Mobile computing:

Ability to compute remotely while on the move. It is possible to access information from anywhere and at anytime.

13. How is 2.5G different from 2G and 3G technologies?

2.5 G technology provided faster data rates over 2G systems but did not offer the multi-megabit data rates which are the characteristics of the 3G.

19. What is hidden problem? *[MAY/JUNE -2016]*

Hidden node problem occurs on a wireless network when two nodes are sending signals to a common destination but are unaware of the other exists.

✓ Slow hopping:

Multiple bits are transmitted on a specific frequency or same frequency.

✓ Fast hopping:

Individual bits are splits and transmitted on different frequency.

Define COA. ***[NOV/DEC -2016]***

Care-of –Address(COA) is the address that is used to identify the present location of a foreign agent. The packets sent to the MN are delivered to COA.

Multiplexing:

* It is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

* It is done using a device called multiplexer. It contains n input lines to generate one output.

* At the end a device called Demultiplexer.

* It is used that seperate singnal into its component signals.

Types of multiplexing:

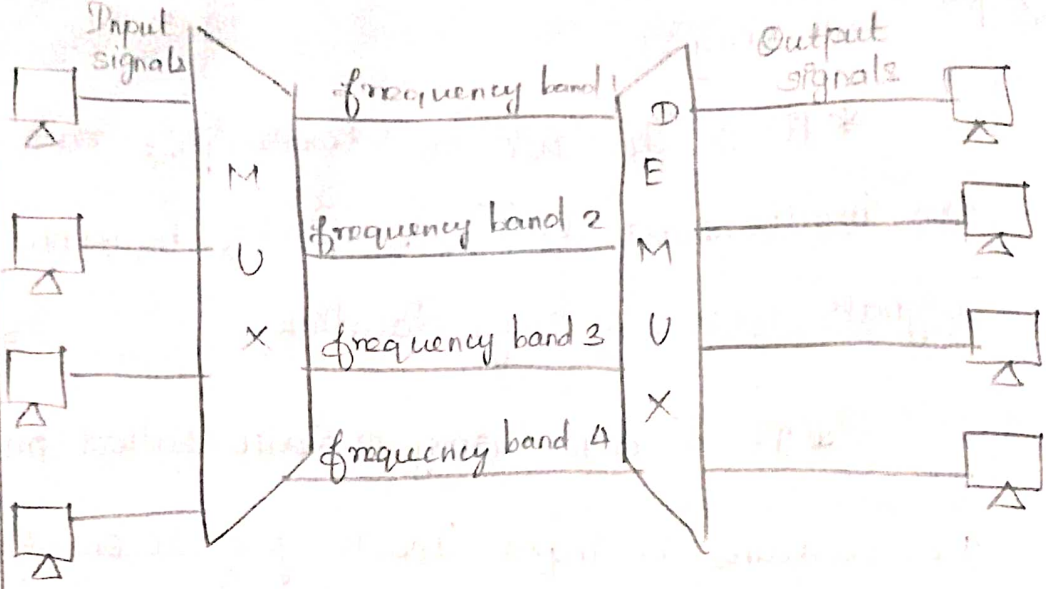
* Frequency division multiplexing
* Time division multiplexing
* code division multiplexing
* Space division multiplexing.

Frequency division multiplexing:

* It is inherently an analog technology.

* It is a multiplexing technique an analog technology by which multiple number of information are in different frequency.

* The applications are television radio, television broadcasting



Advantages of FDM:

* It can be applied both analog signal and digital signals.

* It can be send multiple signals simultaneously within a single connection

Disadvantages:

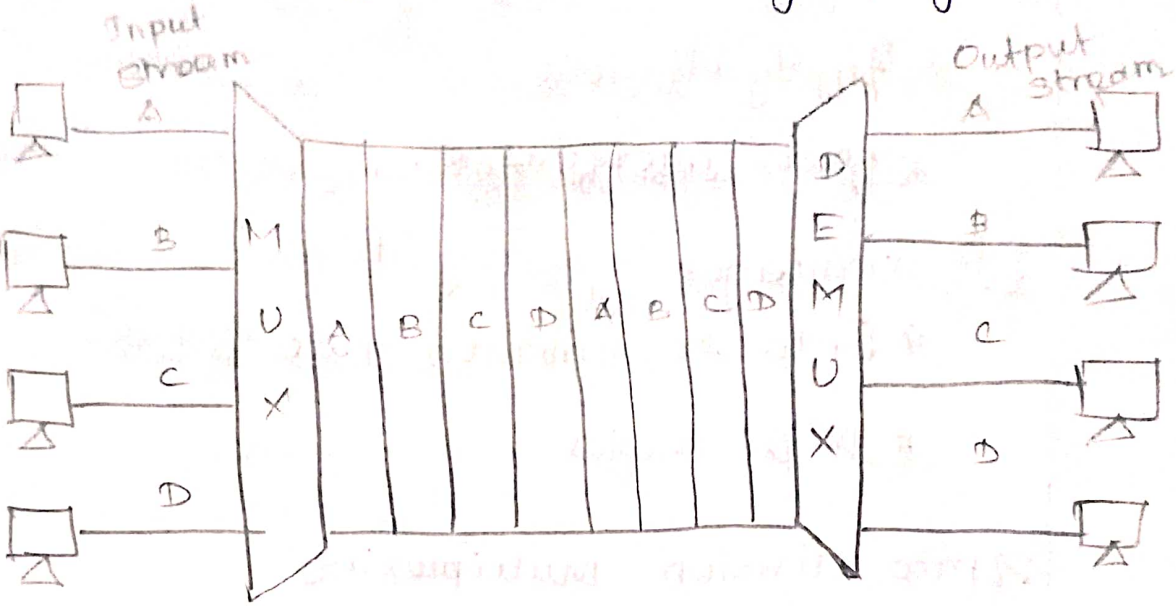
* It is less flexible
* bandwidth wastage is high.

Time Division Multiplexing:

* The multiple number of information are communicate within a different slot of time.

* The time frames of the same intervals are divided so that you can access the entire frequency spectrum at that time frame

* It is used in telegraphy.



Advantages:

* It allows single user at a time
* It is less complicated
* Has more flexible architecture

Disadvantage:

* implementation is difficult.

Code division multiplexing:

* Multiple number of information are multiplexed in different code.
* It allots a unique code to every channel so that each of these channels can use the same spectrum simultaneously at the same time
* It is used in cellphone spectrum technology (2G, 3G etc..)

Advantages:

* Highly efficient
* fewer interference.

Disadvantages

* Data transmission rate is low
* It is complex.

Space division Multiplexing

* we split a communication channel into multiple different physical location and allocated each stream of data onto each of the location.
* It is a combination of FDM and TDM
* It passes messages or data parallel with the use of specific frequency at a specific.
* It is used in Global service for mobile

Advantages:

* The data transmission rate is high
* It uses time and frequency bands at its maximum potential.

Disadvantages

* Inference may occur
* high inference losses.

7 b

✓ ALOHA :

Simplest scheme

* True free for all . When a node needs to send , it does so.

* low delay if light load

* If it hears an acknowledgement , fine ; Otherwise it resends after waiting a range amount of time.

✓ Slotted ALOHA :

* An improvement over pure ALOHA

* Sends packet only at the beginning of a slot.

* Employ beacon signals to mark the beginning of a slot.

* In such case CSMA scheme works better.

* Time is divided into equal sized slots in which a packet can be send size of packet is restricted

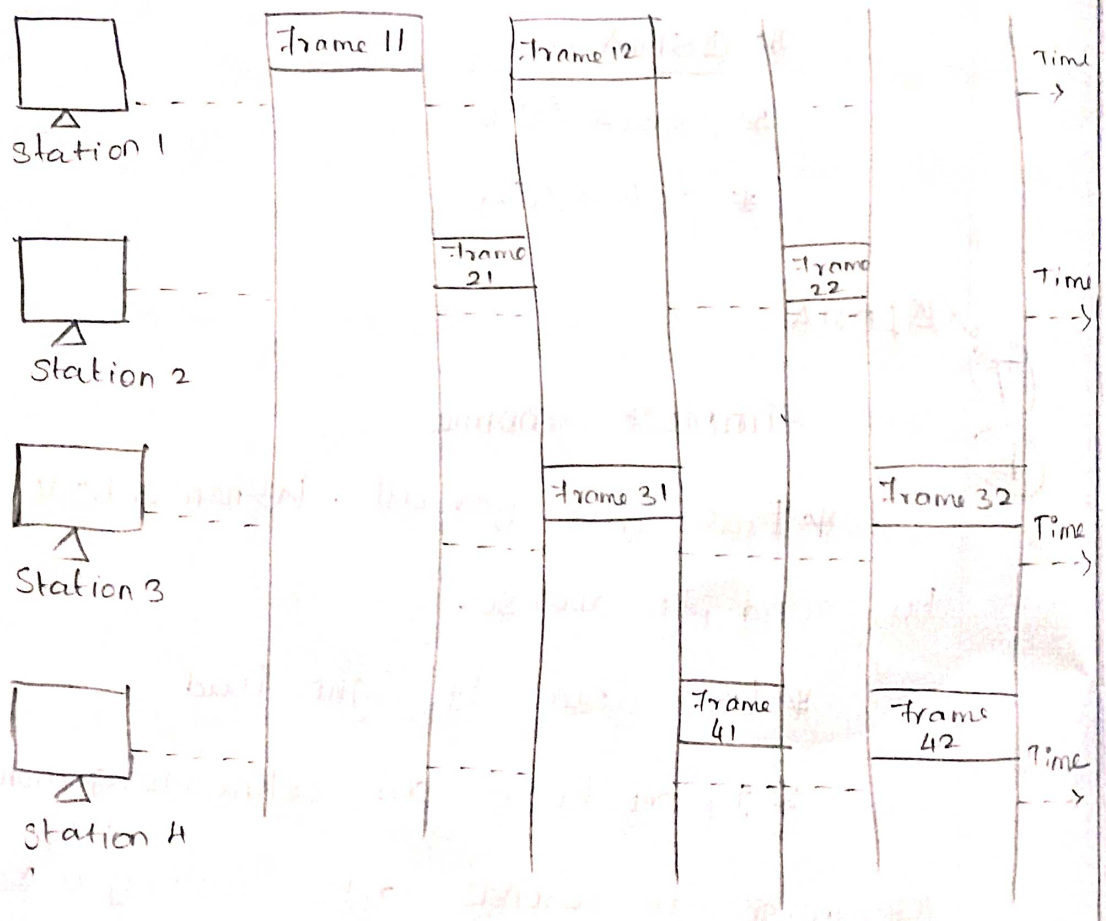


Fig: Frames in slotted ALOHA

In slotted ALOHA the shared channel is divided into a fixed time interval called slots. So that it is a station wants to send

a frame to a shared channel, the frame can only be start at the beginning of the slot and only one frame is allowed to be sent to each slot.

Carrier Sense Multiple Access (CSMA)

* Sense carrier
* if idle, send
* wait for ack

⇒ If there isn't one, assume there was a collision retransmit.

* Vulnerable period: One t_{jump}

Extension of CSMA:

*These are the collision detection CSMA/CD and the collision avoidance CSMA/CA techniques.

* Why CA and CD?

⇒ Difficult to detect

CSMA/CD:

* Each station listens before it transmits.
* If the channel is busy, it wait until the channel goes idle, and then it transmit.
* If the channel is idle it transmit

immediately. continuous sensing.

* If collision is detected transmit a brief jamming signal, then ceaso transmission, wait for a random time and retransmit

* collision detection is not by waiting for an Acknowledgement.

CSMA/CA:

* prevent collision at a moment they are most likely occur, when bus is released after a packet transmission.

* During the time a node is transmitting on the channel, several nodes might be want to transmit and waiting for it to become free.

* The moment of the transmitting node completes it transmission and would all starts transmitting at the same time.

* To overcome in the collision avoidance scheme, all nodes are forced to wait for a random time and then sense the medium again before starting their transmission.

* If the medium is sensed ~~the~~ medium ~~again~~ to be busy, further random

amount of time and so on.

* Thus the chance of two nodes starting to transmit at the sametime would be greatly reduced.

4.1.2 GPRS Architecture

- The GPRS architecture introduces two ***new network elements***, which are also called as ***GPRS Support Nodes (GSN)*** :
  - *(i) Serving GPRS Support Node (SGSN), and*
  - *(ii) Gateway GPRS Support Node (GGSN).*
- All GSNs are integrated into the standard GSM architecture. *The **GGSN** is an interworking unit between GPRS networks and the external **Packet Data Networks (PDN).***
- PDN contains routing information for GPRS users and performs address conversion. The other new element is ***SGSN*** which supports the MS.

- *The SGSN, requests for user addresses from* ***GPRS register (GR),*** *keeps track of an individual MSs location and it is responsible for collecting billing information.*

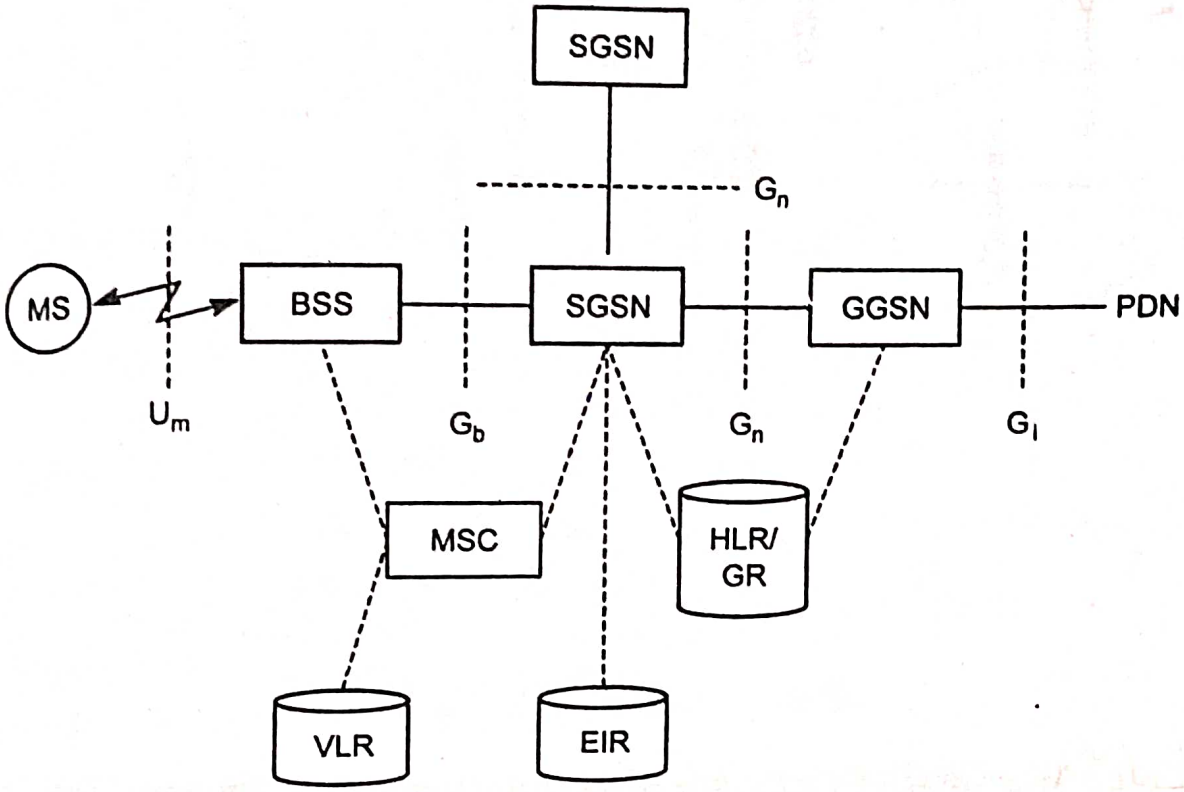


Fig 4.1 GPRS architecture reference model

- The GR, which is the part of HLR, stores all GPRS relevant data in a mobile IP network, GGSN and SGSNs can be compared with home agent and foreign agent respectively.
- As shown in the Fig.4.1, packet data is transmitted from a PDN, via GGSN and SGSN directly to the BSS and finally to MS.
- The packet data is transmitted from a PDN via GGSN and SGSN directly to the BSS and finally to MS.
- Before sending any data over GPRS network, an MS must attach a ***Temporary Logical Link Identity (TLLI)*** and a ***Ciphering Key Sequence Number (CKSN)*** for the data encryption.
- Besides attachment and detachment, ***Mobility Management (MM)*** also comprises of functions authentication, location management etc.

4.1.3 GPRS Transmission Plane Protocol Reference Model

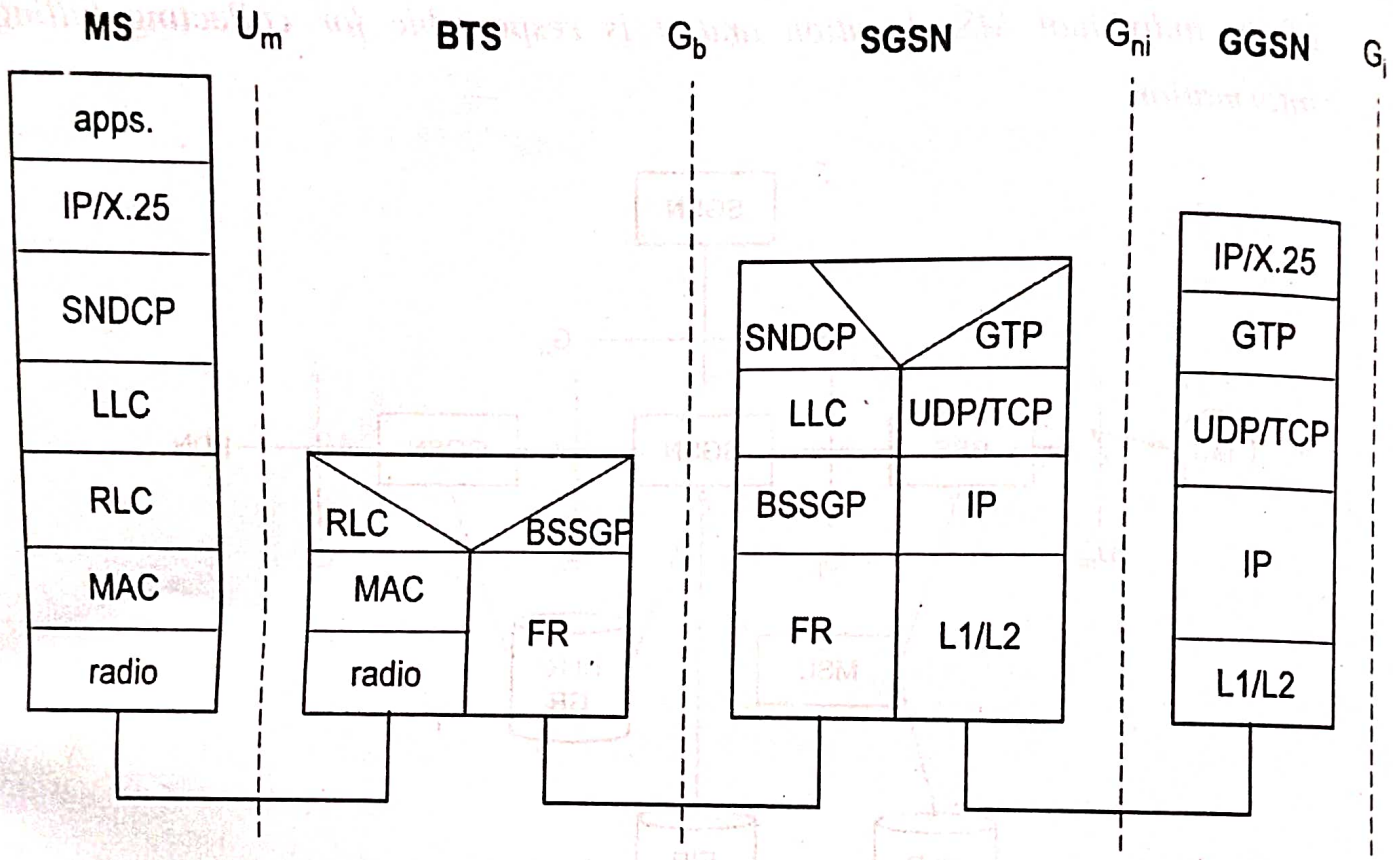


Fig 4.2 GPRS transmission plane protocol reference model

- Fig 4.2 shows the protocol architecture of the transmission plane of GPRS. All data between GSNs, is transferred using ***GPRS tunneling protocol (GTP).***
- GTP can use two different transport protocols which is either the ***reliable TCP*** or the ***non reliable UDP.***
- The ***Subnetwork Dependent Convergence Protocol (SNDCP)*** is used between an ***SGSN*** and ***MS***, to adapt the different characteristics of the underlying networks.
- On the top of SNDCP and GTP, user packet data is tunneled from the MS to the GGSN and vice versa.
- To achieve an high reliability of packet transfer between SGSN and MS, a special LLC is used which comprises ARQ and FEC mechanisms for PTP (Point- To –Point) services.

- A ***Base Station Subsystem GPRS Protocol (BSSGP)*** is used to convey routing and QoS related information between BSS and SGSN.
- BSSGP does not perform error correction and works on the top of a ***Frame Relay (FR)*** network. ***Radio Link Protocols (RLP)*** are needed to transfer data over U_m interface and provides a reliable link.
- One MS can allocate upto eight ***Packet Data Traffic Channels (PDTCHs)***. Capacity can be allocated on demand and shared between circuit-switched channels and GPRS.
- This allocation can be done dynamically with load supervision or alternatively, capacity can be pre-allocated.
- A very important factor for any application working end-to-end is that it does not notice any details from GSM/GPRS related infrastructure.
- All MSs are assigned private IP addresses which are then translated into global addresses at the GGSN. The advantage of this approach is the inherent protection of MSs from attacks.

4.1.4 Advantages, Limitations And Services of GPRS

☑ Advantages

The advantages of GPRS are,

(i) Machine to machine data communications.

(ii) Lower service charges.

(iii) Compatible with E-mail.

(iv) Used in broadcast services and web browsing.

(v) *The* high speed packet-switched communication supported by GPRS enabled applications providing many innovative web-based services, e-commerce, and advertising.

Limitations

Some important GPRS limitations are,

(i) Reduced call capacity.

(ii) Transit delay.

(iii) GPRS standard has no support for any storage mechanism.

GPRS Services

GPRS extends the GSM packet circuit switched data capabilities and makes the following services possible:

(i) SMS messaging and broadcasting.

(ii) "Always on" internet access.

(iii) Multimedia Messaging Service (MMS).

(iv) Push-to-talk over cellular (PoC).

(v) Instant messaging and presence – wireless village.

9) Message Terminated call (MTC)

(b) Message ~~Oriented~~ ea Originated call (MOC)

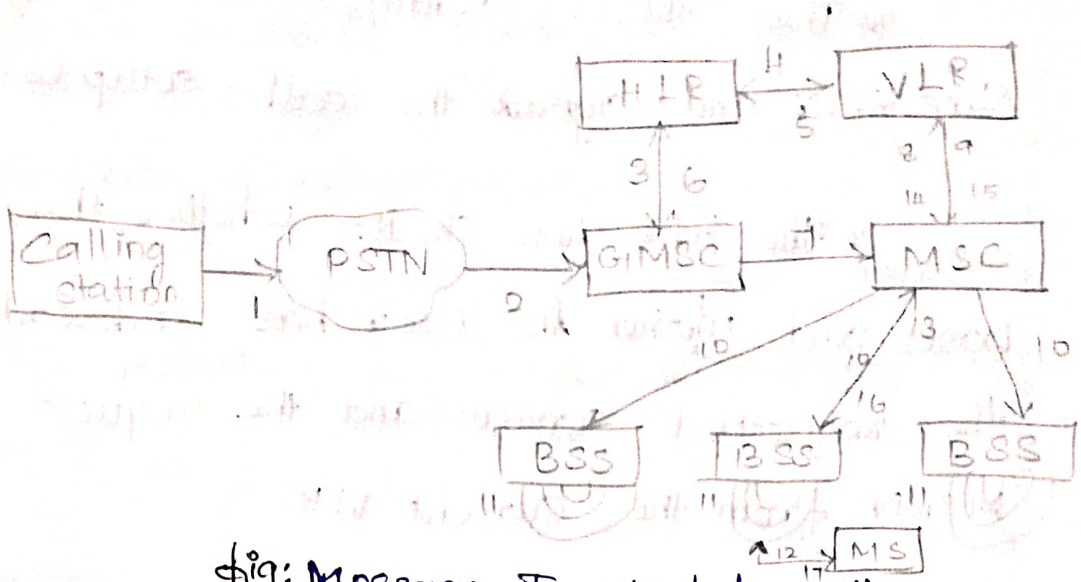


fig: Message Terminated call

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

9,8 → get current status of MS

10,11 → paging of MS

12,13 → MS answers

14, 15 → Security Checks

16, 17 → Setup connection.

Steps:

* A user will dial the phone number of GSM subscriber. The fixed network PSTN notices

belongs to the user in the GSM network and forwards the call setup to the Gateway MSC.

* The GMSC identifies the HLR for the subscriber and signals the call setup to the HLR.

* The HLR now checks whether the number exists and whether the user has subscribed to the requested services, and the request an MSRN from the current VLR.

* After receiving the request from MSRN.

* HLR can determine the MSC responsible for the MS and forward this information to GMSC.

* GMSC can now forward the call setup request to MSC indicated.

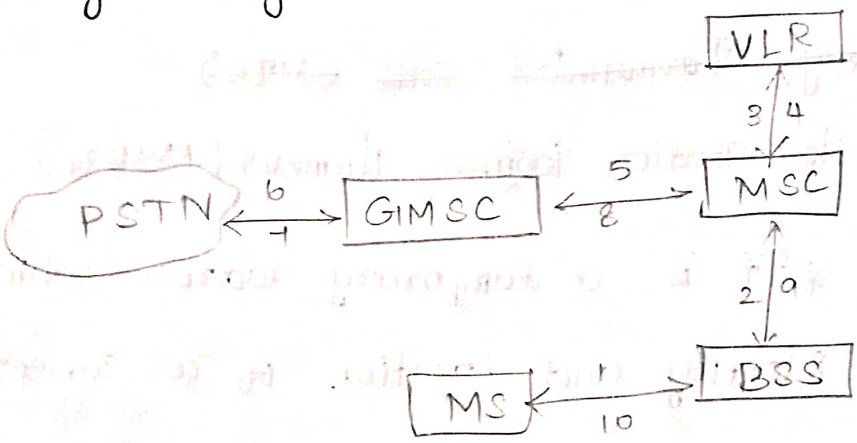
* From this MSC is responsible for all further steps. First it requests the current status of MS from VLR.

* If MS is available then MSC initiates paging in all cells it is responsible for as searching for the right cell would be too time consuming.

* This approach puts some load on signaling channels so optimization exist.

* location area can be determined.

Message Originated call (MOC)



1,2 → Connection request

3,4 → Security check

5,6,7,8 → Check resources

9,10 → Set upcall

Steps:

* MS transmits a request for a new connection.

* BSS forwards the request to MSC

* MSC then checks if the user is allowed to set up a call with the requested services and checks the availability of resource through GSM network into PSTN

* If all resources are available, MSC

Setup a connection between MS and fixed network.

* Its set up a call with the help of BSS and MS

5.2.2 DHCP Configuration

10)

b

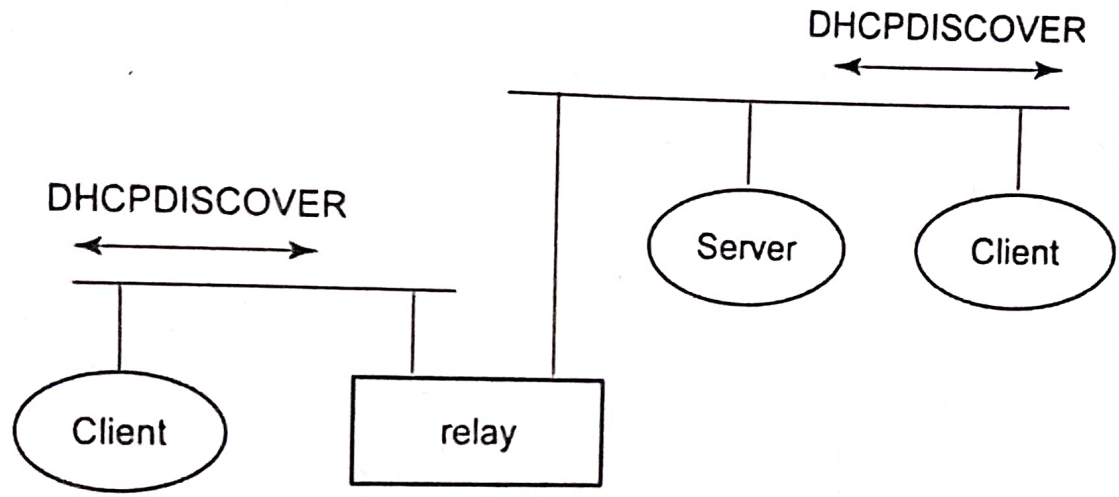


Fig 5.17 Basic DHCP configuration

- DHCP is based on the **client/ server model** as shown in Fig 5.17. DHCP clients send a request to a server, i.e. **DHCPDISCOVER** to which the server responds.
- A client sends the requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across an inter-working units to a DHCP server.

5.2.3 Initialization of DHCP Client

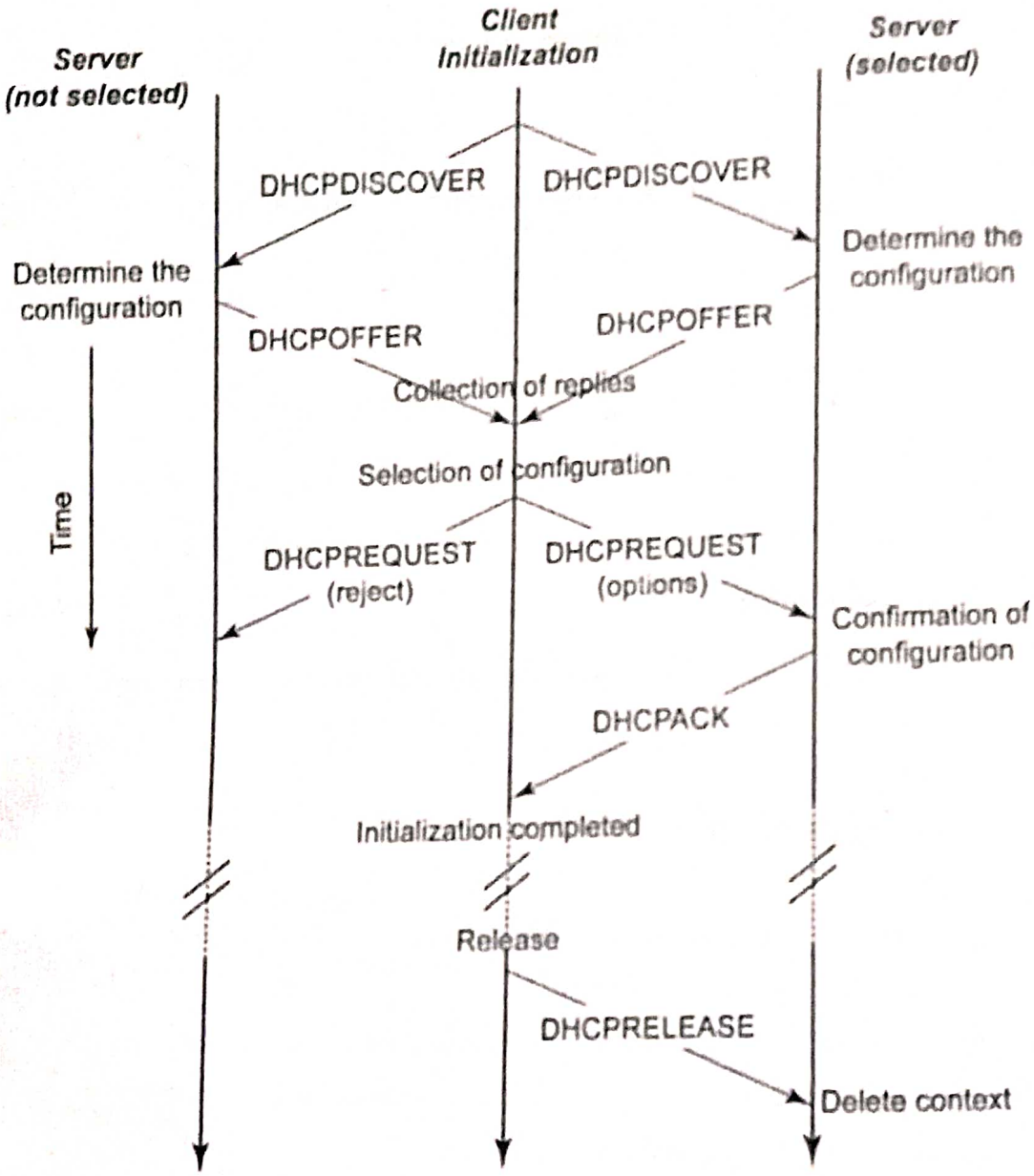


Fig 5.18 Client initialization via DHCP

- The DHCP client initialization using two servers is shown in Fig 5.18.
  - The ***client*** broadcasts a ***DHCPDISCOVER*** into the subnet. The relay is needed to forward this broadcast.
  - Here, two ***servers*** receives this broadcast and determine the ***configuration*** they can offer to the client, i.e., *checking of available IP addresses and choosing one for the client.*

- ***Servers*** reply to the client's request with ***DHCPOFFER*** and offer a list of configuration parameters. ***Client*** can now choose one of the configurations offered.
- The client inturn replies to the servers by accepting one of the configurations and rejecting the others by using ***DHCPREQUEST***.
- If a server receives a ***DHCPREQUEST*** with a rejection, it can ***free*** the ***reserved configuration*** for other possible clients.
- The server with configuration accepted by the client now confirms the ***configuration*** with ***DHCPACK.*** This completes the ***initialization phase.***
- If a client leaves a subnet, it should release the configuration received by the server using ***DHCPRELEASE***, thereby, the server can free the context stored for the client and offer the configuration again.
- The ***configuration*** a client gets from a server is only leased for a ***certain amount of time;*** it has to be ***reconfirmed*** from time to time. Otherwise the server will free up the configuration.
- This ***time out*** of configuration helps in the case of ***crashed nodes*** or nodes ***moved away*** without releasing the context.

Features of DHCP

- It is used for supporting the acquisition of ***care-of-addresses*** for mobile nodes.
- A DHCP server should be located in the subnet of the access point of the mobile node, or atleast a DHCP relay should provide the forwarding of the messages.
- A RFC 3118 should specify the authentication for DHCP messages which is needed to protect the mobile nodes, from ***malicious DHCP*** servers.
- Without authentication, both the mobile node cannot trust a DHCP server, and the DHCP server cannot trust a mobile node.