

GPRS: General Packet Radio Service

As an improvement to the current GSM (Global System for Mobile Communications) community, which was primarily created for voice communication and data transfer(except videos) like SMS, picture messages etc but no direct internet access.

GPRS,a standard bearer of 2.5G is a modified version of GSM with the following features:-

- GPRS is a wireless communication service that allows data to be transmitted over a cellular network.
- GPRS uses packet-switching technology to transmit data, which means that data is divided into small packets and sent over the network in a more efficient way.
- GPRS offers always-on connectivity, which means that a user can stay connected to the network at all times, without having to establish a connection every time they want to send or receive data.
- GPRS provides faster data transfer rates compared to the earlier generation of cellular networks, such as GSM.
- GPRS enables new applications and services to be developed, such as mobile internet browsing and email.

Advantages of GPRS

- A high-speed data transfer is offered to mobile devices through General Packet Radio Service or GPRS.
- Web browsing, email sending and receiving, and online shopping are just a few of the online services that GPRS users can access while they are on the move.
- Because GPRS is always operational, customers can access the internet quickly and without any problems.

GPRS architecture:

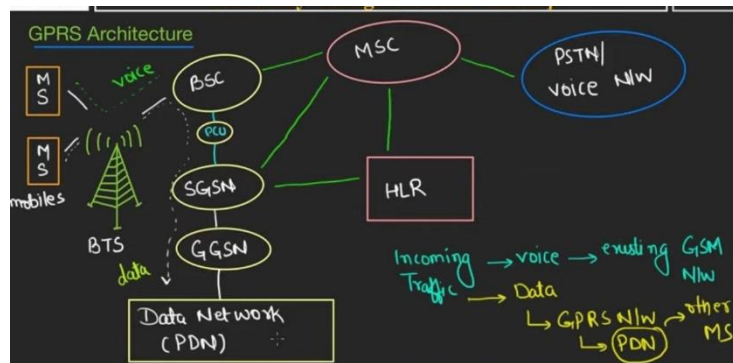
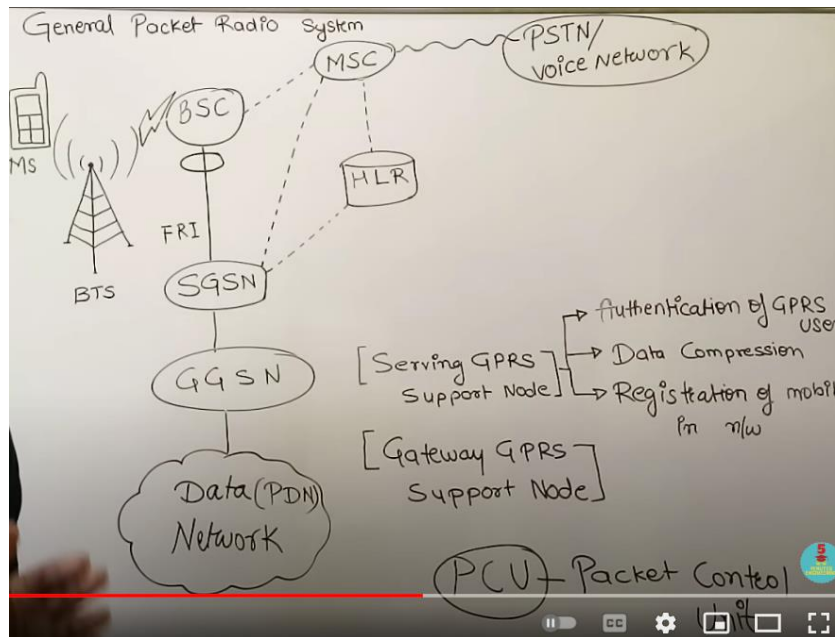
Its modification of GSM , voice communication go to earlier GSM architecture , but data or internet communication goes through PCU till the Public data network.

The BSC is upgraded as compared to GSM as BSC has a new component called PCU (Packet control unit). Software updates are given to BTS, BSC and internet enables Mobile stations are used.

There are 2 types of nodes:

SGSN: Serving GPRS support node, which performs Compression of data , Authentication of users and Registration of new users (CAR).

GGSN: Gateway GPRS support node , it acts like a router to route the data packets to Public data network (PDN).



GSM vs GPRS:

GSM:

Global systems for mobile communications.

No direct internet access.

Standard bearer of 2g.

Uses circuit switching.

Based on FDMA and TDMA.

Slower to connect.

GPRS:

General packet radio service.

Direct internet access.

Standard bearer of 2.5g.

Uses packet switching.

Based on GSM.

Faster to connect.

EDGE: Enhanced data rates for GSM evolution.

This is based on existing GSM architecture to and used to provide enhanced data rates as compared to GSM. GSM uses Gaussian Minimum shift keying (GMSK) modulation and EDGE uses 8 phase shift keying (8 PSK) modulation. Thus software and hardware upgrades are made to provide enhanced data rates.

It is also known as EGPRS(Enhanced GPRS), because the packet switching facility is also provided here.

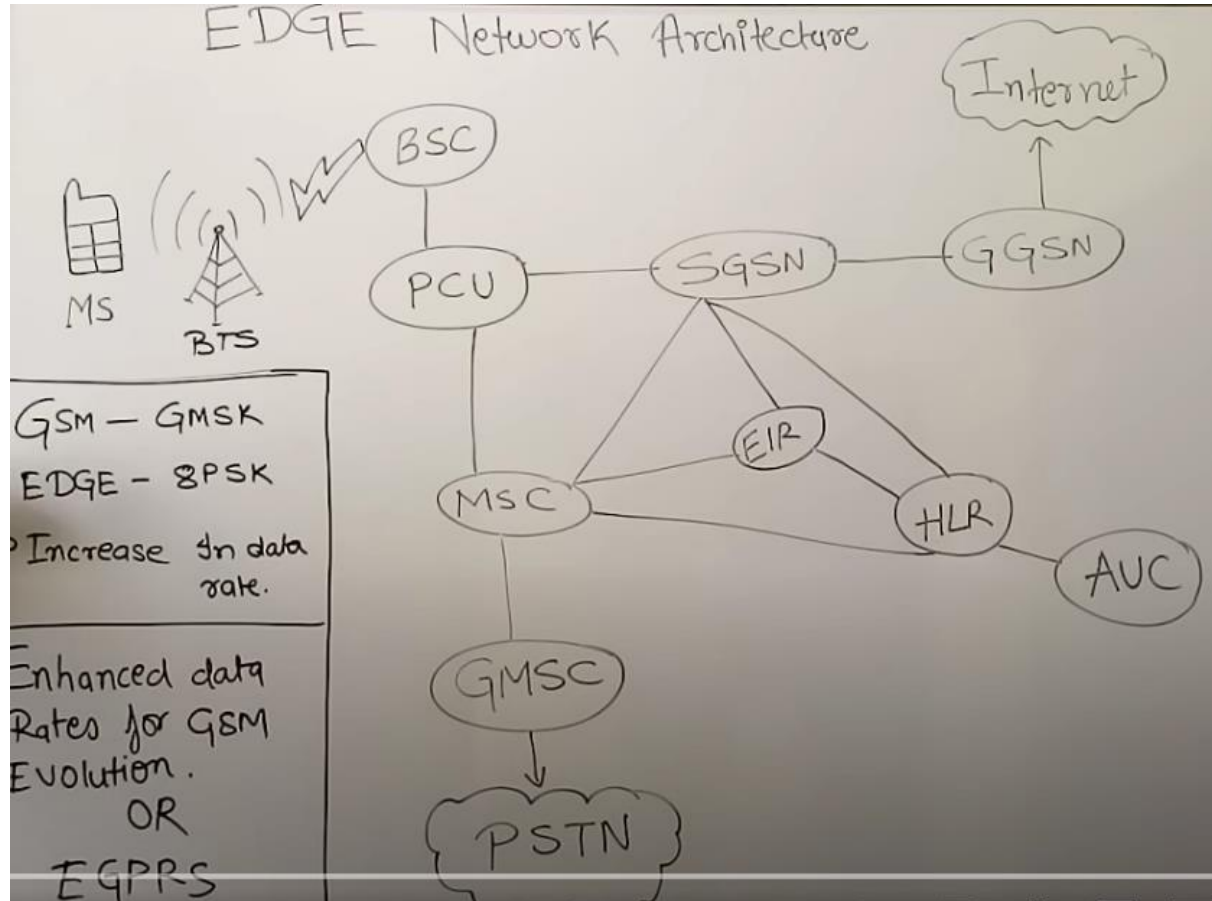
It can be considered as a combination of GSM and GPRS. The mobile station is connected to the BTS, there can be more than one BTS, BSC controls all the BTS. There is a PCU which has its function to direct the user towards a particular service. If user wants voice communication then communication is directed towards PSTN, in case of data/internet its directed towards internet. Packet switching is used for data services and circuit switching is used in voice services.

In case of voice communication, communication is directed towards MSC which can have many BSC's connected to itself. MSC is further connected to GMSC (Gateway mobile switching center) which connects MSC to voice network ie. PSTN

There are 2 support nodes.

SGSN: Serving GPRS support node, has an additional feature of mobility management as compared to GPRS. It does mobility management and hence stores the location of mobile users in HLR. Does authentication of users who ask for data services.

GGSN: Gateway GPRS support node, acts as router, interface of the EDGE system and internet, it also acts as a firewall and monitors incoming and outgoing traffic.



Wireless Local Area Network

Local Area Network : It is a Private Network that connects computers, devices within a limited area like building, office, campus etc.

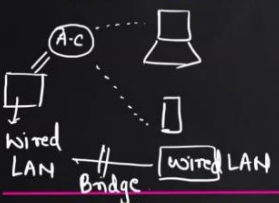
Wireless Local Area Network : It is a wireless computer network that links two or more devices using wireless communication to form a LAN within a limited area such as school, building, office etc.

Wireless Lan takes us closer to Adhoc network where nodes can connect to a network and do peer to peer communication and quit the network when they want. Eg: Zoom meeting.

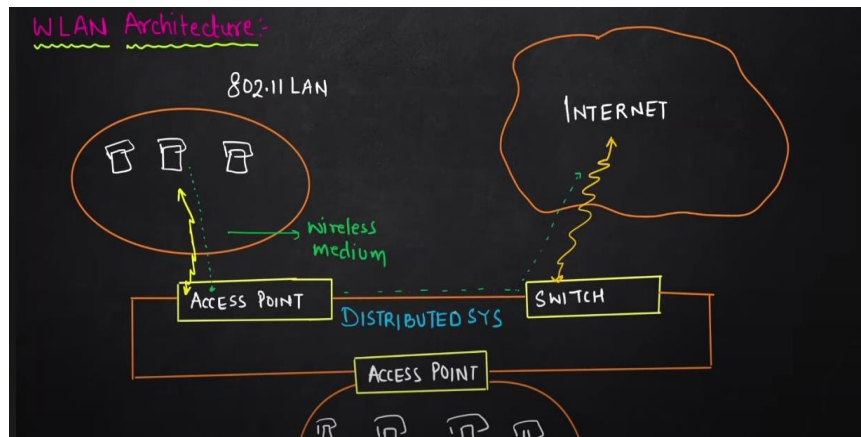
In general the devices are connected to an access point which in turn is connected to the wired network and the devices can access the internet.

Standards of WLAN are WIFI , IEEE 802.11 , HiperLAN.

Components of WLAN:

Easy Engineering Classes – Best YouTube Channel for University/College Semester Exam <i>i</i>	
COMPONENTS	DESCRIPTION
<p>ACCESS POINT:-</p> 	<p>Radio receiver/transmitter (Transceiver)</p> <ul style="list-style-type: none">→ Connects to <u>wired NW</u>.→ Exchanges signals with <u>wireless LAN card</u>.→ Small group of users are supported.
WIRELESS LAN CARD	WLAN Adapters.
BRIDGE	used for connecting <u>two LANs</u> .

Don't write the above like this in exam , write it in paragraph form as we will be expected to write components of IEEE 802.11 under the heading components of WLAN.



In exam we have to draw architecture of IEEE 802.11, this is just for reference.

Advantages:

1. Flexibility: Within the transmission range of the router all the devices can flexibly connect to the router.
2. Simplified Planning: Unlike wired network we don't want to buy wires to connect large number of computers. We can plan our network easily and would require just a wireless router.
3. No wiring difficulties
4. Robust: In case of natural calamities wired network would collapse unlike wireless network.
5. Cost effective: In case we plan to increase no. of computers in a network no need to buy more wires or switches for connecting the computers but just a router.

Disadvantages:

1. Lower bandwidth and transmission quality than wired network.
2. Low data transfer rate.
3. Local regulatory restrictions.
4. Security concerns as in wireless network devices emit radio frequencies which causes lower security of information and data.

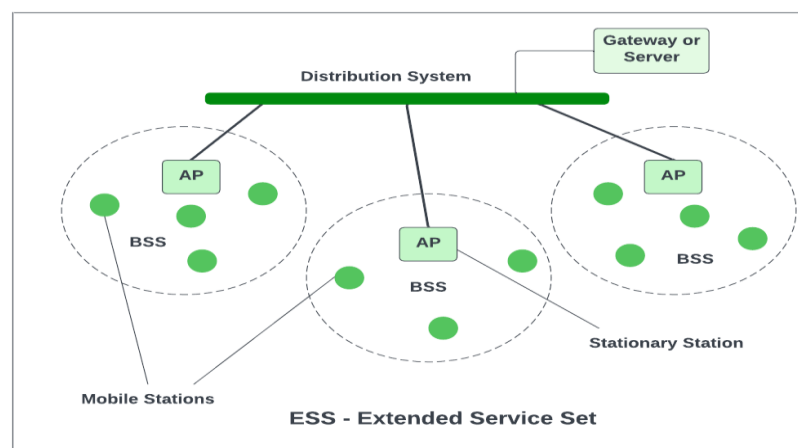
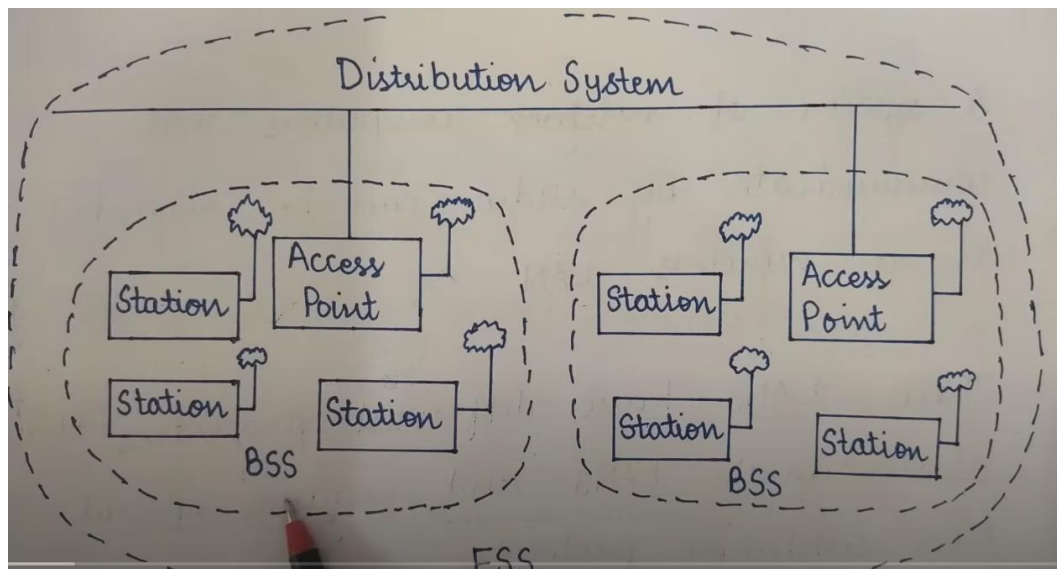
Types of WLANs

As per IEEE standard WLAN is categorized into two basic modes, which are as follows:

1. **Infrastructure:** In Infrastructure mode, all the endpoints are connected to a base station and communicate through that; and this can also enable internet access. A WLAN infrastructure can be set up with: a wireless router (base station) and an endpoint (computer, mobile phone, etc). An office or home WiFi connection is an example of Infrastructure mode.
2. **Ad Hoc:** In Ad Hoc mode WLAN connects devices without a base station, like a computer workstation. An Ad Hoc WLAN is easy to set up it provides peer-to-peer communication. It requires two or more endpoints with built-in radio transmission.

IEEE 802.11 WLAN

As no. of mobile computing and communication devices grow so the need to connect them with outside world. WLAN can be considered as a network of notebook computers , mobile phones , other wireless devices connected using radio waves.



Each BSS has one access point and multiple stations. Each access point is connected to the distribution system. This complete set is called ESS which constitutes of multiple BSS and distribution system.

Components of WLAN Architecture:

Access Point - a networking hardware device that allows other wifi devices to connect to wired network.

We can say an AP (access point) bridges wired and wireless networks.

Station - A device that has the capability to use 802.11 protocol.

for ex: Laptop, desktop, wifi phone
it can be fixed, mobile or portable.

Basic service set (BSS):

A BSS contains multiple Stations and a single access point. Stations from different BSS interact through an Access point.

Modes of operation:

Infrastructure BSS: Communication between stations takes place through access points.

Independent BSS – Supports mutual communication between wireless clients. An ad-hoc network is spontaneously created.

ESS (Extended Service Set) - it is one or more interconnected basic service sets (BSSs) and their associated LANs.

BSS usually provides short range wireless communication but ESS provides long range wireless communication.

ESS supports mobility i.e., clients can move from one place to another without getting disconnected to the network.

As there are more than one AP, whenever a client will move, it will automatically jump from one AP to another AP and get connected. This is also called roaming.

To create long range wireless communication, more than one AP is required and then all of them are connected to a wired LAN.

All APs in ESS are connected to each other by a common DS (Distributed System).

DS (Distribution System) - usually connects more than one AP to form ESS and allows users to move freely.

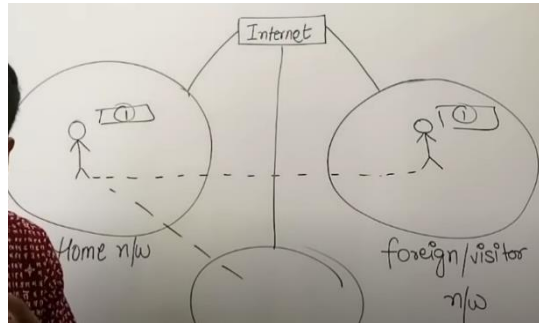
Extra points for knowledge (optional)

A WLAN is based on cellular architecture where each BSS represents a cell. Each cell is controlled by a base station or Access point.

A WLAN may be formed using a single BSS but most WLAN's form using multiple BSS thus the AP's are connected using a backbone called Distribution system. A distribution system can be an ethernet or in some cases a wireless system.

The stations within a BSS can also form an adhoc n/w in which devices in close proximity can form a n/w on the fly without a centralised Access point and can communicate directly. Eg: People with laptop have conference.

Mobile IP:



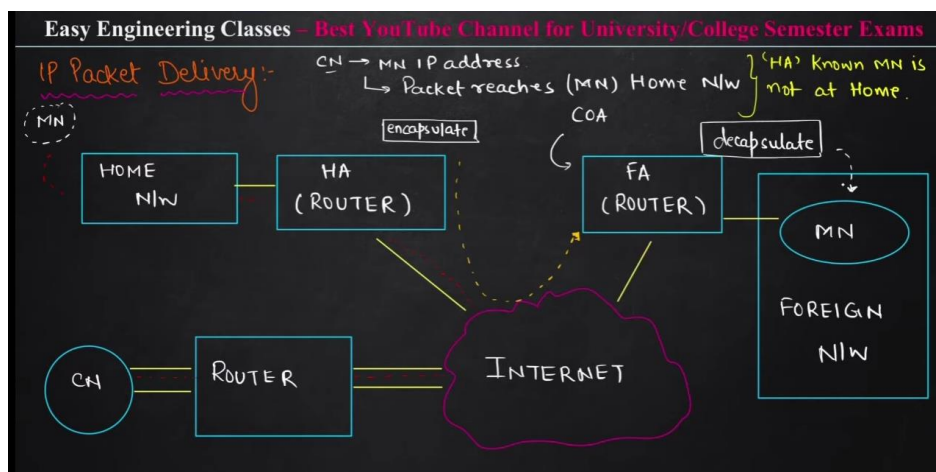
If a device is in home network it can access send and receive data packets using IP routing and hence use internet but when device goes to foreign network IP routing does not work and hence device cant access internet. To overcome this problem Mobile IP is used which keeps the IP address of the device same in foreign network also when it comes to it from home network.

Easy Engineering Classes – Best YouTube Channel for University/College Semester Exams

Mobile IP

- ↳ Mobile Internet Protocol.
- designed by Internet Engineering Task Force (IETF).
- Standard Commⁿ Protocol – that is designed to allow mobile device users to move from one n/w to another w/o changing their IP.
- IP is made mobile since during mobility IP of device changes and system needs to be reconfigured.

A diagram showing two circles representing networks. The left circle is labeled 'N/W 1' and contains a stick figure with a small rectangle labeled 'IP1' above it. The right circle is labeled 'N/W 2' and contains a stick figure with a small rectangle labeled 'IP1' above it. A dashed line connects the two circles.



Just for reference actual diagram at end.

Entities and Terminologies:

1. **Mobile Node (MN)** is the hand-held communication device that the user carries e.g. Cell phone.
2. **Home Network** is a network to which the mobile node originally belongs as per its assigned IP address (home address).
3. **Home Agent (HA)** is a router in-home network. Tunnel starts from here to Care-of-Address which is location of device in foreign network.
4. **Foreign Network** is the current network to which the mobile node is visiting (away from its home network).
5. **Foreign Agent (FA)** is a router in a foreign network. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node. Tunnel from HA ends here.
6. **Correspondent Node (CN)** is a device on the internet communicating to the mobile node.
7. **Care-of Address (COA)** is the temporary address used by a mobile node while it is moving away from its home network. It is used to tell current location of device in Foreign network.

Mobile IP requirements (Just remember the headings and just read the definitions once)

1. **Compatibility:** Mobile IP is compatible with any browser, operating system and service provider. We can use internet irrespective of browser, operating system and service provider.
2. **Transparency:** Information which should not be revealed to the user due to transparency must be hidden from the user. Eg: Location transparency, The location of the sender must not be revealed to the receiver when he receives the message.
3. **Scalability:** The user can send or receive the messages or use the internet irrespective of this presence in the home network or foreign network.
4. **Flawless device mobility:** The IP address of the device will not change whether its in home network or foreign network.
5. **Security :** There must be a security mechanism like authentication so that unauthorized users would not be able to use the Mobile IP network.

Working of Mobile IP:

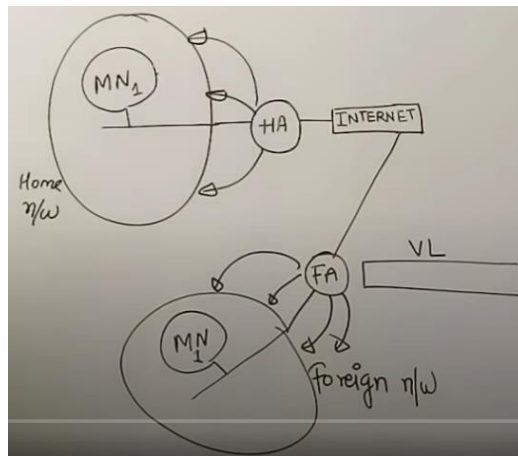
Below are the steps in working of mobile IP.

- 1.Agent discovery
- 2.Registration
- 3.Tunneling

Agent Discovery:

When a new device is introduced in the network, in order to identify its home agent it uses agent discovery, the home agent sends advertisement to all nodes in a home network and from that the new device gets to know about the same and hence can send and receive packets through home agent.

When the new device moves to foreign network, it again uses agent discovery to find foreign agent in by learning from ads of foreign agent and hence gets aware of coa and foreign agent.



Registration:

When a device gets into a foreign n/w, the home agent and foreign agent both must be updated about the care-of-address (COA: current location of user in foreign network) of the device. For this purpose the registration process is carried out.

The device using its Ip address, security keys and advertisements of the foreign agent and creates a registration request and sends it to the foreign agent for validation which authenticates the device and in turn sends the request to the home agent for validation.

The home agent after verifying the mobile device performs 2 operations:

1. Tunneling from the Home agent to COA (Location of device in foreign network)
2. Mobility binding : Associating the device with its COA.

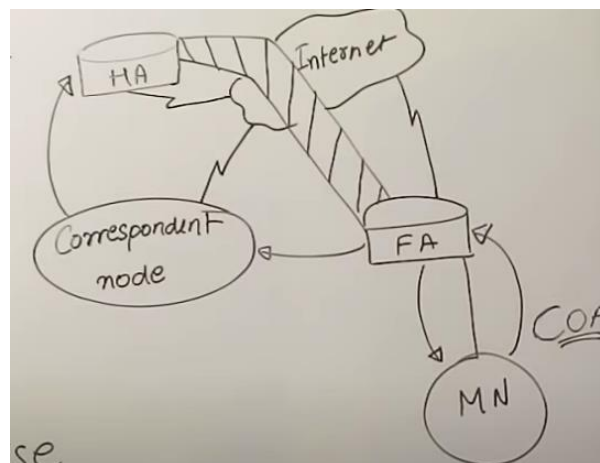
Then Home agent sends a reply to foreign agent and the foreign agent adds the device in the visitors list thus giving the confirmation to the device. The device can now send and receive packets with the help of home and foreign agents.

Tunneling:

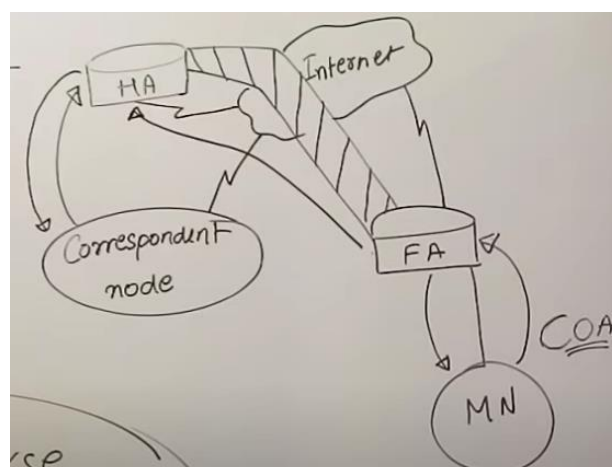
The device has been registered already in the foreign network and tunnel has been created from home agent to Care of Address. Now if there is a correspondent node from another network which wants to send the packets to mobile node, the correspondent node will send the packets to the home agent unaware of the fact that the device has reached the foreign network. The home agent is a router and forwards the packets to the mobile node through tunnel, thus at beginning of the tunnel the packets are encapsulated and at the foreign agent they are decapsulated (packet forwarding, encapsulation and decapsulation are functions of the tunnel).

The mobile node can send a reply/response to the correspondent node through the foreign agent which may be discarded by correspondent node as the correspondent node expects a reply from home agent and not by foreign agent. **Thus to overcome this problem reverse tunneling is used.**

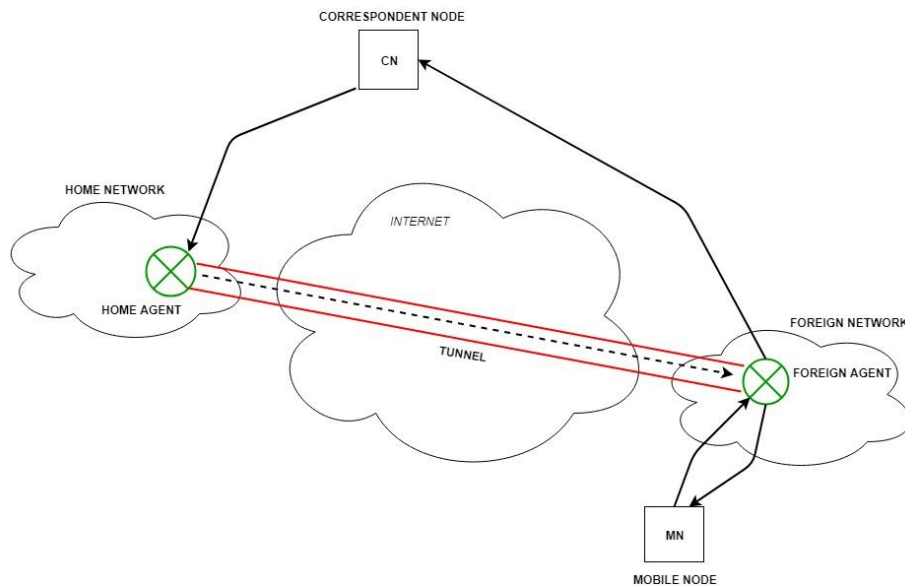
In reverse tunneling the response is sent by the mobile node to the foreign agent which sends it to home agent which sends it to the correspondent node.



Tunneling



Reverse tunneling



Tunneling Diagram for exam

IMT-2000:

The ITU (International telecommunication union) decided 2000Mhz frequency is a **global frequency** to be used all over the world hence IMT-2000 was developed.

IMT-2000 Introduction:

Uplink frequency used is 1185 MHZ – 2025 MHZ

Downlink frequency is 2110-2200 MHZ

FDD is used for satellite and mobile communication , TDD used for pedestrian and indoor environments.

Vision of IMT-2000

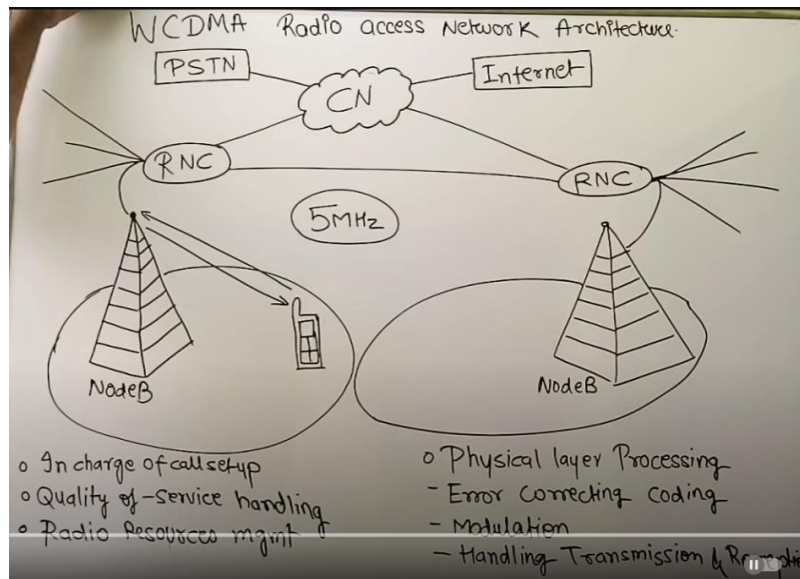
IMT-2000 VISION

- Common spectrum world wide(1.8 to 2.2 GHz)
- Wide range of telecommunication services (voice , data, multimedia, internet)
- Data rates up to 2Mbps.
- Global seamless roaming
- Enhanced security and performance

- Data rates of 9.6 Kbps or more for global(mega cell) , 144Kbps or more for vehicular(macro cell) , 384 Kbps or more for pedestrian (micro cell) and upto 2Mbps for indoors(pico cells).

W-CDMA: Wideband code division multiple access:

Wideband is a direct spread technique. The transmission is spread by 5 MHz when using a wideband.



Node B in W-CDMA terms is called logical node.

The user equipment (mobile) can communication with the logical node or tower using a dedicated channel.

The transmission from mobile to tower is uplink and tower to mobile is downlink.

Node B functions in W-CDMA:

It performs physical layer processing which include:

- Error correcting coding.
- Modulation like PSK, FSK etc.
- Handling transmission and reception of signals with multiple user equipments.

The radio network is controlled by RNC – Radio network controller , many Node B's can be connected to a single RNC and RNC's of different sectors can be connected together also for coordination.

RNC's are connected to the core network (CN).

CN is connected to the internet and PSTN(voice network).

Thus user equipment can communicate with the Node B via uplink.

User can request for a voice or data service to NODE B which is transmitted to RNC , RNC authenticates the user and then if the request is voice related then core network transfers it to the PSTN and if data related then to the internet, this is possible as the RNC is connected to the core network and can forward the user's request to core network.

Functions of Radio Network controller (RNC):

- In charge of call setup (Transfers the user request to PSTN or the internet depending on type of request).
- RNC manages the quality of service.
- Resource management , if traffic on a cell is more than RNC can provide more radio resources like bandwidth etc there.

Voice call request uses circuit switching while the data request uses packet switching.

CDMA-2000

- It gives evolutionary upgrade to 2G(IS-95),2.5G(IS-95B) users to use 3G.
- It's a family of standards.
- A key component in CDMA-2000 is the packet core network(PCN) which delivers packets with high speed and better security.
- Multicarrier modulation is applied to provide wider bandwidth, higher data rates.
- In CDMA 16-QAM(quadrature amplitude modulation) is applied to increase the maximum data rate.

CDMA-2000 family standards:

CDMA 2000 1x : Double voice capacity , provides MMS, games etc.

CDMA 2000 1x EV-DO: Provides always on service.

CDMA 2000 1x EV-DV: Provides integrated voice with high speed data services like video conferencing.

Features:

- Designed for urban as well as rural areas.
- Offers broadcast for mobile devices so cost effective.

Advantages:

- Superior voice quality.
- Flexible network architecture for connectivity with ANSI, IP based networks.
- Improved security and privacy.

Disadvantages:

Does not have international roaming capabilities until the device has GSM radio.

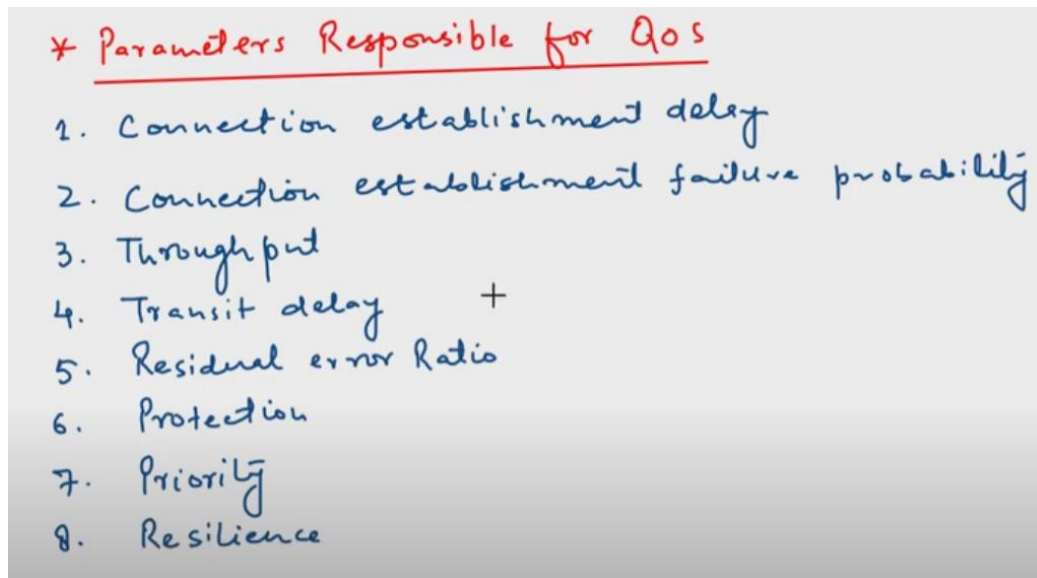
Too many signals come from cells to subscriber's phone but none is dominant degrading the call quality.

Quality of service in 3G:

The quality of service has to be measured from one terminal to another ie. End to end.

Its user dependent as its on the user whether he is satisfied or not from the quality.

Parameters Responsible for Qos:



1. Connection establishment delay:

Delay between the instant when the connection establishment is requested and when the connection establishment is confirmed. It should be less for good quality of service.

2. Connection establishment failure probability:

It means the connection could not be made even after maximum delay. It may happen due to failures like network congestion etc.

3. Throughput:

It is maximum bytes which are transmitted per second. It is measured separately from uplink and downlink.

4. Transit delay:

Delay between the packets being sent from source and being received at destination.

5. Residual error ratio:

Measures the bits lost or distorted messages over total messages sent.

6. Protection:

Data must be protected from being read or being modified by third party.

7. Priority:

The service must prioritize certain connections when needed , it also helps in congestion control. High priority connections should be serviced before low priority connections.

8. Resilience:

The services must be resilient and the probability to terminate a connection during internal problems and connection must be least.

There are 4 classes on which Qos is determined:

Streaming class , background class , interactive class and conversational class.