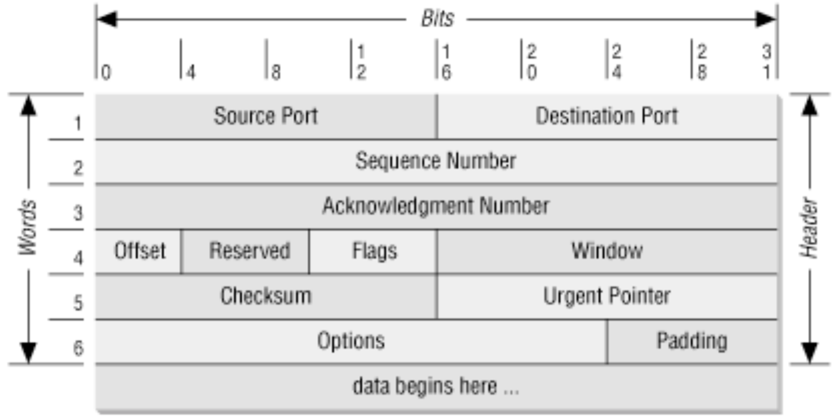
7. Explain about structure of a TCP segment

Transmission Control Protocol

Applications that require the transport protocol to provide reliable data delivery use TCP because it verifies that data is delivered across the network accurately and in the proper sequence. TCP is a *reliable* , *connection-oriented* , *byte-stream* protocol. Let's look at each of the terms - reliable, connection-oriented, and byte-stream - in more detail.

TCP provides reliability with a mechanism called *Positive Acknowledgment with Re-transmission* (PAR). Simply stated, a system using PAR sends the data again, unless it hears from the remote system that the data arrived okay. The unit of data exchanged between cooperating TCP modules is called a *segment*

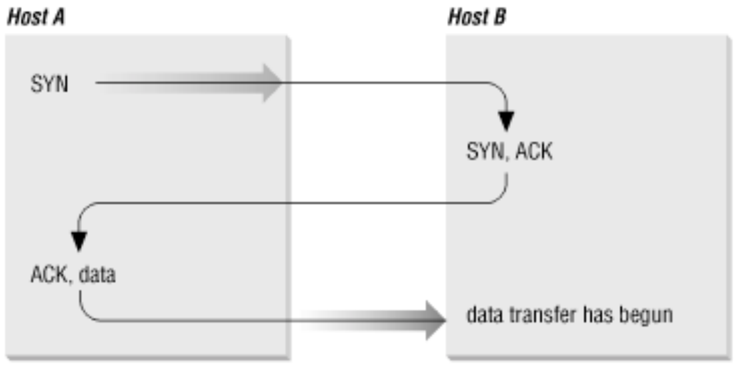
Figure 1.9: TCP segment format



TCP is connection-oriented. It establishes a logical end-to-end connection between the two communicating hosts. Control information, called a *handshake* , is exchanged between the two endpoints to establish a dialogue before data is transmitted. TCP indicates the control function of a segment by setting the appropriate bit in the Flags field in word 4 of the *segment header* .

The type of handshake used by TCP is called a *three-way handshake* because three segments are exchanged. fig shows the simplest form of the three-way handshake. Host *A* begins the connection by sending host *B* a segment with the "Synchronize sequence numbers" (SYN) bit set. This segment tells host *B* that *A* wishes to set up a connection, and it tells *B* what sequence number host *A* will use as a starting number for its segments. (Sequence numbers are used to keep data in the proper order.) Host *B* responds to *A* with a segment that has the "Acknowledgment" (ACK) and SYN bits set. *B* 's segment acknowledges the receipt of *A* 's segment, and informs *A* which Sequence Number host *B* will start with. Finally, host *A* sends a segment that acknowledges receipt of *B* 's segment, and transfers the first actual data.

Figure 1.10: Three-way handshake



After this exchange, host *A* 's TCP has positive evidence that the remote TCP is alive and ready to receive data. As soon as the connection is established, data can be transferred. When the cooperating modules have concluded the data transfers, they will exchange a three-way handshake with segments containing the "No more data from sender" bit (called the *FIN* bit) to close the connection. It is the end-to-end exchange of data that provides the logical connection between the two systems.

TCP views the data it sends as a continuous stream of bytes, not as independent packets. Therefore, TCP takes care to maintain the sequence in which bytes are sent and received. The Sequence Number and Acknowledgment Number fields in the TCP segment header keep track of the bytes.

The TCP standard does not require that each system start numbering bytes with any specific number; each system chooses the number it will use as a starting point. To keep track of the data stream correctly, each end of the connection must know the other end's initial number. The two ends of the connection synchronize byte-numbering systems by exchanging SYN segments during the handshake. The Sequence Number field in the SYN segment contains the *Initial Sequence Number* (ISN), which is the starting point for the byte-numbering system. For security reasons the ISN should be a random number, though it is often 0.

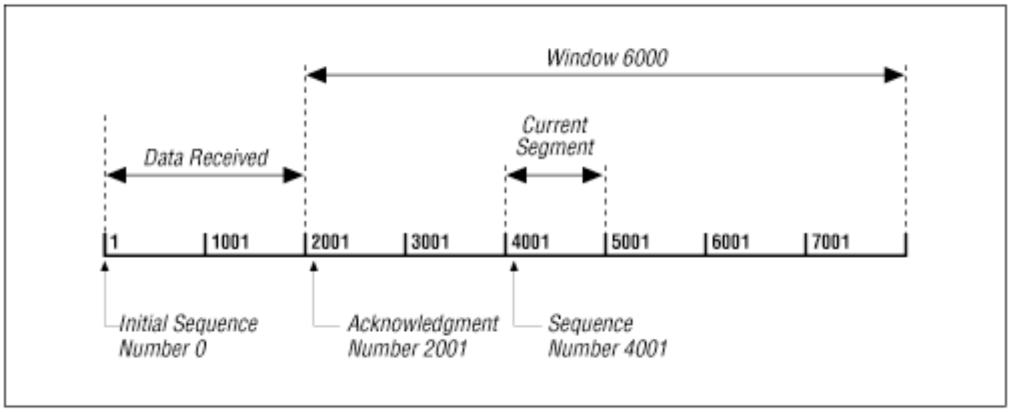
Each byte of data is numbered sequentially from the ISN, so the first real byte of data sent has a sequence number of ISN+1. The Sequence Number in the header of a data segment identifies the sequential position in the data stream of the first data byte in the segment. For example, if the first byte in the data stream was sequence number 1 (ISN=0) and 4000 bytes of data have already been transferred, then the first byte of data in the current segment is byte 4001, and the Sequence Number would be 4001.

The Acknowledgment Segment (ACK) performs two functions: *positive acknowledgment* and*flow control* . The acknowledgment tells the sender how much data has been received, and how much more the receiver can accept. The Acknowledgment Number is the sequence number of the next byte the receiver expects to receive. The standard does not require an individual acknowledgment for every packet. The acknowledgment number is a positive acknowledgment of all bytes up to that number. For example, if the first byte sent was numbered 1 and 2000 bytes have been successfully received, the Acknowledgment Number would be 2001.

The Window field contains the *window* , or the number of bytes the remote end is able to accept. If the receiver is capable of accepting 6000 more bytes, the window would be 6000. The window indicates to the sender that it can continue sending segments as long as the total number of bytes that it sends is smaller than the window of bytes that the receiver can accept. The receiver controls the flow of bytes from the sender by changing the size of the window. A zero window tells the sender to cease transmission until it receives a non-zero window value.

Fig shows a TCP data stream that starts with an Initial Sequence Number of 0. The receiving system has received and acknowledged 2000 bytes, so the current Acknowledgment Number is 2001. The receiver also has enough buffer space for another 6000 bytes, so it has advertised a window of 6000. The sender is currently sending a segment of 1000 bytes starting with Sequence Number 4001. The sender has received no acknowledgment for the bytes from 2001 on, but continues sending data as long as it is within the window. If the sender fills the window and receives no acknowledgment of the data previously sent, it will, after an appropriate time-out, send the data again starting from the first unacknowledged byte.

TCP data stream



8. Write short notes on improvement in TCP performance

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.

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.

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 truster entity

2. 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 wants to improve 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 adopted to the problems arising from lengthy or frequent disconnections.

Advantages

- M-TCP maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.
- If the MH is disconnected, M-TCP avoids useless retransmissions, slow starts or breaking connections by simply shrinking the senders window to zero.
- Since M-TCP doesnot 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.

Disadvantage

- 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 rats, 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 network elements like the bandwidth manager

3. 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.

Advantages:

- It is the preservation of the end-to-end TCP semantic.
- No correspondent needs to be changed, most of the enhancements are in the foreign agent.
- It needs know handover of state as soon as the mobile host moves to another foreign agent.
- It does not matter if the next foreign agent uses the enhancements or not. If not, the approach automatically falls back to the standard solution.

Disadvantage:

Snooping TCP does not isolate the behavior 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.

9. Explain in detail a about application layer protocols of TCP

Application Layer

At the top of the TCP/IP protocol architecture is the *Application Layer* . This layer includes all processes that use the Transport Layer protocols to deliver data. There are many applications protocols. Most provide user services, and new services are always being added to this layer.
The most widely known and implemented applications protocols are:

telnet

The Network Terminal Protocol, which provides remote login over the network.

FTP

The File Transfer Protocol, which is used for interactive file transfer.

SMTP

The Simple Mail Transfer Protocol, which delivers electronic mail.

HTTP

The Hypertext Transfer Protocol, which delivers Web pages over the network.

While HTTP, FTP, SMTP, and telnet are the most widely implemented TCP/IP applications, you will work with many others as both a user and a system administrator. Some other commonly used TCP/IP applications are:

Domain Name Service (DNS)

Also called *name service* , this application maps IP addresses to the names assigned to network devices. DNS is discussed in detail in this book.

Open Shortest Path First (OSPF)

Routing is central to the way TCP/IP works. OSPF is used by network devices to exchange routing information. Routing is also a major topic of this book.

Network Filesystem (NFS)

This protocol allows files to be shared by various hosts on the network.

Some protocols, such as telnet and FTP, can only be used if the user has some knowledge of the network.

10. Write short notes on TCP in multi-hop wireless networks

TCP was originally designed for wired networks. Packet loss is considered to be the result of network congestion and the congestion window size is reduced dramatically as a precaution. However, wireless links are known to experience sporadic and usually temporary losses due to fading, shadowing, hand off, and other radio effects, that should not be considered congestion. After the (erroneous) back-off of the congestion window size, due to wireless packet loss, there may be a congestion avoidance phase with a conservative decrease in window size. This causes the radio link to be underutilized. Extensive research on combating these harmful effects has been conducted. Suggested solutions can be categorized as end-to-end solutions, which require modifications at the client or server, link layer solutions, such as RLP in cellular networks, or proxy-based solutions which require some changes in the network without modifying end nodes.
A number of alternative congestion control algorithms, such as Vegas, Westwood, Veno and Santa Cruz, have been proposed to help solve the wireless problem.

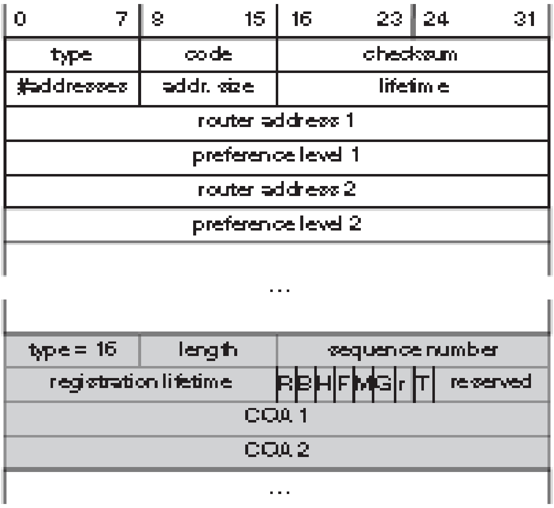
11.(i)Explain the agent discovery process in mobile-IP (April2015)

For this purpose mobile IP describes two methods which are in fact router discovery methods plus extensions. They are

- Agent advertisement
- Agent Solicitation.

Agent advertisement and discovery:

One initial problem of an MN after moving is how to find a foreign agent. For the first method, foreign agents and home agents advertise their presence periodically using special **agent advertisement** messages. These advertisement messages can be seen as a beacon broadcast into the subnet. For these advertisements Internet control message protocol (ICMP) messages according to RFC 1256 are used with some mobility extensions. Routers in the fixed network implementing this standard also advertise their routing service periodically to the attached links. The agent advertisement packet according to RFC 1256 with the extension for mobility is shown in Figure 8.3. The upper part represents the ICMP packet while the lower part is the extension needed for mobility. The fields necessary on lower layers for the agent advertisement are not shown in this figure. Clearly, mobile nodes must be reached with the appropriate link layer address. The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them. The IP destination address according to standard router advertisements can be either set to 224.0.0.1, which is the multicast address for all systems on a link , or to the broadcast address 255.255.255.255.



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			
…			

Agent advertisement packet (RFC 1256+Mobility extension)

The fields in the ICMP part are defined as follows.

- The **type** is set to 9,
- The **code** can be 0, if the agent also routes traffic from non-mobile nodes, or 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
- **addresses:** Addresses of router
- **Lifetime** denotes the length of time this advertisement is valid.
- **Preference** levels for each address help a node to choose the router that is the most eager one 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** the agent can specify the maximum lifetime in seconds a node can request 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. While IP-in-IP encapsulation is the mandatory standard, **M** can specify minimal encapsulation and **G** generic routing encapsulation.
    - ❖ **V** bit specifies the use of header compression
- **CoAs**: CoAs advertised.

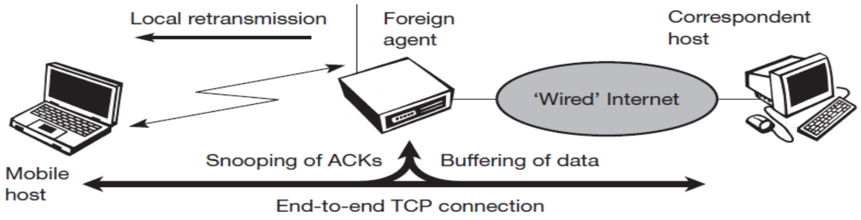
Mobile node must be in apposition to receive an advertisement from either a home agent or a foreign agent depending on its current physical location. If the MN has not received any advertisement or a CoA by some means, then MN must solicit by; means of agent solicitations. Care must be taken to avoid flooding of router solicitations. Agent discovery need not be limited to the time when the MN is disconnected. Even when it is connected it can solicit agents for better connection. After the process of either advertisement or agent discovery, MN can receive a CoA. MN also knows its own location and the capabilities of the agent to which it needs to be connected. Next step is the registration of MN to tis HA through a foreign agent if is currently located in a foreign network.

RFC1256 most be the standard for router advertisements. While the norm of three seconds interval between advertisements is sufficient in wired networks, at times such interval may not be sufficient in wireless networks.

(ii)Explain how snooping TCP ensures end to end connectivity

Snooping TCP

- ❑ Transparent extension of TCP within the foreign agent
- ❑ buffering of packets sent to the mobile host
- ❑ lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called “local” retransmission)
- ❑ the foreign agent therefore “snoops” the packet flow and recognizes acknowledgements in both directions, it also filters ACKs
- ❑ changes of TCP only within the foreign agent (+min. MH change)
- ❑ Data transfer to the mobile host
  - o FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
  - o fast retransmission possible, transparent for the fixed network
- ❑ Data transfer from the mobile host
  - o FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
  - o MH can now retransmit data with only a very short delay



Advantages:

- It is the preservation of the end-to-end TCP semantic.
- No correspondent needs to be changed, most of the enhancements are in the foreign agent.
- It needs know handover of state as soon as the mobile host moves to another foreign agent.
- It does not matter if the next foreign agent uses the enhancements or not. If not, the approach automatically falls back to the standard solution.

Disadvantage:

Snooping TCP does not isolate the behavior 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.

UNIT III Part-A

1. What is the frequency range of uplink, downlink in GSM network?

GSM stands for Global System for Mobile Communications.

GSM 900 : Uplink – 890 – 915 MHz Downlink – 935 – 960 MHz.
GSM 1800: Uplink – 1710-1785MHz Downlink – 1805-1880 MHz

GSM 1900: Uplink – 1850-1910MHz, Downlink – 1930-1990 MHz

2. What are the different services offered by GSM? (April 2014)

- Bearer services
- Tele Services
- Supplementary services.

3. What is transparent bearer service and non transparent bearer services of GSM?

Transparent bearer services only use the functions of the physical layer to transmit data. Non transparent bearer services use protocols of the layers 2 and 3 to implement error correction and flow control.

4. What is voice oriented teleservices?

GSM mainly focus on voice oriented teleservices. These comprise encrypted voice transmission, message services and basic data communication with terminals as known from the public switching Telephone Network (PSTN) or Integrated Services Digital Network (ISDN).

5. What are Tele services provided by GSM?

- Telephony
- Emergency number
- Short message service
- Enhanced message service
- Multimedia message service
- Group 3 fax

6. What are the supplementary services provided by GSM?

The supplementary services provided by GSM are

- User Identification
- Call redirection or
- Forwarding of original calls
- Closed user groups
- Multi party communication

7. Mention the GSM Subsystem.

A GSM system consists of three subsystems namely

- Radio subsystem (RSS) : It comprises of radio specific entities Mobile station(MS),Base station subsystem(BSS), base transceiver station(BTS), Base station controller(BSC)
- Network and switching subsystem (NSS) : It connect wireless networks to standard public networks. It consist of Mobile switching Centre(MSC), Home location register(HLR), Visitor location Register(VLR)
- Operation Subsystem (OSS): It contains all functions necessary for network operation and maintenance. It consist of operation maintenance Centre(OMC),Authentication Centre(AuC), Equipment identity Register(EIR)

8. What are the reasons for the delay in a GSM system for packet data transfer?

- Different data rates provided by traffic channels are low
- Authentication and encryption makes the data transmission low
- Various interferences and noises from the channel also cause delay.

9. Define Burst? What are the types of bursts?

Data is transmitted in small portions called bursts. Different types are normal burst, synchronization burst, access burst and dummy burst.

10. What are the different control channels possible in GSM?

- Broadcast control channel
- Common control channel
- Dedicated control channel.

11. What is a super frame & hyper frame?

- Super frame: By combining 26 multi frames with 51 frames or 51 multi frames with 26 frames to form a super frame.
- Hyper Frame: 2048 super frames build a hyper frame with duration of almost 3.5 hours

12. To locate MS what are the numbers are required for GSM?

- MSISDN :Mobile station international ISDN Number

- IMSI: International subscriber identity
- TMSI : Temporary Mobile subscriber identity
- MSRN: Mobile station roaming number

13.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.

14.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 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.

15. What are the four possible handover in GSM? (Nov 2014)

- Intra-cell hand over
- Inter cell, intra BSC hand over
- Inter BSC, intra MSC handover
- Inter MSC hand over

16. What are the 2 basic reasons for handover?

- The mobile station moves out of range of a BTS. Thus the received signal level continuously until it falls below the minimal requirements for communication.
- The wired infrastructure may decide the traffic in one cell is too high and shifts some MS to other cells with a lower load.

17. List the Security services offered by GSM.

- GSM offers several security services using confidential information stored in the Auc and in the individual SIM. The SIM stores personal secret data and is protected with a PIN against unauthorized user.
- The security services offered by GSM are Access control and authentication, Confidentiality, Anonymity

18. Name the MAC protocol used in GPRS?

Master slave Dynamic Rate Access (MSDRA). Master initiates the packet transfer, slave initiate user data and dedicated signal information

19. What is meant by GGSN, SGSN, BSSGP?

- Serving GPRS Support Node (SGSN) It is similar to MSC of GSM network. Data compression , Authentication of GPRS subscribers, Routing of data to the corresponding GGSN , Mobility management ,Traffic statistics collections.
- Gateway GPRS Support Node (GGSN) GGSN is the gateway to external networks such as PDN (packet data network) or IP network. It does two main functions. It is similar to GMSC of GSM network ,- Routes mobile destined packet coming from external IP networks to the relevant SGSN within the GPRS network, Routes packets originated from a user to the respective external IP network
- BSSGP: The BSSGP layer ensures the transmission of upper-layer data (LLC PDUs) from the BSS to the SGSN or from the SGSN to the BSS. It ensures the transmission of GMM signaling and NM signaling.

20. What is LLC, LLPDU?

Logical Link Control (LLC) which provides a logical link and framing structure for communication between the MS and the SGSN. Any data between MS and SGSN is sent as Logical Link – Protocol

Data Units (LLPDU). LLC supports management of this transfer, including mechanism for the detection and recovery from, lost or corrupted LL-PDU, ciphering and flow control.

21. State the advantages of UMTS.

UMTS stands for Universal Mobile Telecommunications System. UMTS is one of the emerging mobile phone technologies known as third-generation, or *3G*. Third-generation systems are designed to include such traditional phone tasks as calls, voice mail, and paging, but also new technology tasks such as Internet access, video, and SMS, or text messaging. One of the main benefits of UMTS is its speed. This speed makes possible the kind of streaming video that can support movie downloads and video conferencing.

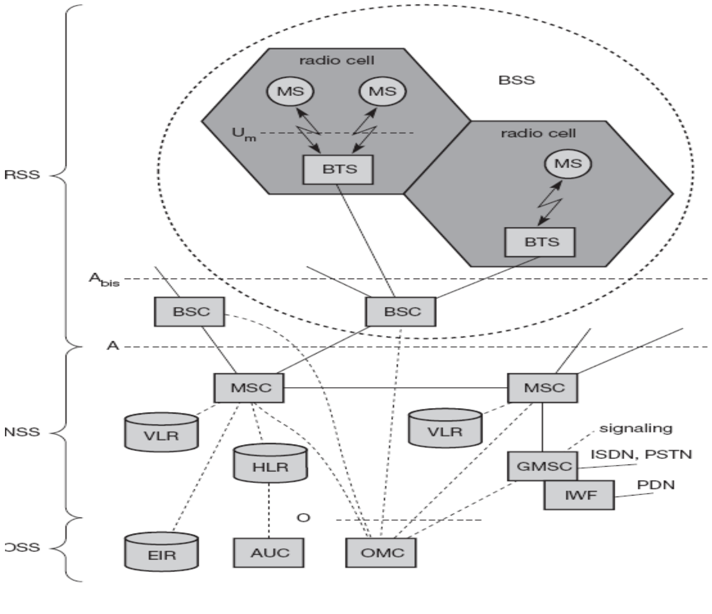
22. Differentiate handover from handoff.

In cellular telecommunications, the term handover or handoff refers to the process of transferring an ongoing call or data session from one channel connected to the core network to another. In satellite communications it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service.

PART-B

1. **Draw and explain the functions of GSM system architecture. (May-2012,Nov-2011,Nov-2012, May/June 2014, Nov/Dec 2014,April-15)**

A GSM network is composed of several functional entities. Following figure shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across the A interface.



Base Station Subsystem.The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The **Base Transceiver Station** houses the radio tranceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile station and the Mobile service Switching Center (MSC).

Network Subsystem. The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjuction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signalling between functional entities in the Network

Subsystem uses Signalling System Number 7 (SS7), used for trunk signalling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signalling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. Note that the MSC contains no information about particular mobile stations --- this information is stored in the location registers.

The other two registers are used for authentication and security purposes.

- The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment
- Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved.

The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

Operation and Support Subsystem (OSS).It is connected to components of the NSS and the BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS. It must be noted that as the number of BS increases with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing savings in the cost of ownership of the system

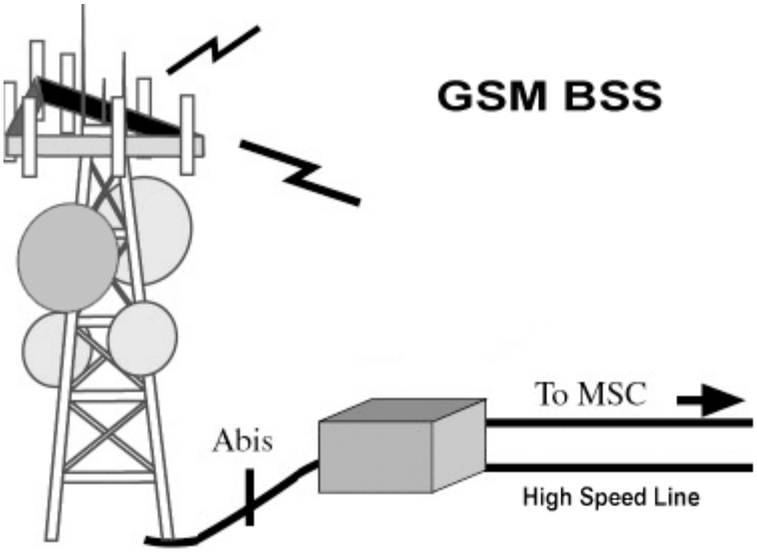
2. Explain in detail about GSM Radio Subsystem

GSM Radio - The base Station Substation

The BSS is composed of two parts:

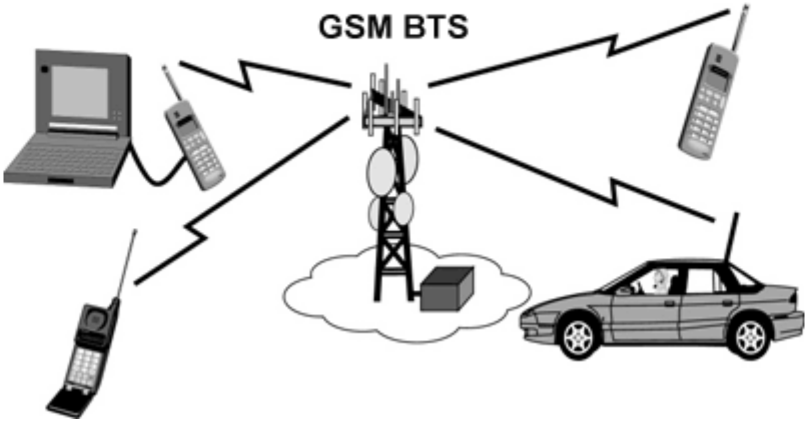
- The Base Transceiver Station (BTS)
- The Base Station Controller (BSC)

The BTS and the BSC communicate across the specified Abis interface, enabling operations between components that are made by different suppliers. The radio components of a BSS may consist of four to seven or nine cells. A BSS may have one or more base stations. The BSS uses the Abis interface between the BTS and the BSC. A separate high-speed line (T1 or E1) is then connected from the BSS to the Mobile MSC.



The Base Transceiver Station (BTS)

The BTS houses the radio transceivers that define a cell and handles the radio link protocols with the MS. In a large urban area, a large number of BTSs may be deployed.



The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between 1 and 16 transceivers, depending on the density of users in the cell. Each BTS serves as a single cell. It also includes the following functions:

- Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the antenna
- Transcoding and rate adaptation
- Time and frequency synchronizing
- Voice through full- or half-rate services
- Decoding, decrypting, and equalizing received signals
- Random access detection
- Timing advances
- Uplink channel measurements

The Base Station Controller (BSC)

The BSC manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers. The BSC is the connection between the mobile and the MSC. The BSC also translates the 13 Kbps voice channel used over the radio link to the standard 64 Kbps channel used by the Public Switched Telephone Network (PSDN) or ISDN.

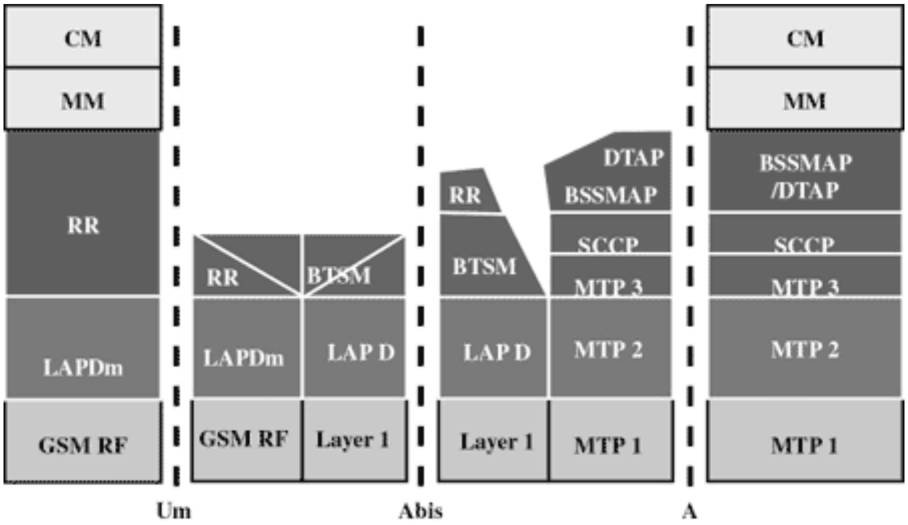
It assigns and releases frequencies and time slots for the MS. The BSC also handles intercell handover. It controls the power transmission of the BSS and MS in its area. The function of the BSC is to allocate the necessary time slots between the BTS and the MSC. It is a switching device that handles the radio resources. Additional functions include:

- Control of frequency hopping
- Performing traffic concentration to reduce the number of lines from the MSC
- Providing an interface to the Operations and Maintenance Center for the BSS
- Reallocation of frequencies among BTSs
- Time and frequency synchronization
- Power management
- Time-delay measurements of received signals from the MS

3. Write short notes on GSM protocol layers for signaling

GSM architecture is a layered model that is designed to allow communications between two different systems. The lower layers assure the services of the upper-layer protocols. Each layer passes suitable notifications to ensure the transmitted data has been formatted, transmitted, and received accurately.

The GMS protocol stacks diagram is shown below:



MS Protocols

Based on the interface, the GSM signaling protocol is assembled into three general layers:

- **Layer 1** : The physical layer. It uses the channel structures over the air interface.
- **Layer 2** : The data-link layer. Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm). Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used.
- **Layer 3** : GSM signalling protocol’s third layer is divided into three sublayers:
    - Radio Resource Management (RR),
    - Mobility Management (MM), and
    - Connection Management (CM).

MS to BTS Protocols

The RR layer is the lower layer that manages a link, both radio and fixed, between the MS and the MSC. For this formation, the main components involved are the MS, BSS, and MSC. The responsibility of the

RR layer is to manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.

The MM layer is stacked above the RR layer. It handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on MS so that incoming call routing can be completed.

The CM layer is the topmost layer of the GSM protocol stack. This layer is responsible for Call Control, Supplementary Service Management, and Short Message Service Management. Each of these services are treated as individual layer within the CM layer. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

BSC Protocols

The BSC uses a different set of protocols after receiving the data from the BTS. The Abis interface is used between the BTS and BSC. At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM). The BTS management layer is a relay function at the BTS to the BSC.

The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS. These services include controlling the initial access to the system, paging for MT calls, the handover of calls between cell sites, power control, and call termination. The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.

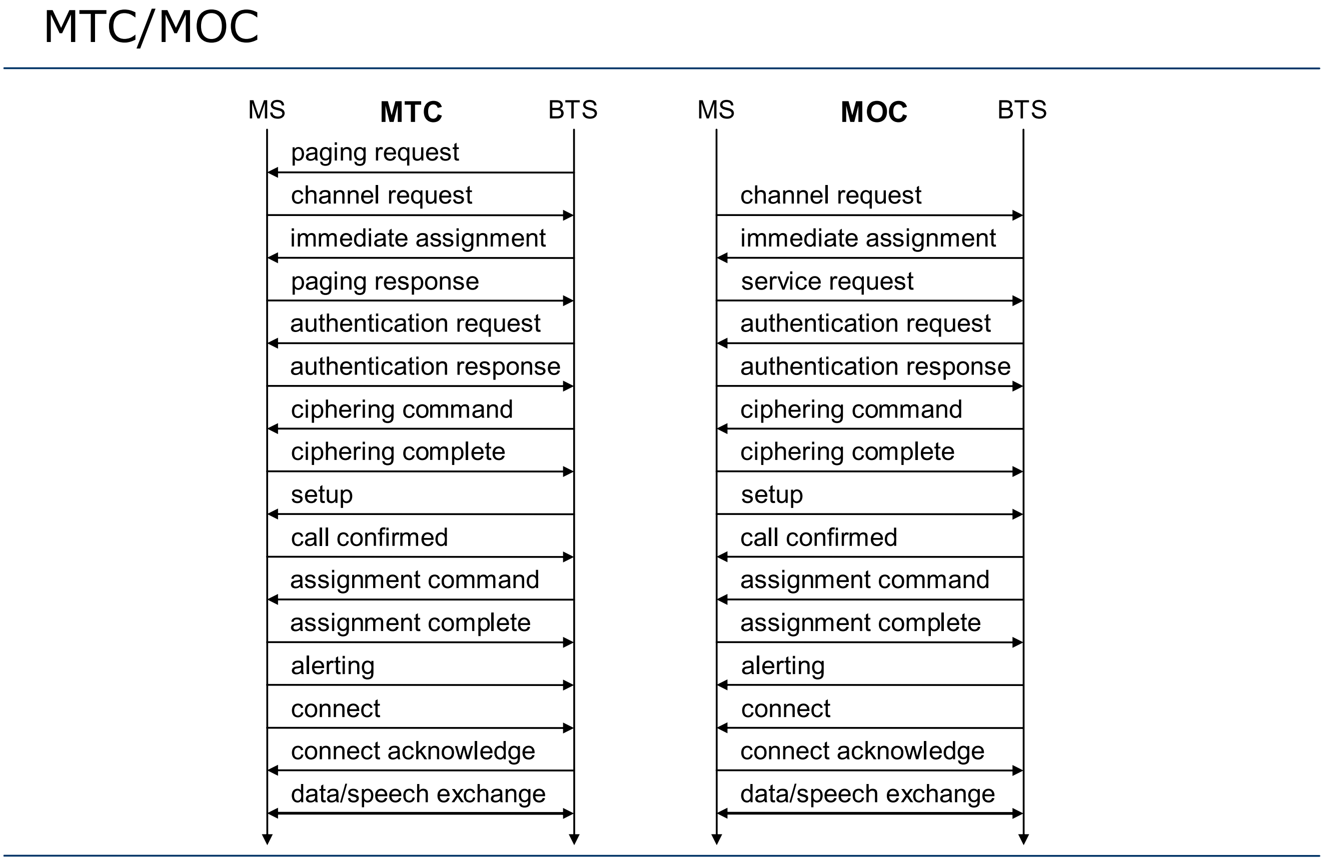
To transit from the BSC to the MSC, the BSS mobile application part or the direct application part is used, and SS7 protocols is applied by the relay, so that the MTP 1-3 can be used as the prime architecture.

MSC Protocols

At the MSC, starting from the BSC, the information is mapped across the A interface to the MTP Layers 1 through 3. Here, Base Station System Management Application Part (BSS MAP) is said to be the equivalent set of radio resources. The relay process is finished by the layers that are stacked on top of Layer 3 protocols, they are BSS MAP/DTAP, MM, and CM. This completes the relay process. To find and connect to the users across the network, MSCs interact using the control-signalling network. Location registers are included in the MSC databases to assist in the role of determining how and whether connections are to be made to roaming users.

Each GSM MS user is given a HLR that in turn comprises of the user's location and subscribed services. VLR is a separate register that is used to track the location of a user. When the users move out of the HLR covered area, the VLR is notified by the MS to find the location of the user. The VLR in turn, with the help of the control network, signals the HLR of the MS's new location. With the help of location information contained in the user's HLR, the MT calls can be routed to the user.

4. Explain the signal required for MOC?



MTC/MOC

MS **MTC** BTS

paging request
channel request
immediate assignment
paging response
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange

MS **MOC** BTS

channel request
immediate assignment
service request
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange

5. Explain the Localization, calling and handover in GSM. (May/June 2013, 2014)

One of the main features of GSM system is the automatic, worldwide localisation of it's users. The GSM system always knows where a user is currently located, and the same phone number is valid worldwide. To have this ability the GSM system performs periodic location updates, even if the user does not use the MS, provided that the MS is still logged on to the GSM network and is not completely switched off. The HLR contains information about the current location, and the VLR that is currently responsible for the MS informs the HLR about the location of the MS when it changes. Changing VLRs with uninterrupted availability of all services is also called roaming. Roaming can take place within the context of one GSM service provider or between two providers in one country, however this does not normally happen but also between different service providers in different countries, known as international roaming.

To locate an MS and to address the MS, several numbers are needed:

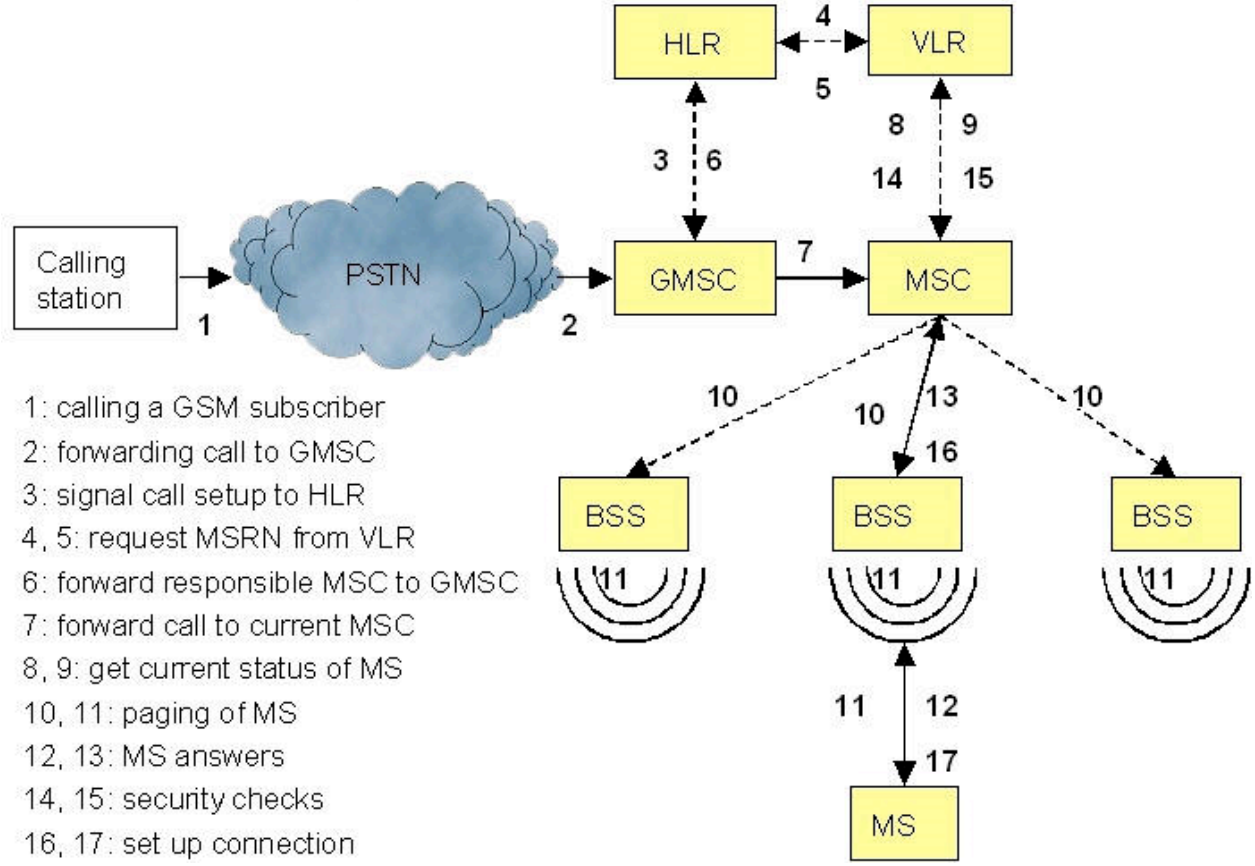
MSISDN (Mobile Station International ISDN Number)16. The only important number for the user of GSM is the phone number, due to the fact that the phone number is only associated with the SIM, rather than a certain MS. The MSISDN follows the E.164, this standard is also used in fixed ISDN networks.

IMSI (International Mobile Subscriber Identity). GSM uses the IMSI for internal unique identification of asubscriber.
TMSI (Temporary Mobile Subscriber Identity). To disguise the IMSI that would give the exact identity of the user which is signaling over the radio air interface, GSM uses the 4 byte TMSI for local subscriber

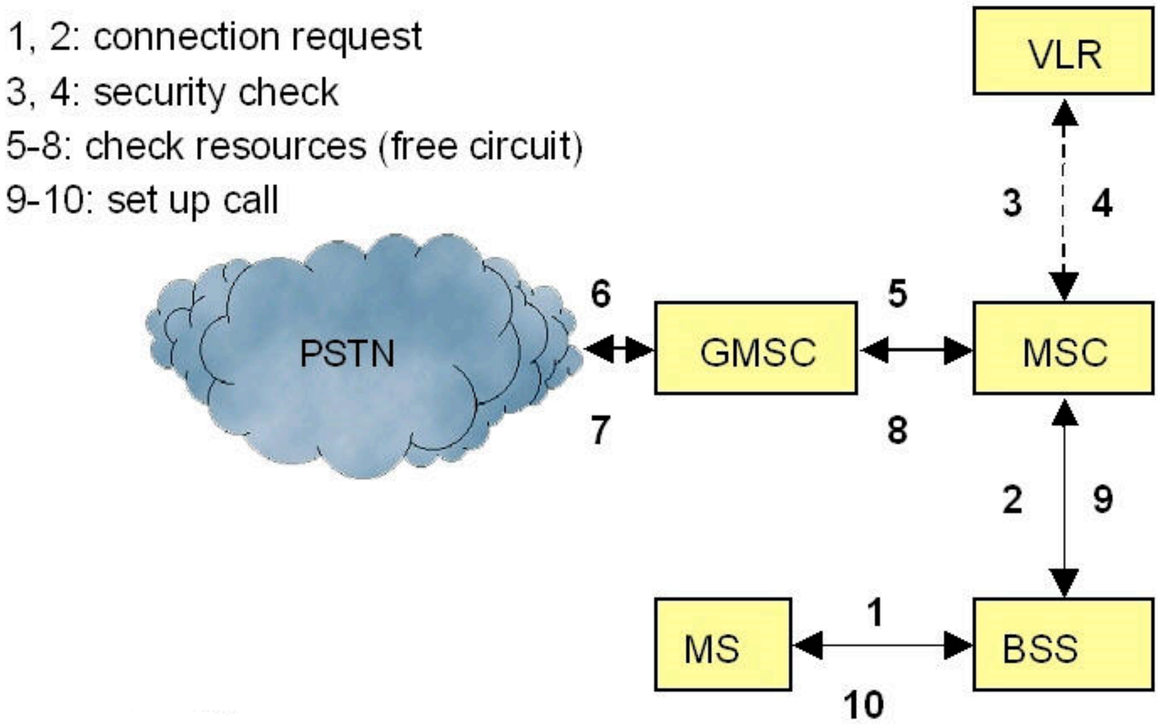
identification. The TMSI is selected by the VLR and only has temporary validity within the location area of the VLR. In addition to that the VLR will change the TMSI periodically.

MSRN (Mobile Station [Subscriber] Roaming Number)17. This is another temporary address that disguises the identity and location of the subscriber. The VLR generates this address upon request from the MSC and the address is also stored in the HLR. The MSRN is comprised of the current VCC (Visitor Country Code), the VNDC (Visitor National Destination Code) and the identification of the current MSC together with the subscriber number, hence the MSRN is essential to help the HLR to find a subscriber for an incoming call.

All the numbers described above are needed to find a user within the GSM system, and to maintain the connection with a mobile station. The following scenarios below shows a MTC (Mobile Terminate Call) and a MOC (Mobile Originated Call).


HLR
4
VLR
5
3
6
8
9
14
15
Calling station
PSTN
GMSC
7
MSC
1
2
1: calling a GSM subscriber
2: forwarding call to GMSC
3: signal call setup to HLR
4, 5: request MSRN from VLR
6: forward responsible MSC to GMSC
7: forward call to current MSC
8, 9: get current status of MS
10, 11: paging of MS
12, 13: MS answers
14, 15: security checks
16, 17: set up connection
10
10
13
10
16
BSS
BSS
BSS
11
11
11
11
12
17
MS

Mobile Terminated Call



Mobile Originated Call

6. How security is implemented in GSM? (April 2015)

The security services offered by GSM are explained below:

Access control and Authentication: To authenticate a valid user for the SIM. The user needs a secret PIN to access the SIM.

Confidentiality: After authentication, BTS and MS apply encryption to voice, data and signaling**.**

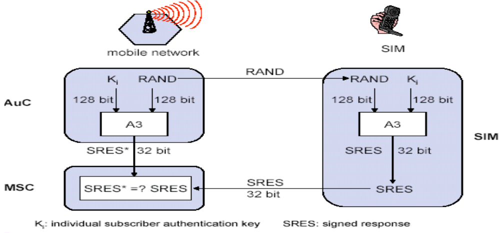
Anonymity: To provide user anonymity, all data is encrypted before transmission

Three algorithms have been specified to provide security services in GSM

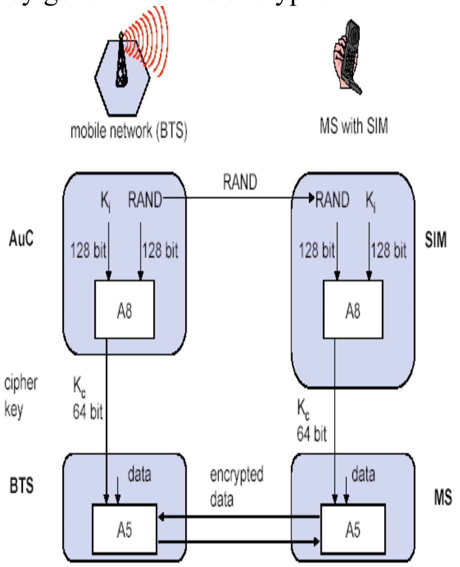
- ❑ Algorithm A3 is used for authentication
- ❑ Algorithm A5 is used for encryption
- ❑ Algorithm A8 is used to generate a cipher key

Authentication

Before a subscriber can use any service from the GSM network, he or she must be authenticated. Authentication is based on the SIM, which stores the individual authentication key Ki, the user identification IMSI, and the algorithm used for authentication A3. Authentication uses a challenge-response method:



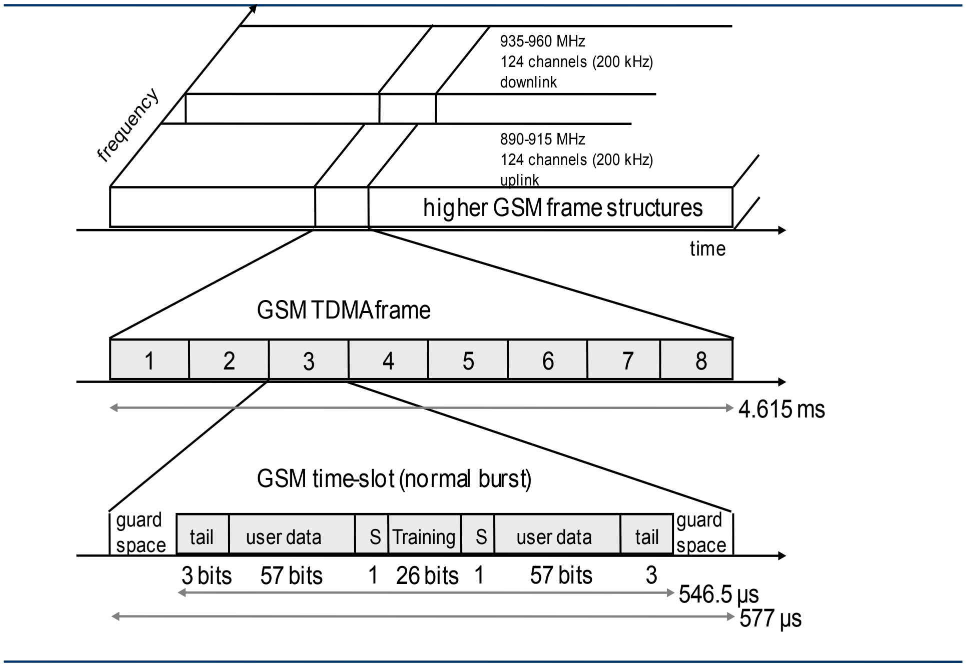
Key generation and encryption



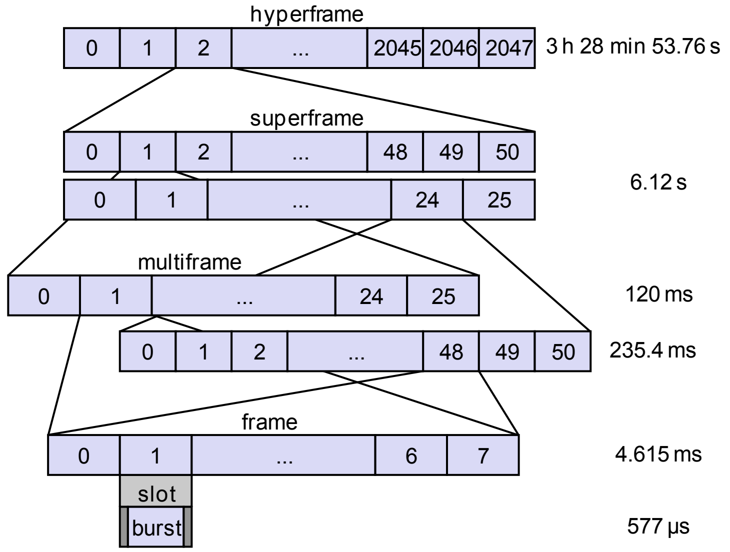
To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface. After authentication, MS and BSS can start using encryption by applying the cipher key Kc (the precise location of security functions for encryption, BTS and/or BSC are vendor dependent). Kc is generated using the individual key Ki and a random value by applying the algorithm A8. Note that 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 overthe air interface.

7. Explain GSM frame format and frame hierarchy

GSM - TDMA/FDMA



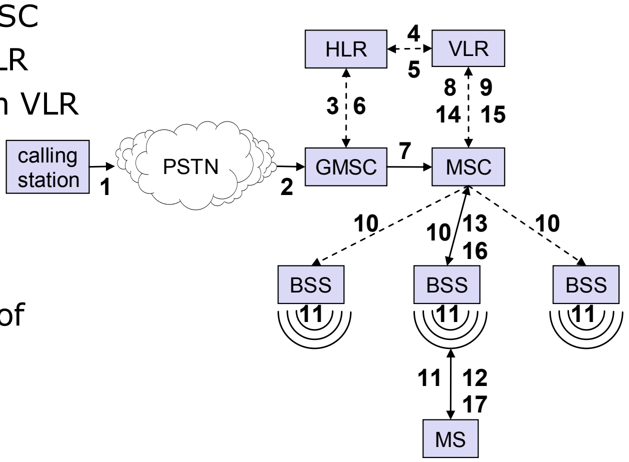
GSM hierarchy of frames



8. Write the Connection Establishment between PSTN and Cellular Architecture? (Nov/Dec 2013)

Mobile Terminated Call

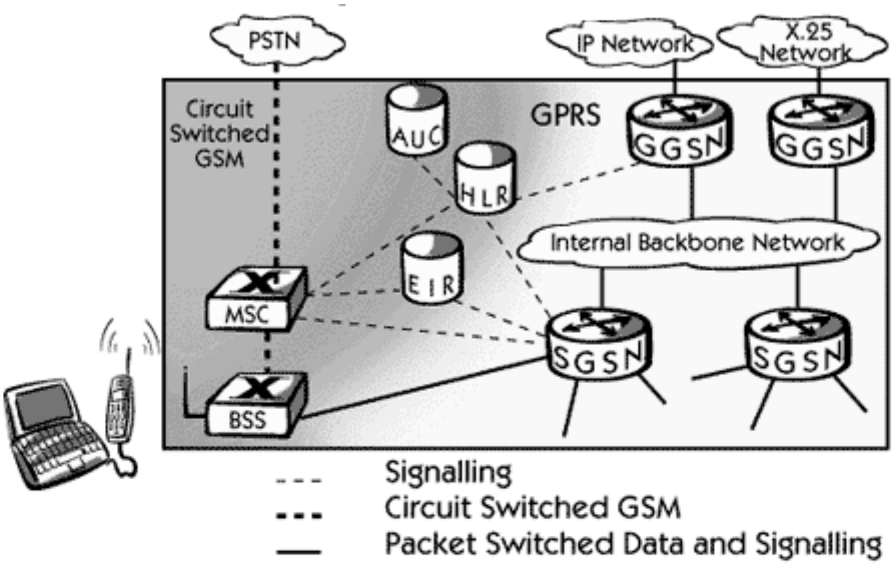
- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4, 5: request MSRN from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to
- current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: set up connection



9. Draw and explain the GPRS architecture (Nov-2011,May/June 2014, Nov/Dec 2014,April2015)

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

Following is the GPRS Architecture diagram:



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

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

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

GPRS Mobile Stations

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

GPRS Base Station Subsystem

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

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

GPRS Support Nodes

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

Gateway GPRS Support Node (GGSN)

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

Serving GPRS Support Node (SGSN)

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

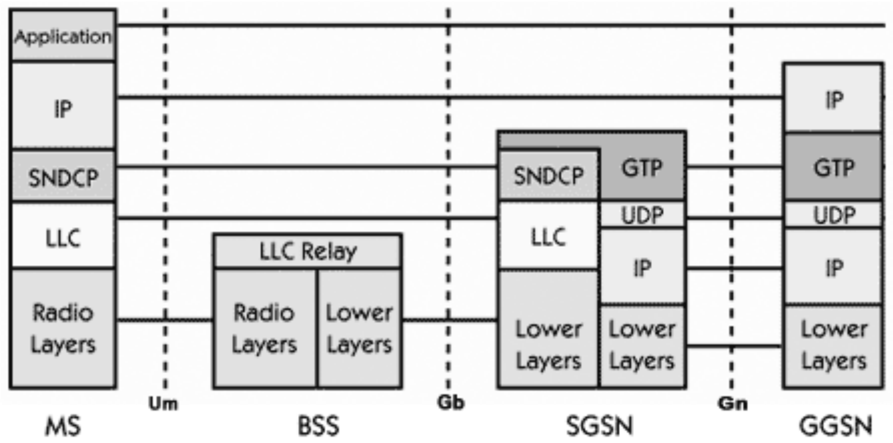
Internal Backbone

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

Routing Area

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

The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface. This is a Layer 3 tunneling protocol.



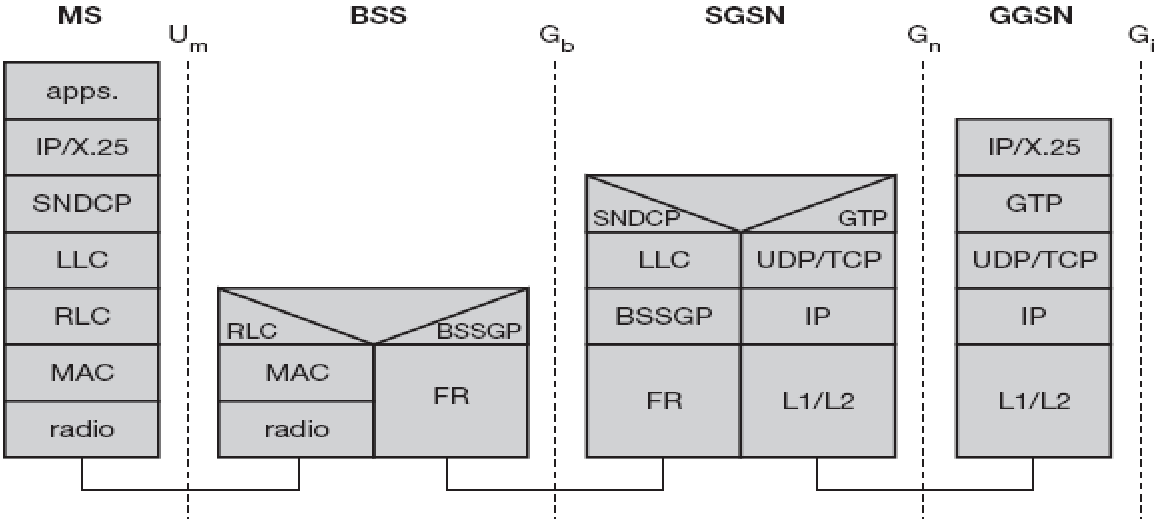
The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The vital thing that needs attention is, the application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.

SubNetwork Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.

In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

10. Write short notes on GPRS Transmission Plane Protocol Reference Model (Nov/Dec 2013)

GPRS Transmission Plane Protocol Reference Model**:**



In any telecommunication system, signalling is required to coordinate the necessarily distributed functional entities of the network.

The transfer of signalling information in GSM follows the layered OSI model

‘Layer 1: Physical Layer

- Radio TransmissionRadio layer (layer 1)
- Handles all radio specific functions, Um uses GMSK for digital modulation & performs encryption / decryption of data

Functions are

- Creation of burst
- Multiplexing of bursts
- Synchronization with BTS
- Detection of Idle channel
- Measurement of channel quality on downlink
  - Synchronization between MS and BTS
    - Based on RTT (Round Trip Time)
    - Ms close to BTS will have less RTT
    - Ms far-away from BTS have more RTT (0.23 ms)
- Main function of physical layer
  - Channel coding
  - Error detection

Channel coding

- Extensive use of different Forward Error Correction (FEC) scheme
- FEC Adds redundancy to user data allowing for the detection & correction of selected errors
- Power of FEC depends on
  - Amount of redundancy
  - Coding algorithm
  - Interleaving of data to minimize the effects of burst errors

Layer 2: Data Link Layer (DLL)

- provides error-free transmission between adjacent entities, based on the ISDN’s LAPD protocol for the Um and Abis interfaces, and on SS7’s Message Transfer Protocol (MTP) for the other Layer interfaces

It offers

- Reliable data transfer over connections
- Re-sequencing of data frames
- Flow control
- Segmentation
- Acknowledged/ un-Acknowledged data transfer

Layer 3: Networking or Messaging Layer

RR (Radio Resource management)

- Implemented in BTS & supported by BSC through BTS Management (BTSM)
- Main tasks are
  - Connection setup
  - Maintenance
  - Release of radio channels

- Responsible for the communication of network resources, mobility, code format and call-related management messages between various network entities

MM (Mobility Management)

- Functions are
    - Registration
    - Authentication
    - Identification
    - Location updating
    - Provision of TMSI which replaces IMSI for security reasons

CM (Call Management)

- Contains 3 entities
    - Call control (CC)
    - Short message Services (SMS)
    - Supplementary services (SS)

PCM - Pulse code modulation

SS7 – Signaling system no. 7

- Signaling between BSC & MSC
- Ss7- used to transfer management information between MSCs, VLR, HLR, EIR, AuC and OMC

BSSAP (BSS Application Part)

- Ms controls various BSS Via BSS Application Part

- **Um**
    - Radio interface between MS and BTS
    - each physical channel supports a number of logical channels
- **Abis**
    - between BTS and BSC
    - primary functions: traffic channel transmission, terrestrial channel management, and radio channel management

- **A**
    - between BSC and MSC
    - primary functions: message transfer between different BSCs to the MSC

The data link layer (layer 2) over the radio link is based on a modified LAPD (Link Access Protocol for the D channel) referred to as LAPDm (m like mobile). On the A-bis interface, the layer 2 protocol is based on the LAPD from ISDN. The Message Transfer Protocol (MTP) level 2 of the SS7 protocol is used at the A interface.

At the MS, there is RF interface, above which are Radio Link Control and Medium Access Control functions. Above these are Logical Link Control (LLC) which provides a logical link and framing structure for communication between the MS and the SGSN. Any data between MS and SGSN is sent as Logical Link – Protocol Data Units (LLPDU). LLC supports management of this transfer, including mechanism for the detection and recovery from, lost or corrupted LL-PDU, ciphering and flow control.

Above LLC, is Sub Network Dependent Convergence Protocol (SNDCP) which resides between LLC and the network layer (such as IP and X.25) . The purpose of SNDCP is to enable support for multiple network protocols without having to change the lower layers such as LLC. It also help to multiplex several packet streams into a single logical channel between MS and SGSN.

At the BSS, a relay function relays LL_PDU from Gb interface to the air interface (the Um interface). Similarly, at SSGN, a relay function relays PDP PDUs between the Gb interface and the Gn interface.

GTP- GPRS Tunneling Protocol: All data within GPRS backbone is transferred GTP. It can use different transport protocols either the reliable TCP (needed for reliable transfer of X.25 packets) or the non reliable UDP – used for packet IP. Tunneling is the procedure of wrapping up the connection and its associated packets in a wrapper for transmission through the IP network between GGSN and SGSN. In this case, the IP network nodes (routers) between the SGSN and GGSN consider the GTP packets to be application and those routers do not examine the contents of the GTP layer. At the SGSN, the wrapper is removed and the packet is passed to the MS using SNDCP, LLC and the lower layers. For the packets from MS to external network- such as internet, the GGSN removes the wrapper and forwards the IP packets

11. Explain in detail about Universal Mobile Telecommunication System

The Universal Mobile Telecommunications System (UMTS) is a third generation mobile cellular system for networks based on the GSM standard. Developed and maintained by the 3GPP (3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set and compares with the CDMA2000 standard set for networks based on the competing cdmaOne technology. UMTS uses wideband code division multiple access (W-CDMA) radio access technology to offer greater spectral efficiency and bandwidth to mobile network operators.

Features

UMTS specifies a complete network system, which includes the radio access network (UMTS Terrestrial Radio Access Network, or UTRAN), the core network (Mobile Application Part, or MAP) and the authentication of users via SIM (subscriber identity module) cards.

The technology described in UMTS is sometimes also referred to as Freedom of Mobile Multimedia Access (FOMA)[1] or 3GSM.

Unlike EDGE (IMT Single-Carrier, based on GSM) and CDMA2000 (IMT Multi-Carrier), UMTS requires new base stations and new frequency allocations.

UMTS supports maximum theoretical data transfer rates of 42 Mbit/s when Evolved HSPA (HSPA+) is implemented in the network.[2] Users in deployed networks can expect a transfer rate of up to 384 kbit/s for Release '99 (R99) handsets (the original UMTS release), and 7.2 Mbit/s for High-Speed Downlink Packet Access (HSDPA) handsets in the downlink connection. These speeds are significantly faster than the 9.6 kbit/s of a single GSM error-corrected circuit switched data channel, multiple 9.6 kbit/s channels in High-Speed Circuit-Switched Data (HSCSD) and 14.4 kbit/s for CDMAOne channels.

Since 2006, UMTS networks in many countries have been or are in the process of being upgraded with High-Speed Downlink Packet Access (HSDPA), sometimes known as 3.5G. Currently, HSDPA enables downlink transfer speeds of up to 21 Mbit/s. Work is also progressing on improving the uplink transfer speed with the High-Speed Uplink Packet Access (HSUPA). Longer term, the 3GPP Long Term Evolution (LTE) project plans to move UMTS to 4G speeds of 100 Mbit/s down and 50 Mbit/s up, using a next generation air interface technology based upon orthogonal frequency-division multiplexing.

The first national consumer UMTS networks launched in 2002 with a heavy emphasis on telco-provided mobile applications such as mobile TV and video calling. The high data speeds of UMTS are now most often utilised for Internet access: experience in Japan and elsewhere has shown that user demand for video calls is not high, and telco-provided audio/video content has declined in popularity in favour of high-speed access to the World Wide Web—either directly on a handset or connected to a computer via Wi-Fi, Bluetooth or USB

Technology:

UMTS combines three different air interfaces, GSM's Mobile Application Part (MAP) core, and the GSM family of speech codecs.

Air interfaces

UMTS provides several different terrestrial air interfaces, called UMTS Terrestrial Radio Access (UTRA).[3] All air interface options are part of ITU's IMT-2000. In the currently most popular variant for cellular mobile telephones, W-CDMA (IMT Direct Spread) is used.

Please note that the terms W-CDMA, TD-CDMA and TD-SCDMA are misleading. While they suggest covering just a channel access method (namely a variant of CDMA), they are actually the common names for the whole air interface standards.[4]

W-CDMA (UTRA-FDD)

3G sign shown in notification bar on an Android powered smartphone.

W-CDMA uses the DS-CDMA channel access method with a pair of 5 MHz wide channels. In contrast, the competing CDMA2000 system uses one or more available 1.25 MHz channels for each direction of communication. W-CDMA systems are widely criticized for their large spectrum usage, which has delayed deployment in countries that acted relatively slowly in allocating new frequencies specifically for 3G services (such as the United States).

The specific frequency bands originally defined by the UMTS standard are 1885–2025 MHz for the mobile-to-base (uplink) and 2110–2200 MHz for the base-to-mobile (downlink). In the US, 1710–1755 MHz and 2110–2155 MHz are used instead, as the 1900 MHz band was already used.[5] While UMTS2100 is the most widely deployed UMTS band, some countries' UMTS operators use the 850 MHz and/or 1900 MHz bands (independently, meaning uplink and downlink are within the same band), notably in the US by AT&T Mobility, New Zealand by Telecom New Zealand on the XT Mobile Network and in Australia by Telstra on the Next G network. Some carriers such as T-Mobile use band numbers to identify the UMTS frequencies. For example, Band I (2100 MHz), Band IV (1700/2100 MHz), and Band V (850 MHz).

W-CDMA is a part of IMT-2000 as IMT Direct Spread.

UMTS-FDD, is an acronym for Universal Mobile Telecommunications System (UMTS) - frequency-division duplexing (FDD) and a 3GPP standardized version of UMTS networks that makes use of frequency-division duplexing for duplexing over an UMTS Terrestrial Radio Access (UTRA) air interface.[6]

W-CDMA or WCDMA (Wideband Code Division Multiple Access), along with UMTS-FDD, UTRA-FDD, or IMT-2000 CDMA Direct Spread is an air interface standard found in 3G mobile telecommunications networks. It supports conventional cellular voice, text and MMS services, but can also carry data at high speeds, allowing mobile operators to deliver higher bandwidth applications including streaming and broadband Internet access.[7]

W-CDMA is the basis of Japan's NTT DoCoMo's FOMA service and the most-commonly used member of the Universal Mobile Telecommunications System (UMTS) family and sometimes used as a synonym for UMTS.[8] It uses the DS-CDMA channel access method and the FDD duplexing method to achieve higher speeds and support more users compared to most previously used time division multiple access (TDMA) and time division duplex (TDD) schemes.

While not an evolutionary upgrade on the airside, it uses the same core network as the 2G GSM networks deployed worldwide, allowing dual mode mobile operation along with GSM/EDGE; a feature it shares with other members of the UMTS family.

UNIT IV Part-A

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

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

2. Define MANET (Nov 2012)

Temporary or Adhoc networks that are established and maintained and work without the support of any form of fixed infrastructure such as base station are known as Mobile Adhoc Networks(MANET). It is traditionally defined as self configuring networks set up among handheld devices of mobile users.

3. Why the routing is complex in MANET

- Very difficult to assign a global identifier assigned to every node due to mobility.
- MANET the topology of the network and consequently the routes between different device changes dynamically as nodes move away or fail.
- link breakage
- Centralized approaches will not work. Many nodes need routing capabilities

4. List out the characteristics of MANET?

- Lack of fixed infrastructure, Dynamic Topologies
- The speed of the movement of a mobile device can vary with time of the day, Bandwidth constrains such as fading, noise, interference, variable capacity links,
- Energy constrained operation, increased vulnerability, Autonomous terminal, Multi hop environment.

5. Write the applications of MANET

- Communications among portable computer: To reduce the mobility of the device
- Environmental monitoring: continuous data collection from remote location,
- Military: information network among the soldiers, vehicles and military information
- Emergency operation: quickly setup to provide network connectivity to rescue personnel in order to facilitate the rescue operation.

6. List out the MANET design issues

- Network size and node density: geographical coverage area of the network and network density refers to the number of network in the area.
- Connectivity: bandwidth of the link
- Network topology: connectivity among the various nodes to the network
- User traffic: Bursty traffic, large packet sent periodically
- Operational environment: LOS
- Energy constraint: Allow the node to go into sleep mode whenever possible

7. What is routing and MANET routing?

- Routing: To find the best path between the source and destination for forwarding packets in any store and forward network.

- MANET Routing: Each node in an adhoc network needs to have routing capability and also need s to participate in routing to keep the network operational.

8. Write the steps involved in transferring the packet in MANET

Forward the packet to the next hop

While forwarding, the sender needs to ensure that

- The packet moves towards its destination
- The number of hop/path length is minimized.
- Delay is minimized
- The packet loss is minimized
- The packet does not move around the network endlessly.

9. Write the essentials of traditional routing protocols

- Require a node to determine the next hop along the shortest path towards a given destination.
- The shortest path is computed according to some specific cost metric such as number of hops in the route.
- Example: distance vector, link state routing

10. What is LSPDB? and its advantages.

- A router in the network receives the link state advertisement; it stores the packet in a data base called LSPDB.
- Each router constructs the connectivity information for the entire network as a graph using shortest path algorithm.

11.Write the basic characteristics of LSP

- Every router construct a graph representing the connectivity between the various nodes in the network based on the information received from other routers.
- The graph representing the network is usually constructed in the form of a tree with local router forming the root of the tree.
- The graph captures the shortest path route from the root to any other router.

12. Write the contents of LSP advertisement message

- The identity of the router originating message, Identity of its entire neighbors
- The delay along various links to its neighbors, A unique sequence number, which is formed by increasing the count every time the router forms a new link state advertisement.
- This link state advertisement is then flooded throughout the network as follows: send a copy of a state advertisement to all of its neighbors
- A router receiving this message examines the sequence number of the last link state advertisement from the originating router by consulting its LSPDB.

13. What is distance vector routing protocol

The term vector means that routes are advertised as a vector such as distance direction. Where distance the number of hops between the two nodes and direction is defined in terms of the next hop router to which the packets need to be forward.. It is based on Bellman ford algorithm.. Based on calculating the distance and direction to any router in a network.. The cost is calculated using various route metrics.

14. Compare routing in MANET vs routing in traditional network

MANET	Traditional Network
Each node act as a router	Do not participate in routing packet
Topology is dynamic	Topology is static
No IP based addressing	IP based addressing

15. Write the three types of communication

- Unicast: Message is sent to single destination
- Multicast: Message is sent to a selected subset of the network.
- Broadcast: Message is sent to all the nodes in the network
- MANET can broadly be classified into unicast and multicast types.

16. Write a classification of Unicast MANET routing protocol (Nov 2014, June 2013)

The classification is based on how a protocol manages to determine the route correctly in the presence of topology changes. They are proactive and reactive protocols

- Proactive: they are table driven routing protocol. It maintains information about routes to every other node in the network. E.g. Destination sequenced Distance Vector.
- Reactive protocols: On demand routing protocol EG Dynamic source routing, Adhoc on demand distance vector routing.

17. What is destination sequenced distance vector Routing Protocol?

- It maintains a routing table in which all of the possible destinations and number of hops to each destination are recorded.
- Each node maintains information regarding routes to all the known destinations.
- The routing information is updated periodically.
- To maintain a traffic overhead ,each node maintain routes which they may never use.

18. What is dynamic source routing?

It maintains a routing cache which contains the list of all routes that the node has learnt. When a node finds a new route it adds the new route to its cache.. each mobile node also maintain sequence counter called request id to uniquely identify the last request it had generated.. It works in two phase: Route discovery (ii) route maintenance.

19. What is VANET?

Vehicular Adhoc Network (VANET).It is a special type of MANET in which moving automobiles from the nodes of the network. Vehicle communicates with other vehicles that are within a range about 100m to 300 mts.

20. Explain MANET VS VANET

MANET	VANET
Collection of mobile nodes communicates with each other over bandwidth constrained wireless links	Can communicate with certain roadside infrastructure or base station
Mobility is more random.	Node mobility is considered to the road Topology
Battery power is major constrain	Battery power is adequate.

21. Write the characteristics of secure ad hoc networks

- Availability: to service DOS attacks
- Confidentiality: preventing its access by unauthorized users
- Integrity: No transferred message has been tampered
- Authentication: True identification of a peer node
- Non repudiation: sent message cannot deny it

22. Write the attacks on different Layers

- Application Layer: Malicious code, repudiation, data corruption
- Transport Layer: session hijacking, SYN flooding
- Network Layer: Wormhole, black hole, fabrication attack
- Data Link Layer: Resource consumption
- Physical layer: Traffic analysis, monitoring, disruption
- Multilayer: DOS, impersonation, replay

23. Write any two factors that affect the performance of ADHOC networking? (Nov 2013)

Node speed, pause-time, network size, number of traffic sources, and type of routing (source Versus distributed), that affect the performance of ad hoc networks.

24. What do you mean by zone routing protocol? (Nov 2013)

ZRP is a hybrid Wireless Networking routing protocol that uses both proactive and reactive routing protocols when sending information over the network. ZRP was designed to speed up delivery and reduce processing overhead by selecting the most efficient type of protocol to use throughout the route.

25. List the applications of Mobile Adhoc Network

Environmental monitoring -Traffic, habitat, security

Industrial sensing and diagnostics-Manufacturing, supply chains

Context-aware computing-Intelligent homes

Military applications: Multi-target tracking

Infrastructure protection: Power grids

Part B UNIT IV

1. **What are the characteristics to design on a MANET? Explain its implications**

Characteristics to design on a MANET

Lack of fixed infrastructure: A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omni directional (broadcast), highly- directional (point-to-point). At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi hop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.--is often much less than a radio's maximum transmission rate.

Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation due to substantial amount of energy causing the batteries to get rapidly drained out unless the protocol is carefully designed.

Increased vulnerability: Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

2. (i) Explain in detail about MANET design issue

Network Size and Node Density: Network size refers to the geographical coverage area of the network and network density refers to the number of nodes present per unit geographical area. The cluster size Depend on node density.

Connectivity: The Term connectivity of a node usually refers to the number of neighbors it has. Connectivity between two nodes also sometimes used to refer to a link between the two nodes. The term link capacity denotes the bandwidth of the link.

Network Topology: The topology of a network denoted connectivity among the various nodes of thee network. The mobility of the nosed affects a network topology. Other than mobility nodes can become in operative due to discharge batteries or hardware failures, and thereby causing changes topology. It should be appropriate in design of Network.

User Traffic: The traffic in a network can be various types: They are Bursty Traffic, Large packet sent periodically, Combinations of the above two Types.

Operational Environment: The operational environment supports the Line of Sight (LOS) Communication. But there can be significant difference in the node density and mobility values in different operational environments requiring different design of mobile network to suit an operational environment.

Energy constraint: There is no fixed infrastructure exist in a MANET. The Mobile node themselves store and forward packets. This additional role of mobile nodes as routers leads to nodes incurring perennial routing related workload and this consequently results in continual battery drainage. Though this overhead is indispensible if the network is to be kept operational the energy spent can be substantially reduced by allowing the nodes to go into a sleep node whenever possible.

(ii) Write about routing

The purpose of routing is to find the best path between the source and destination for forwarding packets in any store and forward network. It is necessary to find a new route each time a node needs to transmit a message making routing an expensive and difficult task. Routing is usually performed by a dedicated device called a router. Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a *routing table* to determine the best path

Forward the packet to the next hop

While forwarding, the sender needs to ensure that

- The packet moves towards its destination
- The number of hop/path length is minimized.
- Delay is minimized
- The packet loss is minimized
- The packet does not move around the network endlessly

3. (i)Explain in detail about LSP with example

The term link denotes the connection of one router to its neighboring router. A neighbor of a router is one with which it can directly communicate without taking any help from any of the intervening routers. Each router determines its local connectivity information and flood the network with this information with Link state advertisement. As a router in the network receives this Link state advertisement it stores this packet in a link state packet Data Base (LSPDB).. The storage of link state advertisement in an LSPDB is in addition to the routing table that each router maintains. All routers in the network have identical LSPBDs.. Based on the bits and piece of information stored in the LSPDB, each router construct the connectivity information for the entire network as a graph using Dijastras Shortest Path Algorithm.. Once a router construct this graph it computes the routing table from this and uses in all its routing decision. Thus Routing in the LSP bases its routing decision on message s received from other routers in the network regarding their link state or the state of this connectivity with other routers. The basic characteristics of LSP is that every router construct a graph representing the connectivity between the various nodes in the network based on the information received from other routers.

In a Link state protocol each router periodically determines the state of its neighbors by exchanging hello packets with them across all its network interfaces.. A router is connected to the other routers through link established by its network interface. Based on the reply received from its neighbors the router determines the state of the link in terms of the delay and other characteristics. Subsequently the router forms a short message called the link state advertisement and sends to its neighbors.. A link state advertisement is also sent by router whenever it experiences any connectivity changes. The Link state advertisement messages are usually the following:

The identity of the router originating the message

The identities of all its neighbors

The delay along various links to its neighbors

A unique sequence number formed by increasing the count every time the router forms a new link state advertisement.

The LS advertisement is then flooded throughout the Network as follows

A router sends a copy of a link state advertisement to all of its neighbors. A router receiving this message examines the sequence number of the last link state advertisement from the originating router by consulting its LSPDB. It is recent it replaces the last message with the currently received message in its LSPDB and also forwards a copy of this link state advertisement to each of its neighbors.

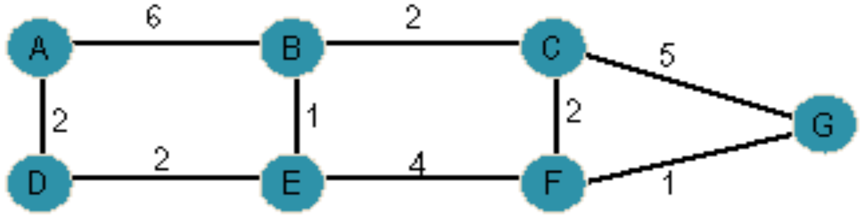
Construction of Link state Tree: A router maintains two data structure tree containing nodes which are done and a list of candidates..This tree is essentially ashotest path first (SPF) tree.

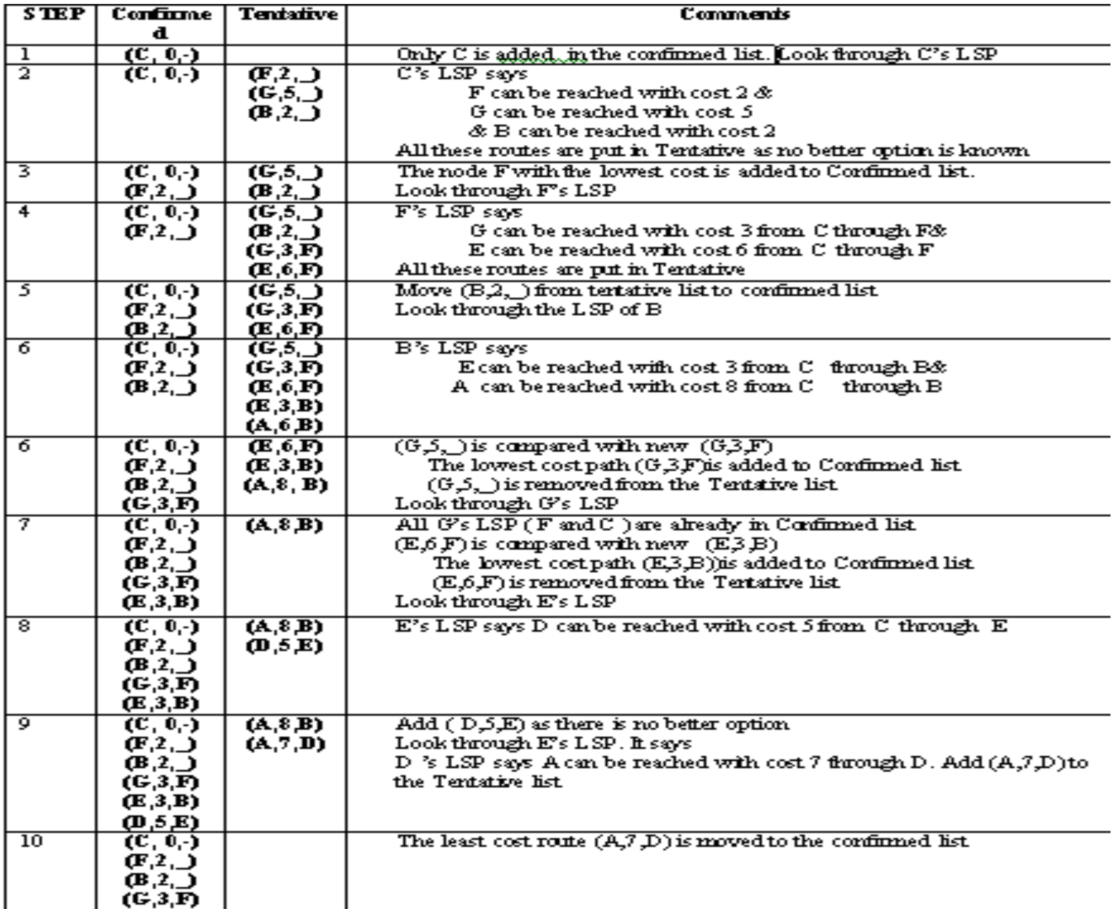
- Greedy iterative Algorithm: All routes are connected to the router just added to the tree excepting any routers which are either already present in the tree or in the candidate list are added to the candidate list.

- The delay from each router in the candidate list to every other router in the tree is compared. The candidate router having the shortest delay is moved into the tree and attached to the appropriate neighbor router. Whenever a router is moved from the candidate list into the tree it is removed from the candidate list.

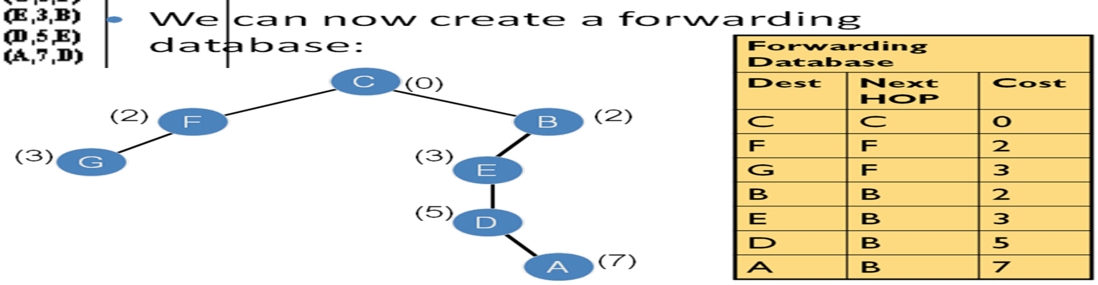
The above two steps are repeated till there are no more routers left in the candidate list.. If different routers somehow have maps that are inconsistent the routing loops can form.

Example:





STEP	Confirmed	Tentative	Comments
1	(C, 0,-)		Only C is added. in the confirmed list. Look through C's LSP
2	(C, 0,-)	(F,2,_) (G,5,_) (B,2,_)	C's LSP says F can be reached with cost 2 & G can be reached with cost 5 & B can be reached with cost 2 All these routes are put in Tentative as no better option is known
3	(C, 0,-) (F,2,_)	(G,5,_) (B,2,_)	The node F with the lowest cost is added to Confirmed list. Look through F's LSP
4	(C, 0,-) (F,2,_)	(G,5,_) (B,2,_) (G,3,F) (E,6,F)	F's LSP says G can be reached with cost 3 from C through F& E can be reached with cost 6 from C through F All these routes are put in Tentative
5	(C, 0,-) (F,2,_) (B,2,_)	(G,5,_) (G,3,F) (E,6,F)	Move (B,2,_) from tentative list to confirmed list Look through the LSP of B
6	(C, 0,-) (F,2,_) (B,2,_)	(G,5,_) (G,3,F) (E,6,F) (E,3,B) (A,6,B)	B's LSP says E can be reached with cost 3 from C through B& A can be reached with cost 8 from C through B
6	(C, 0,-) (F,2,_) (B,2,_) (G,3,F)	(E,6,F) (E,3,B) (A,8, B)	(G,5,_) is compared with new (G,3,F) The lowest cost path (G,3,F)is added to Confirmed list (G,5,_) is removed from the Tentative list Look through G's LSP
7	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B)	(A,8,B)	All G's LSP (F and C) are already in Confirmed list (E,6,F) is compared with new (E,3,B) The lowest cost path (E,3,B))is added to Confirmed list (E,6,F) is removed from the Tentative list Look through E's LSP
8	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B)	(A,8,B) (D,5,E)	E's LSP says D can be reached with cost 5 from C through E
9	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B) (D,5,E)	(A,8,B) (A,7,D)	Add (D,5,E) as there is no better option Look through E's LSP. It says D 's LSP says A can be reached with cost 7 through D. Add (A,7,D)to the Tentative list
10	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B) (D,5,E) (A,7,D)		The least cost route (A,7,D) is moved to the confirmed list



- We can now create a forwarding database:

Forwarding Database

Dest	Next HOP	Cost
C	C	0
F	F	2
G	F	3
B	B	2
E	B	3
D	B	5
A	B	7

4. Write short notes on Distance Vector protocol

Distance Vector Routing :Each node constructs a one-dimensional array (a vector) containing the "distances" (costs) to all other nodes.

distributes that vector to its immediate neighbors.

- Each node knows the cost of the link to each of its directly connected neighbors.
- A link that is down/unknown is assigned an infinite cost.

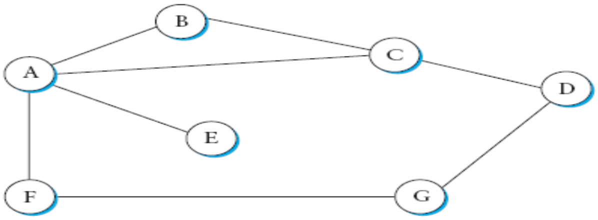
PRINCIPLE: Constructing RIP message

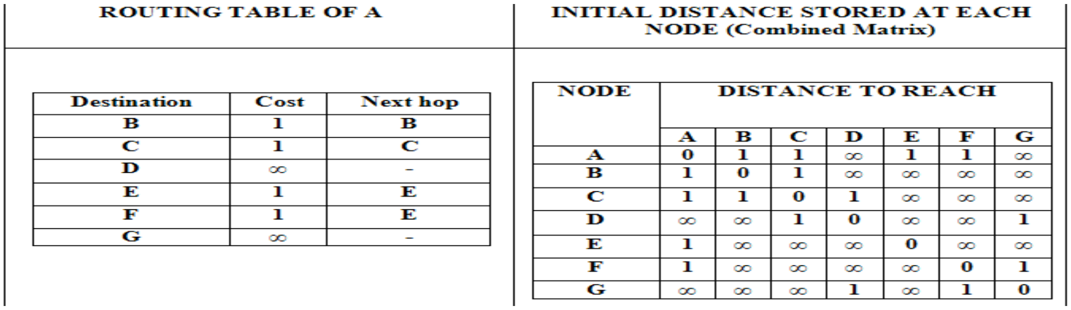
Step 1: Each node sets a cost of 1 (one) to all directly connected neighbors and cost of ∞ to others in the neighbors.

Step 2: Each node sends a message to its directly connected neighbor s containing its knowledge of distances of all nodes in the network.

```
Repeat the following steps for each advertised destination:
        1. If (destination not in the routing table)
            Add the advertised information to the table by adding
          the two costs
       2. Else (
    one. (Because this may be new)
             Else (next-hop field destination in the routing table)
             If (next-hop field is the same) Replace entry in the
        table with the advertised is not the same)
             If (advertised hop count smaller than one in
           the table) Replace entry in the routing table. (better one
3. Return.
```

- Initially, each node sets a cost of 1 to its directly connected neighbors and ∞ to all other nodes.
- Thus, A initially believes that it can reach B ,C, E, F in one hop and that D is unreachable.





ROUTING TABLE OF A

Destination	Cost	Next hop
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	E
G	∞	-

INITIAL DISTANCE STORED AT EACH NODE (Combined Matrix)

NODE	DISTANCE TO REACH						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

5. Explain in detail about proactive routing protocol with example (Nov 2014, June 2013)

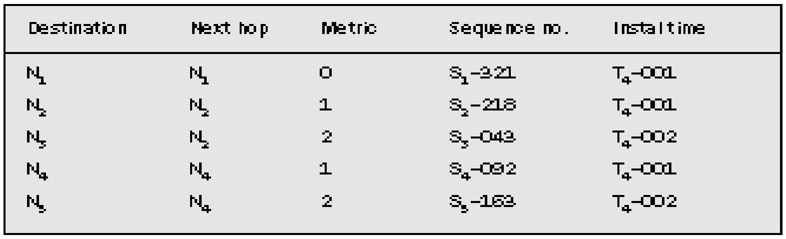
Proactive protocols: In networks utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain a up-to-date routing information from each node to every other node.

DESTINATION SEQUENCE DISTANCE VECTOR (DSDV) routing is an enhancement to distance vector routing for ad-hoc networks (Perkins, 1994). DSDV can be considered historically, however, an on-demand version (ad-hoc on-demand distance vector, AODV) is among the protocols currently discussed (see section 8.3.5). Distance vector routing is used as routing information protocol (RIP) in wired networks. It performs extremely poorly with certain network changes due to the count-to-infinity problem. Each node exchanges its neighbor table periodically with its neighbors. Changes at one node in the network propagate slowly through the network (step-by-step with every exchange). The strategies to avoid this problem which are used in fixed networks (poisoned-reverse/splithorizon (Perlman, 1992)) do not help in the case of wireless ad-hoc networks, due to the rapidly changing topology. This might create loops or unreachable regions within the network.

DSDV now adds two things to the distance vector algorithm:

● **Sequence numbers:** Each routing advertisement comes with a sequence number. Within ad-hoc networks, advertisements may propagate along many paths. Sequence numbers help to apply the advertisements in correct order. This avoids the loops that are likely with the unchanged distance vector algorithm.

● **Damping:** Transient changes in topology that are of short duration should not destabilize the routing mechanisms. Advertisements containing changes in the topology currently stored are therefore not disseminated further. A node waits with dissemination if these changes are probably unstable. Waiting time depends on the time between the first and the best announcement of a path to a certain destination.



Destination	Next hop	Metric	Sequence no.	Instaltime
N_1	N_1	0	S_1-321	T_4-001
N_2	N_2	1	S_2-218	T_4-001
N_3	N_2	2	S_3-043	T_4-002
N_4	N_4	1	S_4-092	T_4-001
N_5	N_4	2	S_5-163	T_4-002

For each node N1 stores

- the toward this node,
- the metric (next hop here number of hops),
- the sequence number of the last advertisement for this node,
- the time at which the path has been installed first.

The table contains flags and a settling time helping to decide when the path can be assumed stable. Router advertisements from N1 now contain data from the first, third, and fourth column: destination address, metric, and sequence number. Besides being loop-free at all times, DSDV has low memory requirements and a quick convergence via triggered updates.

6. Explain about Dynamic source routing **(May/June 2013,April 15)**

DYNAMIC SOURCE ROUTING:

Imagine what happens in an ad-hoc network where nodes exchange packets from time to time, i.e., the network is only lightly loaded, and DSDV or one of the traditional distance vector or link state algorithms is used for updating routing tables. Although only some user data has to be transmitted, the nodes exchange routing information to keep track of the topology. These algorithms maintain routes between all nodes, although there may currently be no data exchange at all. This causes unnecessary traffic and prevents nodes from saving battery power.

- **Dynamic source routing (DSR)**, therefore, divides the task of routing into two separate problems:
- **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
- **Route maintenance:** If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative. The basic principle of source routing is also used in fixed networks, e.g. token rings.

Dynamic source routing eliminates all periodic routing updates and works as follows.

If a node needs to discover a route, it broadcasts a route request with a unique identifier and the destination address as parameters. Any node that receives a route request does the following.

❖ If the node has already received the request (which is identified using the unique identifier), it drops the request packet.

● If the node recognizes its own address as the destination, the request has reached its target.

● Otherwise, the node appends its own address to a list of traversed hops in the packet and broadcasts this updated route request.

Using this approach, the route request collects a list of addresses representing a possible path on its way towards the destination. As soon as the request reaches the destination, it can return the request packet containing the list to the receiver using this list in reverse order. One condition for this is that the links work bi-directionally. If this is not the case, and the destination node does not currently maintain a route back to the initiator of the request, it has to start a route discovery by itself. The destination may receive several lists containing different paths from the initiator. It could return the best path, the first path, or several paths to offer the initiator a choice. Applying route discovery to the example in Figure 8.20 for a route from N1 to N3 at time t1 results in the following.

● N1 broadcasts the request ((N1), id = 42, target = N3), N2 and N4 receive this request.

● N2 then broadcasts ((N1, N2), id = 42, target = N3), N4 broadcasts ((N1, N4), id = 42, target = N3). N3 and N5 receive N2's broadcast, N1, N2, and N5 receive N4's broadcast.

● N3 recognizes itself as target, N5 broadcasts ((N1, N2, N5), id = 42, target = N3). N3 and N4 receive N5's broadcast. N1, N2, and N5 drop N4's broadcast packet, because they all recognize an already received route request (and N2's broadcast reached N5 before N4's did). N4 drops N5's broadcast, N3 recognizes (N1, N2, N5) as an alternate, but longer route.

● N3 now has to return the path (N1, N2, N3) to N1. This is simple assuming symmetric links working in both directions. N3 can forward the information using the list in reverse order.

The assumption of bi-directional links holds for many ad-hoc networks. However, if links are not bi-directional, the scenario gets more complicated. The algorithm has to be applied again, in the reverse direction if the target does not maintain a current path to the source of the route request.

● N3 has to broadcast a route request ((N3), id = 17, target = N1). Only N5 receives this request.

● N5 now broadcasts ((N3, N5), id = 17, target = N1), N3 and N4 receive the broadcast.

● N3 drops the request because it recognizes an already known id. N4 broadcasts ((N3, N5, N4), id = 17, target = N1), N5, N2, and N1 receive the broadcast.

● N5 drops the request packet, N1 recognizes itself as target, and N2 broadcasts ((N3, N5, N4, N2), id = 17, target = N1). N3 and N5 receive N2's broadcast.

● N3 and N5 drop the request packet.

Now N3 holds the list for a path from N1 to N3, (N1, N2, N3), and N1 knows the path from N3 to N1, (N3, N5, N4, N1). But N1 still does not know how to send data to N3! The only solution is to send the list (N1, N2, N3) with the broadcasts initiated by N3 in the reverse direction. This example shows clearly how much simpler routing can be if links are symmetrical. The basic algorithm for route discovery can be optimized in many ways.

● To avoid too many broadcasts, each route request could contain a counter. Every node rebroadcasting the request increments the counter by one. Knowing the maximum network diameter (take the number of nodes if nothing else is known), nodes can drop a request if the counter reaches this number.

● A node can cache path fragments from recent requests. These fragments can now be used to answer other route requests much faster (if they still reflect the topology!).

● A node can also update this cache from packet headers while forwarding other packets.

● If a node overhears transmissions from other nodes, it can also use this information for shortening routes.

After a route has been discovered, it has to be maintained for as long as the node sends packets along this route. Depending on layer two mechanisms, different approaches can be taken. If the link layer uses an acknowledgement the node can interpret this acknowledgement as an intact route.

● If possible, the node could also listen to the next node forwarding the packet, so getting a passive acknowledgement.

● A node could request an explicit acknowledgement. Again, this situation is complicated if links are not bi-directional. If a node detects connectivity problems,

- It has to inform the sender of a packet, initiating a new route discovery starting from the sender.
- Alternatively, the node could try to discover a new route by itself.

Although dynamic source routing offers benefits compared to other algorithms by being much more bandwidth efficient, problems arise if the topology is highly dynamic and links are asymmetrical.

7. Explain the following

i) AODV

- Ad Hoc On-demand Distance Vector
- Source floods route request in the network.
- Reverse paths are formed when a node hears a route request.
- AODV does make use of hop- by-hop routing, sequence numbers and beacons.
- The node that needs a route to a specific destination generates a route request. The route request Is forwarded by intermediate nodes which also learn a reverse route from the source to themselves.
- Each node forwards the request only once (pure flooding).
- Each route has a lifetime after which the route expires if it is not used.
- A route is used.

only when it is used and hence old and expired routes are never ns only one route between a source-destination pair.

(ii) Zone routing

Zone Routing is a hybrid protocol. It incorporates the merits of both on demand and proactive routing protocols.

- Routing zone comprise a few MANET notes within a few hops from the central zone.

Zone Routing is a hybrid protocol. It incorporate the merits of both on demand and proactive routing protocol. A routing zone is similar to a cluster. A routing zone comprises a few MANET nodes within a few hops from the central zone. Within a central zone, table-driven routing protocol is used. Each node therefore has a route to all other nodes within the zone. If a destination node happens to be outside the sources zone's employs an on demand route discovery procedure which works.

- If a packet's destination is in the same zone as the origin, the proactive protocol using an already stored routing table is used to deliver the packet immediately.
- If the route extends outside the packet's originating zone, a reactive protocol takes over to check each successive zone in the route to see whether the destination is inside that zone.
- This reduces the processing overhead for those routes. Once a zone is confirmed as containing the destination node, the proactive protocol, or stored route-listing table, is used to deliver the packet.

Multicast routing

- Multicast is communication between a single sender and multiple receivers on a network. Typical uses include the updating of mobile personnel from a home office and the periodic issuance of online newsletters
- Efficient delivery to multiple destinations
- (e.g. video broadcast)
- IP Multicast service model
- Communications based on groups
- Special IP addresses (Class D in IPv4) represent "multicast groups"
- Anyone can join group to receive packets Anyone can send to groupSender need not be part of group
- Dynamic group membership – can join and leave at will Unreliable datagram service

- Extension to unicast IP
- Group membership not visible to hosts
- No synchronization

8. Explain in detail about VANET

In VANETs, wireless communication has been a critical technology to support the achievement of many applications and services. However, due to the characteristics of VANETs such as high dynamic topology and intermittent connectivity, the existing routing algorithms in MANETs are not available for most application scenarios in VANETs.

- Driver and Vehicle Model. This model aims to reflect the behavior of a single vehicle. This behavior needs to consider two main factors: different driving styles and the vehicle characteristics, such as an aggressive or passive driver and a sports car.
- Traffic Flow Model. This model aims to reflect interactions between vehicles, drivers, and infrastructures and develop an optimal road network. In [31], according to various criteria (level of detail, etc.), the authors discuss three classes of traffic flow models: microscopic, microscopic, and macroscopic.
- Communication Model. This model is a pretty important part of research methodologies to address the data exchange among the road users. Thanks to the constraints of many factors (the performance of the different communication layers, communication environment, and the routing strategies), communication model plays an important role in the research. The authors in [17] give a detailed overview in the research field.(iv)Application Model. This model is very useful for the market introduction because it can address the behavior and quality of cooperative VANETs applications.

Characteristics Of VANET

• High node mobility, solution scalability requirements and wide variety of environmental conditions are three of the most important challenges of these decentralized self-organizing networks. A particular problem that has to be faced comes from the high speeds of vehicles in some scenarios such as highways. These characteristics collude with most iterative algorithms intended to optimize the use of
the channel bandwidth or of predefined routes.

• Security and privacy requirements in VANET shave to be balanced. On the one hand, receivers want to make sure that they can trust the source of information but on the other hand, this might disagree with privacy requirements of the sender.

• The radio channel in VANET scenarios present critical features for developing wireless communications, which degrade strength and quality of signals.

• The need for standardization of VANET communications should allow flexibility as these networks have to operate with many different brands of equipment and vehicle manufacturers.

• Real-time communication is a necessary condition because no delay can exist in the transmission of safety-related information. This implies that VANET communication requires fast processing and exchange of information.

• The existence of a central registry of vehicles, possible periodic contact with it, and qualified mechanisms for the exigency of fulfillment of the law are three usual assumptions that are necessary for some proposed solutions.

• Communication for information exchange is based on node-to-node connections. This distributed nature of the network implies that nodes have to relay on other nodes to make decisions, for instance about route choice, and also that any node in a VANET can act either as a host requesting information or a router distributing data, depending on the circumstances.

9. Explain in detail about security issues in MANET

There are several general security requirements, such as authenticity, scalability, privacy, anonymity, cooperation, stability and low delay of communications, which must be considered in any wireless network, and which in VANETs are even more challengingbecause of their specific characteristics such as high mobility, no fixed infrastructure andfrequently changing topology that range from rural road scenarios with little traffic to citiesor highways with a huge number of communications. The lack of a centralized infrastructure in charge of synchronization and coordination of transmissions makes that one of the hardest tasks in the resulting decentralized and self-organizing VANETs is the management of the wireless channel to reach an efficient use of its bandwidth.

Security issues in MANET

- **Lack of physical boundary**
  Each mobile node functions as a router and forwards packets from other nodes. As a result network boundaries become blurred. The distinction between nodes that are internal or external to a network becomes meaningless, making it difficult to deploy firewalls or monitor the incoming traffic.
- **Low owner RF Transmissions:**
  It is possible for a malicious node having high power RF transmission capability to continuously transmit and monopolies the medium and cause its neighbors nodes or the entire targeted MANET to wait endlessly for transmitting their messages.
- **Limited computational capabilities:**
  Nodes in an adhoc network usually have limited computational capabilities. It therefore becomes difficult to deploy compute intensive security solutions such as setting up a public key cryptosystems.
- **Limited power Supply:**
  Since nodes normally rely on battery power an attacker might attempt tpppppo exhaust batteries by causing unnecessary transmissions to take lace pat the targeted node or might cause excessive computations to be carriedout by the targeted nodes.

10. Explain in detail about the attacks in MANET of various layers

- **Dropping attacks**: Here data packets that are transmitted are dropped at compromised or selfish
  node.
- **Modification attacks**: In this type of attack they alter the packets and disrupt the communication
- between the nodes in the network
- **Fabrication attacks**: Here the attacker node send fake message without getting any related message.and this can be called as forge reply.
- **Timing attacks**: Here attacker attack other nodes to it by advertising itself as node near to actual
  node Indicate that it is having a fresh shortest path to destination.

Network layer: Network layer contains the following attacks they are:

- **Black hole attack**: In this type of attack node advertises itself having shortest route to destination and thus attracts the data in the network.
- **Wormhole attack**: This type of attack makes a tunnel between two malicious nodes and attracts
  the data flow through these attacker nodes.
- **Internal Attacks**

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes. B. External attacks.

- **External attacks**
- These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. . External attacks prevent thenetwork from normal communication and producingadditional overhead to the network. External attacks can classify into two categories:
- **Passive attacks**
  MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network
  traffic or accumulates data from it.
- **Active Attacks**
  Active attacks are very severe attacks on the network that prevent message flow between the nodes. However activeattacks can be internal or external. Active external attacks
  can be carried out by outside sources that do not belong to the network.
- **Gray-Hole Attack**
  Gray-Hole attack has its own characteristic behavior. It too drops DATA packets, but node's malicious activity is limited to certain conditions or trigger. Two most common type of behavior:
- **Node dependent attack** – drops DATA packets destined towards a certain victim node or coming from certain node while for other nodes it behaves normallyby routing DATA packets to the destinationnodes correctly.
- **Time dependent attack** – drops DATA packets based on some predetermined/trigger
  time while behaving normally during the other instances.

UNIT V Part-A

1. What is Mobile OS?

- The os of mobile device is to facilitate efficient utilization of the resources of the device by performing multiple tasks.
- It manages processor, memory, files, and attached devices such as camera, speaker, keyboard, and screen.

2. **What are the problems in Monolithic Kernel design**

The traditional OS such as UNIX, Windows are known to have monolithic kernel design.
It makes the kernel maasive,non modular, hard ti tailor,maintain,extend,and configure.

3. What is micro kernel

- Microkernel tries to minimize the size of the kernel code.
- Only the basic hardware dependent functionalities and a few critical functionalities are implemented in a kernel mode and all other functionalities are implemented in the user mode.
- It is easier to port, extend, and maintain os code.

4. List the special constraints under which the mobile device needs to operate?

- Limited memory: Less permanent and volatile storage
- Limited screen Size: Limits the size of the display screen.
- Miniature Keyboard: typing in the document and entering the string commands is difficult
- Limited processing Power: ARM based processor with restricted processor power, storage, and battery power, Limited battery power,Flucating bandwidth of the wireless medium.

5. Give example for mobile OS and its features

- Windows mobile: Graphics/windows/event manager handles all input and output

- Palm OS: It is single tasking operating system.
- Symbian OS: Real time multitasking,pre-emptive,32 bit operating system
- IOS: contetual OS
- Android OS: Code is structured into four different layers
- Blackberry OS: High level of security

6. What is HDML?

Handheld Markup Language(HDML). A HDML consist of many cards. So its is called deck. An advantage of the card and deck model in the context of mobile networks is that a click on a web page causes downloading of the entire deck associated with the web page on to the mobile device. This reduces latency of access.

7. List out the protocols used in Wap

- Application Layer: WAE(Wireless application environment
- Session Layer: WAP(wireless session protocol
- Transaction layer: WTP(Wireless transaction protocol)
- Security Layer: WTLS(Wireless Transport layer security)
- Transport Layer: WDP(wireless Data ram protocol)
- Network Layer: Bearer interfaces.

8. Write the important capabilities of j2ME programs

- Opening UDP connections between two device
- Establishing HTTP connections with a server
- Making socket connections
- Bluetooth programming
- Barcode scanning

9. What is writing once run everywhere?

J2ME is meant for tiny devices such as mobile phones which includes a miniature version of JVM called KVM which can run small java programs on mobile device. They are lightweight programs

10. What are the two configurations of J2ME?

- *Connected limited device configuration for handheld devices*: Low range of consumer electronic device using 16-32 bit small computing device.eg device .eg pager, cell phones
- *Connected device configuration for plug in device*: Higher end device e.g. Set top box, smart phones.

11. What is Android SDK ?

- The Android SDK (Software Development Kit) is a set of development tools used to develop applications for Android platform.
- The Android SDK includes the following: Required libraries.

12. What do you meant by Broadcast receivers?

Simply respond to broadcast messages from other applications or from the system itself. These messages are sometime called events or intents. For example, applications can also initiate broadcasts to let other applications know that some data has been downloaded to the device and is available for them to use, so this is broadcast receiver who will intercept this communication and will initiate appropriate action.

13. What are the key components of android architecture?

Activities	They dictate the UI and handle the user interaction to the smart phone screen
Services	They handle background processing associated with an application.
Broadcast Receivers	They handle communication between Android OS and applications.
Content Providers	They handle data and database management issues.

14. What is the use of log message in android?

The Android logging system provides a mechanism for collecting and viewing system debug output. Logcat dumps a log of system messages, which include things such as stack traces when the emulator throws an error and messages that you have written from your application by using the Log class.

15. Give the important Android API's

- Android Graphics
- Android media
- Android opengl
- Android telephony
- Android widget

16. What is the use of Content providers?

Content providers are used for reading and writing data that are either private to an application or shared across applications. By using the content provider, an application can query or modify the stored data.

17. What are the different android broadcast classes?

- Normal broadcasts (sent with Context.sendBroadcast) are completely asynchronous. All receivers of the broadcast are run in an undefined order, often at the same time. This is more efficient, but means that receivers cannot use the result or abort APIs included here.
- Ordered broadcasts (sent with Context.sendOrderedBroadcast) are delivered to one receiver at a time. As each receiver executes in turn, it can propagate a result to the next receiver, or it can completely abort the broadcast so that it won't be passed to other receivers.

18. What are the different features of SDK

- A client program which runs on the developers machine.
- A daeman program which runs as a process on each emulator or device instance.
- A server program which runs as a background process on the host machine

19. Define MIDP

- The Mobile Information Device Profile (MIDP) is a key element of the Java 2 Platform, Mobile Edition (J2ME).
- When combined with the Connected Limited Device Configuration (CLDC), MIDP provides a standard Java runtime environment for today's most popular mobile information devices, such as cell phones and mainstream personal digital assistants (PDAs).

20. What is M- commerce?

- It carries out any activity related to buying and selling of commodities, services or information using the mobile handheld device.
- It is how payment can be made securely and rapidly as soon as a buyer decides to make a purchase

21. List out the applications of M Commerce

- Business to consumer application*:* advertising, shopping comparision,mobile ticketing, Information about a product, interactive advertisement and catalogue shopping
- Business to Business : ordering and delivery confirmation, stock tracking and control, supply chain mamagement,Mobile inventory management

22. Write the structure of mobile commerce

Content provider implements an application by providing two sets of programs

- Client side: Run on micro browser installed on the users mobile device
- Server side: Performing database access and computation reside on the host computer.

Part B

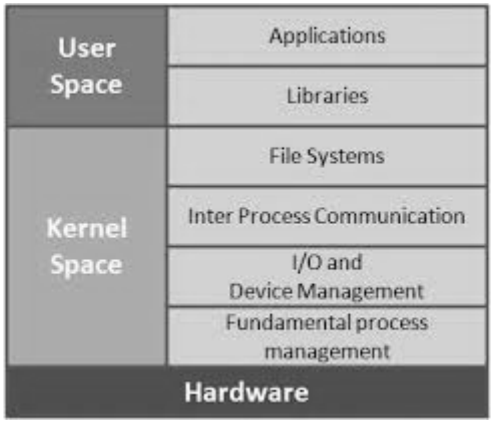
1. **Explain monolithic design versus microkernel design of an operating system**

Basic OS services such as process management, memory management, interrupt handling, IO communication, file system, device drivers, networking, etc all run in kernel space. Entire services are loaded on boot up and reside in memory and work is done using system calls. Linux is an example on a monolithic kernel based OS.

Microkernel

The idea behind microkernel OS is to reduce the kernel to only basic process communication and IO control and let other system services run in user space just like any other normal processes. These services are called servers and kept separate and run in different address spaces. Contrary to monolithic OS where services are directly invoked, communication in a microkernel is done via message passing (inter process communication IPC). Mac OS and WinNT are two examples on microkernel OS architecture.

Microkernel Advantages


User Space
Applications
Libraries
Kernel Space
File Systems
Inter Process Communication
I/O and Device Management
Fundamental process management
Hardware

Monolithic kernel is a single large process running entirely in a single address space. It is a single static binary file. All kernel services exist and execute in the kernel address space. The kernel can invoke functions directly. Examples of monolithic kernel based OSs: Unix, Linux.

In microkernels, the kernel is broken down into separate processes, known as servers. Some of the servers run in kernel space and some run in user-space. All servers are kept separate and run in different address spaces. Servers invoke "services" from each other by sending messages via IPC (Interprocess Communication). This separation has the advantage that if one server fails, other servers can still work efficiently. Examples of microkernel based OSs: Mac OS X and Windows NT.

2. Write short notes on special constraints and requirements of mobile OS

Enables an application to run by simply abstracting the mobile system hardware • Enables the programmer to abstract the devices such that the application need not know full details of the font and font size of the mobile device display • Application need not know how the message will be displayed by the LCD hardware

PalmOS • Windows CE • Symbian • Android─ released in 2008 by Google

Facilitates execution of software components on diversified mobile device hardware • Application need not be aware of the details of the LCD driver and memory at which the CPU will send the message for display

Provides interfaces for communication between processes, threads, and ISRs at the application and middleware layers • Provides middleware for the system hardware • Provides management functions (such as creation, activation, deletion, suspension, and delay) for tasks

Provides memory management • Enables running of processes • Helps the processes in obtaining access to system resources

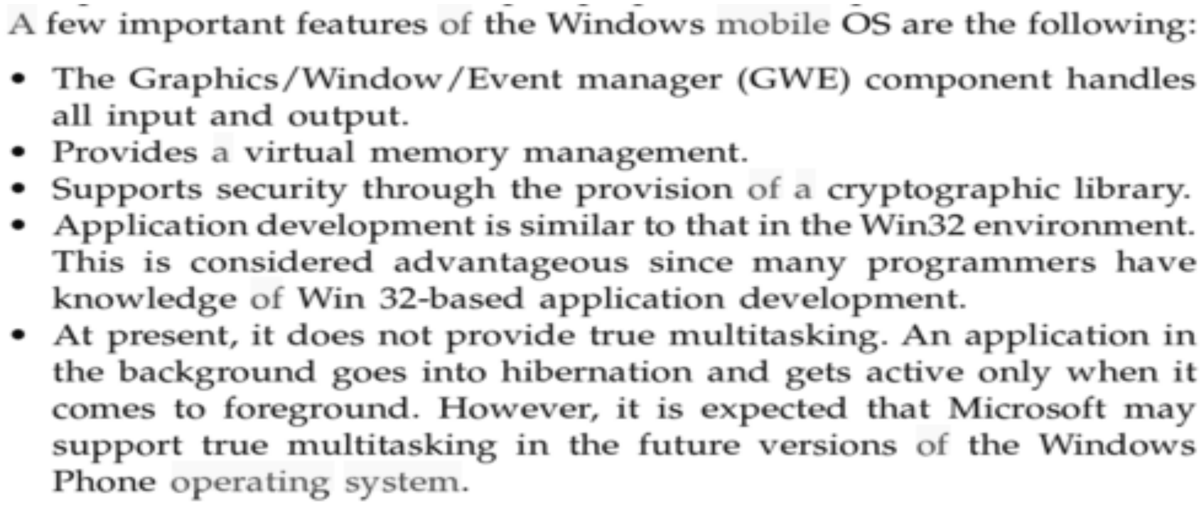
Application tasks • The OS provides the functions used for scheduling the multiple tasks in a system • Synchronization of the tasks by using semaphores (tokens) • A task may have multiple threads

Provides for synchronization of the threads and their priority allocation • Accomplishes real-time execution of the application tasks and threads

Mobile OS─ An OS which enables running of application tasks taking into account mobile system constraints of hardware and network • Enables a programmer to develop application without considering the specifications, drivers, and functionalities of the hardware of the system

3. Write in detail about a survey of commercial mobile operating system

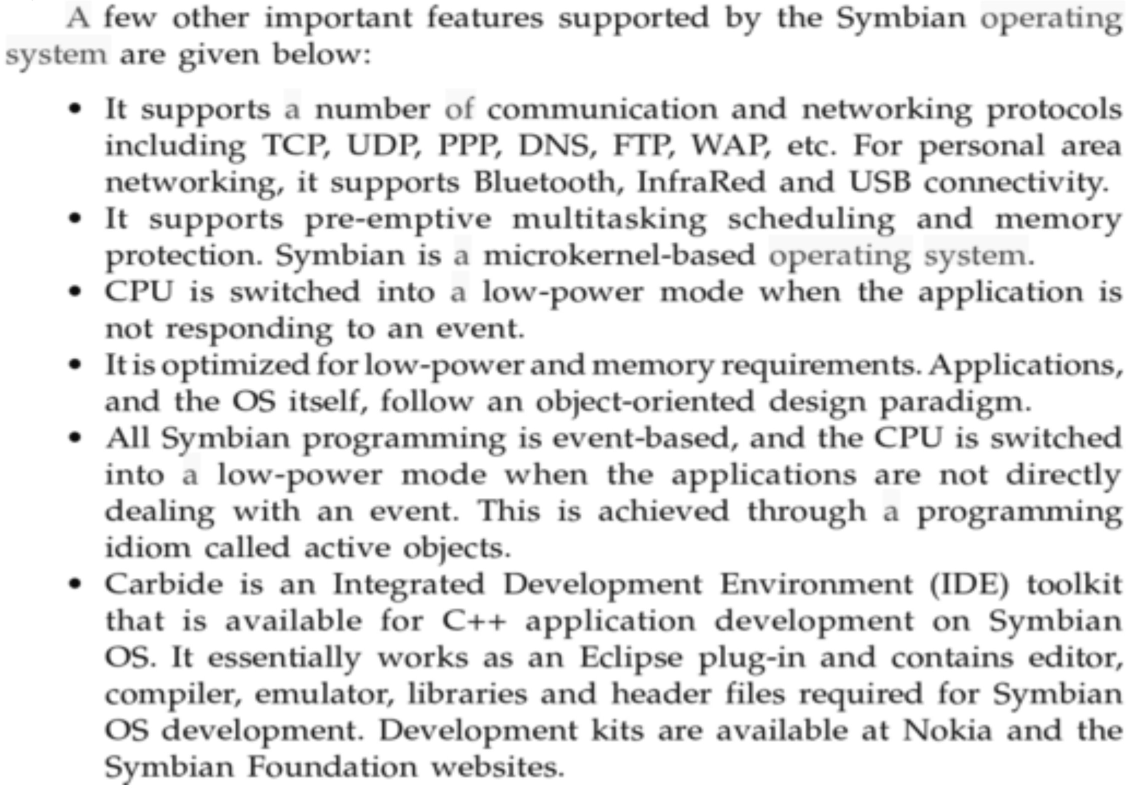
Windows OS



A few important features of the Windows mobile OS are the following:

- The Graphics/Window/Event manager (GWE) component handles all input and output.
- Provides a virtual memory management.
- Supports security through the provision of a cryptographic library.
- Application development is similar to that in the Win32 environment. This is considered advantageous since many programmers have knowledge of Win 32-based application development.
- At present, it does not provide true multitasking. An application in the background goes into hibernation and gets active only when it comes to foreground. However, it is expected that Microsoft may support true multitasking in the future versions of the Windows Phone operating system.

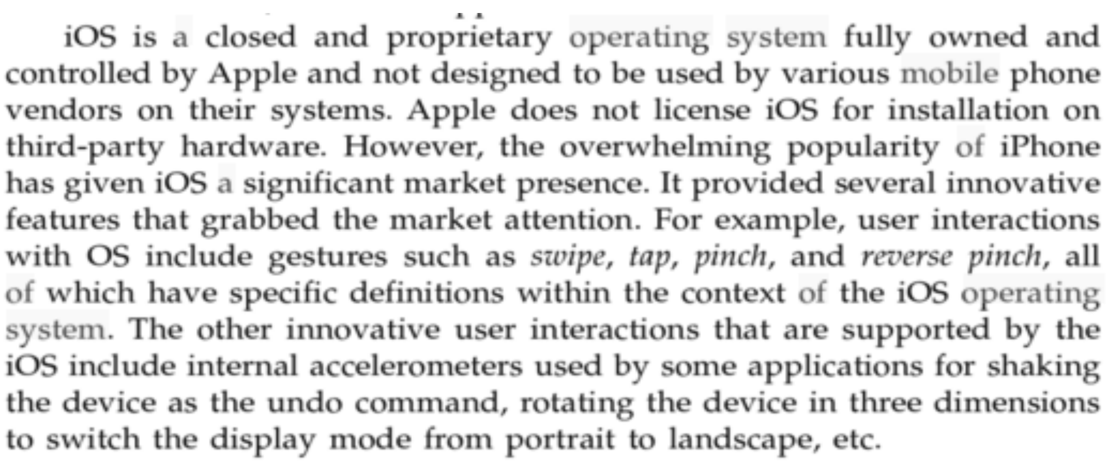
Symbian OS



A few other important features supported by the Symbian operating system are given below:

- It supports a number of communication and networking protocols including TCP, UDP, PPP, DNS, FTP, WAP, etc. For personal area networking, it supports Bluetooth, InfraRed and USB connectivity.
- It supports pre-emptive multitasking scheduling and memory protection. Symbian is a microkernel-based operating system.
- CPU is switched into a low-power mode when the application is not responding to an event.
- It is optimized for low-power and memory requirements. Applications, and the OS itself, follow an object-oriented design paradigm.
- All Symbian programming is event-based, and the CPU is switched into a low-power mode when the applications are not directly dealing with an event. This is achieved through a programming idiom called active objects.
- Carbide is an Integrated Development Environment (IDE) toolkit that is available for C++ application development on Symbian OS. It essentially works as an Eclipse plug-in and contains editor, compiler, emulator, libraries and header files required for Symbian OS development. Development kits are available at Nokia and the Symbian Foundation websites.

IOS



iOS is a closed and proprietary operating system fully owned and controlled by Apple and not designed to be used by various mobile phone vendors on their systems. Apple does not license iOS for installation on third-party hardware. However, the overwhelming popularity of iPhone has given iOS a significant market presence. It provided several innovative features that grabbed the market attention. For example, user interactions with OS include gestures such as *swipe*, *tap*, *pinch*, and *reverse pinch*, all of which have specific definitions within the context of the iOS operating system. The other innovative user interactions that are supported by the iOS include internal accelerometers used by some applications for shaking the device as the undo command, rotating the device in three dimensions to switch the display mode from portrait to landscape, etc.

4. Explain in detail about WAP architecture

WAP stands for Wireless Application Protocol ,WAP is an application communication protocol

WAP is used to access services and information ,WAP is inherited from Internet standards

WAP is for handheld devices such as mobile phones ,WAP is a protocol designed for micro browsers ,WAP enables the creating of web applications for mobile devices.

WAP uses the mark-up language WML (not HTML) WML is defined as an XML 1.0 application

Figure gives an overview of the WAP architecture, its protocols and components, and compares this architecture with the typical internet architecture when using the World Wide Web. This comparison is often cited by the WAP Forum and it helps to understand the architecture (WAP Forum, 2000a). This comparison can be misleading as not all components and protocols shown at the same layer are comparable For consistency reasons with the existing specification, the following stays with the model as shown in Figure.

The basis for transmission of data is formed by different bearer services WAP does not specify bearer services, but uses existing data services and will integrate further services. Examples are message services, such as short message service (SMS) of GSM, circuit-switched data, such as high-speed circuit switched data (HSCSD) in GSM, or packet switched data, such as general packet radio service (GPRS) in GSM. Many other bearers are supported, such as CDPD, IS-136, PHS. No special interface has been specified between the bearer service and the next higher layer, the transport layer with its wireless datagram protocol (WDP) and the additional wireless control message protocol (WCMP), because the adaptation of these protocols are bearer specific (WAP Forum, 2000u). The transport layer offers a bearer independent, consistent datagram-oriented service to the higher layers of the WAP architecture. Communication is done transparently over one of the avail-able bearer services. The transport layer service access point (T-SAP) is the common interface to be used by higher layers independent of the underlying net-work.

The next higher layer, the security layer with its wireless transport layer security protocol WTLS offers its service at the security SAP (SEC-SAP).WTLS is based on the transport layer security (TLS, formerly SSL, secure sockets layer) already known from the www. WTLS has been optimized for use in wireless net-works with narrow-band channels. It can offer data integrity, privacy, authentication, and (some) denial-of-service protection

The WAP transaction layer with its wireless transaction protocol (WTP) offers a lightweight transaction service at the transaction SAP (TR-SAP) This service efficiently provides reliable or unreliable requests and asynchronous transactions as explained in section 10.3.4. Tightly coupled to this layer is the next higher layer, if used for connection-oriented service The session layer with the wireless session protocol (WSP) currently offers two services at the session-SAP (S-SAP), one connection-oriented and one connectionless if used directly on top of WDP. A special service for browsing the web (WSP/B) has been defined that offers HTTP/1.1 functionality, long-lived session state, session suspend and resume, session migration and other features needed for wireless mobile access to the web.

Finally the application layer with the wireless application environment (WAE) offers a framework for the integration of different www and mobile telephony applications. It offers many protocols and services with special service access points. The main issues here are scripting languages, special markup languages, interfaces to telephony applications, and many content formats adapted to the special requirements of small, handheld, wireless devices.

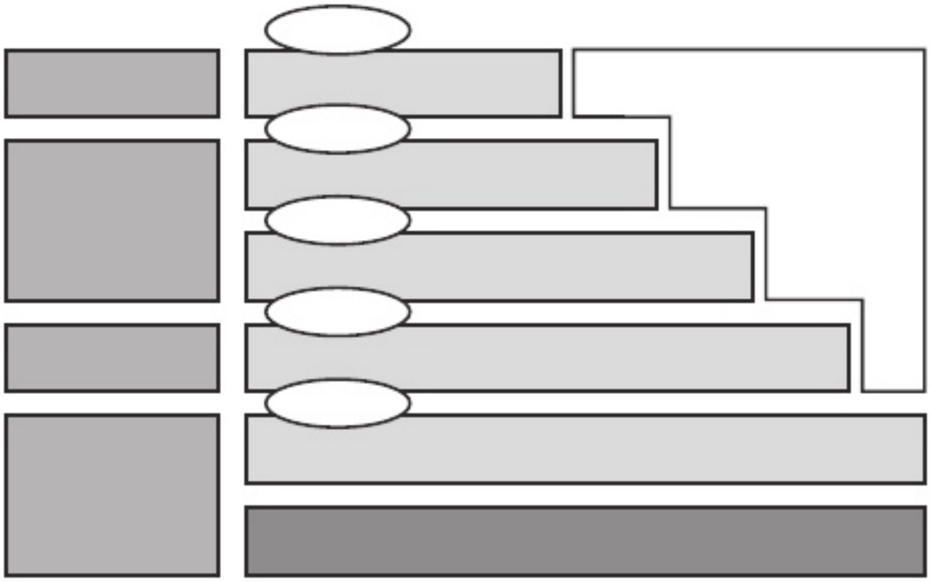
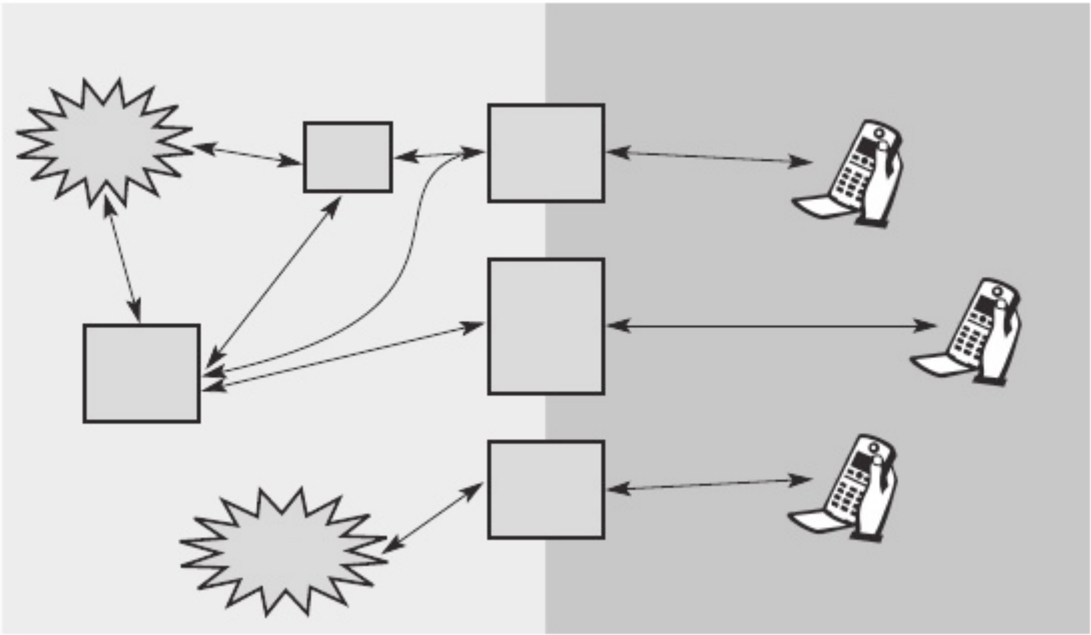


Figure not only shows the overall WAP architecture, but also its relation to the traditional internet architecture for www applications. The WAP transport layer together with the bearers can be (roughly) compared to the ser-vices offered by TCP or UDP over IP and different media in the internet. If a bearer in the WAP architecture already offers IP services (e.g., GPRS, CDPD) then UDP is used as WDP. The TLS/SSL layer of the internet has also been adopted for the WAP architecture with some changes required for optimization. The functionality of the session and transaction layer can roughly be compared with the role of HTTP in the web architecture. However, HTTP does not offer all the additional mechanisms needed for efficient wireless, mobile access (e.g., session migration, suspend/resume). Finally, the application layer offers similar features as HTML and Java. Again, special formats and features optimized for the wireless scenario have been defined and telephony access has been added.

WAP does not always force all applications to use the whole protocol architecture. Applications can use only a part of the architecture as shown in Figure10.9. For example, this means that, if an application does not require security but needs the reliable transport of data, it can

directly use a service of the trans-action layer. Simple applications can directly use WDP.

Different scenarios are possible for the integration of WAP components into existing wireless and fixed networks On the left side, different fixed networks, such as the traditional internet and the public switched telephone network (PSTN), are shown. One cannot change protocols and services of these existing networks so several new elements will be implemented between these networks and the WAP-enabled wireless, mobile devices in a wireless net-work on the right-hand side.



The current www in the internet offers web pages with the help of HTML and web servers. To be able to browse these pages or additional pages with hand-held devices, a wireless markup language (WML) has been defined in WAP. Special filters within the fixed network can now translate HTML into WML, web server scan already provide pages in WML, or the gateways between the fixed and wireless network can translate HTML into WML. These gateways not only filter pages but also act as proxies for web access, as explained in the following sections.WML is additionally converted into binary WML for more efficient transmission.

In a similar way, a special gateway can be implemented to access traditional telephony services via binary WML. This wireless telephony application (WTA) server translates, e.g., signaling of the telephone network (incoming call etc.) into WML events displayed at the handheld device. It is important to notice the integrated view for the wireless client of all different services; telephony and web, via the WAE

5. Write notes on J2ME configuration

To make it applicable devices with a specific range of capabilities. Parameters

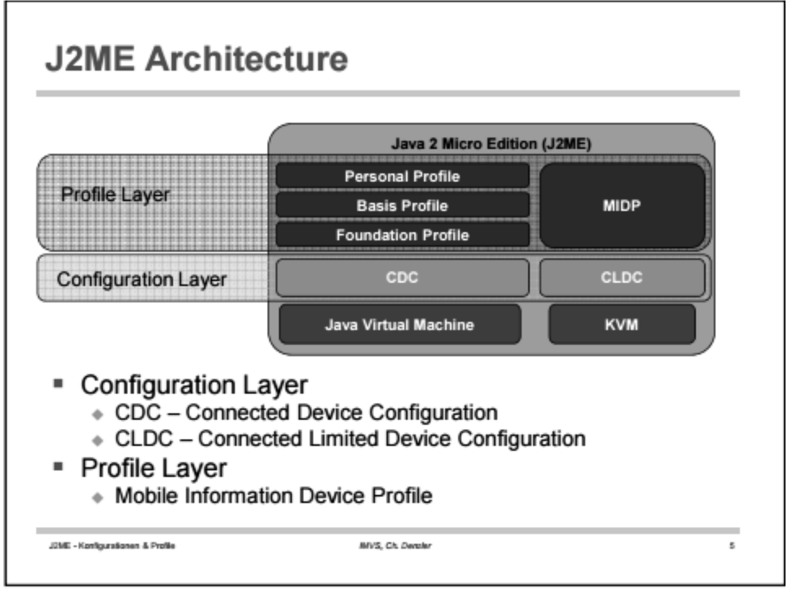
1. Availability of memory space and memory type

2. Specification of processor in terms of speed and type.
3. Network connectivity of the device

Two configurations

1. Connected limited device configuration for hand held device: It usually have low memory powered by battery, low bandwidth, Network wireless connection. It includes pagers, PDA,Cellphones,Dedicated Terminal, Handheld Devices.
2. Connected Device configuration foe plug-in device

These are high end device used in 32 bit processor ,2 GB memory, implemented by JVM.It included Digital Set top boxes, Home Appliance, Navigation System, Smart Phones



J2ME Architecture

- Configuration Layer
  - CDC – Connected Device Configuration
  - CLDC – Connected Limited Device Configuration
- Profile Layer
  - Mobile Information Device Profile

J2ME - Konfigurationen & Profile MVS, Ch. Denzler 5

J2ME Connected, Limited Device Configuration (CLDC) Specifies Java environment for mobile phone, pager, and PDA class devices CLDC devices are usually wireless J2ME Connected Device Configuration (CDC) Specifies Java environment for digital television settop boxes, high end wireless devices, and automotive telematics systems. CDC devices may be wired (DTV cable, etc.)

A set of Java based APIs which supplements a Configuration to provide capabilities for a specific vertical market or device type Subject to compatibility tests The specification may not be completely implemented UI and presentation capabilities are generally defined at this layer EX: CLDC => MIDP (Mobile Information Device Profile) CDC => Personal Profile CDC => Foundation Profile

CLDC provides the lowest common denominator for small and resource-constrained devices.

Mobile Information Device Profile (MIDP) Profile for wireless devices implementing CLDC J2ME Foundation Profile Profile for non-GUI networked devices implementing CDC J2ME Personal Basis, Personal, RMI Profiles Basic graphics, next generation PersonalJava environment, and RMI support for CDC & Foundation Profile based devices

6. Explain in detail about Android SDK

The Android SDK (software development kit) is a set of development tools used to develop applications for Android platform. The Android SDK includes the following:

- Required libraries
- Debugger
- An emulator

Relevant documentation for the Android application program interfaces (APIs)

Sample source code

Tutorials for the Android OS

A software development kit that enables developers to create applications for the Android platform. The Android SDK includes sample projects with source code, development tools, an emulator, and required libraries to build Android applications.

7. Briefly write how an application can be developed using the android SDK

Android is an Operating System for mobile devices developed by Google, which is built upon Linux kernel. Android competes with Apple's iOS (for iPhone/iPad), RIM's Blackberry, Microsoft's Windows Phone, Symbian OS, and many other proprietary mobile OSes.

setup a working environment using the Android SDK, Eclipse IDE, and ADT Plugin.

To compile your application against a particular version of Android, you must use the SDK Manager to download and install the SDK Platform for that release. Launch Android Studio.

1. Choose "Start a new Android Studio Project".
2. In "Create New Project" dialog Set "Application Name" to "Hello Android" (which is the title in your app menu) Set your "Company Domain" to "example.com" Take note of your "Project Location" Next.
3. In "Target Android Devices" dialog Check "Phone and Tablet" For minimum SDK, choose "API 14: Android 4.0 (IceCreamSandwich)" Next.
4. In "Add an activity to Mobile" dialog Select "Blank Activity" Next.
5. In "Customize the Activity" dialog Set "Activity Name" to "MainActivity" Set "Layout Name" to "activity_main" Set "Title" to "MainActivity" Set "Menu Resource Name" to "menu_main" (These are actually the default values) Finish.
6. Take a while to set up the "first" app. The app appears after "Indexing..." completes. By default, a hello-world app is created.

8. **Write short notes on Android software stack and Android application components**

They are four components

Activity

Content providers

Service

Broadcast receiver

Components	**Description**
Activities	They dictate the UI and handle the user interaction to the smart phone screen
Services	They handle background processing associated with an application.
Broadcast Receivers	They handle communication between Android OS and applications.
Content Providers	They handle data and database management issues.

Activities

An activity represents a single screen with a user interface,in-short Activity performs actions on the screen. For example, an email application might have one activity that shows a list of new emails, another activity to compose an email, and another activity for reading emails. If an application has more than one activity, then one of them should be marked as the activity that is presented when the application is launched.

An activity is implemented as a subclass of **Activity** class as follows –

- public class Main Activity extends Activity {}

Services

A service is a component that runs in the background to perform long-running operations. For example, a service might play music in the background while the user is in a different application, or it might fetch data over the network without blocking user interaction with an activity.

A service is implemented as a subclass of **Service** class as follows −

```
public class MyService extends Service {}
```

Broadcast Receivers

Broadcast Receivers simply respond to broadcast messages from other applications or from the system. For example, applications can also initiate broadcasts to let other applications know that some data has been downloaded to the device and is available for them to use, so this is broadcast receiver who will intercept this communication and will initiate appropriate action.

A broadcast receiver is implemented as a subclass of BroadcastReceiverclass and each message is broadcaster as an Intent object.

```
public class MyReceiver  extends  BroadcastReceiver {
   public void onReceive(context,intent){}}
```

Content Providers

A content provider component supplies data from one application to others on request. Such requests are handled by the methods of the ContentResolverclass. The data may be stored in the file system, the database or somewhere else entirely.

A content provider is implemented as a subclass of ContentProvider class and must implement a standard set of APIs that enable other applications to perform transactions.

```
public class MyContentProvider extends  Cont
```

9. **What do you understand by M-Commerce?**

A content provider implements on application by providing two sets of programs (i) server side(II) client side

. The client side programs run on the micro Brower installed on the user mobile device .The server side programs performing data base accesses and computation reside on the host computers

i)**What are the advantages and Disadvantages of M-Commerce**

Advantages

4. For the business organization the benefits of using M commerce includes customer convenient, cost saving and new business opportunities
5. It provides flexibility, Anywhere any time shopping using a light weight device

6. Mobile device can be highly personalized, They provide additional level of convenience to the customer

Disadvantages:

1. Do not generously offer graphics or processing power of the PC
2. The small screen of the mobile devices limit the complexity of applications
3. Underlying network may impose severer types of restrictions
4. Security

ii) Applications of M-Commerce

Business to consumer application

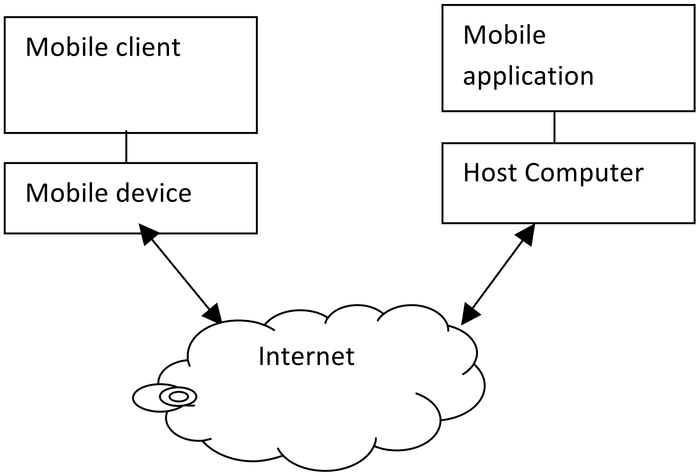
- Advertisement,
- Comparison Shopping,
- Info about the product,
- Mobile ticketing,
- Loyalty and payment services,
- Interactive advertisement

Business to Business application

- Ordering and delivery conformation
- Stock track-in and control
- Supply chain management
- Mobile Inventory Management

10. Explain the following

i) Structure of mobile Commerce



Mobile devices: The users specify the request through appropriate interfaces, which are then transmitted through the internet to the mobile commerce application the internet

Mobile Middleware: The main purpose of is to seamlessly and transparently map the internet content to mobile phone they may spot wide variety of OS markup languages, Micro Browsers, Protocols

Network: Wireless network are at the core of every M- commerce. User request are delivered either to the closest AP or to a base station

Host Computer: They are powerful servers that process and store all the information's need for mobile commerce application

ii) Mobile Payment System.

It is defined as initiation, authorization, and confirmation of a financial transaction using a mobile device.

Payment scheme:

1. Bank account based
2. Credit card Based
3. Micro payment Based

Bank account based: In this scheme the bank account of the customer is linked to his mobile phone numbers. When the customers makes on mobile payment to a vendor through blue tooth or wireless LAN connectivity with a vendor Machine, a bank account of the customer is debited and the value is credited to the vendor account

Credit card Based: In the payment system the credit card number is linked to the mobile phone of the customer. When the customer makes on M payment transaction with the merchant, the credit card is charged and the value is credited to the merchant account

Micro payment Based: It is indented for payment for small purchases such as items from vending machines, the mobile device can communicate with the vending machine directly using Bluetooth or WLAN connection to negotiate the payment and the micropayment is carry out

Properties of Mobile Payment system

- Easy to use
- General purpose
- Interoperability
- Trust
- Cost
- Swiftness
- Global payments

Payment Solutions

SMS Based

POS based (Physical point of scale)

Barcode Based

NFC (Near Field Communication)

Mobile Wallet