UNIT : I

WIRELESS LAN

Introduction – WLAN Technologies – IEEE 802.11 ; System Architecture, Protocol Architecture, 802.11b, 802.11a - Hiper LAN : WATM, BRAN, Hiper LAN 2 – Bluetooth - Architecture, WPAN – IEEE 802.15.4, Wireless USB. Zigbee, 6Lo WPAN, Wireless HART.

INTRODUCTION :-

WLAN :-

A wireless local Area network (WLAN) is a wireless Computer networks that links two or more devices using a wireless distribution method (often Spread Spectrum or OFDM radio) With in a limited area such as a home, School, Computer laboratory or office buildings

This gives users the ability to move around with in a local Coverage area and yet still be Connected to the network. Most modern WLAN are based on IEEE802.11 Standards and are marked under the Wi-Fi band name.

List the WLAN Advantage, disadvantage & goals ?

*) WLAN Advantages :

1) Flexibility - Within radio Coverage nodes can

Communicate without further restriction Radio waves can penetrate walls.

2) planning :-

Wireless adhoc networks allow for Communication without planning, wired networks need wiring plans.

3) Robustness :

Wireless network can Survive disasters eg) earth quake or users pulling a plug. If the wireless devices Survive people can Still Communicate.

WLAN Disadvantages :

1) Quality of Service :

WLANs offer typically lower QoS. Lower bandwidth due to limitations in radio transmission and higher error rates due to interferences.

2) Proprietary Solutions :-

Slow Standardization procedures lead to many Proprietary Solutions only working in an homogeneous environment.

3) Safety and Security :-

Using radio waves for data transmission might interfere with other high tech equipment.

WLAN main design Goals :-

1) Global operation :-

WLAN products should sell in all countries, so national international frequency regulation have to be considered.

LAN equipment may be carried from one country to another and this operation should be legal.

2) Low power :

The LAN design take into account that devices communicating via WLAN are typically running on battery power. Special power saving modes and power management functions must be implemented.

3) Simplified Spontaneous Co-operation :

WLANs should not require complicated set up routines but operate spontaneously after power-up.

4) Easy to use :

WLANs are made for simple users, they should not require complex management but rather work on a plug and play basis.

5) Protection of Investment :

A lot of money has been invested for

Wired LANs, WLANs should be able to inter-operate with existing network.

WLAN TECHNOLOGIES :-

Explain about the basic transmission technologies of WLAN ?

There are two different basic transmission technologies used in WLANs to setup such as,

1. Infrared technology.
2. Radio transmission

Other types are UHF narrow band, Spread Spectrum techniques

1. Infrared Technology :-

*) Infrared is based on transmission of infrared light.

*) Infrared uses diffuse light reflected at walls or directed light if a line of sight [LOS] exists between sender and receiver.

*) It has frequencies just below the visible light

*) Senders can be simple light emitting diodes (LED's)

Advantages :-

*) Senders and receiver are very cheap.

*) No license is needed for infrared technology.

*) Electrical devices do not interfere with infrared transmission shielding is very simple.

Disadvantages :-

*) Low bandwidth Compared with other LAN technologies
*) It has limited transfer rate.
*) Infrared transmission cannot penetrate walls or other obstacles.
*) for good transmission Los is needed.

(2) Radio wave transmission :

It uses radio transmission in the GHz range for example 2.4 GHz in the license free ISM band.

Advantages :

*) Long term experience for wide area networks and mobile Cellular phones.
*) It can Cover larger area and Can penetrate walls, furniture.
*) It does not need los.
*) Current radio based products offer higher transmission rate. (10 Mbits)

Disadvantages :-

*) Shielding is not Simple
*) It is only Permitted in certain frequency band
*) Very limited ranges of license free bands are available but they are not the same in all Countries.

IEEE 802.11

Explain about IEEE 802.11 with neat illustrations

Explain in detail about IEEE 802.11 infrastructure type and Adhoc.?

The IEEE Standard 802.11 Specifies the most famous family of WLANS in which many products are available. The primary goal of the Standard was the Specification of a simple and robust WLAN which offers time-bounded and asynchronous Service.

(i) System Architecture :

Wireless network can have to different basic System architecture Such as,

→ Infrastructure type networks, where stations Communicate through access point.

→ Ad hoc type network, where stations Communicate directly.

2) IEEE 802.11 architecture of an infrastructure network

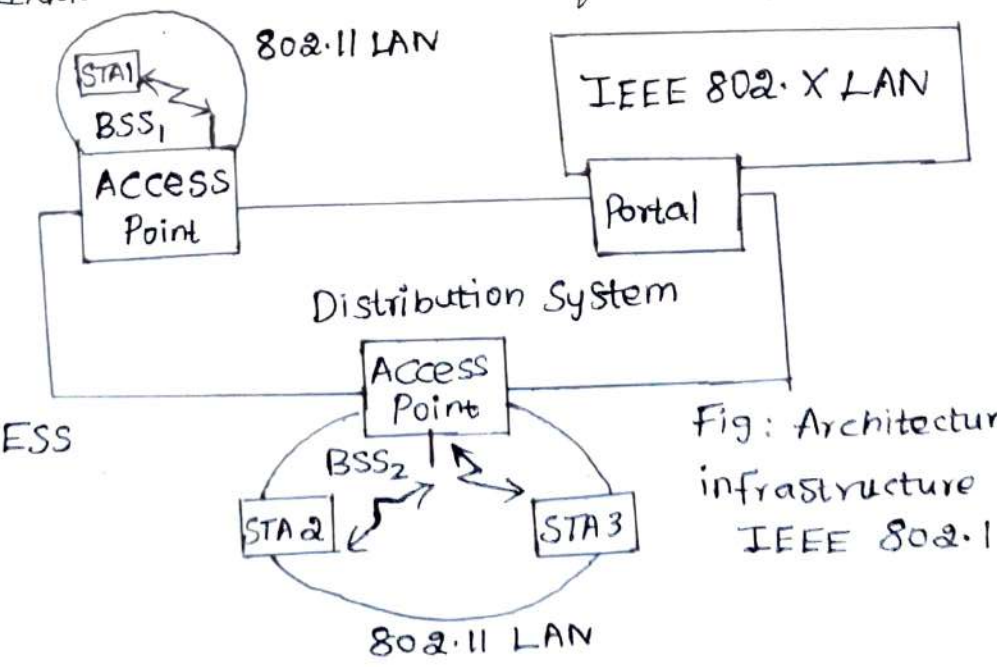


Fig: Architecture of an infrastructure based IEEE 802.11

Fig shows the components of an infrastructure and a wireless part as specified for IEEE 802.11

*) Station (STA):

*) In this architecture model, each nodes called as stations (STA) and those stations are connected to access point (AP).

* Access point (AP)

→ It is used to station integrated into the wireless LAN and the distribution system.

*) Portal:-

→ The distribution system connects the wireless networks via the APs with a portal, which act as a bridge to other networks (wired)

*) Distribution System:

→ More than one basic service set (BSS) can be connected via a distribution system.

⇒ It connects several BSS via the AP to form a single network and it extends the wireless coverage area. This network is now called an Extended Service Set (ESS).

IEEE 802.11 Services:

The two types of services are,

1. Basic Service Set (BSS)
2. Extended Service Set (ESS)

1) Basic Service Set (BSS) :-

* The basic Service Set (BSS) Contain Stationary or mobile network (wireless) stations and a central base station called access point (AP)

⇒ The use of access point is optional.

*) If the access point is not present, it is known as Stand-alone network. Such a BSS cannot Send data to other BSSs. This type of architecture is known as ad-hoc architecture.

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

2) Extended Service Set (ESS)

⇒ An ESS is created by joining two or more basic Service Sets (BSS) having access points. (APs)

⇒ These extended networks are created by joining the access points of basic Services Set through a wired LAN known as distribution System.

The distribution System can be any IEEE LAN

There are two types of Stations in ESS

(i) Mobile Stations : These are normal Station inside a BSS.

(ii) Stationary Stations : These are Ap Stations that are part of a wired LAN.

→ Extended Service Set identifier (ESSID):

*) ESS has its own identifier, the ESSID

*) The ESSID is the name of a network and is used to Seperate different networks.

*) Without knowing the ESSID, it should not be possible to participates in the WLAN.

→ Uses of STA, AP and distribution System:.

⇒ Stations can select an Ap and associated with it. The APs can support Roaming ie changing access points.

⇒ Access points Provide Synchronization with in a BSS, System power management and it can control medium access to support to time bounded services.

The distribution System can handle data transfer between the different APs.

b) IEEE 802.11 Architecture of an Ad-hoc network:

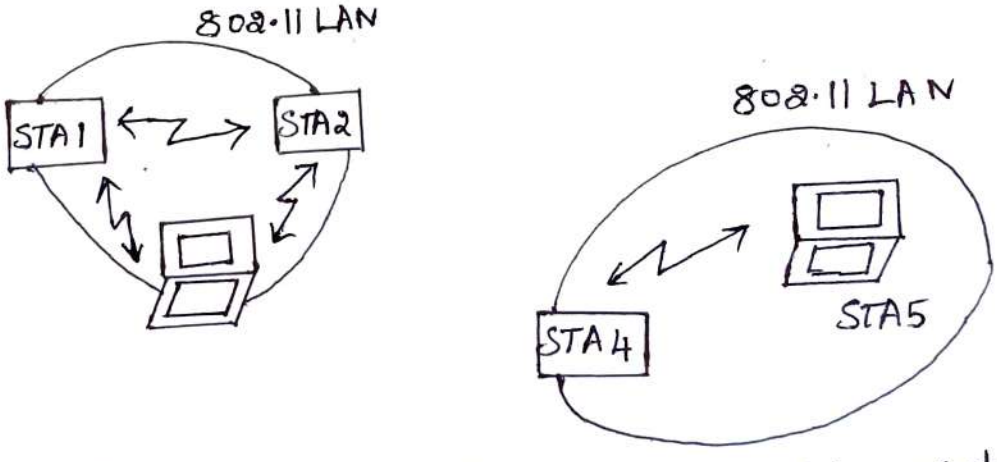


Fig: Architecture of IEEE 802.11 ad-hoc wireless LANS.

IEEE 802.11 allows the building of Ad hoc networks between stations thus forming one or more independent BSSs. (IBSS)

→ IBSS (Independent Basic Service Set)

In IBSS, STAs can communicate directly to each other and Providing that they are within each other's transmission range.

STA 1, STA 2 and STA 3 are in IBSS1, STA 4 and STA 5 in IBSS2. For (eg) STA 3 can communicate directly with STA 2 but not with STA 5.

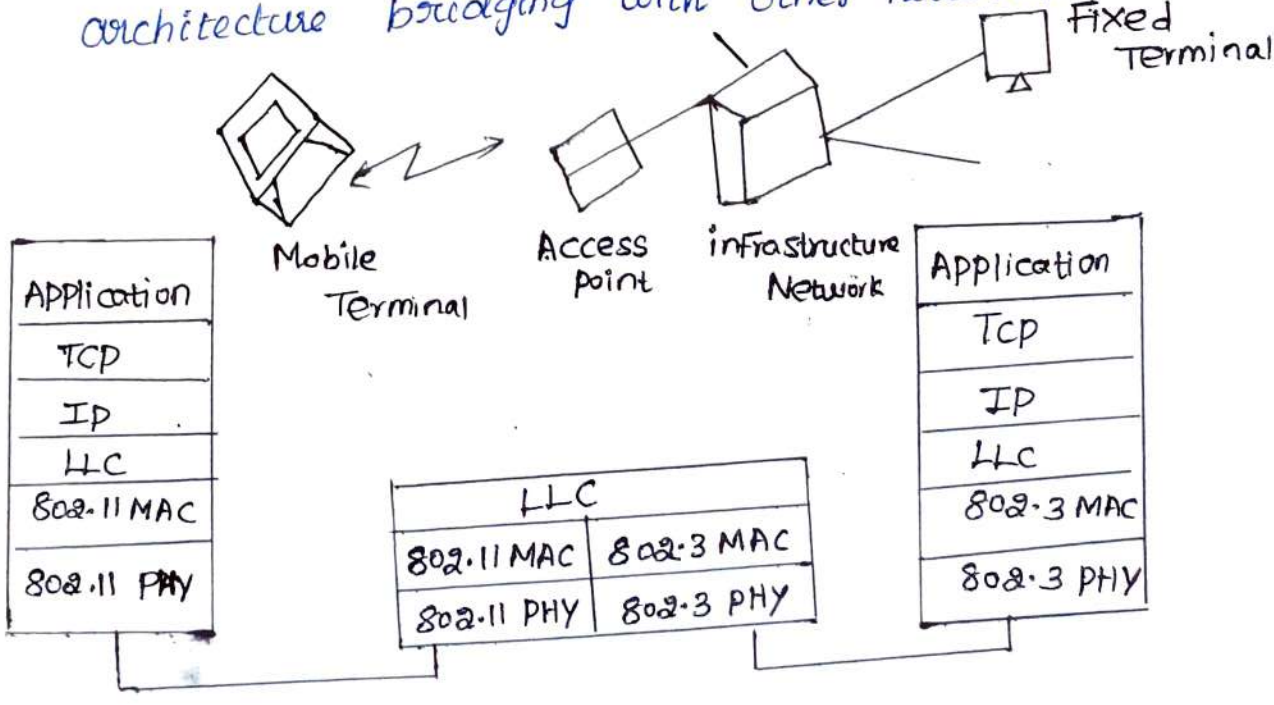
Several IBSSs can either be formed via the distance between the IBSSs or by using different Carrier frequencies.

(ii) PROTOCOL ARCHITECTURE :-

Describe about Protocol architecture of IEEE 802.11

(or)

Explain in detail about IEEE 802.11 protocol architecture bridging with other network.



⇒ An IEEE 802.11 wireless LAN is connected to a switched IEEE 802.3 Ethernet via a bridge. The WLAN behaves like a show wired LAN.

⇒ The higher layer (Application, TCP, IP) look the same for both wireless nodes and wired nodes.

⇒ The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media.

⇒ The IEEE 802.11 standard only covers the physical layer (PHY) and Medium Access Layer (MAL) like the other 802.x Lan do.

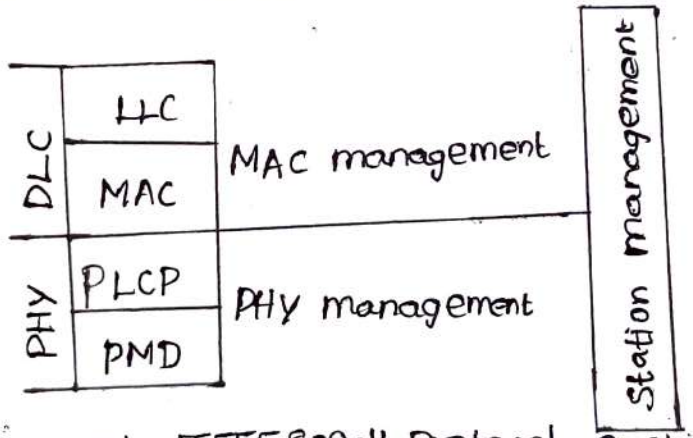


Fig: Detailed IEEE 802.11 protocol architecture and management

MAC Layer function :-

⇒ The basic tasks of the MAC layer comprise medium acess, fragmentation of user data and encryption.

*) physical layer :-

The physical layer is subdivided into

i) physical layer Convergence protocol (PLCP)

⇒ The PLCP Sub layer Provides a Carrier Sense Signal Called Clear channel Assessment (CCA) and Provides a Common PHY Service access point (SAP) independent of the transmission technology.

(ii) Physical Medium dependent Sublayer (PMD):

The PMD Sublayer handles modulation and encoding and decoding of Signals.

Management Layer:-

⇒ The management layer subdivided into

(i) MAC management:

The MAC management Supports the association and re-association of a Station to an access point and roaming between different access points.

It also Controls authentication mechanism, encryption Synchronization of a Station with regard to an accesspoint and power management to Save battery power. It maintains the MAC management information base (MIB).

(ii) PHY management:-

The main tasks of the physical (PHY) management include Channel tuning and PHY MIB maintenance.

Station Management :-

⇒ It has co-ordination of all management functions.

⇒ It is responsible for additional higher layer function. for (eg) Control of bridging and interaction with the distribution system in case of an access point.

IEEE 802.11b :-

Explain in detail about IEEE 802.11 b Standard.

IEEE 802.11 b Standard describes a new PHY Layer which has 2.4 GHz band.

Depending on the current interference and the distance between Sender and receiver 802.11 b System offer 11, 5.5, 2 or 1 Mbps.

*) Maximum user data rate is approximately 6Mpbs and the lower data rates 1 and 2 Mbps use the 11 chip Basker Sequence and new data rates 5.5 and 11 Mbps use of chip Complementary Code keying (CCK).

802.11 b packet format :-

There are two kinds of packet format which has supported by 802.11 b Such as

1. Long PLCP PPDU
2. Short PLCP PPDU

Explain in detail about IEEE 802.11 b S

1. Long PLCP PPDU :

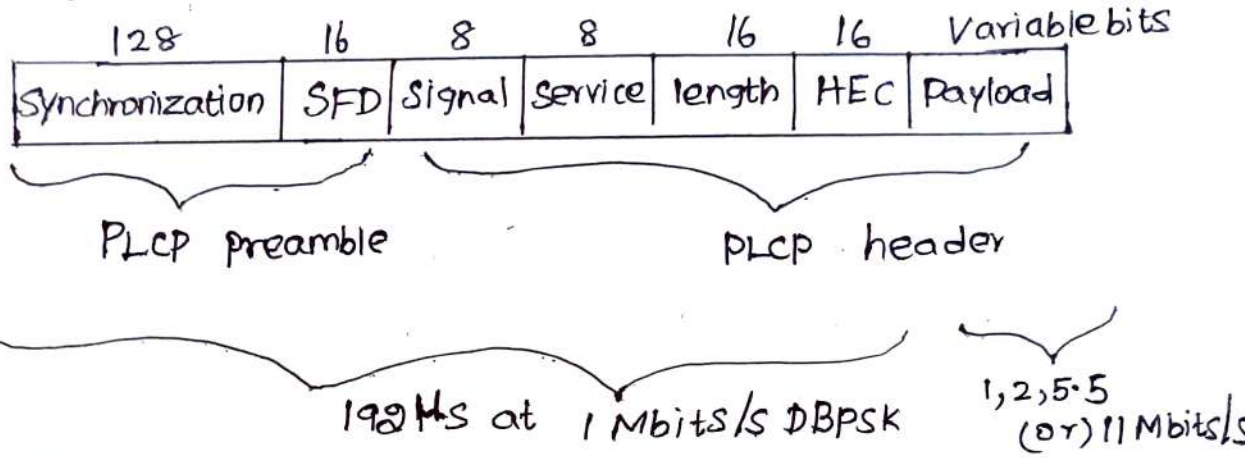


Fig: Long PLCP PPDU Frame format

PLCP Preample :-

→ Synchronization:

With Synchronization it also gain setting, energy detection and frequency offset compensation. This field only consists of Scrambled 1 bits.

→ Start frame Delimiter :

This 16 bit field is used for Synchronization at the begining of a frame and consists of the pattern 1111001110100000.

PLCP Header :-

→ Signals

There are 4 different values used to indicate the datarate of payload.

*) Value 0x0A represents 1 M bits/s
*) Value 0x14 is used for 2 M bit/s
*) Value 0x37 is used for 5.5 Mbit/s
*) Value 0x6E used for 11 M bit/s

Service :

This field is reserved for future use.

Length :

This 16-bit used for length indication of the Payload in microsecond.

Header Error Check (HEC) :

Signal, Service and length field are protected by this checksum using the ITU-T, CRC-16 standard polynomial.

2) Short PLCP PPDU :-

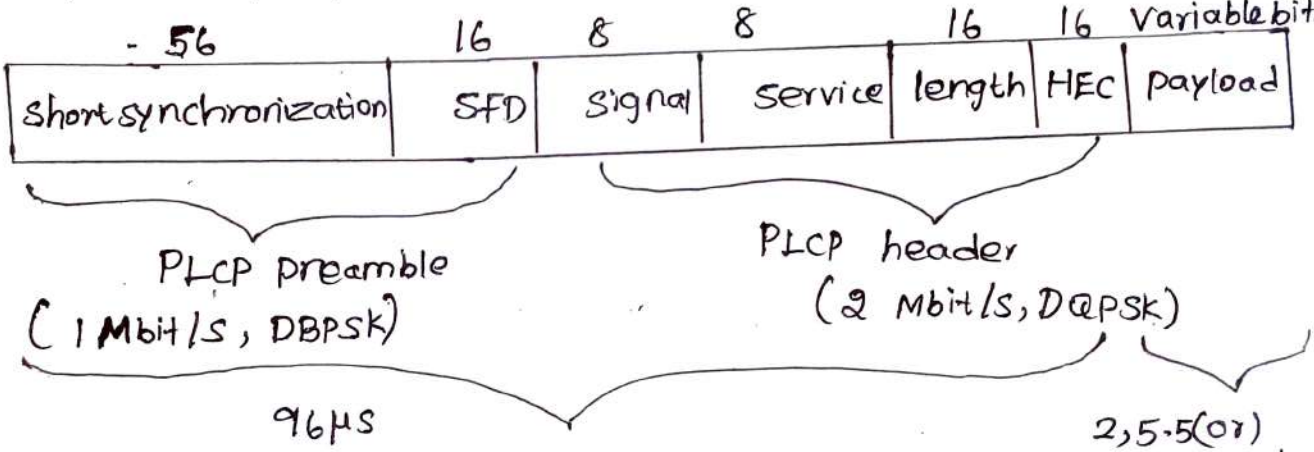
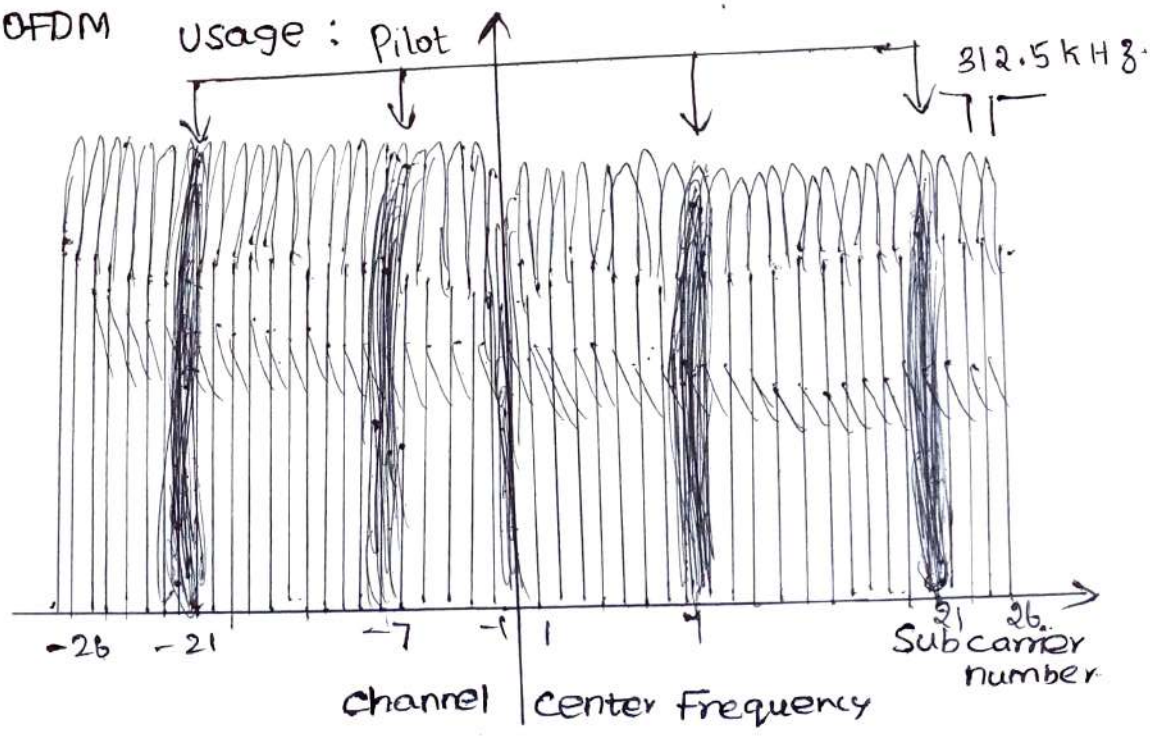


Fig: Short PLCP PPDU Frame format

OFDM usage : Pilot



OFDM is used for reduction of the Symbol rate, by distributing bits over numerous sub carriers.

⇒ In this figure, 52 Subcarriers are equally Spaced around a center frequency. The Spacing between the Subcarrier is 312.5 KHz.

⇒ In that 26 Sub carriers are left of the centre frequency and 26 are right of it Sub carriers with the numbers −21, −7, 7 and 21 are used for pilot Signals to make the Signal detection.

802.11a packet format:-

PLCP preamble:-

It Consists of 12 Symbols and is used for frequency acquisition, Channel estimation and Synchronization.

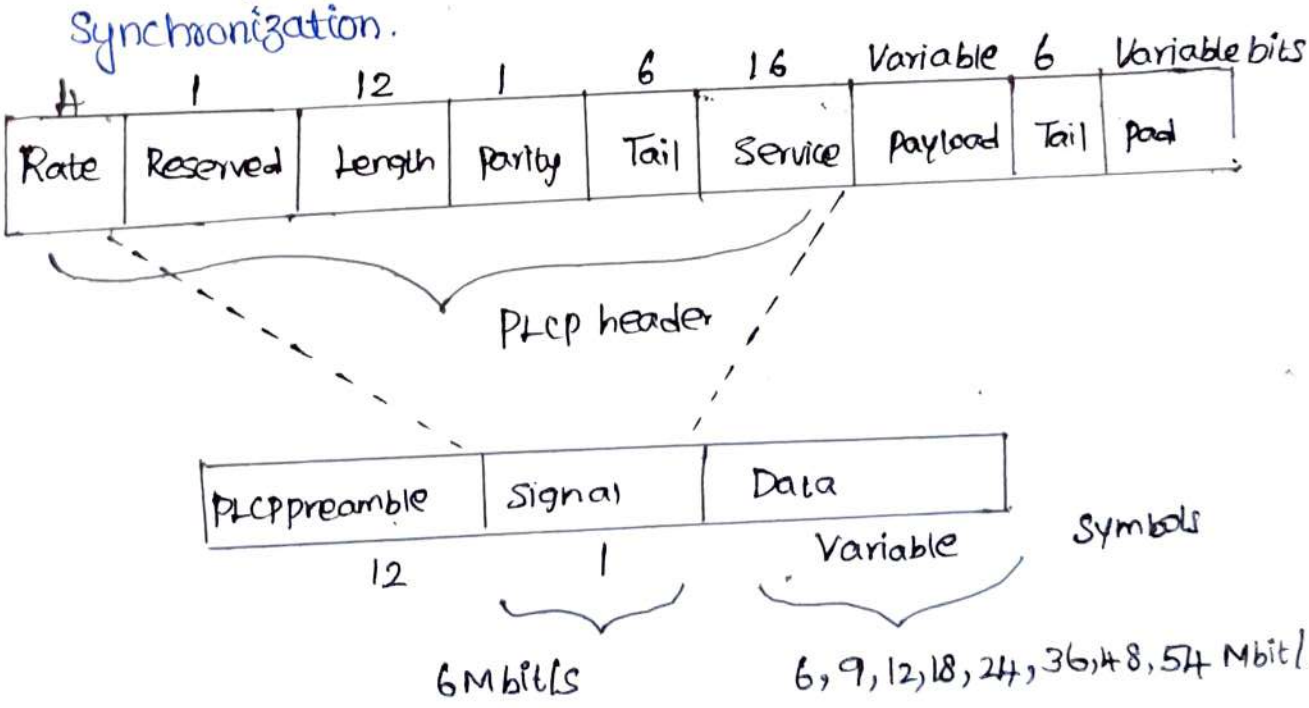


Fig: IEEE 802.11a physical layer PDU

PLCP preamble :-

→ Short Synchronization

The Short Synchronization field Consists of 56 Scrambled zeros instead of Scrambled ones Compared to long Synchronization field.

→ Start frame Delimiter :-

SFD Consist of a mirrored bit pattern Compared to the SFD of the long format such as

0000 0101 1100 1111 – for short PLCP PPDU

1111 0011 1010 0000 – for long PLCP PPDU.

PLCP Header :-

→ Signal

The encoding Signal rate 2, 5.5 or 11 Mbit/s

→ Service

This field reserved for future use

→ length

This 16-bit used for length indication of the payload in μs.

⇒ Header Error Check (HEC)

Signal, Service, length fields are Protected by this checksum using the ITU-T, CRC-16 Standard polynomial.

⇒ In Short PLCP, PPDU, the Pre-amble is transmitted at 1 Mbps and header is transmitted as 2 Mpbs.

⇒ In long PLCP PPDU both preample and header are transmitted at 1 Mbps.

IEEE 802.11 a :

Explain in detail about IEEE 802.11 a Standard ?

IEEE 802.11 a offer upto 54 Mbps using OFDM. IEEE 802.11 a uses many different technologies to offer data rates upto 54 Mbps.

⇒ It will use 52 sub carriers (48 data + 4 pilot) that are modulated using BPSK, QPSK, 16 QAM (or) 64 QAM.

*) Signal :-

It contains the following fields and is BPSK modulated.

→ Rate :

The 4 bit rate field determines the data rate and the modulation of the rest of the packet.

→ Length

The length field indicates the number of bytes in the payload field.

→ Parity :

The parity bit may be even parity for the first 16-bits of the Signal field (ie) rate length and reserved bit.

→ Tail

The six tail bits are set to zero

*) Data:

The data field is sent with the rate determined in the rate field.

→ Service

It is used to synchronize the descrambler of the receiver and which contains bits for future use

→ payload

The payload Contains the MAC PDU

→ Tail

The tail bits are used to reset the encoder

→ pad

The pad field ensures that the number of bits in the PDU maps to an integer number of OFDM symbols.

Sl. No	802.11 a	802.11 b
1.	operates in the 5.15 GHz to 5.35 GHz	Operates in the 2.4 GHz radio spectrum.
2.	Speed : Upto 54 Mbps	Speed : upto 11 Mbps
3.	Range : 50 feet	Range : 100 feet
4.	More expensive	Least expensive wireless LAN Specification.

HIPER LAN:

Evolution of HIPERLAN and other improvements - Explain in detail ?

Hiper Lan (High Performance Local Area network is a wireless LAN Standard.)

It is defined by the European Telecommunications Standard Institute.

In HiperLAN radio waves are used instead of a cable as a transmission medium to connect stations.

There are four kinds of family available for Hiper LAN.

1. Hiper LAN 1
2. Hiper LAN 2
3. Hiper LAN 3
4. Hiper LAN 4

Hiper LAN 1:

Explain the AccessSchemes of HIPER LAN 1 Protocol?

*) HIPER LAN 1 is a wireless LAN

⇒ It has Supporting priorities and packet life time for data transfer at 23.5 M bit/s.

⇒ It also has forwarding mechanisms, topology discovery, user data encryption, network identification and power Conservation mechanism.

⇒ Hiper LAN 1 Should operate at 5.1 - 5.3 GHz with a range of 50m in building at 1W transmit power.

phase :

Elimination - yield non-preemptive priority multiple access (EY-NPMA) is the heart of the Channel access providing priorities and different access Schemes.

EY-NPMA divides the medium access into three different phases.

*) Prioritization
*) Contention
*) Transmission

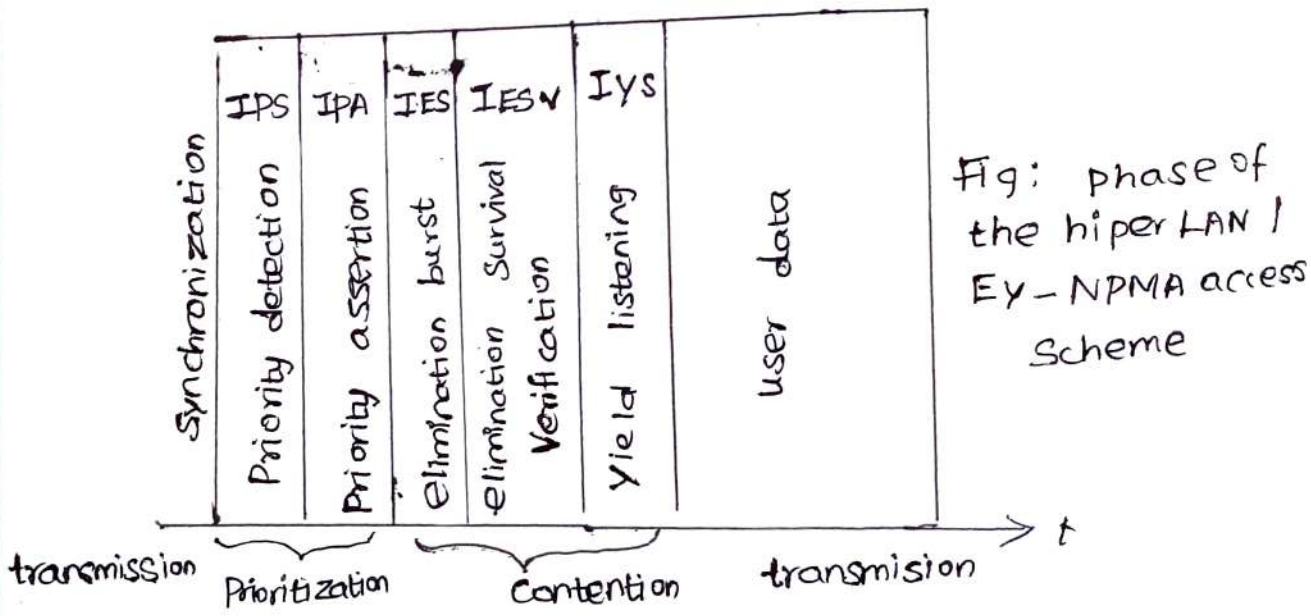


Fig: phase of the hiperLAN / EY-NPMA access Scheme

(i) Prioritization phase :-

⇒ It is used to determine the highest Priority of a data packet ready to be Sent by Competing nodes.

⇒ Hiper Lan 1 offers five different Priorities for data packets ready to be Sent.

*) Quality of Service is mapped on to a Priority level with the help of the packet lifetime (sent by an application)

*) The main objective of this phase is the to make sure that no needs with a lower priority gains access to the medium while packets with a higher priority are waiting at other nodes.

(ii) Contention phase :

The Contention phase is divided into an

a) Elimination phase

b) Yield phase

a) Elimination phase :

The purpose of the elimination phase is to eliminate as many Contending nodes as possible

The result of the elimination phase is a more or less Constant number of remaining nodes, almost independent of the initial number of Competing nodes.

b) Yield phase :

Yield phase Completes the work of the elimination phase with the goal of only one remaining node.

→ Elimination Burst

All remaining terminals Send a burst to eliminate Contenders

→ Elimination Survival Verification

Contenders now Sense the Channel, if the Channel is free they Can Continue otherwise They have been eleminated.

→ Yield listening :

Contenders again listen in slots with a non-zero probability, if the terminal senses its slot idle, it is free to transmit at the end of the contention phase.

(iii) Transmission phase :-

The winner of prioritization and contention phase can now send its data.

*) If the channel was idle for a longer time, then a bit terminal can send at once without using EY-NPMA.

Quality of Service Support :-

The quality of service offered by the MAC layer is based on three parameters.

1. Packet forwarding

→ It can be performed in two ways.

(i) Direct forwarding (point-to-point)

(ii) Broadcast forwarding (if no path information is available)

→ At the time of forwarding it has to support QoS.

2. Encryption / Decryption mechanism :

Hiper LAN 1, MAC offers user data encryption and decryption using a simple XOR-scheme together with random numbers.

⇒ The random sequence is XORed with the user data to generate the encrypted data.

⇒ Decryption of the encrypted user data works the same way and using the same random number sequence

3. power conservation mechanism :.

Power conservation is achieved by setting up certain recursing patterns when a node can receive data instead of constantly ready to receive.

⇒ All nodes participating in a multicast group must be ready to receive.

All nodes participating in a multicast group must be ready to receive at the same time when a sender transmit data.

WATM :-

Explain in detail about mobile ATM (or) WATM ?

Wireless ATM does not only describe a transmission technology but tries to specify a complete communication system.

⇒ It is also known as wireless mobile ATM, WMATM.

Motivation for WATM :-

1) The primary need for seamless integration of wireless terminals into a ATM network. An integrated services high performance network supporting different types of traffic streams.

2) ATM networks scale well from LANs to WANs and mobility is needed in local and wide area applications.

3) WATM could offer QoS for adequate support of multimedia data streams.

4) for telecommunication service providers it appears natural that merging of mobile wireless communication and ATM technology leads to wireless ATM.

5) for ATM to be successful it must offer a wireless extension otherwise it cannot participate in the rapidly growing field of mobile communications.

Wireless ATM working group :-

*) The ATM forum formed the wireless ATM working group in 1996.

⇒ These wireless networks should cover many different networking scenarios such as private and public, local and global, mobility and wireless.

⇒ The main goal of this working group involved ensuring the compability of all new proposals with existing ATM forum standard

⇒ It should be possible to easily upgrade existing ATM network with mobility functions and radio access.

There are two main sub groups of work items are

1. Mobile ATM Protocol Extensions.
2. Radio Access Layer (RAL) protocols

Mobile ATM:-

The following are the extensions to be Considered for a mobile ATM.

(i) Location management:

WATM networks must be able to locate a wireless terminal or a mobile user (ie) to find the current access point of the terminal to the network

(ii) Mobile Routing:-

Even if the location of a terminal is known to the System, it still has to route the traffic through the network to AP currently responsible for the wireless terminal.

Each time a user moves to a new access Point, the System must reroute traffic

(iii) Handover Signaling:

The network must Provide mechanism to Search a new access point and set up new Connections between intermediate Systems and Signal the actual change of the access point

(iv) QoS and traffic Control

WATM Should be able to offer many QoS parameter. To maintain these parameters all actions such as rerouting handovers etc.

(v) Network management :-

All extensions of protocols or other mechanism also require an extension of the management functions to control the network.

2) Radio Access Layer (RAL)

To ensure wireless access, the following working group must be considered for a radio Access Layer (RAC).

(i) Radio Resource Control :

As far any wireless networks, radio frequencies, modulation schemes, antennas, channel coding etc must be determined for WATM.

(ii) Wireless Media Access :-

different media access schemes are possible.

(iii) Wireless Data link Control :

The data link control layer must offer header Compression for an ATM cell and this layer can apply ARQ or FEC schemes to improve reliability.

(iv) Handover issues :-

During hand over, cell cannot be last, cells must be re-sequenced and lost cells must be retransmitted if required

*) WATM Services :-

WATM Systems to be designed for transferring voice, classical data, Video, multimedia data, Short messages etc

*) office Environment :

A broad range of Internet / Intranet access multimedia Conferencing, online multimedia data base access and telecommuting using WATM technology.

*) Universities, Schools, Training Centres :-

Distance learning, wireless and mobile access to data base internet access or teaching in the area of mobile multimedia Computing.

*) Industry :

WATM offer database Connection, information retreval, Surveillance and real time factory management.

*) Hospitals :

WATM for reliable, high bandwidth mobile and wireless networks transfer of medical images. Remote access to patients records, remote monitoring of patients.

*) Home :

Many electronic devices at home could be Connected using WATM technology (TV, CD, PC ....)

Networked Vehicles:-

Vehicles such as trucks, aircraft, buses or cars can communicate via GSM or UMTS.

Generic reference model:

With neat diagram explain WATM generic reference model?

A mobile ATM (MATM) terminal uses a WATM terminal adapter to gain wireless access to a WATM RAS (Radio) Access System).

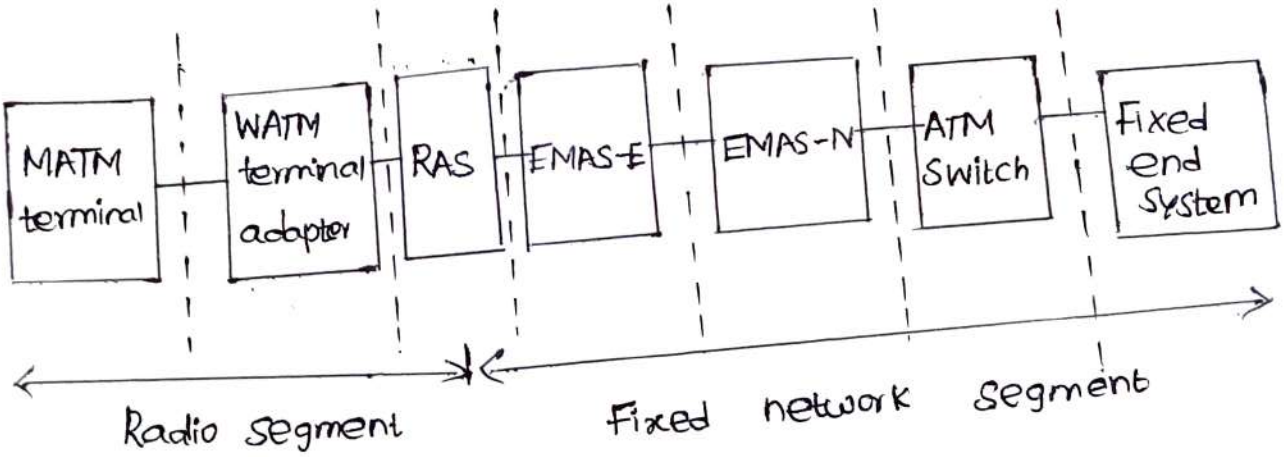


Fig: Generic WATM reference model.

⇒ MATM terminals could be represented by example, laptops using an ATM adaptor for wired access plus software for mobility

⇒ The WATM terminal adapter enables wireless access (ie) it includes the transceiver but it does not support mobility.

*) RAS with radio transceivers is connected to a mobility enhanced ATM Switch (EMAS-E) which in turn connects with ATM network with mobility aware Switches (EMAS-N) and other Standard ATM Switches.

⇒ finally, a wired, non-mobility aware ATM end System is connected.

HANDOVER :-

The main Problem for WATM during the handover is rerouting all connections and maintaining Connection quality.

Requirements of Handover :-

(i) Handover of multiple Connections :-

WATM must Support more than one Connection. This results in the rerouting of every Connection after handover.

(ii) Handover of Point-to-multipoint Connections :-

WATM handover must Support point-to-multipoint Connections.

(iii) QoS Support :-

⇒ WATM handover should aim to Preserve the QoS for all Connections during handover

*) However, due to limited resources this is not always possible

(iv) Data integrity and Security :-

WATM handover should minimize cell loss and avoid all cell duplication or re-ordering

Location Management :-

Location management is used for looking up the current position of a mobile terminal, for Providing the moving terminal with a permanent address and for ensuring Security features.

Requirements for location management :

(i) Transparency of mobility :-

*) A user should not notice the location management function under normal operation. Any change of location should be performed without user activity.

(ii) Security :

Essential Security features include authentication of users and terminals, but also of access points.

(iii) Identification :

Location management must Provide the means to identify all entities of the network.

(iv) Internetworking and Standards :-

⇒ All location management functions

must Co-operate with existing ATM functions from the fixed network, especially routing.

Mobile Quality of Service :-

⇒ It is composed of three different parts.

(i) Wired-QoS :

The infrastructure network needed for WATM has the same QoS properties as any wired ATM network.

(ii) Wireless QoS :

The QoS Properties of the wireless part of a WATM network differ from those of the wired part.

(iii) Handover QoS :-

Two types of QoS during handover.

→ Hard handover QoS

→ Soft handover QoS.

Access Scenarios :-

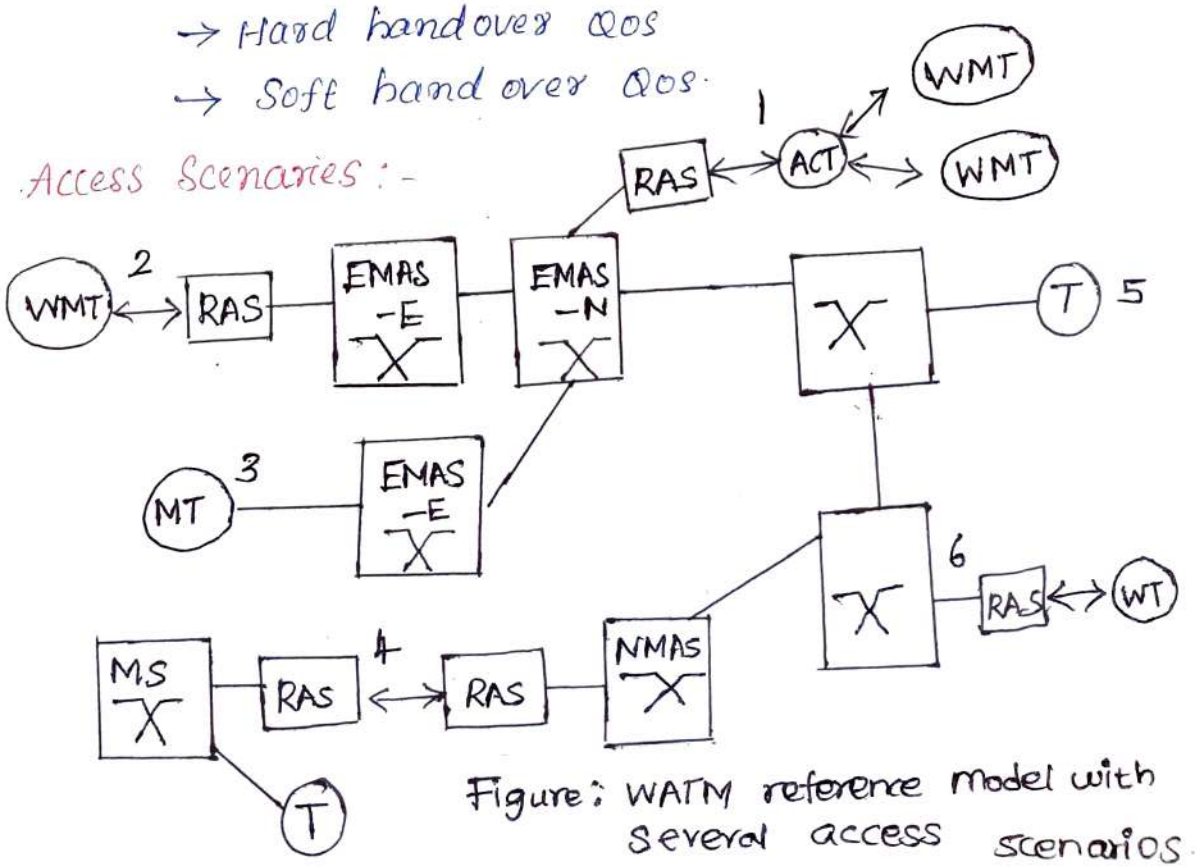


Figure: WATM reference model with several access scenarios.

The above figure shows possible access scenarios for WATM and illustrates what was planned during the specification of WATM.

T (terminal) :- A standard ATM terminal offering ATM services defined for fixed ATM networks.

MT (Mobile Terminal)

⇒ It is a standard ATM terminal with the additional capability of reconnecting after access point change.

WT (wireless Terminal) :

⇒ This terminal is accessed via a wireless link.

WMT (Wireless Mobile Terminal) :

⇒ Combination of wireless and a mobile terminal is known as WMT.

RAS (Radio Access System) :

Point of access to a network through a radio link.

EMAS (End user mobility supporting ATM Switch) :

⇒ Switches with the support of end-user mobility.

NMAS (Network Mobility supporting ATM Switch) :

⇒ A whole network can be mobile not just terminals. Certain additional functions are needed to support this mobility from the fixed network.

MS (Mobile ATM Switch):-

→ ATM Switches can also be mobile and can use wireless access to another part of ATM network

ACT (Ad hoc Controller Terminal):

→ Special terminal types must be required with in the wireless network These terminals control wireless access without an RAS.

Based on these entities the following Scenario which is supported by WATM.

→ Wireless Ad hoc ATM network (Scenario 1)

*) WATM can communicate with each other without a fixed network.

⇒ Access Control can be accomplished via the ACT

*) If ad-hoc network needs a connection to a fixed network means it can be provided by means of an RAS.

→ Wireless Mobile ATM terminals (Scenario 2)

A WMT Cannot Communicate without the Support Provided by entities within the fixed network Such as EMAS-E

→ Mobile ATM Terminals (Scenario 3)

This Configuration Supports device Portability

and allows for simple network reconfiguration.

With the help of EMAS-E, the users can change the access points of their ATM equipment overtime without the need for reconfiguration by hand.

→ Mobile ATM Switches (Scenario 4)

Entities supporting switch mobility are needed with in the fixed network. This Scenario can be used in aircraft, trains or ships.

Fixed ATM Terminals (Scenario 5)

Terminals and switches do not include capabilities for mobility or wireless access.

Fixed wireless ATM terminals (scenario 6)

To provide simple access to ATM networks without wiring a fixed wireless link is the ideal solution. This Scenario does not require any change or enhancements in the fixed network.

Advantages:-

WATM Specifies radio access, mobility management, handover schemes, mobile QoS, security etc

Disadvantages:-

* A resource reservation is needed for checking available resources.

⇒ It is difficult to maintain QoS parameters for connections during handover.

BRAN (Broad band Radio Access Network)

Explain in detail about BRAN network?

The Broad band Radio Access Network is standardized by the European Tele Communications Standards Institute (ETSI)

⇒ Radio is used to provide network access for Customers. The main advantages of Radio access are high flexibility and quick installation.

⇒ Transfer rates of 25-155 Mbps and a transmission range 50m - 5km.

Types :-

BRAN has specified four different network types.

1. Hiper LAN 1:

This high speed WLAN supports mobility of data rates above 20 Mbps. Range is 50m, connections are multipoint - to - multipoint using adhoc or infrastructure networks.

2. Hiper LAN 2

It can be used for wireless access to ATM or IP networks and supports up to 25 Mpbs user data rate in a point - to - multipoint configuration.

3 Hiper Access:

Transmission range is upto 5 km and data rate of upto 25 Mpbs are supported.

4. Hiper link:

It provides a point-to-point connection with upto 155 Mbps. It can be used to connect different Hiper LAN access points.

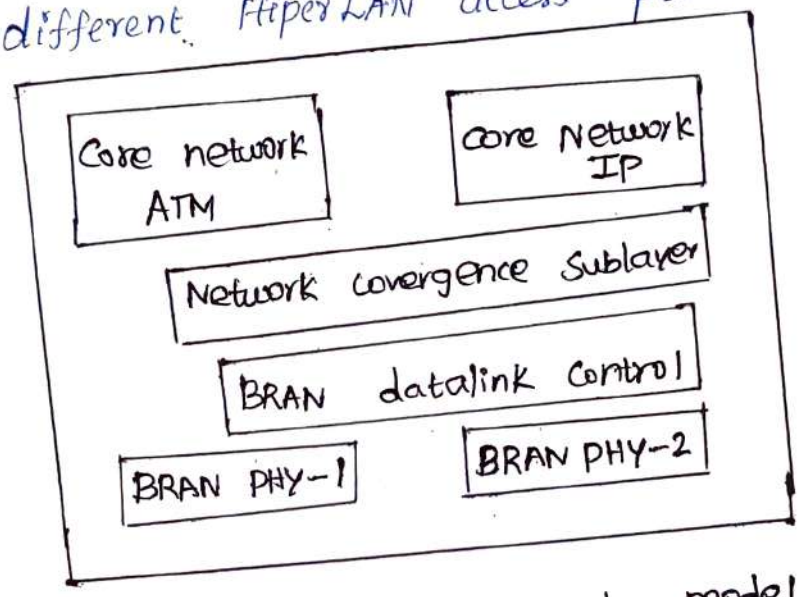


Fig: BRAN Layered model

BRAN technology is independent from the protocols of the fixed network. It can be used for ATM and TCP/IP networks. which is shown in the above figure.

⇒ BRAN physical layer, DLC layer provide common interface to the higher layers.

⇒ Network Convergence Sublayer is used to cover special characteristics of wireless links and to adapt directly to different higher layer network technologies.

HIPER LAN 2:

Define hiper LAN 2. Discuss about various operation modes & Protocol Stack in Hiper LAN 2.

It provides more benefits compared to Hiper LAN 1. It can work at 5 GHz and offers data rates of upto 54 Mbps including Qos support and enhanced Security features.

(i) features:

*) High - throughput transmission

Using OFDM in the physical layer and a dynamic TDMA / TDD based MAC Protocol, Hiper LAN 2 offers upto 34 Mbps at the physical layer and 25 Mbps at the network Layer.

*) Connection - oriented:-

Hiper LAN 2 networks establish logical Connections between a Sender and a receiver.

*) Quality of Service Support:-

With the help of Connections. Support of Qos is much simple. and each connection has its own set of Qos parameter.

*) Dynamic frequency Selection:-

Hiper LAN 2 automatically selects an appropriate frequency with in their coverage area.

Security Support:

Authentication as well as encryptions are supported by Hiper LAN 2. Both mobile terminal and AP can authenticate each other.

*) power Save:

Mobile terminals can negotiate certain wake up patterns to save power.

(ii) Architecture:

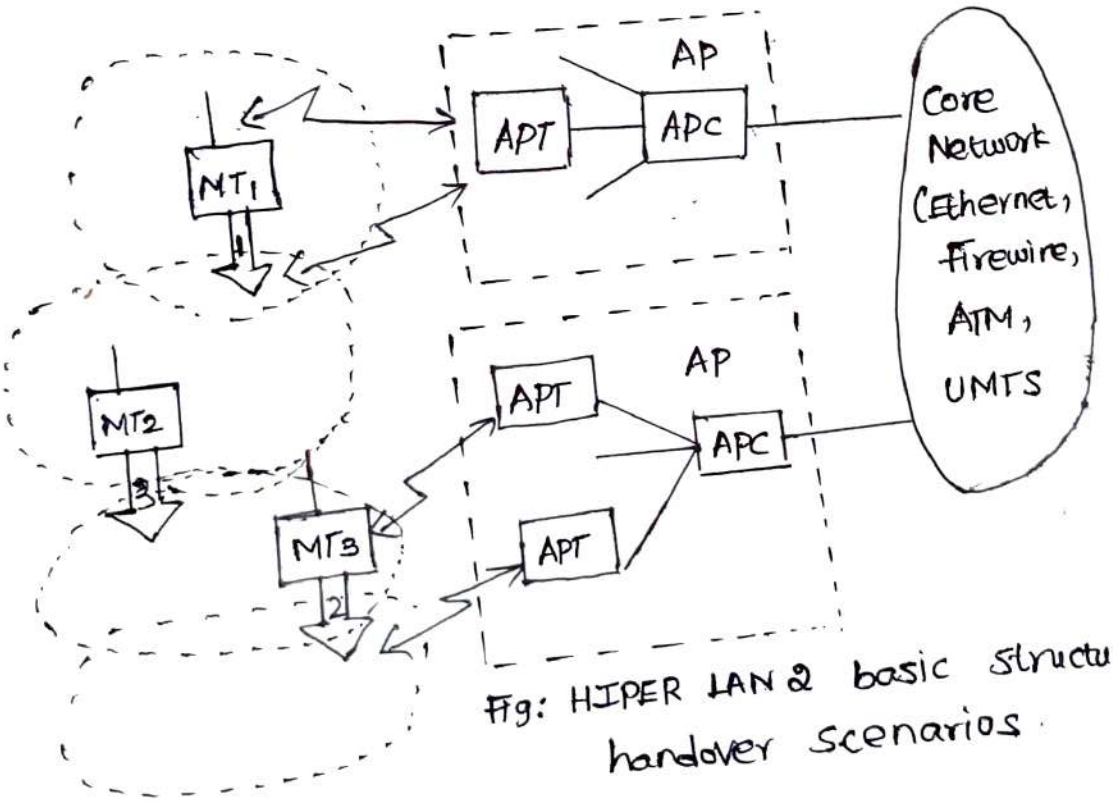


Fig: HIPER LAN 2 basic structure and handover scenarios.

Above figure shows the standard architecture of an infrastructure based Hiper LAN 2 network

*) Two Access points are attached to a core network.

*) The core network may be Ethernet LANS, ATM networks, firewire connection between audio and video equipment etc.

*) Each AP consists of an Access point controller and one or more access point transceivers (APT)

*) An APT can comprise one or more Sectors.

Four mobile terminals (MT) are move around in the cell area.

*) The System automatically assign the APT/AP with the best transmission quality. No frequency planning is necessary, the APs automatically Select the appropriate frequency via dynamic frequency Selection (DFS).

iii) Handover:

In HIPER LAN 2, three handover Situation may occur.

(i) Sector Handover (Inter Section)

When Sector antennas are used for an AP, then the AP may Support Sector handover. This type of handover is handled insider the DLC layer, So it is not visible outside the AP.

(ii) Radio Handover (Inter-APT/Intra-AP):

This handover is handled with in the AP and no external interaction is needed.

It can Support encryption keys, authentication and Connection parameter.

(iii) Network Handover (Inter-AP / Intra-Network)

In this handover the core network and higher layers are also involved. This handover might be supported by the core network.

iv) Operation modes :-

HIPER LAN 2 networks can operate in two different modes.

(i) Centralized mode :

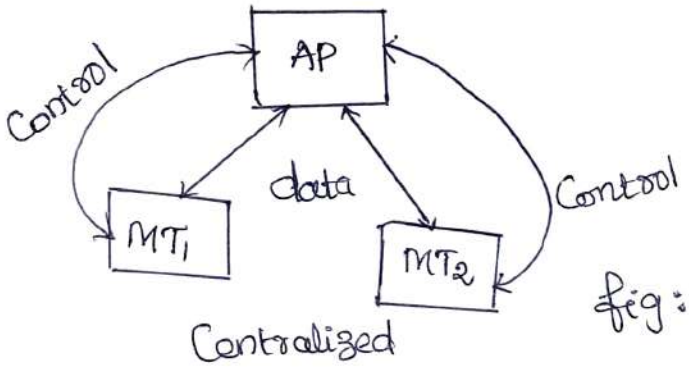


fig: centralized mode.

All Ap's are connected to a core network and MTs are associated with APs. Even if two MTs share the same cell, all data is transferred via the AP. In this mode, the Ap takes complete control of everything.

(ii) Direct Mode :

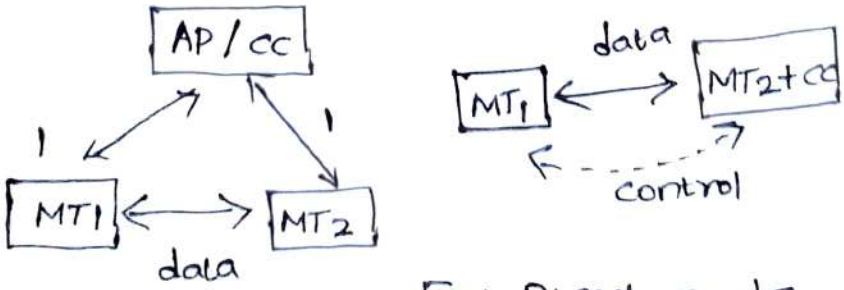


Fig: Direct mode

Data is directly exchanged between MTs if they can received each other, but the network still has to Controlled. This can be done via on AP that Contains a central Controller (CC).

(v) Protocol Stack :

This Standard Covers the following layers.

(i) physical layer
(ii) Data link Control (DLC) Layer
(iii) Convergence layer.

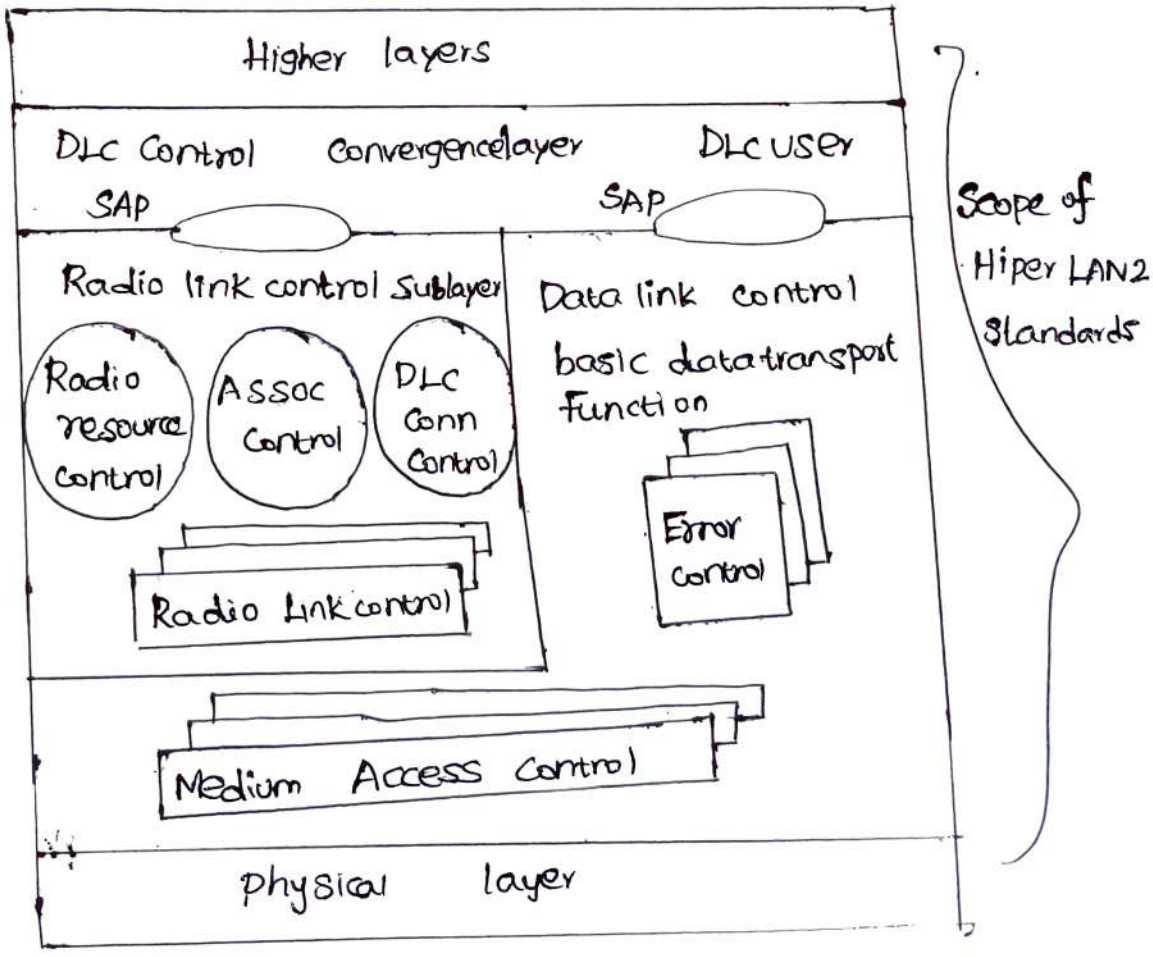


Fig: HIPERLAN 2 protocol stack.

(1) Physical layer:-

Physical layer handles all functions related to modulation forward error correction, signal detection etc.

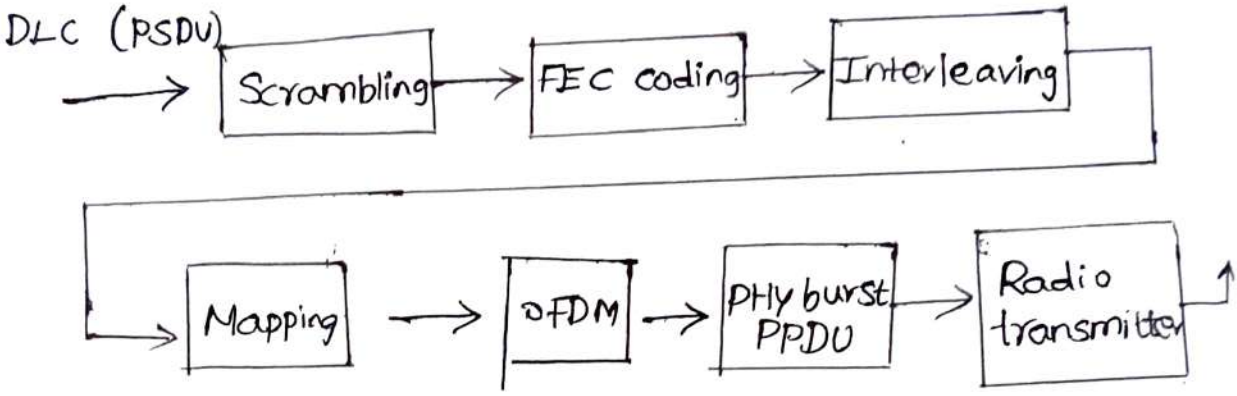


Fig: Hiper LAN 2 physical layer reference configuration.

→ After selecting any one of transmission modes, the DLC layer passes a PSDU to the physical layer.

→ Scrambling of all data bits with the generator polynomials $x^7 + x^4 + 1$ for DC blocking and whitening of the spectrum.

→ FEC coding performs the error protection coding depends on the type of data and usage of sector.

→ Interleaving ensures that adjacent encoded bits are mapped on to non-adjacent sub carriers

→ Mapping divides the bit sequence in group of 1, 2, 4 or 6 bits depending on the modulation schemes.

→ The OFDM modulation converts these symbols into a baseband signal with the help of the inverse FFT.

→ PHY burst Consists of a preamble and a payload.

→ Radio transmission shifts the baseband signal to a carrier frequency depending on the channel number.

(ii) Data link Control layer:

It Contains the MAC functions, the RLC Sub layer and error Control functions. DLC layer is Sub-divided into three layers.

1. Medium Access Control (MAC) layer
2. Logical link Control (LLC) layer.
3. Radio link Control (RLC) layer.

1. MAC layer:

The medium access Control Creates frames of 2ms duration which is Shown in below fig. Each MAC frame is further divided into four phases with variable boundaries.

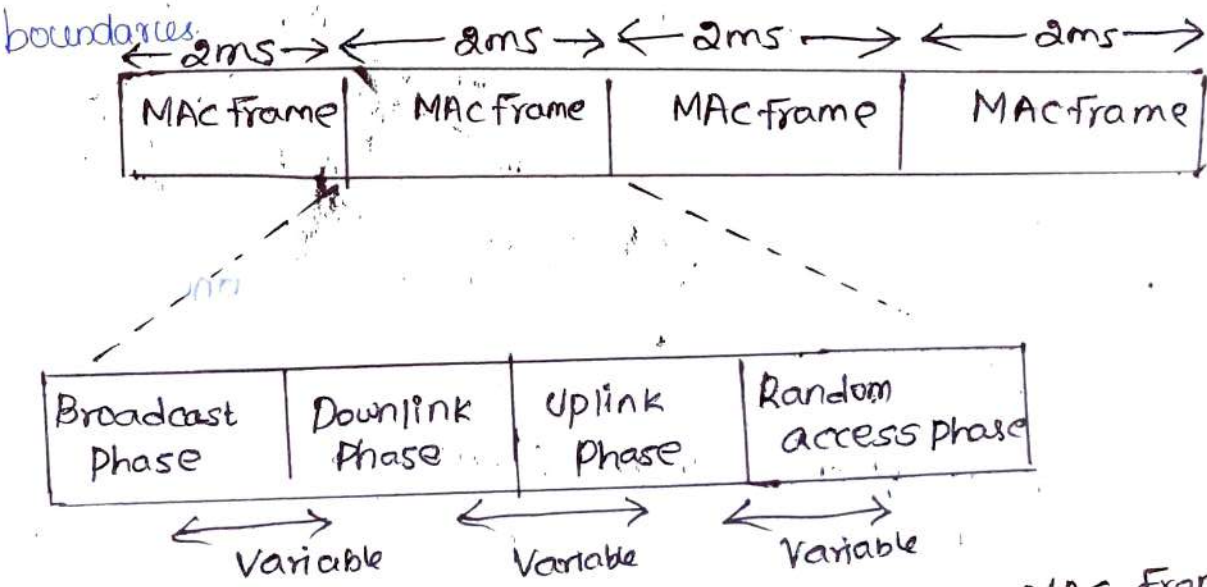


Fig: Basic Structure of Hiper LAN & MAC Frame

Broadcast phase :-

The Ap of a cell broadcasts the Content of the current frame plus information about the cell.

Downlink phase :-

Transmission of user data from an Ap to the MTs.

Uplink phase : Transmission of user data from MTs to an Ap.

Random Access phase :

Capacity requests from already registered MTs and access request from non-registered MTs.

Transport channels :-

Hiper LAN 2 defines Six different transport channels for data transfer in the above listed phases.

These transport channels describe the basic message format with in a MAC frame.

* (1) Broadcast channel :- (BCH)

→ It is a 15 byte channel used to convey basic information for the radio cell to all MTs.

(2) Frame channel (FCH):

→ It is a 27 bytes channel Contains a directory of the downlink and uplink phases.

(3) Access feedback channel (ACH):

→ It is a 9 bytes channel gives feedback to MTs regarding the Random Access during

the RCH of the Previous frame.

4) Long Transport Channel (LCH):

→ It is a 54 bytes Channel used to transport user and Control data for downlinks and uplinks.

5) Short Transport Channel (SCH):

→ It is a 9 bytes Channel Controls for data for downlinks and uplinks.

6) Random Channel (RCH):

→ It is a 9 byte Channel, to Send information to the AP/CC even without a granted SCH.

② Logical Channels in LLC layer:

Data between entities of the RLC layer are transferred via logical channels. The type of a logical channel is defined by the type of information it carries and the interpretation of the values in the corresponding message.

Hiper LAN 2 uses the following logical channels.

① Broadcast Control channel :- (BCCH)

This channel on the down link conveys a Constant amount of broadcast information Concerning the whole radio cell.

2) Frame Control Channel (FCCH)

It describes the structure of the remaining parts of the MAC frame This Comprises resource grants for SCH and LCHs belonging to Certain MTs

3) Random Access feedback channel (RFCH):

→ This Channel informs MTs that have used an RCH in the Previous frame about the Success of their access attempt.

4) RLCH Broadcast Channel:- (RBCH)

→ This channel transfer information regarding RLC control information

5) User broadcast Channel (UBCH):

→ It transfer broadcast messages from the Convergence layer transmission is performed in the un acknowledged or repetition mode.

6) User Data Channel (UDCH):

This Channel can be used for point to-point data between an AP and an MT or between two MTs

Radio Link Control Layer:

The radio link Control (RLC) Sublayer Composes most Control functions in the DLL layer ETSI defined three main Services for the RLC sub layer

1. Association Control function (ACF)

ACF contains all procedures for association, authentication and encryption.

2. Radio Resource Control (RRC):

An important function of the RRC is handover support.

3. DLC user Connection Control (DCC or DUCC)

This service is used for setting up, releasing or modifying unicast connections.

(iii) Convergence Layer:-

This higher layer of HIPER LAN 2 Standardization may comprise segmentation and reassembly functions and adaptations to fixed LANs, 3G Networks etc.

→ cell based CL: expects data packets of fixed size or ATM cells.

→ packet based CL: handles packets that are variable in size (eg) ATM cells.

BLUETOOTH (IEEE 802.15.1):

Describe the user scenario architecture and protocol stack of Bluetooth technology.

Bluetooth wireless technology is a short range radio technology which is developed for personal

area network. Bluetooth is an ad-hoc type network operable over a small area such as room.

It is a global standard that,

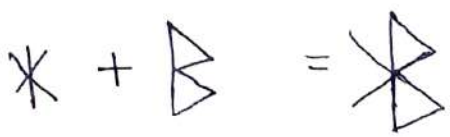
→ Eliminates wires and cables between both stationary and mobile devices.

→ offers the possibility of ad-hoc network and delivery the ultimate synchronicity between all our personal devices.

→ Bluetooth is a dynamic standard where devices can automatically can find each other, establish connections and discover what they can do for each other on an adhoc basics.

Symbol of bluetooth:

Bluetooth's logo combines the representation of the Nordic Runes Hagalaz and Berkana is the same symbol. This is HB like Herald Blat and King.



Architecture:

→ Bluetooth operates in the 2.4 GHz ISM band and operates on 79 RF channels with 1MHz carrier spacing.

→ Piconet is a Collection of devices Connected in an ad-hoc fashion.

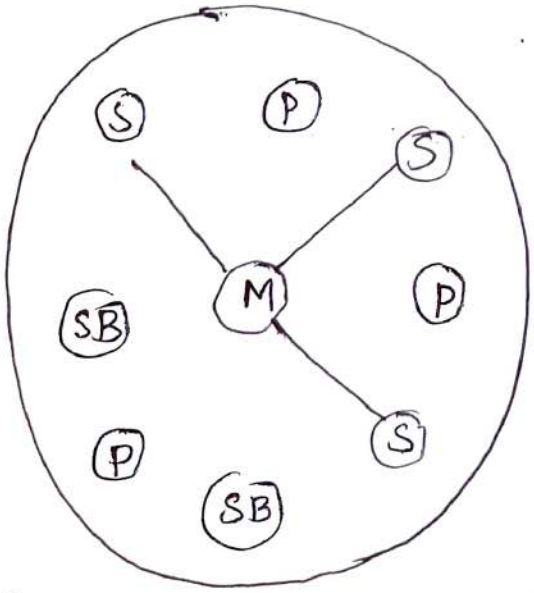
→ One unit act as master and the other as Slaves for the lifetime of the piconet.

→ Master determines hopping pattern in the piconet and the Slaves have to Synchronize to this pattern.

→ Each piconet has a unique hopping pattern. If a device wants to participate it has Synchronize to this pattern.

→ Each piconet has one master and upto 7 Simultaneous Slaves.

→ Parked devices and devices in Stand by do not participated in the piconet. More that 200 devices Can be parked.



M – Master
S – Slave
P – Parked
SB – Stand by

Fig: Piconet structure of Bluetooth

→ All devices is a piconet use the Same hopping Sequence master Sending its Clock and device ID.

→ The hopping pattern is determined by device ID, it is a 48 bit unique identifier.

→ All active devices are assigned a 3 bit active member address. All parked devices use an 8 bit parked member address. Devices in stand-by do not need an address.

Scatternet :-

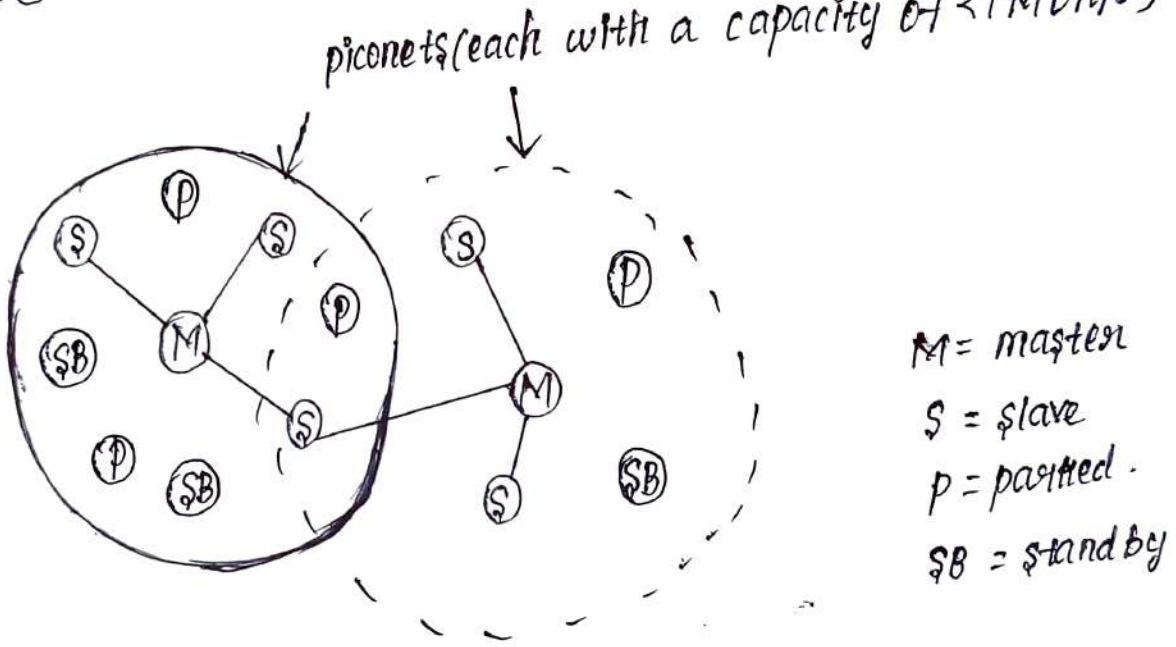


Fig: Bluetooth scatternet

Scatternet is the process of linking of multiple co-located piconets through the sharing of common master or slave devices.

→ Device can act as slave in one piconet and master of another piconet.

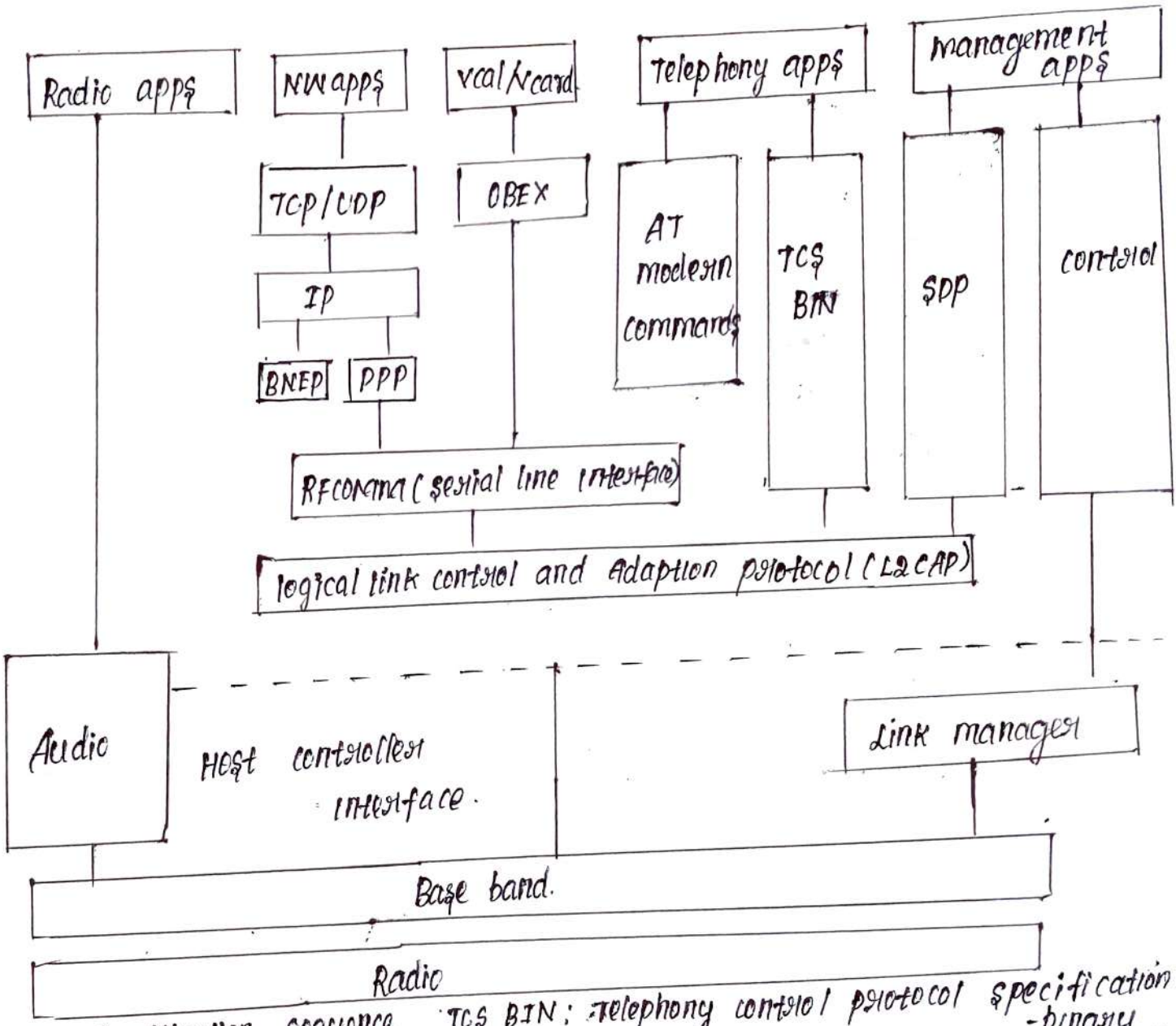
Protocol Stack :-

The bluetooth protocol stack can be divided into

1. Core Specification
2. Profile Specification

⇒ The Core Specification describes the protocols from physical layer to the data link Control together with management functions.

⇒ The Core protocols of Bluetooth Comprise the following elements.



AT: Attention sequence TCS BIN: Telephony control protocol specification - binary
OBEX: object exchange BNEP: Bluetooth network encapsulation protocol
Radio: RF COMM: Radio frequency comm SDP: service discovery protocol.

It specifies details of the air interface, including frequency, frequency hopping, modulation scheme and transmission power.

Baseband :

It concerned with connection establishment with a piconet addressing, packet format, timing and power control.

Link manager protocol : (LMP) :

⇒ It establishes the link set up between Bluetooth devices and manages ongoing links, including security aspects (eg. authentication and encryption), and control negotiation of baseband packet size.

Logical link Control and Adaption Protocol (L2CAP)

⇒ It adapts upper layer protocols to the baseband layer. It provides both connectionless and connection oriented services.

Service discovery Protocol (SDP) :

It handles device information, service and queries for service characteristics between two or more bluetooth devices.

Host Controllel Interfaces :

It provides an interface method for accessing the bluetooth hardware capabilities. It contains a command interface, which acts between the baseband controller and link manager.

TCS BIN (Telephony Control Protocol Specification - Binary)

It is a bit oriented protocol that defines the Call Control signaling for the establishment of voice and data calls between bluetooth devices.

OBEX (Object Exchange)

It is a Session layer protocol for the exchange of objects, Providing a model for objects and operation representation.

RFComm :-

It is a reliable transport protocol, which provides emulation of RS 232 Serial ports over the L2CAP protocol.

WAE/WAP :-

Bluetooth incorporates the wireless application Environment (WAE) and the wireless Application protocol (WAP) into its architecture.

Wireless personal Area network (WPAN):

Discuss about wireless personal area network ?

⇒ A personal area network (PAN) is an interconnection of devices for personal use with in the operating space of an individual usually in the range of 1-10 meters (short range).

⇒ It's main aim to achieve this interconnectivity.

and give greater flexibility, mobility and freedom from the hassle of finding the right cable.

WPAN differ from WLAN is that they are not intended to replace Ethernet type local network, giving neither the range nor, at least at present, the data capacity or variety of WLAN services.

* Common goals:
  - → getting rid of cable connections
  - → little or no infrastructure.

Applications

→ Short range (<10m) connectivity for multimedia applications

*) PDAs, Cameras, Voice (hands free devices)

*) High QoS, high data rate (IEEE 802.15.3)

→ Industrial Sensor Applications

*) Low speed, Low battery, low cost Sensor networks (IEEE 802.15.4)

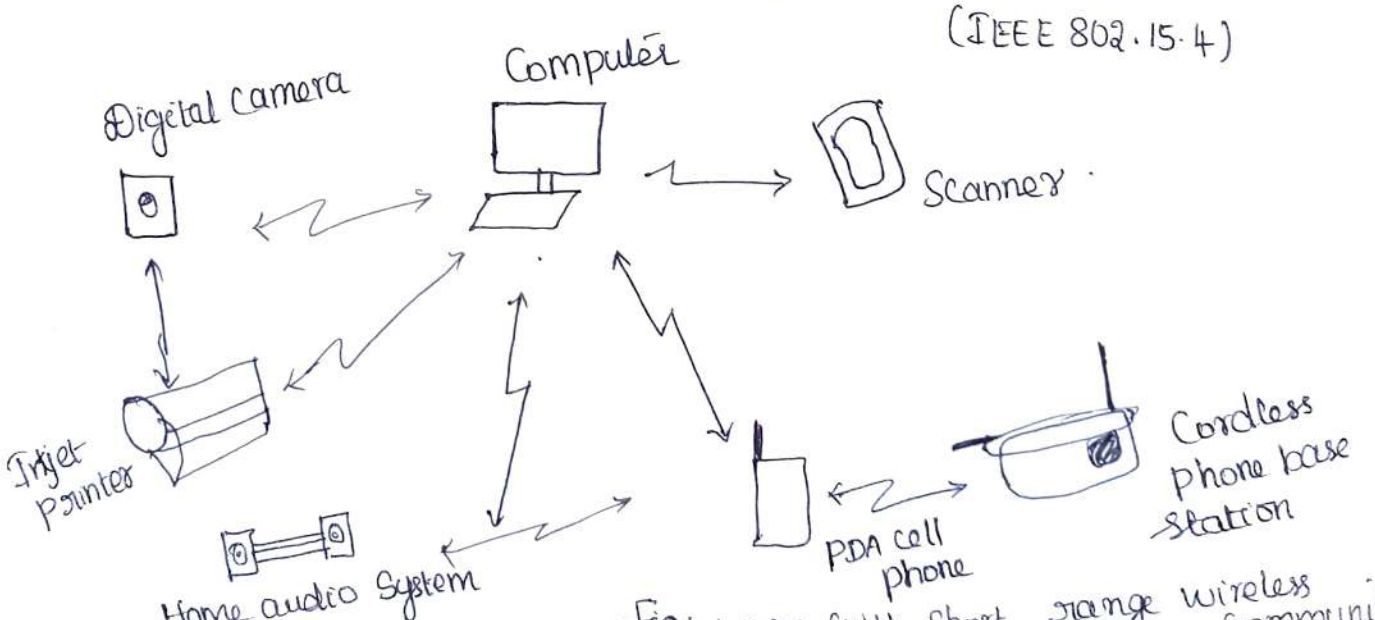


Fig: WPAN with short range wireless community

WPAN Standards (IEEE 802.15)

IEEE Standard	Topic	Data throughput	Suitable Applications	Qos needs
802.15.1	Bluetooth	1Mbps	Cell phones, Computers, PDAs, printers, micro phones, speaker, pcs	Qos suitable for voice applications
802.15.2	Co-existance of Bluetooth and 802.11b	N/A	N/A	N/A
802.15.3	High rate WPAN	>20Mbps	Low power, Low cost, Solution for portable Consumer of digital imaging and multi-media applications	Very high Qos
802.15.4	Low-rate WPAN (Zig-bee)	<0.25 Mbps	Industrial, agricultural, residential & medical application	Relaxed need for data rate & Qos.

IEEE 802.15.14 :

Explain in detail architecture of IEEE 802.15.4 Standard ?

→ It is a technical standard which defines the operation of low-rate wireless personal area Networks (LR-WPAN)

⇒ It is the basic for the zigbee, wireless HART, & 6LoWPAN each of which further extends the standard by developing the upper layers which are not defined in IEEE 802.15.14

Features:

→ Real time Suitability by reservation Guaranteed Time slots (GTS)

→ Collision avoidance through CSMA/CA and integrated support for Secure Communications

→ Devices include power management functions such as link quality and energy detection

→ It uses three possible frequency bands such as 868, 915, 2450 MHz

Protocol Architecture:

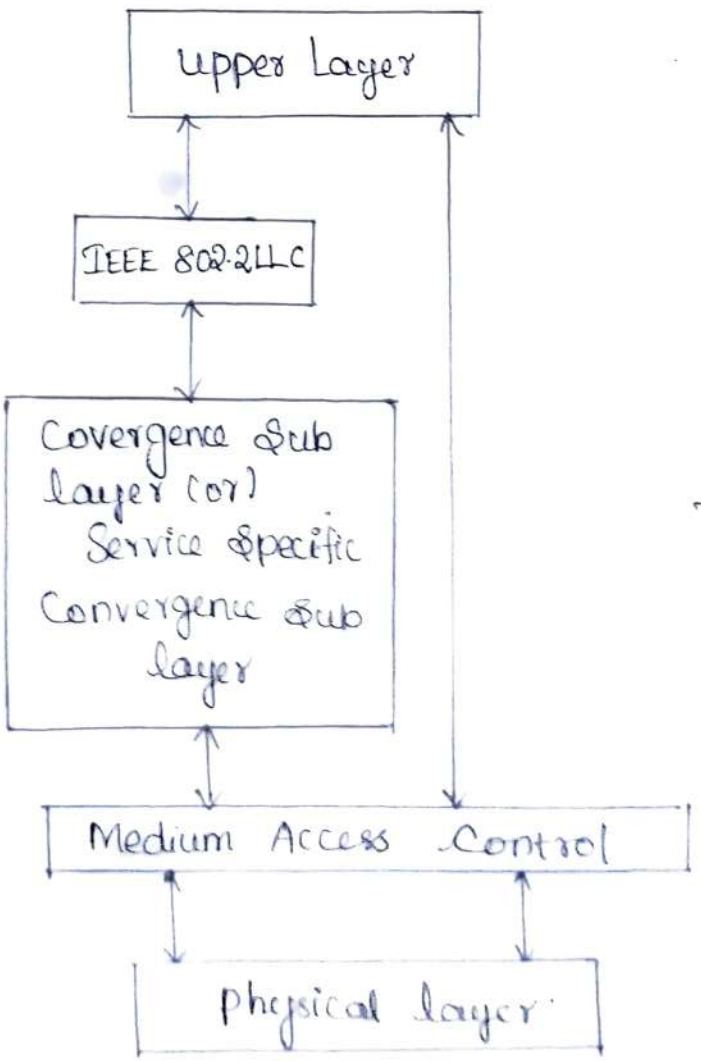


fig: IEEE 802.15.4 protocol stack.

(i) Physical layer:

The physical layer provides the two types of services.

(i) physical data services.

(ii) physical management services.

① Physical data services:-

It enables the transmission and reception of physical protocol data units (PPDUs) across the physical radio channel.

② physical management service:

It is used to interfacing the physical management entity (PLME)

*) The standard provides two options based on the frequency band.

*) Both are based on the direct sequence spread spectrum (DSSS).

→ Data rate is 250 Kbps at 2.4 GHz.

→ Data rate is 20 Kbps at 868 MHz.

→ Data rate is 40 Kbps. at 915 MHz.

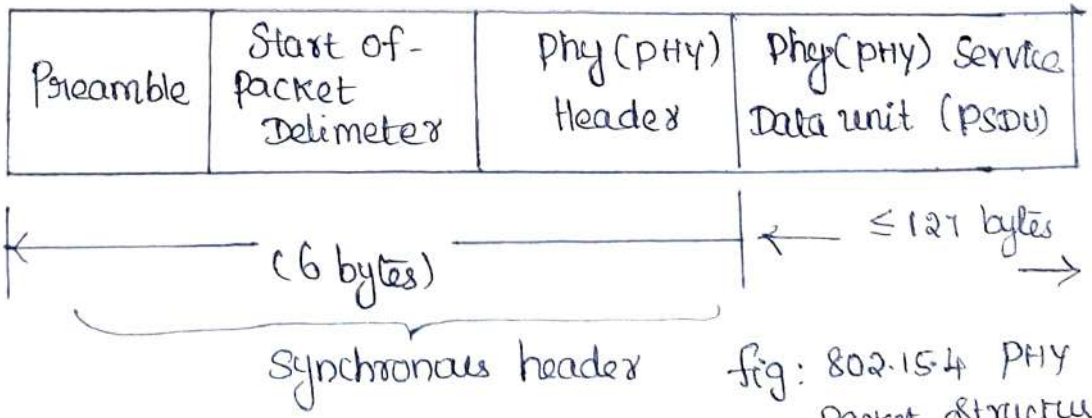


fig: 802.15.4 PHY Packet Structure

*) Preamble (32-bit)

It is designed for the acquisition of Symbol and Chip timing and frequency adjustment.

*) Start-of-packet Delimeter (8 bits)

→ It's signify end of preamble.

PHY header (8-bits):

→ It's is used specify the length of the pay load.

PSDU (127 bytes)

It support the packets of length 0-127 bytes

(ii) Data link layer:

*) The data link layer of IEEE 802.15.4 is divided into two sub layers, MAC & LLC sub layer.

*) The logical link control is standardized in IEEE 802.2 type LLC three the service specific Convergence sub layer.

IEEE 802.15.14 features:

* Association, disassociation, acknowledged frame delivery, Channel access mechanism, frame Validation guaranteed time slot management.

MAC Services

Two types of services to higher layer that can be accessed through two service access points (SAP).

① MAC data service → It is accessed through the MAC Common part sublayer (MCPS-SAP)

② MAC management service → It is accessed through the MAC layer management entity (MLME-SAP)

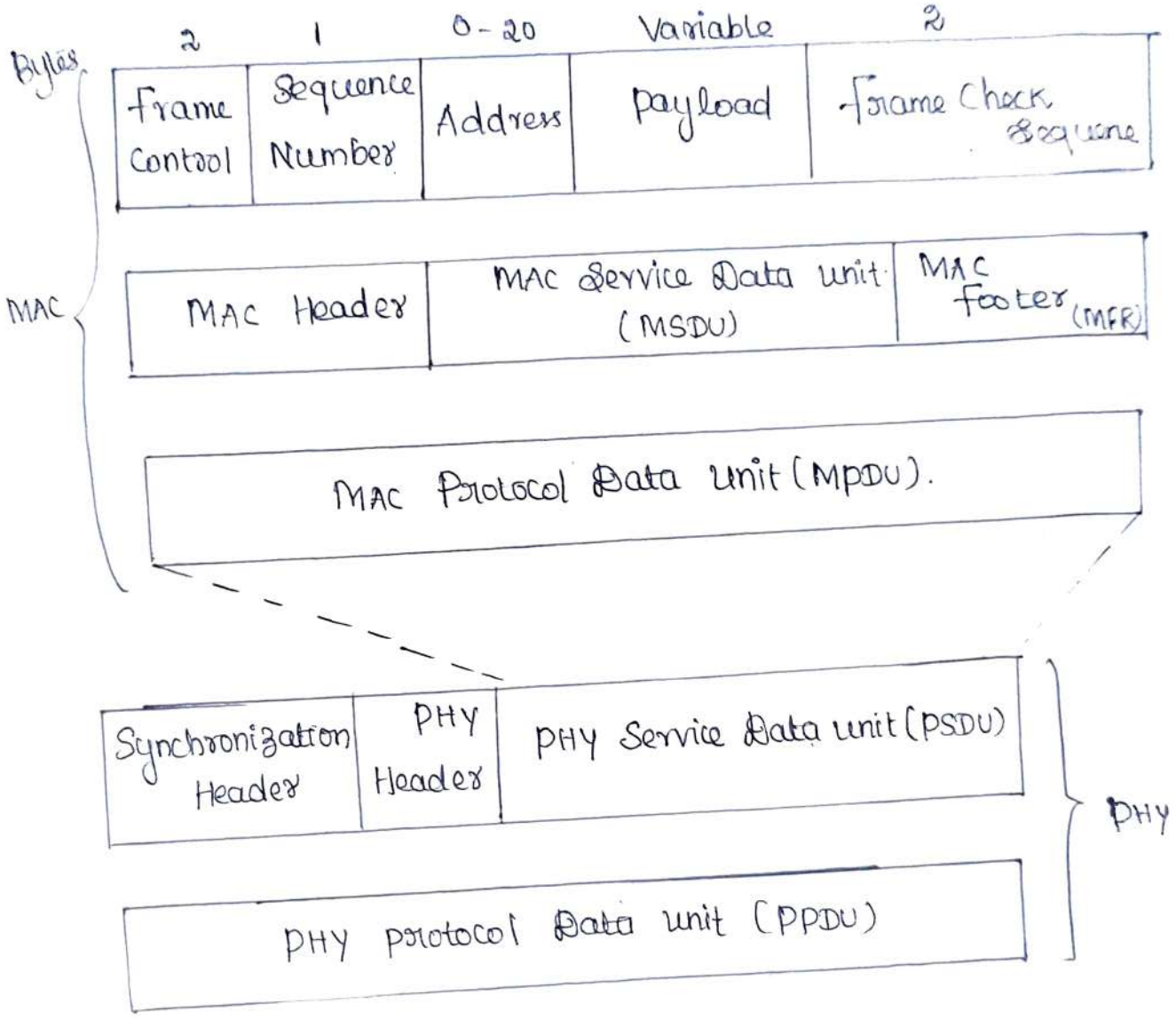


fig. General MAC frame format.

MAC Protocol Data unit (PSDU):

⇒ It consist of MAC header (MHR), MAC Service data unit (MSDU) and MAC footer (MFR)

*) MAC Header (MHR).

→ Frame Control (2 byte):

⇒ It Indicates the type of MAC frame being transmitted, Specifies the format of the address

field and Controls the acknowledgement. Also it specifies how the rest of the frame looks and what it Contains.

Sequence Number (1 byte)

The Sequence number in the MAC header matches the acknowledgement frame with the previous transmission.

→ Address (0–20) byte :-

The size of the address field may vary between 0–20 bytes.

*) MAC Service Data Unit (MSDU):

→ pay load

It is variable in length. however, the Complete MAC frame may not exceed 127 bytes in length.

The data Contained in the payload dependent on the frame type four different frame type are,

① beacon frame } Actually Contain information Sent
② data frame } to higher layer.

③ ACK frame
④ MAC Command frame. } → Originates the MAC and are used to peer-peer Communication.

*) MAC footer :-

It Contains FCS field → It helps to verify the integrity of the MAC frame.

Super-frame Structure :-

Explain with neat diagram of IEEE 802.15.4 Super frame Structure.

⇒ Some application may require a dedicated bandwidth to achieve less latencies.

To accomplish these two latencies, IEEE 802.15.4 LR-WPAN Can operate in an operational Super-frame mode.

beacons :-

In fig below, a dedicated PAC Co-ordinator transmits Super-frame beacons in pre determined intervals

→ These intervals can be short as 15 ms and long as 245 sec

→ The time between two beacons divided into 16 equal time slots independent of the duration of the Superframe.

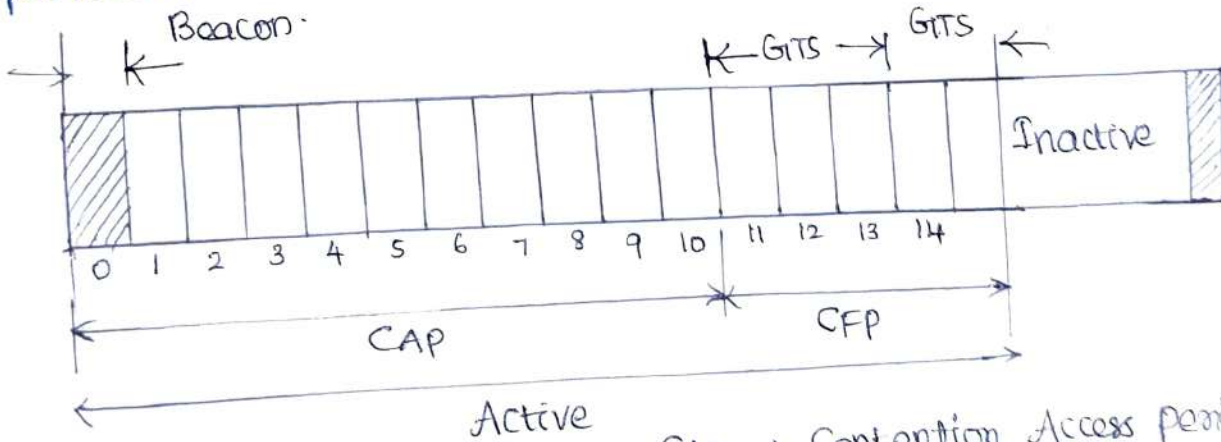


fig: IEEE 802.15.14 Superframe structure,

CAP → Contention Access Period
CFP → Contention free Period
GTS → Guaranteed timeslot

*) The Super-frame is divided into an Active period and Inactive period.

→ Active Period is Subdivided into an active Period and inactive Period.

⇒ Active period is Sub divided into 16 time Slots. first Slot is beacon frame. Remaining Slots Conforms the Contention Access period (CAP) followed by Guranteed Time Slot (GTS).

⇒ The beacon frame is Sent in the first time Slot of each Super-frame. The beacons are used to Synchronize the attached devices to identify PAN. A device Can transmit at any time during the Slot, but must Complete the transaction before the next Super frame Sent. CAP → during this period Something to transmit.

⇒ GTS :- The PAN Co-ordinator may assign time Slots to a Single device that requires a dedicated bandwidth or low latency transmission. These assigned time Slots are guaranteed time Slots (GTS).

→ CFP :- It's located immediately before the next beacon.

Channel mechanism :-

⇒ Depending on the network Configuration two channel mechanisms are used.

① beacon enabled network using Slotted Carrier Sense multiple access – Collision Avoidance (CSMA-CA)

* In this mechanism, during CAP wait for the begining of the next time slot then determines whether another device using the same slot.

*) Same slot used by another devices means back off for a random number of slots or indicate the transmission as failure.

(3) Co-ordinator:-

This is the node that Contools the IEEE 802.15.4 network. This is a special form of FFD.

In addition to the normal FFD functions it also sets the IEEE 802.15.4 network up and acts as the Co-ordinator or manager of the network.

Zigbee Network Topologies:-

There are three types of network topologies,

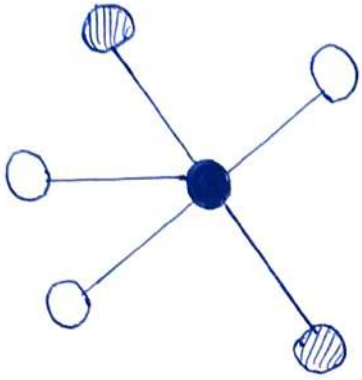
1. Star topology
2. Peer-to-peer topology
3. Cluster tree topology.

Star topology:

→ All the different nodes are required to talk only to the Central PAN Co-ordinator.

→ Even if the nodes are FFDs and are within range of each other in a Star network topology. They are only allowed to communicate with the Co-ordinator node.

→ It also limit to overall distance that can be covered. It is limited to one hop.



● – PAN Co-ordinator

◍ – FFD

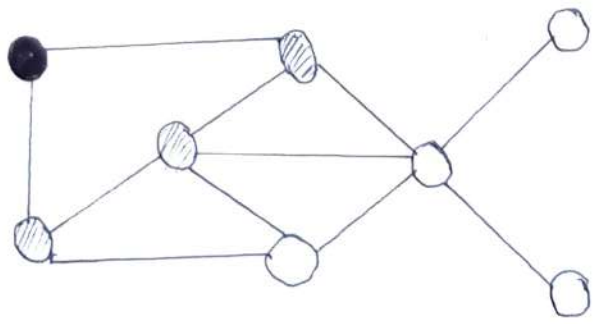
○ – RFD.

2. Peer-to-peer topology:.

*) It contrast to star topology, any device can communicate with any other device as long as they are in range of one another.

*) It can be adhoc, Self-organizing and Self healing

*) It also allows multiple hops to route messages from any device to other device in the network.



● — PAN

◍ — FFD

○ — RFD.

→ It is a special type of peer-to-peer network in which most devices are FFD and RFD may connect to a cluster three network as a leaf node at the end of a branch.

⇒ Any of the FFD can act as a Co-ordinator and provide synchronization service to other devices and co-ordinator

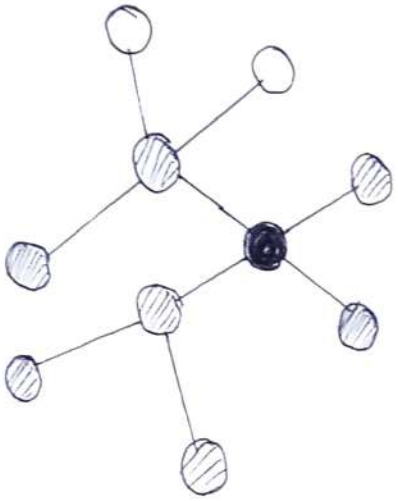


fig: Cluster tree topology.

Zigbee Protocol Architecture :-

In zigbee specification includes an upper layer Protocol stack building on the IEEE 802.15.4 PHY & MAC layer.

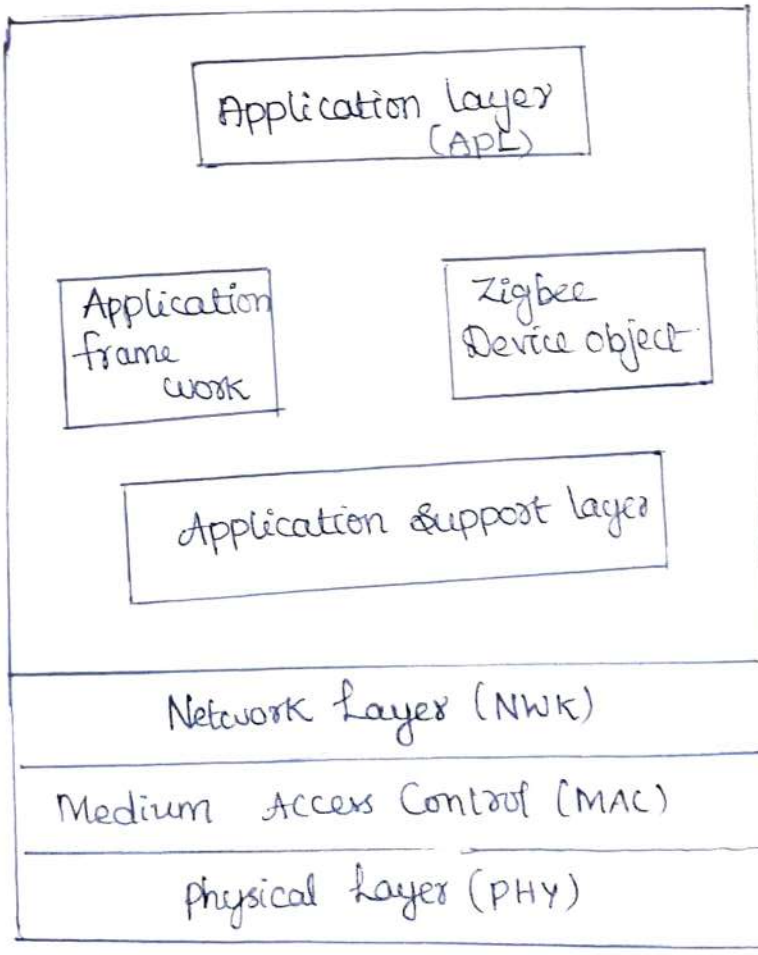


fig: Zigbee Protocol Stack

* The PHY and MAC lower layer protocol uses IEEE802.15.4 Standard directly and additional Specifications of network layer (NWK), Application Support Layer (APS), AP frame work, ZDO (zigbee Device object)

* Physical Layer:-

In 2.4 GHz band, direct Sequence Spread Spectrum is used, with one of the 16, 32-bit Chipping Codes mapped on to a 4 bit data symbol.

MAC Layer:-

To support upto 64,000 nodes in a Variety of Simple Connection topologies. In an extended network. device access to the physical Channel is Controlled using a Combination of TDMA and CSMA/CA.

⇒ It uses the Super frame Structure for special modes.

* Network layer:-

It Supports three kinds of network topology Such as Star, tree and Mesh.

⇒ The network layer is located between the MAC layer and the application Support Sublayer (APS)

⇒ It also Support routing.

→ It Starts a network, assigns node addresses, Configures new devices discovers other network and applies Security.

*) Application layer:

Application Support Sub-layer:

⇒ This layer enables the services necessary for Zigbee device object and application objects to interface with the network layers for data managing services.

This layer is responsible for matching two devices according to their services and needs.

→ Application frame work:

It provides two types of data services as key value pair and generic message services.

Generic message is a developer defined structure, whereas the key value pair is used for getting attributes with in the application objects.

Zigbee device object (ZDO):

ZDO provides an interface between application objects and APS layer in Zigbee devices. It is responsible for detecting, initiating and binding other devices to the network.

Applications:

① Wireless monitoring systems for industrial automation
② Intelligent home.
③ medical care & military use and security

WIRELESS USB:-

Explain in detail about wireless USB?

* Wireless USB is the result of the drive by

the USB is the result of the drive by the USB implementers forum to ensure that the highly successful wired USB interface - evolves into the wireless future.

It uses the ultra wide band (UWB) radio technology to deliver a PHY layer data rate of 480 Mbps, with low power consumption and a range of upto 10 meters.

It mainly used multimedia consumer electronic devices, high speed connections to pc peripherals and other mobile devices.

Protocol Stack:-

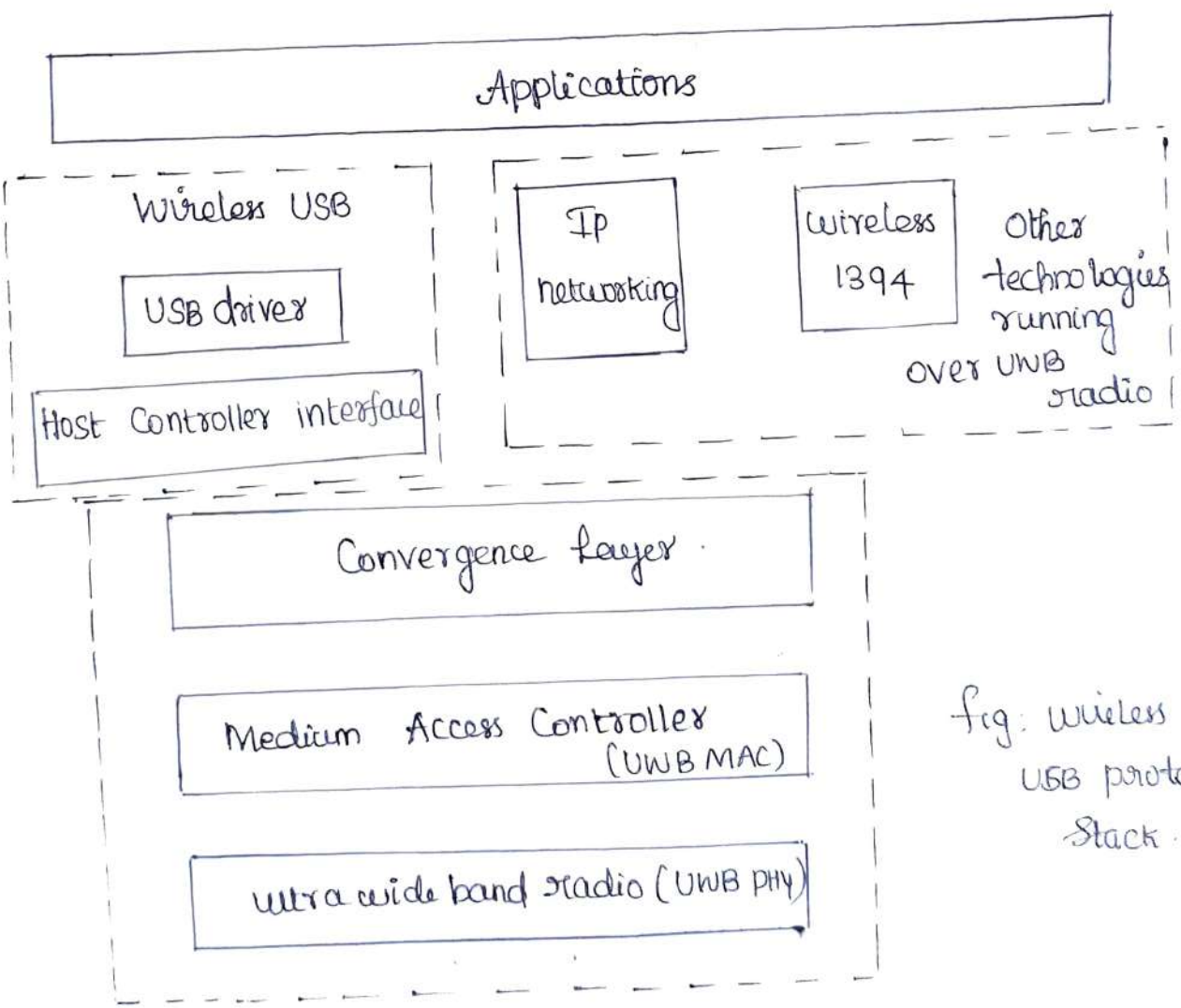


fig: Wireless USB protocol Stack.

Wireless USB Radio (UWB PHY):-

*) The wireless USB PHY layer is the multiband OFDM alliance (MBOA) UWB radio, operating across the 3.1 to 10.6 GHz frequency bands

*) Support for data rates of 53.3, 106.7 & 200 Mbps.

*) Media Access Control layer:-

*) It's responsibility for medium control is shared by all devices, reducing vulnerability to single point failure and eliminating the bandwidth penalty of maintaining Central Control.

MAC layer timing is defined with in the Super-frame structure.

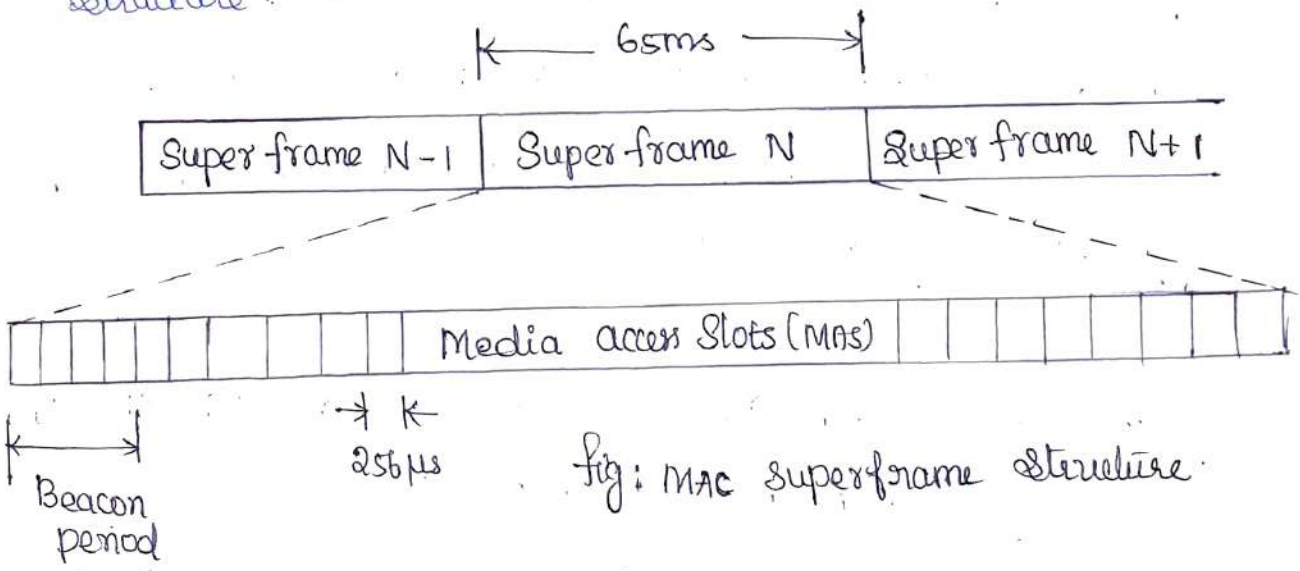


fig: MAC superframe structure.

⇒ Each 65 ms Super-frame is devided into 256 media access Slots (MAS) each of 256 μs duration.

⇒ The leading MAS in each Super frame are used as a beacon Period during which device exchange information with the host on their capabilities and resource requirements

*) Device can reserve one or more medium access slots using distributed reservation protocol (DRP) messages during the beacon period

*) Transport layer

*) It provides host - host communication services for applications.

*) It provides services such as connection - oriented communication, reliability, flow control and multiplexing.

*) Ip Protocol suite using Tcp/UDP.

Host Controller Interface (HCI)

It is a register level interface that enables a host controller for USB or IEEE 1394 hardware to communicate with a host controller driver in software.

*) USB driver: hardware device to communicate with operating system of pc.

Topology:

*) Wireless USB connects USB devices with the USB host using a hub and spoke model.

*) wireless USB host is the hub at the center, and each devices sits at the end of a spoke.

Each spoke is a point - to - point connection between the host and device wireless USB hosts can support upto 127 devices and because wireless USB does not have physical ports there is no need, nor any definition provided, for hub devices to provides ports expansion

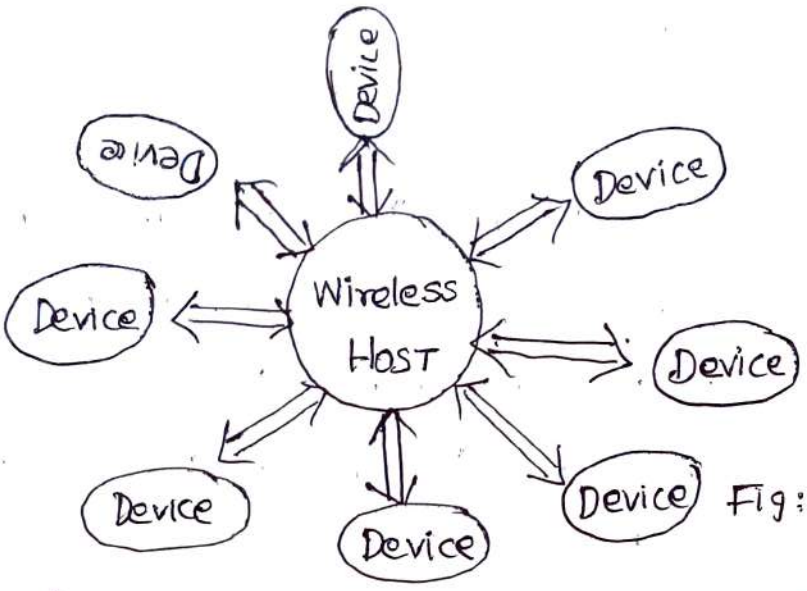


Fig: Hub & Spoke Topology

USB devices → printers, digital camera, wire adaptor

Advantage over USB:

1. Ease of moving
2. Less mess
3. Increased range.

Disadvantage over USB:

1. The hardware is small, it can get damaged, Lost or Stolen.
2. Unless the security is not properly setup, data can be accessed and read by others.

6LoWPAN:

Describe the user Scenario architecture of 6LoWPAN?

⇒ The 6LoWPAN system is used for variety of applications including wireless sensor networks.

⇒ It's stands for IPV6 over low power wireless Personal Area networks.

*) It Provides Packet data in the form of IPV6 over IEEE 802.15.4 and other networks.

*) Also provides end-to-end IPV6 and as such it is able to provide direct Connectivity to the internet.

*) This protocol is used to enable IPV6 packets to be carried on the top of the Low power wireless personal area networks. (WPAN)

*) Architecture (protocol stack):

6LOWPAN adopts the physical and media Access Control (MAC) layer protocols defined IEEE 802.15.4

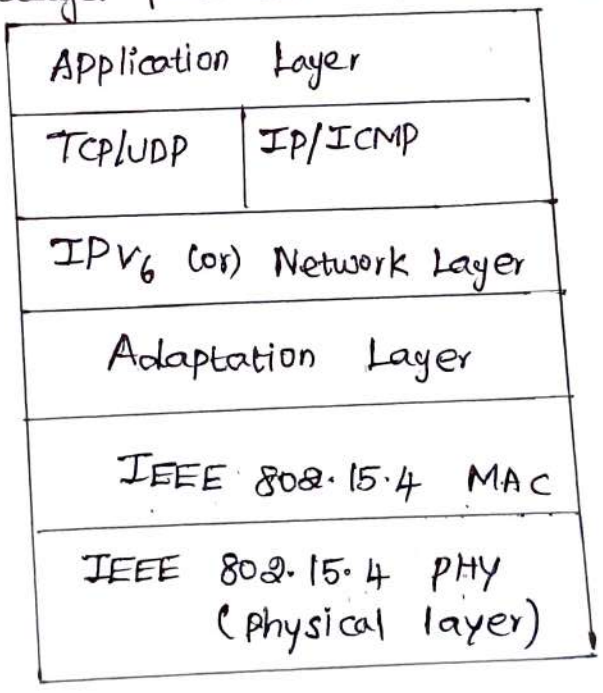


Fig: 6 LOWPAN protocol Architecture

Physical Layer: (refer basic IEEE 802.15.4)

→ It provides basic communication capabilities of the medium.

PHY layer provides two Services

① PHY data Services

② PHY management Services.

① PHY data Service :-

→ To provide transmission and reception of data packets between MAC & PHY through the physical radio Channel.

② PHY management Service :

It is based on the IEEE 802.15.4 Standard which operates at the frequency of 2400 - 2483.5 MHz at 250 kbps.

Data link layer :

It provides the Services to enable reliable, Single-hop Communication links between 6LoWPAN node. The MAC Protocol enabled to transmit data ~~format~~ frames via Channel access method CSMA/CA.

*) The MAC protocol data unit (PPDU) is IEEE 802.13.4 which operates in non beacon-enabled mode.

⇒ In non-beacon-enabled networks, data-frames (including those carrying IPV6 packets) are transmitted via the contention-based channel access method such as unslotted CSMA/CA.

*) Adaptation layer :

① The main function of this layer is TCP/IP header compression.

In IEEE 802.15.4 frame has a max packet size of 128 bytes. where as IP V6 header size is 40 bytes, user diagram protocol (UDP). and internet Control message protocol (ICMP) header sizes are both 4 bytes, fragmentation header adds another 5 bytes overhead. So without Compression not to transmit.

② Fragmentation and Reassembly:

→ IPV6 requires a maximum transmission unit (MTU) of 1280 bytes. It handled by means of adaptation layer.

*) Network layer:

It provides the internetworking capability to sensor nodes

⇒ The main Consideration of this layer are addressing, mapping and routing protocols.

Addressing ⇒ It address IPV6 requirement and Security Services.

Routing mapping → Supports routing and network management with SNMP (Simple network Management protocol)

*) It's responsible for finding the best route and forward.

Transport layer:

*) It's responsible for process-to-process delivery

*) It delivers data segment to the appropriate application process on the sensor node.

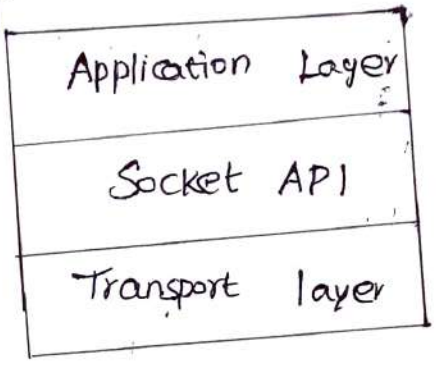
→ Two types of transport protocols are used

① TCP ② UDP.

At the source side either TCP, UDP connections is established based on the application. hence either TCP or UDP process is created.

Application Layer:

⇒ It uses a socket interface for a specific application as shown in fig.



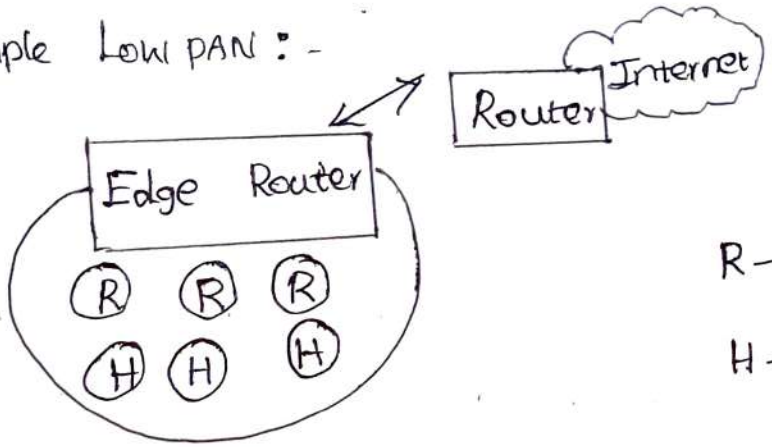
→ Each 6LoWPAN application opens a socket to receive or send packets. Each socket is associated with a protocol such as Tcp or UDP and ports namely source and destination ports.

Architecture:

The architecture of 6LoWPAN consists of three types.

① Simple LoWPAN
② Extended LoW PAN
③ Adhoc LoW PAN

(1) Simple LoWPAN :-



*) Single Edge router can be used which resulting in a Simple LoWPAN. The Edge Router (ER) placed at the edge of 6LoWPAN Route traffic in and out of the header compression task.

Extended LoWPAN :

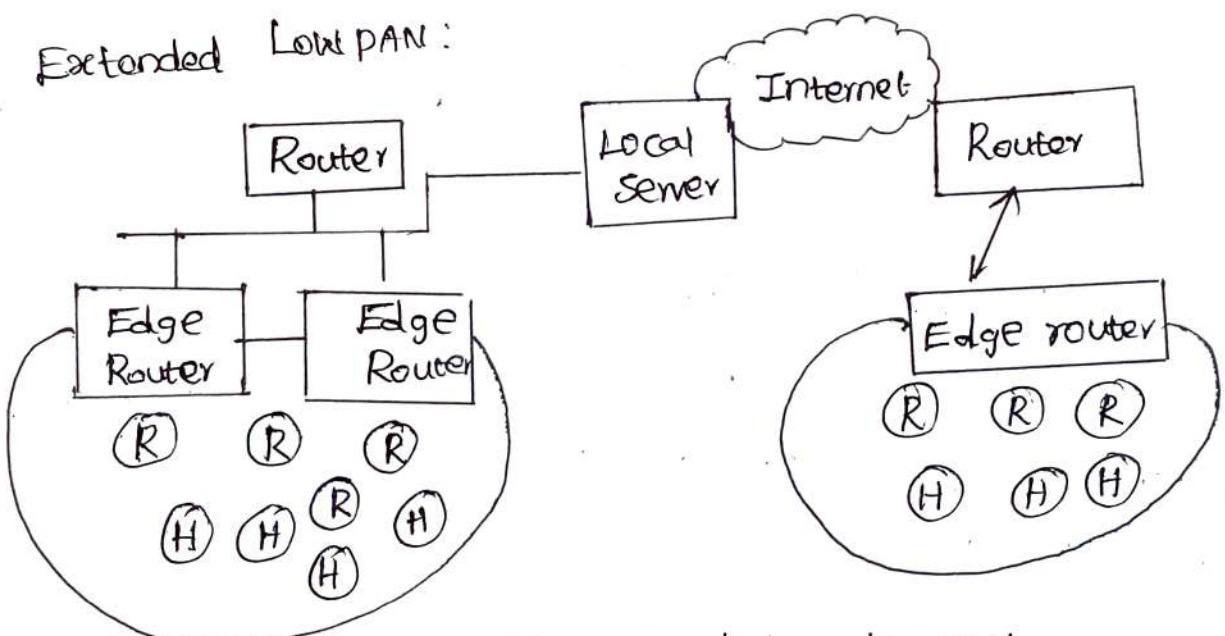


Fig: Extended LoWPAN

*) To address the network scalability multiple edge routers (ERs) can be used which resulting in a Extended LoWPAN.

*) The nodes in 6LoWPAN plays the role of host or router, along with one (or) more edge routers.

*) The nodes in a LoWPAN share the same IPV6 Prefix which is distributed by the ER and router through out the LoWPAN.

③ Adhoc LoWPAN :-

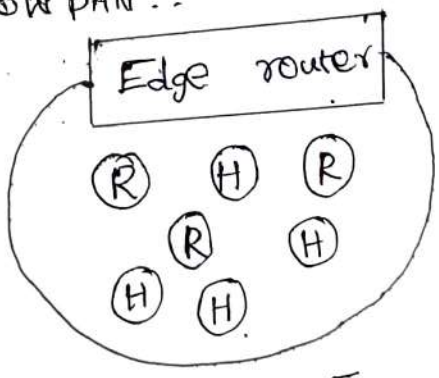


Fig: Ad-Hoc LowPAN

*) An Ad-hoc LowPAN operates without an infrastructure and is connected to the internet. In this topology, a router is randomly configured to act as a simplified ER.

Advantages:

*) Open, long lived, reliable standards
*) Transparent Internet Intagrations
*) Network maintainability.
*) Global scalability.
*) Multi topology options.

WIRELESS HART:

Explain about HART technologies?

Wireless HART is a wireless Sensor networking technology based on the Highway Addressable Remote transducer protocol.

*) The Protocol utilizes a time Synchronized, Self-organizing and Self-healing mesh architecture.

*) This protocol Supports operation in the 2.4 GHz ISM band using IEEE 802.15.4 Standard radios.

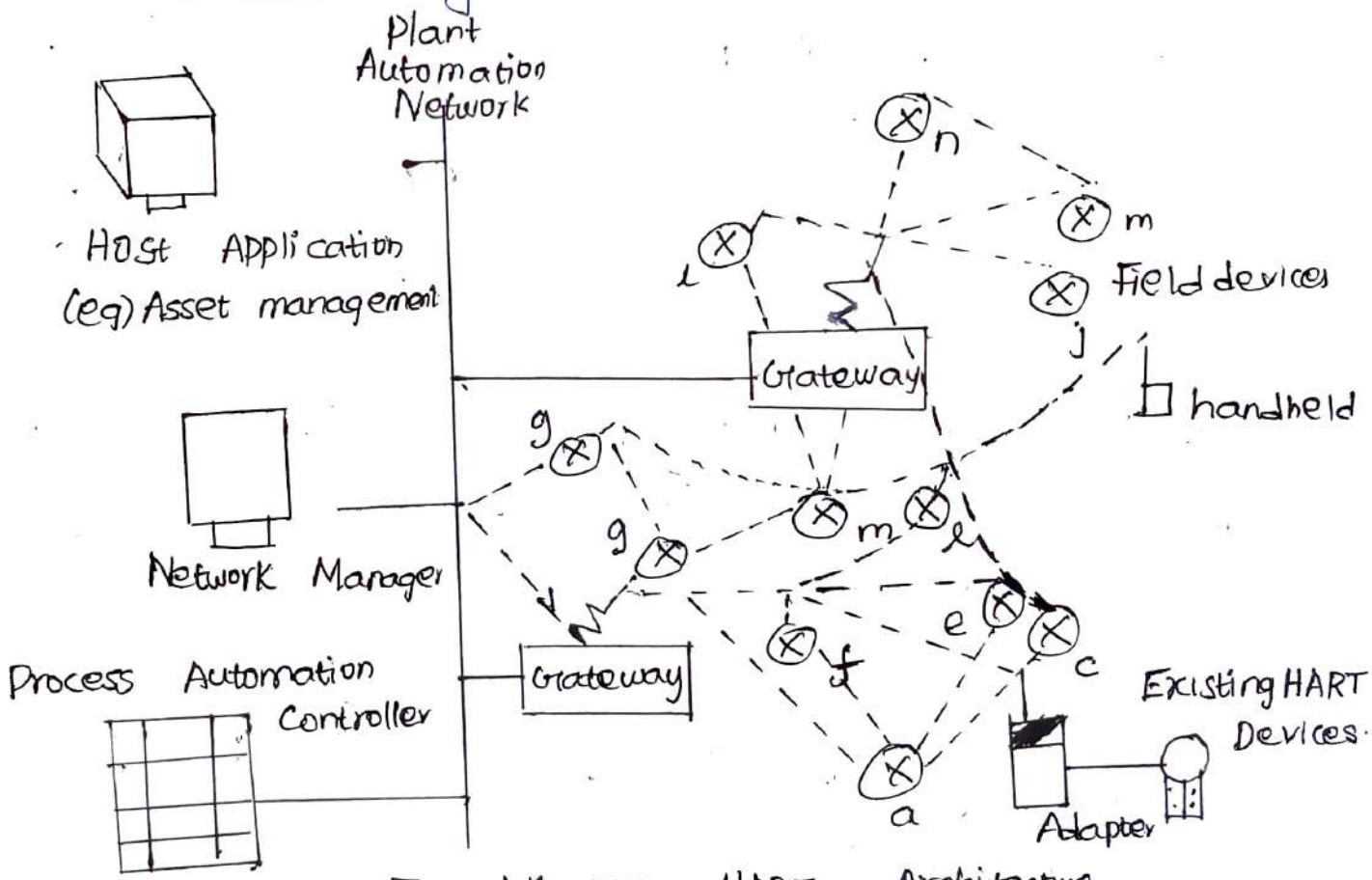


Fig: Wireless HART Architecture

*) Each individual instrument in the HART Wireless Connection is Connected through a mesh network.

*) Each individual instrument is connected to a common input and adjustment instruments.

*) If an instrument is far from the gateway or the route is blocked, it cannot connect to the gateway.

*) Although you can communicate with the gateway through other instruments. ∴ Each device in the mesh network can serve as a router for messages from other devices.

Mesh network (mesh net):

⇒ It is local network topology in which the infrastructure nodes (ie. bridges, switches and other infra-structure devices) Connect directly to other nodes.

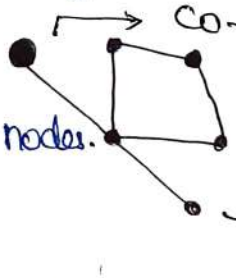


fig: mesh network

Uses:

It is used to provide redundant data path ways in case of device failure or changes in the environment interrupting radio communication between devices.

*) Field devices:

⇒ Sensors / actuators connected to process or plant equipment.

*) Adapter:

⇒ Enables HART devices with wireless communication.

*) Handheld:

⇒ Portable, HART devices with wireless communication.

Handheld : Portable devices used to configure, diagonse and calibrate field devices.

Network manager :

→ Creates routes and schedules communications.

→ Support devices joining / leaving the network

→ Adapt the schedule and routes upon network changes.

Gateway :

*) Connects host applications with field devices.

*) Translates commands between two protocols.

WIRELESS HART PROTOCOL STACK :

*) Physical layer :

The physical layer of wireless HART is the IEEE 802.15 standard physical layer. It's used basic signal encoding and data transmission.

*) Data link layer :

It support network - wide time synchronization, channel hopping, dedicated & slotted unicast communication bandwidth, link layer ACK, and concurrent link activation.

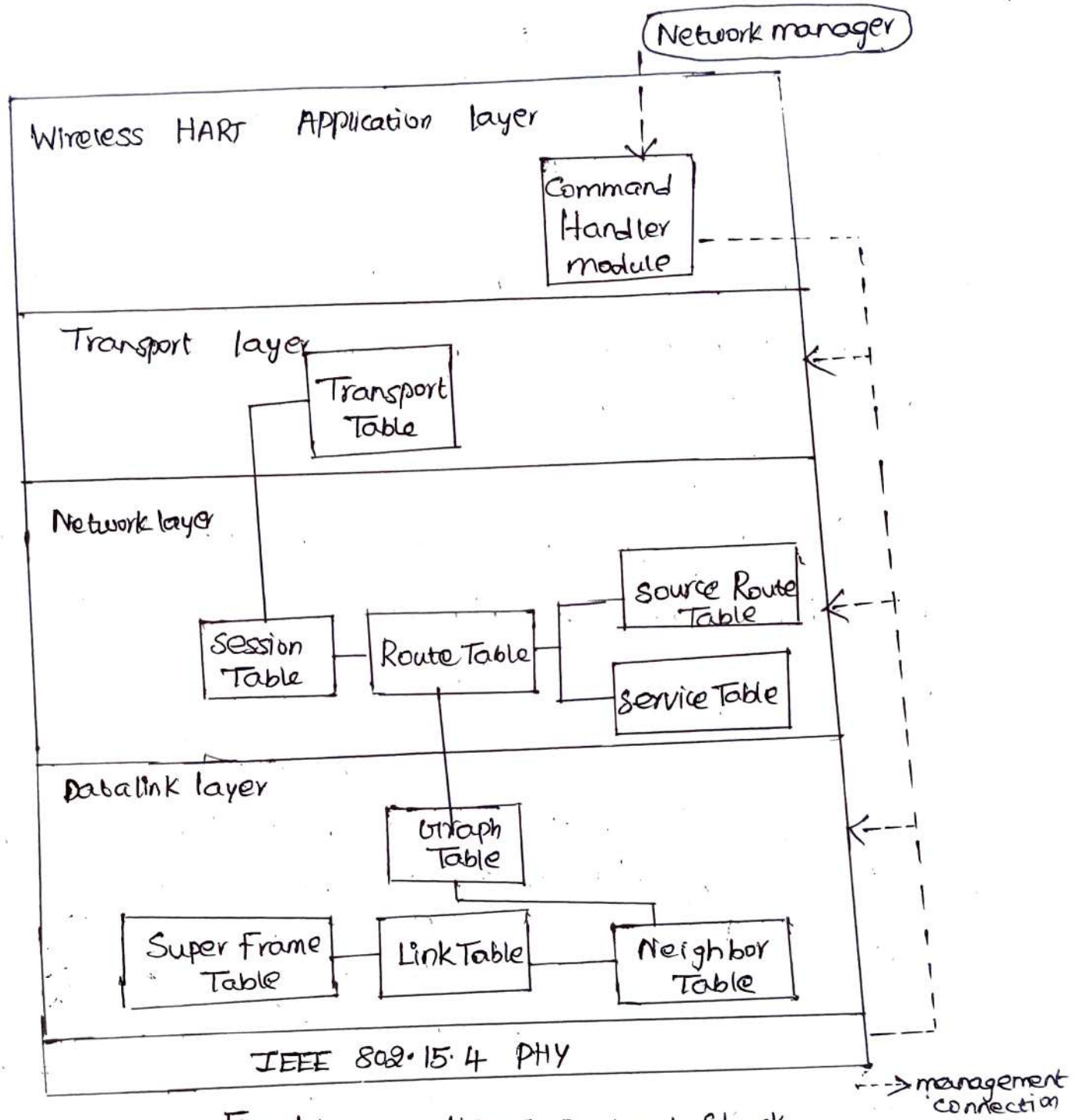


Fig: Wireless HART protocol Stack

Super frame table :

This table contains a collection of super frames. Based on the required communication schedule, multiple super frames of different length can be configured for each devices by filling in this table.

⇒ The practical length is defined as 2^ns $(-2 \leq n \leq 9)$ from 250ms (2^{-2})s to 8 min and 32 s.

Link Table :

This table contains a collection of link. This table together with the superframe table, identifies the communication schedule.

*) Graph table :

In graph table, each graph lists the potential next-hop neighbors to which the data can be forwarded.

Neighbour table.

Unlike the other communication tables, this table is not filled by the NM. The neighbour table contains list of neighbour the device can communicate with.

*) Network Layer :-

*) It provides routing and secure end-to-end communication for network devices in wireless HART.

*) To provide secure communication, a security sub layer is implemented in the network layer itself.

*) As there is no session layer defined in the wireless HART stack a session is defined in the network layer.

Sessions:

Sessions ensure Secure (end-to-end encrypted) Communication between two devices in the network.

*) A unicast session between the NM and the device. This session is used to manage and Configure the network by the NM.

*) A broadcasting session between NM and all the devices

*) A unicast session between the gateway and all devices

Services:

In wireless HART, Services are used to allocate bandwidth for a specific type of data.

Four types of Services are,

1. maintenance and Configuration
2. Publish
3. Block Transfer
4. Event

Security Sublayer:-

It provides Secure Communication between end devices.

*) This is achieved by using Cryptographic Services in different layers such as data link layer & network layer.

Transport layer:

⇒ It ensures that packets are delivered Success fully across multiple hops to their final destinations

*) This layer supports either acknowledged or unacknowledged transactions

*) Application Layer:

The application layer of wireless HART is a Command based layer.

Commands, the basis of HART Communications are sent from the gateway or field devices.

→ Each Command can be identified by a command number, which determines the content of the message.

Applications:

1. Extraction of Crude Oil
2. Monitoring ground water
3. Production of catalyzers.

Problems:

(1) OFDM uses a set of orthogonal Sub-Carrier for transmission of data. OFDM is used in WLANs. Consider an OFDM system that uses 52 Sub-carriers out of which 48 are data Sub-carriers and 4 are pilot Sub-carriers. System bandwidth is 20MHz and OFDM symbol duration including cyclic prefix (guard interval for ISI Mitigation) is 4 μs. If code rate is 3/4 and 64 QAM is used what is the data rate?

Soln

64 QAM corresponds to 6 bits per symbol Total number of data bits transmitted per OFDM symbol in 4 μs is $6 \times 48 \times 3/4 = 216$.

$\therefore$ data rate is $= \frac{216 \times 1000000}{4} = 54$ Mbps

2) Consider the HIPER LAN 2 that uses BPSK and $R = 3/4$ Codes for 9 Mbps information transmission and 16-QAM with the same coding for the actual payload data transmission rate of 36 Mbps. Calculate the coded symbol transmission rate per sub carrier for each of the two modes. What is the bit transmission rate per sub carrier for each of the two modes.

Solution:

User data transmission rate per carrier with $R = 3/4$ Convolution encoder.

$$\text{mode I (9 Mbps)} = \frac{9 \times 10^6}{48} = 187.5 \text{ Kbps}$$

$$\text{Mode II (36 Mbps)} = \frac{36 \times 10^6}{48} = 750 \text{ Kbps}$$

$\therefore$ Carrier transmission rate with $R = 3/4$ Convolutional encoder

$$\text{mode I} = \frac{187.5}{3/4} = 250 \text{ Kbps}$$

$$\text{mode II} = \frac{750}{3/4} = 1000 \text{ Kbps}$$

$\therefore$ Carrier Symbol rate

mode I (BPSK): 250 Kbps

mode II (16 QAM) $= \frac{1000}{4} = 250$ Kbps.

3) What is the user data for HIPER LAN/2 with 64 QAM modulation with R = 3/4 Convolutional Coder.

Soln:

Carrier Symbol rate = 250 kpbs, bit per Symbol for 64-QAM = 6

User data rate = (250) x (3/4) x 6 x 48 = 54 Mbps.

4) The IEEE802.11a WLAN uses a 64-Sub Channel implementation of multicarrier modulation (OFDM). Forty eight Sub carriers are used for information transmission, 4 Sub Carriers for Pilot tones are used for Synchronization, and 12 are reserved. Each Sub Channel has a Symbol rate of 250 kilo Symbols per Seconds (ksps). The occupied bandwidth is 20MHz. Find the band width of a Sub Channel. What is modulation efficiency? What is the user Symbol rate? If 16 QAM modulation is used, what is the user data rate if the information bits are encoded with a rate of 3/4? If the guard time between two transmitted Symbol is 800 ns, What is the time utilization efficiency of the S/m?

Soln

Total no of Subcarrier = 48 + 12 + 4 = 64

Bandwidth of Subchannel = $\frac{24 \times 10^6}{64} = 312.5$ KHz

modulation efficiency = $\frac{250}{312.5} = 0.8$ Symbols/sec/Hz

user Symbol transmission rate = 48 x 2.50

= 1.2 Msps.

User bit per symbol = 4 for 16-QPSK modulation

User data rate = $3/4 \times 4 \times 12 = 36$ Mbps.

Symbol duration = $\frac{1}{250 \times 10^3} = 4000$ ns.

Time utilization efficiency = $\frac{4000}{4800} = 0.83$

UNIT : II

MOBILE NETWORK LAYER

Introduction – Mobile Ip : Ip packet delivery, Agent discovery, tunneling and encapsulation, IPV6 – Network layer in the internet – Mobile Ip Session initiation protocol – mobile ad-hoc network : Routing : Destination Sequence distance Vector, IOT – COAP.

Mobile Ip :

Explain in detail about mobile Ip and its requirement ? (8m)

(or)

Name the requirements for a mobile Ip and justify them. Does mobile Ip fulfill them all ? (8m)

(or)

Explain in detail about design goals and its requirement ? (8m)

(i) Need for mobile Ip :-

Mobile Ip is a network layer solution for homogeneous and heterogeneous mobility on the global internet which is scalable, robust, Secure and which allows nodes to maintain all ongoing communications while moving.

Design goals :

*) Mobile Ip was developed as a means for transparently dealing with problems of mobile users.

*) Mobile Ip was designed to make it simple to implement mobile node software, also designed to avoid solutions that require mobile nodes to use multiple addresses.

*) Requirements :-

The basic requirements for mobile IP is

*) Compatibility
*) Transparency
*) Scalability and efficiency
*) Security.

Compatibility :-

*) The architecture of internet is very huge and a new standard cannot introduce changes to the applications or network protocols already in use.

*) Mobile Ip is to be integrated into the existing operating systems. Also for routers it may be possible to enhance its capabilities to support mobility instead of changing the routers which is highly impossible.

Transparency :-

*) Mobility remains invisible for many higher layer protocols and applications.

*) Higher layers continue to work if even if the mobile computers has changed its point of attachment to the network and even cha notice a lower bandwidth and some interruption in the service.

3. Scalability and efficiency :-

⇒ The efficiency of the network should not be effected even if a new mechanism is introduced into the internet.

⇒ Enhancing Ip for mobility must not generate many new messages flooding the whole network.

⇒ Special care is necessary to be taken for Considering the lower bandwidth of wireless links.

4. Security :

*) Mobility panes many security problems. A minimum requirement is the authentication of all messages related to the management of mobile Ip.

(ii) Entities and terminology :-

State the entities and terminologies used in mobile Ip ?

(or)

How the entities and terminologies in mobile network ?

(or)

List the entities and terminologies used in mobile Ip ?

(or)

Discuss the entities and terminology of mobile Ip network ?

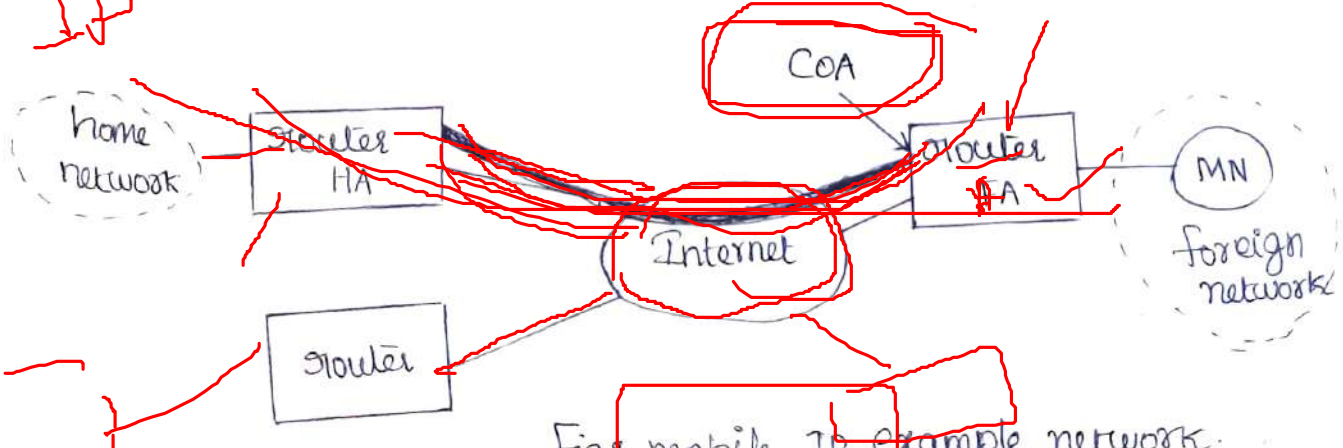
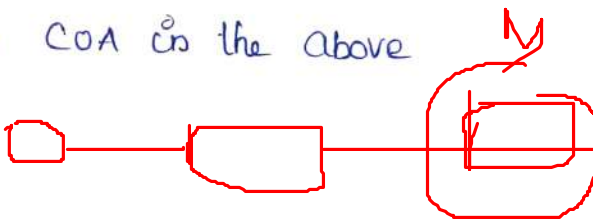


Fig: mobile Ip example network.

⇒ A CN is connected via a router to the internet, as are the home network & foreign network.

⇒ The HA is implemented on the router connecting the home network with the internet, an FA is implemented on the foreign network.

⇒ The MN is currently in the foreign network. The tunnel for the packets towards the MN starts at the HA and ends at the FA, for the FA has the COA in the above example.



(i) 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 it Ip address and can continuously communicate with any other system in the internet as long as link layer connectivity is given (eg) laptop, mobile phone aircraft.

(ii) Correspondent node :-

At least one partner is needed for communicaton. The CN can be fixed or mobile node.

(iii) 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.

iv) Foreign Network :

The foreign network is the current Subnet the MN visits and which is not the home network.

(v) Foreign Agent :

⇒ The FA can provide several Services to the MN during its visit to the foreign network.

⇒ The FA can have the CoA, acting a tunnel end Point and forwarding packets to the MN.

⇒ The FA can be acting as default router for the MN.

vi) 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, not directly to the Ip address of MN.

*) There are two different possibilities for location of CoA.

→ foreign agent CoA :-

The CoA is Co-located if the MN temporarily acquired an additional Ip address which acts as CoA. This address is now topologically correct and the tunnel end point is at the MN.

vii) Home agent : COA

The HA provides several Services for the MN

starts at the HA. The HA maintains a location registry that is informed MN's location by the current COA.

Ip packet delivery :-

Discribe data transfer from a mobile node to a fixed node viceversa.

(or)

How the Ip packet delivery is achieved WLAN?

(*) CN sends an Ip packet with MN as a destination address and CN as a source address

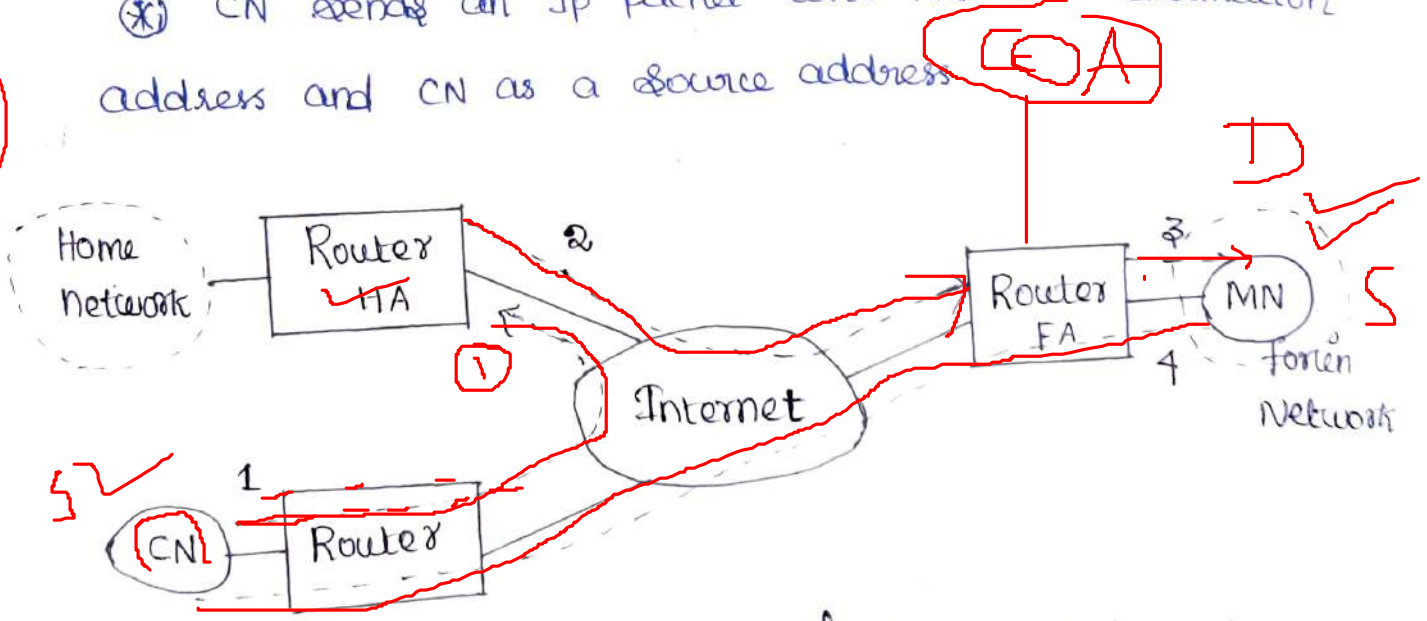


fig: packet delivery to and from the mobile node.

⇒ 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 mechanism 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 tunnelled to the COA.

⇒ 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.

*) The foreign agent now decapsulates the packet i.e. remove the additional header, and forwards the original packet with CN as source and MN as destination to the MN.

⇒ 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.

⊛ Sending packets from the mobile node (MN) to the CN is comparatively simple. The MN sends the packet as usual with its own fixed Ip address as source and CN's address as destination

Agent Discovery :-

Give the Short notes of Agent Discovery ?

(Or)

Describe the methods to identify the foreign agent ?

⇒ The mobile node is moving from one location to another location. During the movement it has to

identify the foreign agent. The mobile Ip describes two methods to identify the foreign agent.

1. Agent advertisement
2. Agent Solicitation

1. Agent advertisement:-

⇒ for this method, foreign agents and home agents advertise their presence periodically using special agent advertisement messages

⇒ The advertisement messages can be seen as a beacon broadcast into the subnet.

⇒ The upper part represents the ICMP (Internet Control message protocol) packets while the lower part is the extension needed for mobility.

for advertisement the TTL field of the Ip packet is set to 1.

Type	Code	Checksum
#addresses	addr size	life time
Router address 1		
Preference level 1		
Router address 2		
Preference level 2		

....

Fig: Agent advertisement

type = 16	length	Sequence number
registration life time	R B H F M G V T	reserved
CoA 1		
CoA 2		

...

*) The fields of the agent advertisement packets are

Type : It is set to 9

Code : It is set to 0, when the agent routes traffic from both mobile and non-mobile nodes. It is set to 16 when the agent routes traffic from mobile nodes and not from non-mobile nodes.

Address : The number of addresses advertised with this packet is in # addresses

Lifetime : It denote the length of time this advertisement is valid.

Preferences : It defines the preference level of each router. It is used to choose the most preferable one.

*) The field of the extension of the packet for mobility.

Type : It is set to 16 length : It depends on the number of COAs provided with the message and equals 6+4*(No. of address) *

6+4

Sequence Number : Total number of advertisement sent.

registration life time : Agent can specify the maximum lifetime in seconds. Eight bits are used to specify the characteristics of the agent.

R : It especifies that the registration is required with this agent

B : The agent is busy to accept the new registration.

H: offer services as a home agent.

F: offer services as a foreign agent.

M and G: Specify the method of encapsulation used for the tunnel.

r: Set to zero and must be ignored

T: reverse tunneling is supported by the FA.

2. Agent Solicitation:-

When a MN enters a new network, It verifies the advertisement message. If the advertisement messages are not there it will send agent Solicitation message

⇒ In high dynamic wireless networks, the MN Sends three Solicitation messages, one per Second. Before getting the agent address the MN will loss many data packets.

⇒ When the MN receives the address of the agent, it will use it for data transmission. It does not receive the answer it should decrease the rate of Solicitations.

⇒ The Solicitation messages will Create Collision, After the advertisements and Solicitations, the MN receives the COA for an FA. By using it the MN can make Communication

Registration:-

Explain in detail about registration process?

(or)

How does registration on layer 3 of mobile node work?

⇒ The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets

⇒ Registration can be done in two different ways depending on the location of the COA.

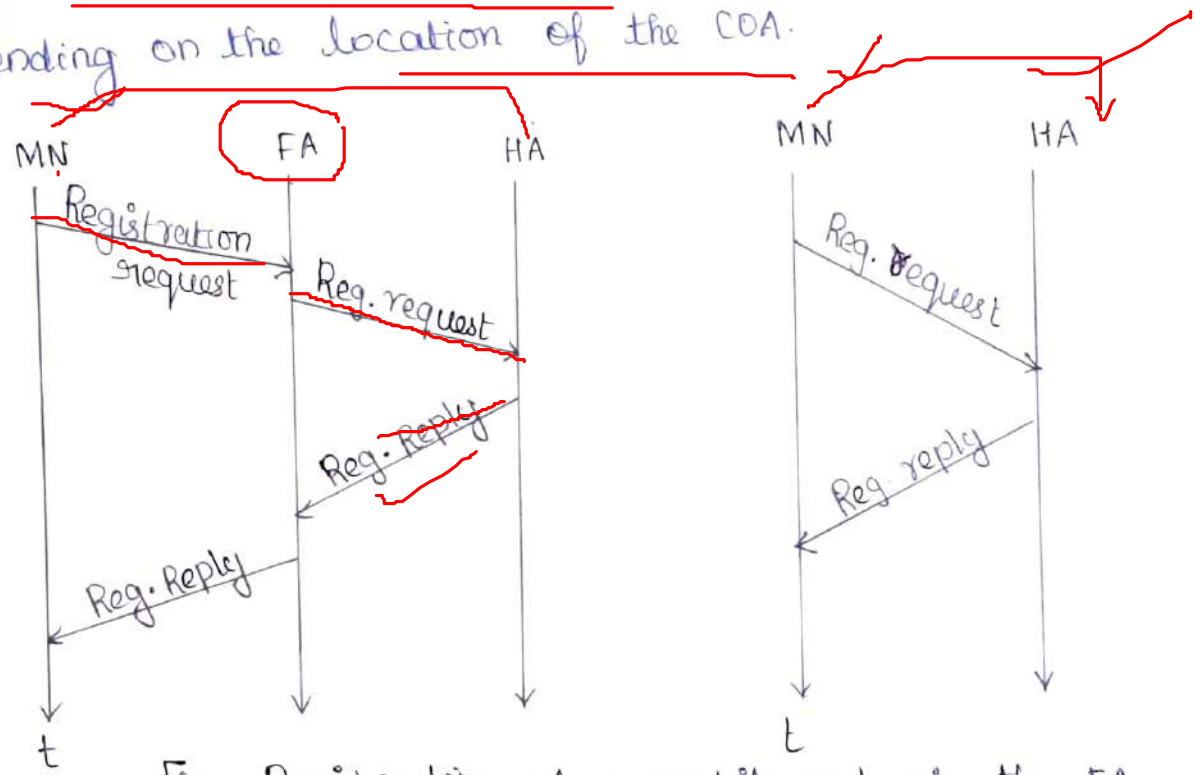


Fig: Registration of a mobile node via the FA or directly with HA.

⇒ If the CoA is at the FA, registration is done as illustrated in above fig (left).

① The MN Send its registration request Containing the CoA to the FA which forwards the request to the HA.

The HA now sets up a mobility binding, Containing the mobile nodes home IP Address and the current CoA

② After Setting up the mobility binding, ~~Containing the mobile nodes home IP~~ the HA Sends a reply message back to the FA which forwards it to the MN.

⇒ If the CoA is colocated registration can be simpler as shown in fig (right).

The MN may send the request directly to the HA and

0 7	8						15	16 23	24 31
type 1	S	B	D	M	G	r	T	x	life time
	home address								
	home agent								
			COA						
	Identification								
	extensions ...								

fig: registration request

0 7	8 15	16 31
Type = 3	Code	lifetime
home address		
home agent		
identification		
extensions ...		

fig: registration reply

Type : is set to 1 for a registration request

S: MN can specify if it wants the HA to retain prior mobility binding. This allows for simultaneous binding.

B: It generally indicates that an MN also wants to receive the broadcast packets which have been received by the HA is home network.

D: Decapsulation.

→ M&G: minimal and generic routing encapsulation.

If x : Set to zero

Life time : denotes the validity of the registration in seconds. A value of zero indicates deregistration.

Home address : It is the fixed IP address of the HA and CoA represent the tunnel end point.

Identification : (64 bit) It is generated by the MN to identify the request and match it with registration replies

extensions : It must atleast contain parameters for authentication

⇒ A registration reply which is conveyed in a UDP contains a type field set to 3 and a code indicating the result of the registration request.

Life time : Indicates how many seconds the registration is valid if it was successful.

Home address and home agent are the addresses of the MN and HA respectively.

Optimizations :-

Explain the optimizations used in mobile IP networks?

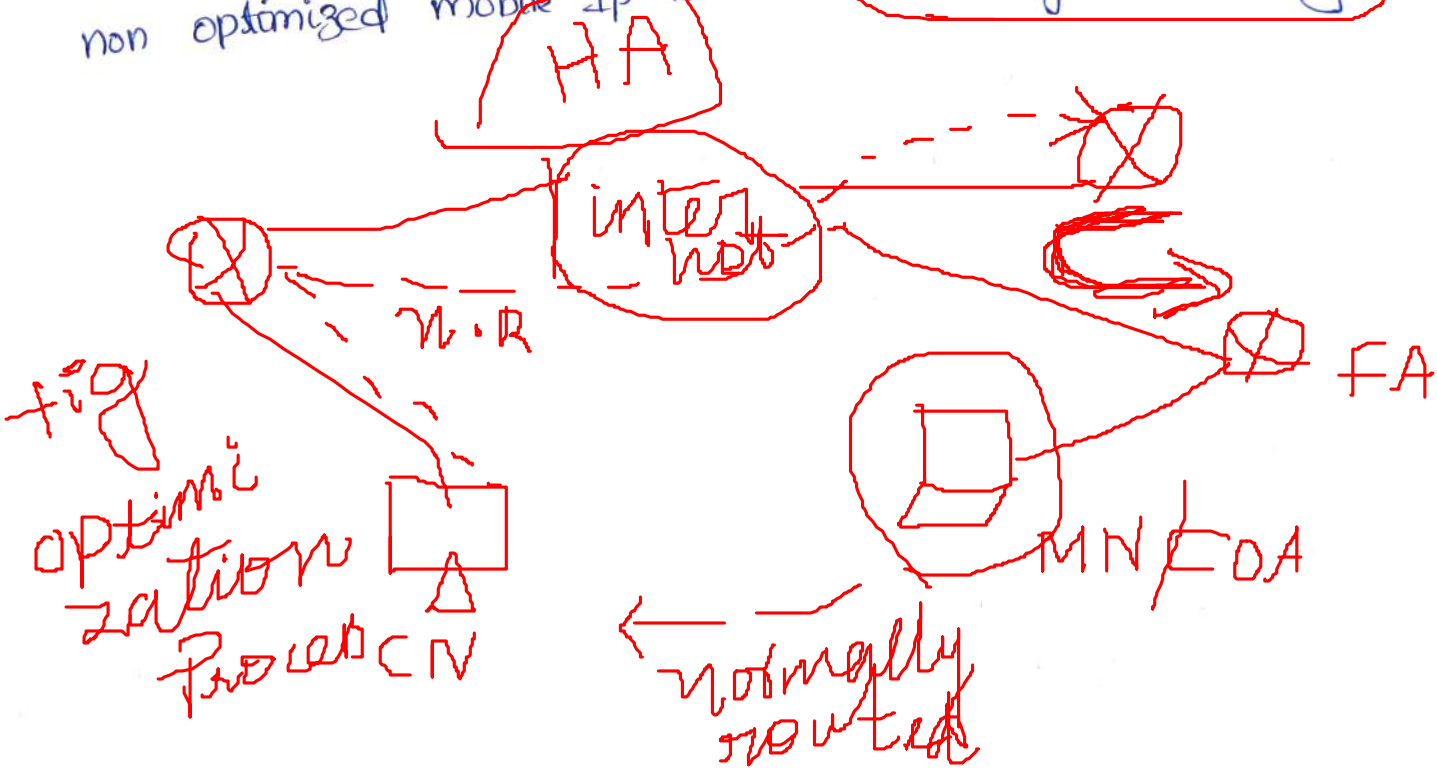
(or)

Imagine the following scenario. A Japanese and a German meet a Conference on Hawaii. Both want to use their laptops for exchanging data, both run mobile IP for mobility support. Explain the optimization technique?

(or)

Name the inefficient of mobile Ip regarding data forwarding from CN to MN. What are optimizations and what additional problems do they cause (8m).

Imagine the following Scenario :- A Japanese and a Germen meet a Conference on Hawaii. Both want to use their laptops for exchanging data, both run mobile Ip for mobility support. If the Japanese sends a packet to a German, his Computer sends the data to the HA of the German, from Hawaii to Germany. The HA in Germany now encapsulates the packets and tunnels them to the CoA of the laptop on Hawaii. This means the although the Computers might be only meters away, the packets have to travel around the world. The efficient behaviour of a non optimized mobile Ip is called triangular routing.



→ If MN is in the same Sub network as the node, to which it is communicating and HA is on the

other side of the world. It is called triangular routing problem as it causes unnecessary overheads for the network between CN and the HA.

A solution to this problem is to inform the CN of the current location of the MN.

The CN can learn the location by caching it in a binding cache, which is a part of the routing table for the CN HA informs the CN of the location.

It needs four additional messages :-

① Binding Request :-

It is sent by the node that wants to know the current location of an MN to the HA. HA checks if it is allowed to reveal the location and then sends back a binding update.

② Binding Update :-

It is sent by the HA to the CN revealing the current location of an MN. It contains the fixed IP Address of the MN and the CoA. This message can request ACK.

③ Binding ACK :

If requested, a node returns this ack after receiving a binding update message.

④ Binding warning:-

A node sends a binding warning if it decapsulates a packet for an MN, but it is not the current FA for this MN this node sends a building warning. This warning contains MN's home address and target node address.

The following fig shows how the four additional messages are used together if an MN changes its FA.

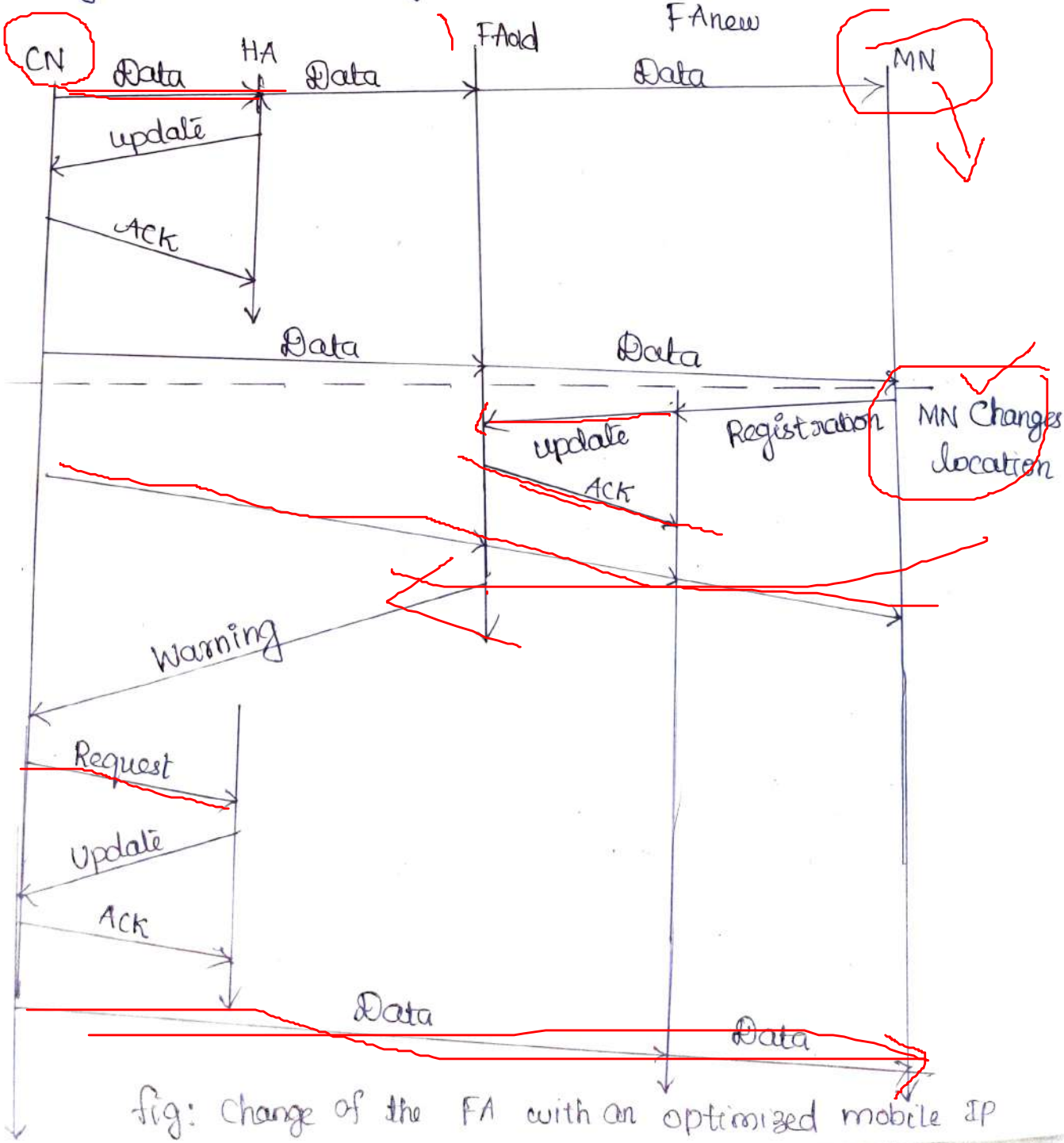


fig: Change of the FA with an optimized mobile IP

⇒ The CN can request the current location from the HA. the HA returns the COA of the MN via an update message and

⇒ The CN acknowledges this update message and stores the mobility binding. Now the CN can send its data directly to the FA old

⇒ FAold forward the packets to the MN

⇒ The MN might now change its location and register with a new foreign agent, this registration is also forwarded to the HA to update its location.

⇒ FAnew informs FAold about the new registration

⇒ Without the information provided by the new FA, the old FA would get to know anything about the new location of MN.

⇒ CN does not know anything about the new location. So it still tunnels its packets for MN to the FAold. Now FAold gives binding warning message to CN.

Tunneling and Encapsulation :-

Explain how tunneling works in general and especially for mobile IP using IP-in-IP minimal, and generic routing encapsulation respectively. Discuss the advantages and disadvantages of these three methods.

(or)

How the tunneling and IP in IP encapsulation occur in mobile IP?

*) A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel end point. packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.

*) Encapsulation is the mechanism of taking a packet consisting a 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.

1. IND - in - IP Encapsulation :-

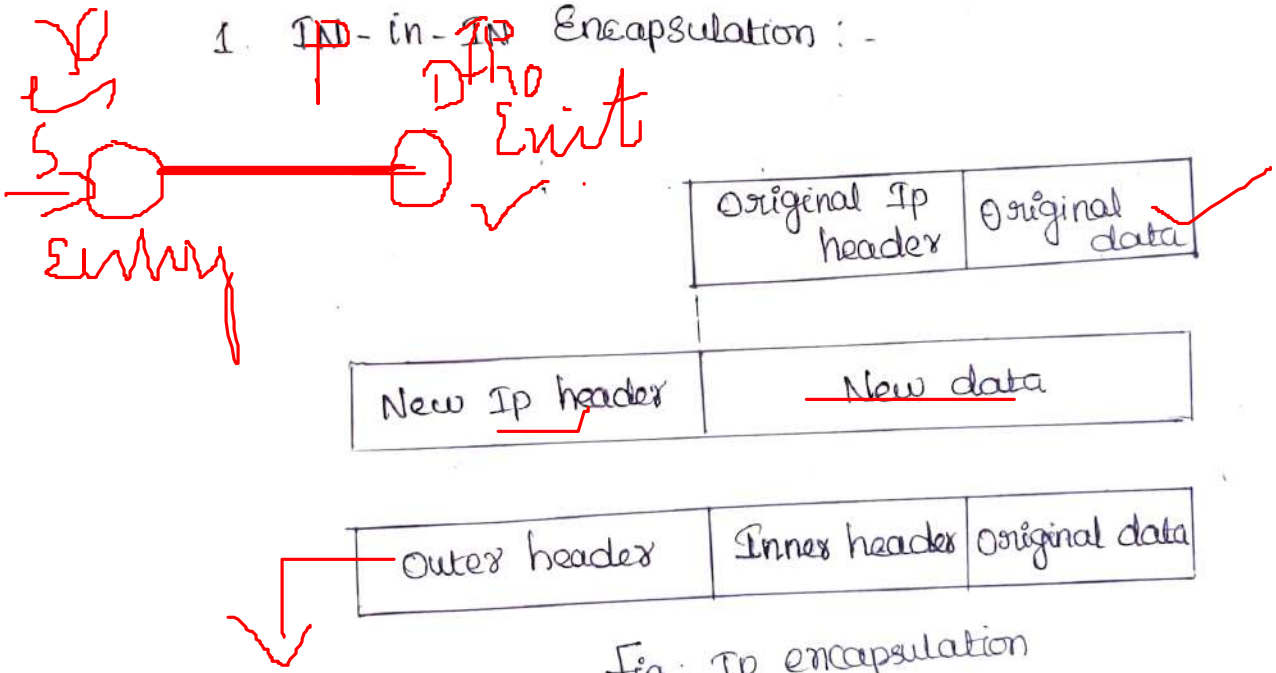


Fig: Ip encapsulation

⇒ 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 so that the packet is routed to the COA. The new header is called outer header.

⇒ Additionally, there is an inner header which can be identical to the orginal header as this in

the case for Ip-in-Ip encapsulation or the inner header can be computed during encapsulation

fig below shows the Ip-Ip encapsulation frame format

Ver	IHL	DS (TOS)	length
Ip identification		flags	fragment offset
TTL	Ip-in-Ip	Ip checksum	
Ip address of HA			
Care of address of COA			
Ver	IHL	DS (TOS)	length
Ip identification		flags	fragment offset
TTL	Lay 4 Prot	Ip checksum	
Ip address of CN			
Ip address of MN			
Tcp/UDP/... Payload			

fig : Ip-in-Ip encapsulation

Version : It denotes the Ip version 4

Internet header length : It specify the length of the outer header in 32-bit words.

DS (TOS) : It is just copied from the inner header

length : The length field covers the encapsulated packet

TTL : It define the packet can reach the tunnel end point

IP-in-IP : It is the type of the protocol used in the IP payload.

*) IP checksum is calculated as usual. The next fields are the tunnel entry as source address and the tunnel exit point as destination address.

*) The inner header remains almost unchanged during encapsulation original sender CN and the tunnel receiver MN of the packet. ⇒ DTO !!!

*) The only change is TTL which is decremented by 1. This means that the whole tunnel is considered a single hop from the original packets point of view.

2. Minimal encapsulation:

⇒ It is an optional encapsulation method of mobile IP fig below shows the minimal encapsulation method.

⇒ In this case, the field for the type of the following header contains the value of 55 for the minimal encapsulation protocol.

⇒ If the S bit is set, the original sender address of the CN in included as omitting the source is quite often not an option.

⇒ No field for fragmentation offset is left in the inner header and minimal encapsulation does not work with already fragmented packets.

12

Ver	IHL	DS(TOS)	length	
Ip identification			flags	fragment offset
TTL	min-encap		Ip Checksum	
Ip address of HA				
CoA of CoA				
lay.4.Proto	S	reserved	Ip Checksum	
Ip address of MN				
TCP/UDP .... payload.				

3. Generic routing encapsulation: -

It allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.

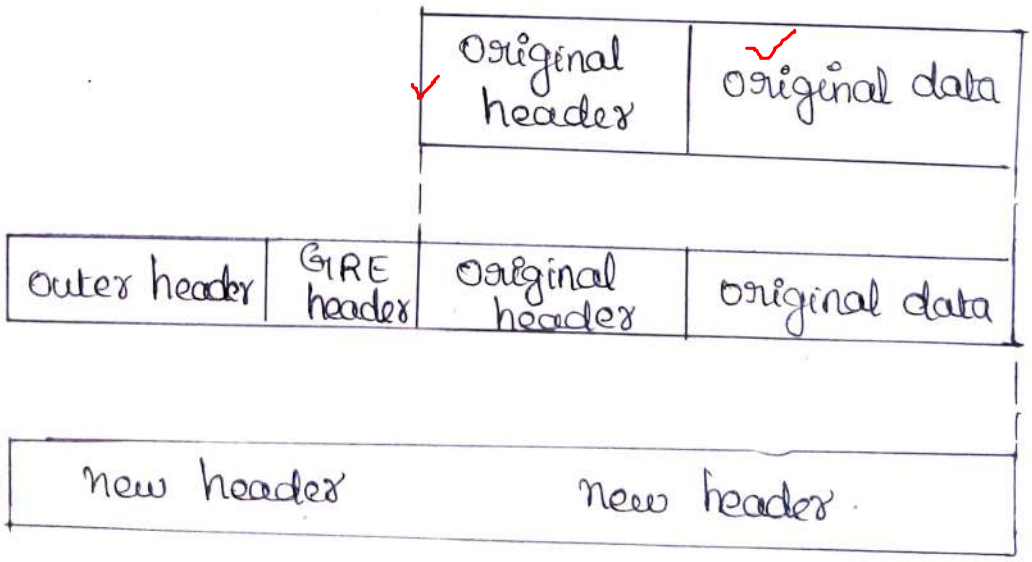


fig: GRE.

⇒ The outer header is the standard Ip header with HA as source address and COA as destination address

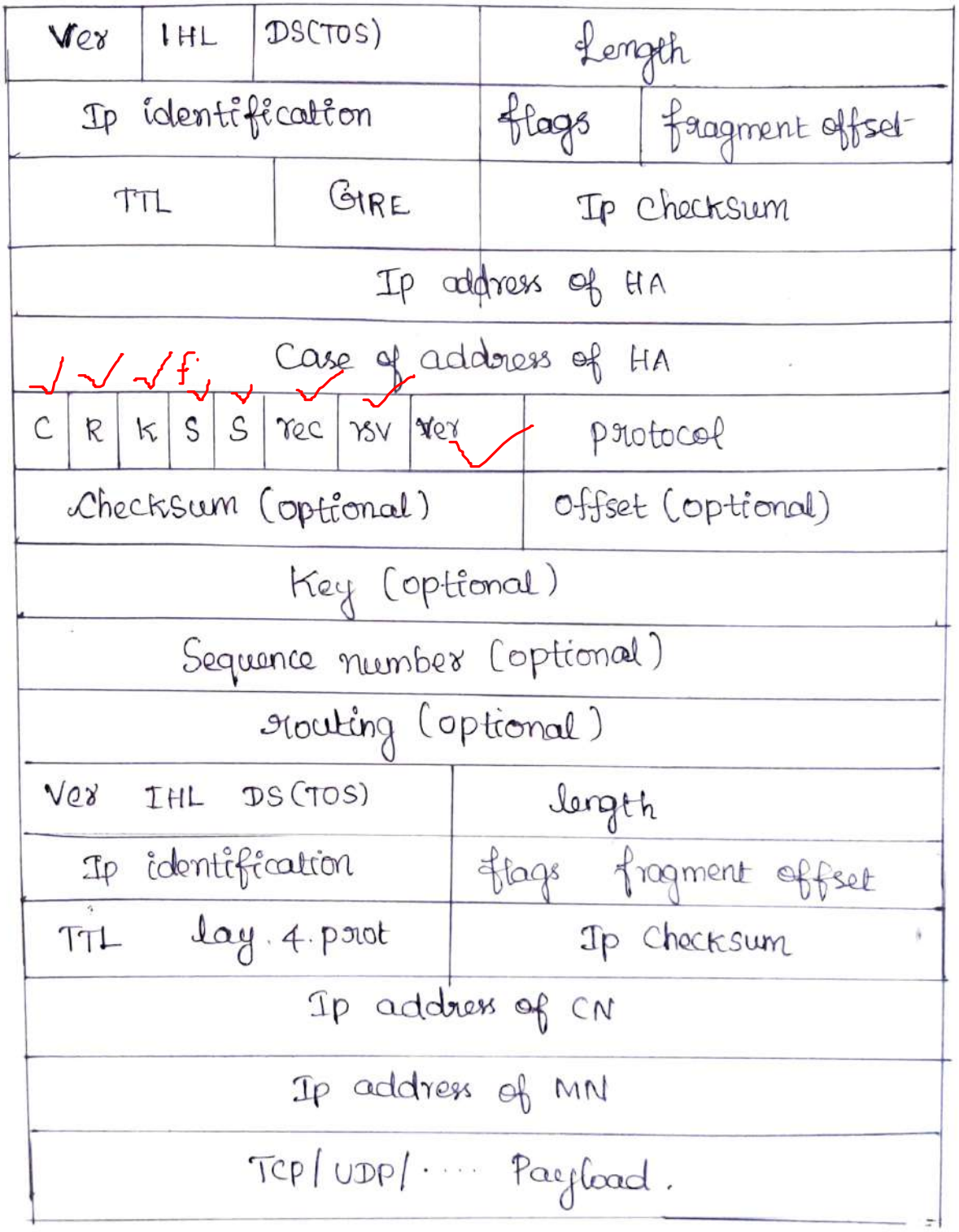


fig : Protocol field for GRE

C bit : It indicate if the checksum field contains a valid Ip checksum of the GRE header and the payload.

R bit : It indicates if the offset in bytes for the first and routing fields are present and contain valid information.

Offset: The offset represents the offset in bytes for the first Source routing entry.

Checksum: R bit is Set Checksum field must be present

Key: Key field may be used for authentication. If this field is Present, the K bit is present Set.

Sequence Number: The Sequence number bit S indicates if the Sequence number field is present

Routing: If the S bit is Set Strict Source routing is done

recursion field: It represents a Counter that shows the number of allowed recursive encapsulation.

If the field is not zero, additional encapsulation is allowed the packet is encapsulated and the field decremented by 1.

Reserved: This field must be zero and are ignored on reception.

Ver: The version field Contain 0 for the GRE.

Protocol: It represent the protocol of the packet

*) Reverse tunneling :-

Explain packet flow if two mobile nodes Communicate and both are in foreign networks. What additional routes do packets take if reverse tunneling is required? (6m)

(or)

Explain the reverse tunneling technique used in WLAN? (6m)

The MN can directly send its packets to the CN as in any other standard IP situation. The destination address in the packets is that of CN. But there are several severe problems associated with this simple solution.

*) Firewalls

Firewalls are designed to only allow packets with topologically correct addresses to pass to provide simple protection against misconfigured system of unknown address.

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

Firewall after filter packets coming from outside containing a source address from internal network.

*) Multicast :-

→ Nodes in the home network might participate in a multicast group, an MN in a foreign network cannot transmit multicast packets in a way that they emanate from its home network. without a reverse tunnel. The foreign network might not even provide the technical infrastructure for the multicast communication.

TTL :

If the MN moves to a new foreign network, the older TTL might be too low for the packets to reach

the same destination nodes as before. mobile Ip is no longer transparent if a user has to adjust the TTL while moving. A reverse tunnel is needed that represents only one hop, no matter how many hops are really needed from the foreign to the home network.

IPV6 :

Explain in detail about IpV6 micro-mobility support?

(or)

What advantages does the use of IpV6 offer for mobility? Where are the entities of mobile Ip now?

(or)

Explain in detail about approaches used in micro-mobility problem.

IpV6 Advantages :-

*) IpV6 network requires very few additional mechanism of CN, MN & HA

*) A CN only has to be able to process binding updates

*) The MN itself has to be able to decapsulate packets, to detect when it needs a new CoA and determine when to send binding updates to the HA & CN

*) HA must be able to encapsulate packets IpV6 does not solve any firewall or privacy problems. Additional mechanisms on higher-layer are needed for this.

(i) Ip micro-mobility Support :-

Assuming a large number of mobile devices changing networks quite frequency, a high load on the home agents as well on networks is generated by registration and binding updates messages.

*) Ip micro-mobility protocols can complement mobile Ip by offering fast and almost seamless handover Control is limited geographical areas.

There are three approaches are used to solve the micro-mobility problem. They are.

① Cellular Ip
② HAWAII
③ Hierarchical mobile Ip (HMIP)

① Cellular Ip :

Cellular Ip provides local handovers without registration by installing a Single Cellular Ip gateway (CIpGw) for each domain

*) For accessing MN's based on the origin of packets all nodes collect routing information.

*) With respect of lower layer protocols, a mobile node moving between adjacent Cells with temporarily be able to receive packets via both old and new base station.

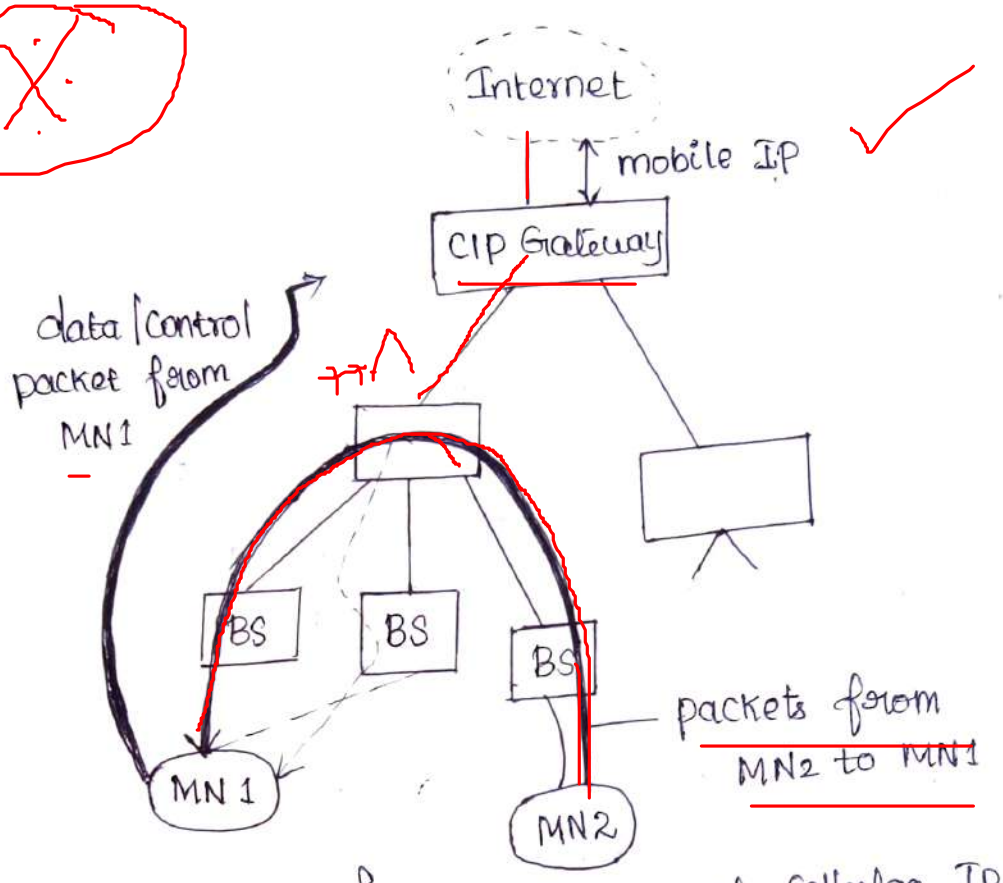


fig: Architecture of Cellular IP.

Advantages:-

Initial registration involves authentication of MNs and is processed centrally by CIP Gateway.

*) All Control messages by MNs are authenticated.

*) Simple and ~~elegant~~ architecture.

*) Mostly Self Configuring.

*) Integration with firewalls / private address support possible.

Disadvantages:-

*) Efficiency: Additional network load is induced by forwarding packets on multiple paths.

Transparency :- Changes to MNs are required.

Security : Routing tables are changed based on message sent by mobile nodes.

HAWAII :

HAWAII (Hand off - Aware wireless Access Internet Infra-Structure)

tries to keep micro mobility support as transparent as possible for both home agents and mobile nodes.

Operation :-

On entering an Hawaii domain, a mobile node obtains a Co-located CoA and registers with the HA.

*) Additionally When moving to another cell inside the foreign domain, the MN sends a registration request to the new base station as to a foreign agent, thus mixing the Concepts of Colocated CoA and foreign agent CoA.

*) The base station intercepts the registration request and sends out a handoff update message, which configures all routers on the path from the old and new BS, to the So-Called Crossover router.

*) After the successful routing, BS sends a registration reply to the MN.

Advantages :-

*) Security : Challonge - response extensions are mandatory.

*) Transparency : Hawaii is mostly transparent to mobile nodes.

Disadvantages :-

*) Security : There are no provisions regarding the set up of IpSec tunnels

*) Implementation : No private address support is possible

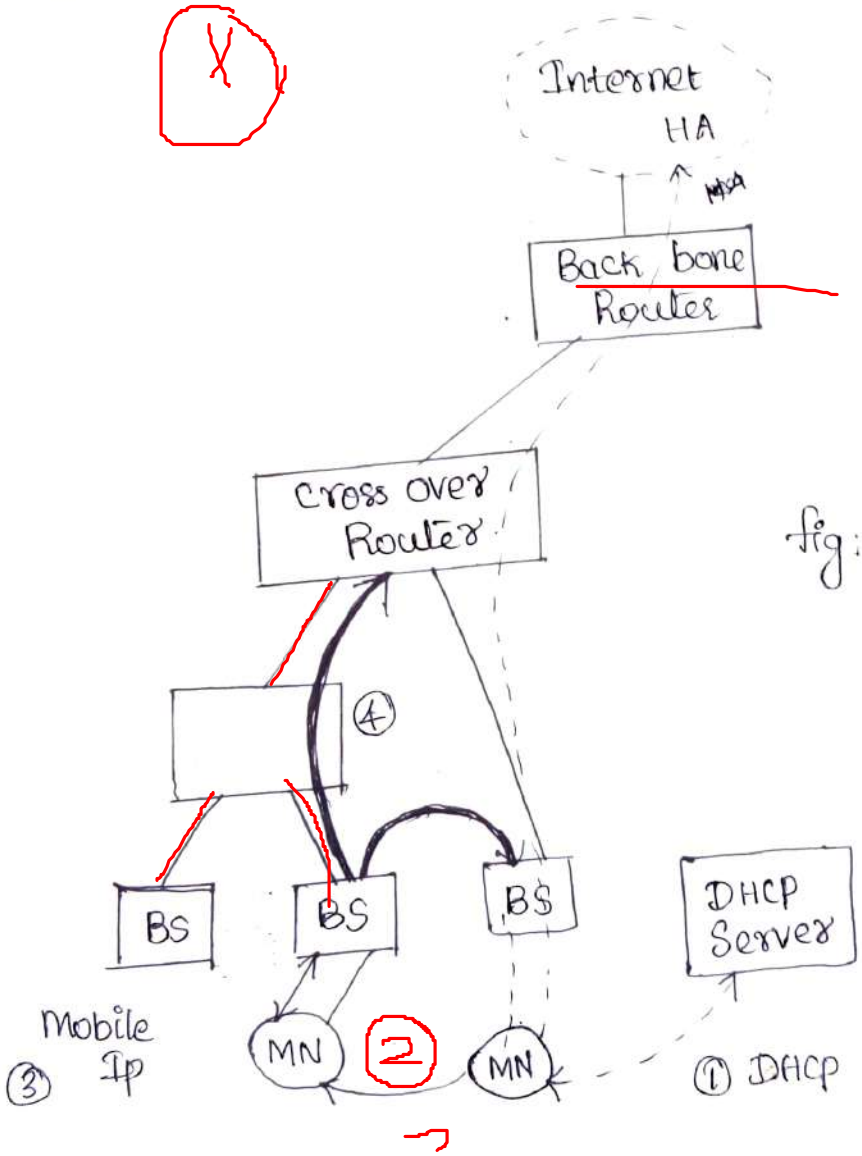


fig: Basic Architecture of HAWAII

③ Hierarchical mobile IPV6 (HMIPV6)

HMIPV6 provides micro-mobility support by installing a mobility Anchor point, which is responsible for a certain

domain act as a local HA, within this domain for the visiting MNs.

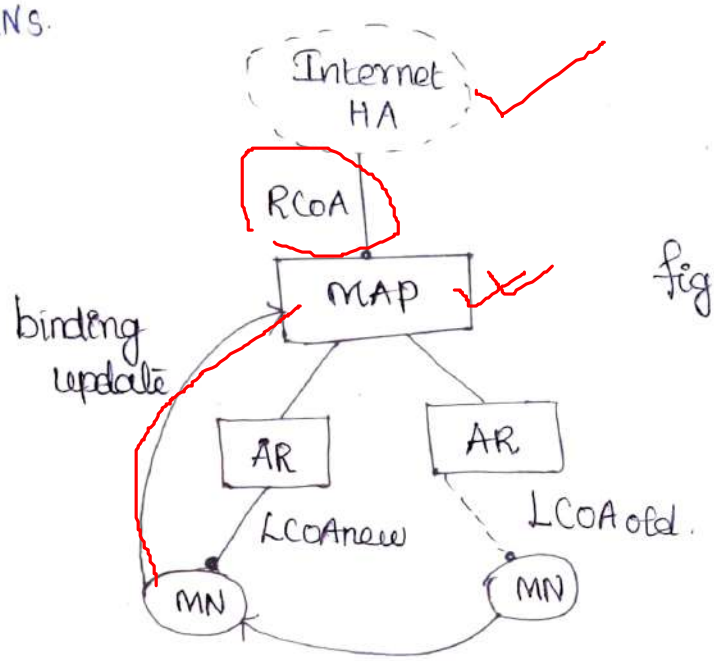


fig: Basic architecture of HMIP

→ The MAP receives all packets on behalf of the MN, encapsulates and forwards them directly to the MN's current address.

→ A MAP domain boundaries are defined by the access router (AR) advertising the MAP information to the attached MN's mobile node register their RCOA with the HA using a binding update when a MN moves locally it must only register its new LCOA with its MAP.

⇒ The RCOA stays unchanged To support smooth hand overs between MAP domains, an MN can send a binding update to its former MAP.

Advantages:-

*) Security : MNs can have location privacy because LCOAs can be hidden.

*) Efficiency : Direct routing between CNs sharing the same link is possible.

Disadvantages :-

*) Transparency : Additional infrastructure Component

*) Security : ~~Direct~~ routing tables are changed based on messages sent by mobile nodes.

Dynamic host Configuration protocol (DHCP) :

a) What is the basic purpose of DHCP ? Name the entities of DHCP.

(or)

How Can DHCP be used for mobility and support of mobile IP ?

(or)

State the concepts used in Dynamic Host Configuration protocol technique.

(i) Basic configuration in DHCP :-

The dynamic host Configuration protocol is mainly used to simplify the installation and maintenance of networked computers.

If a new Computer is connected to a network. DHCP Can provide it with all the necessary information for full system integration into the network.

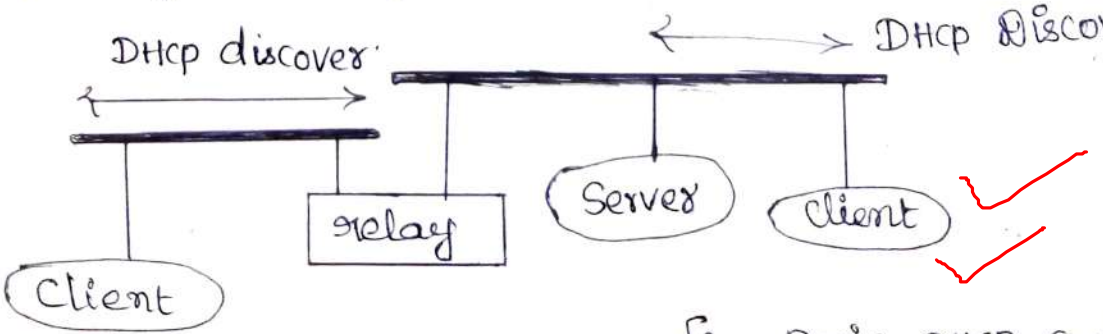


fig : Basic DHCP Configuration

*) DHCP clients send a request to a server to which the server responds. A client sends request using MAC broadcast to reach all devices in the LAN.

*) DHCP relay might be needed to forwards requests across intercowking units to a DHCP Server.

(ii) DHCP initialization :-

⇒ Here client broadcasts DHCP DISCOVER into the Subnet.

⇒ Servers that receives this broadcast determine the configuration they can offer to the client.

⇒ Server replies to the client request by sending DHCPOFFER and offers a list of configuration parameters.

⇒ Client chooses one of the configuration offered and rejects other using DHCP REQUEST.

⇒ If a Server receives a DHCP REQUEST with a rejection, it can free the reserved configuration for other possible clients.

⇒ The server with the configuration accepted by the client now confirms the configuration using DHCPACK. This completes the initialization phase.

⇒ When client leaves the Subnet it release the configuration it has received using DHCPRELEASE.

⇒ The configuration the client received is to be reconfirmed periodically else the server will free the configuration.

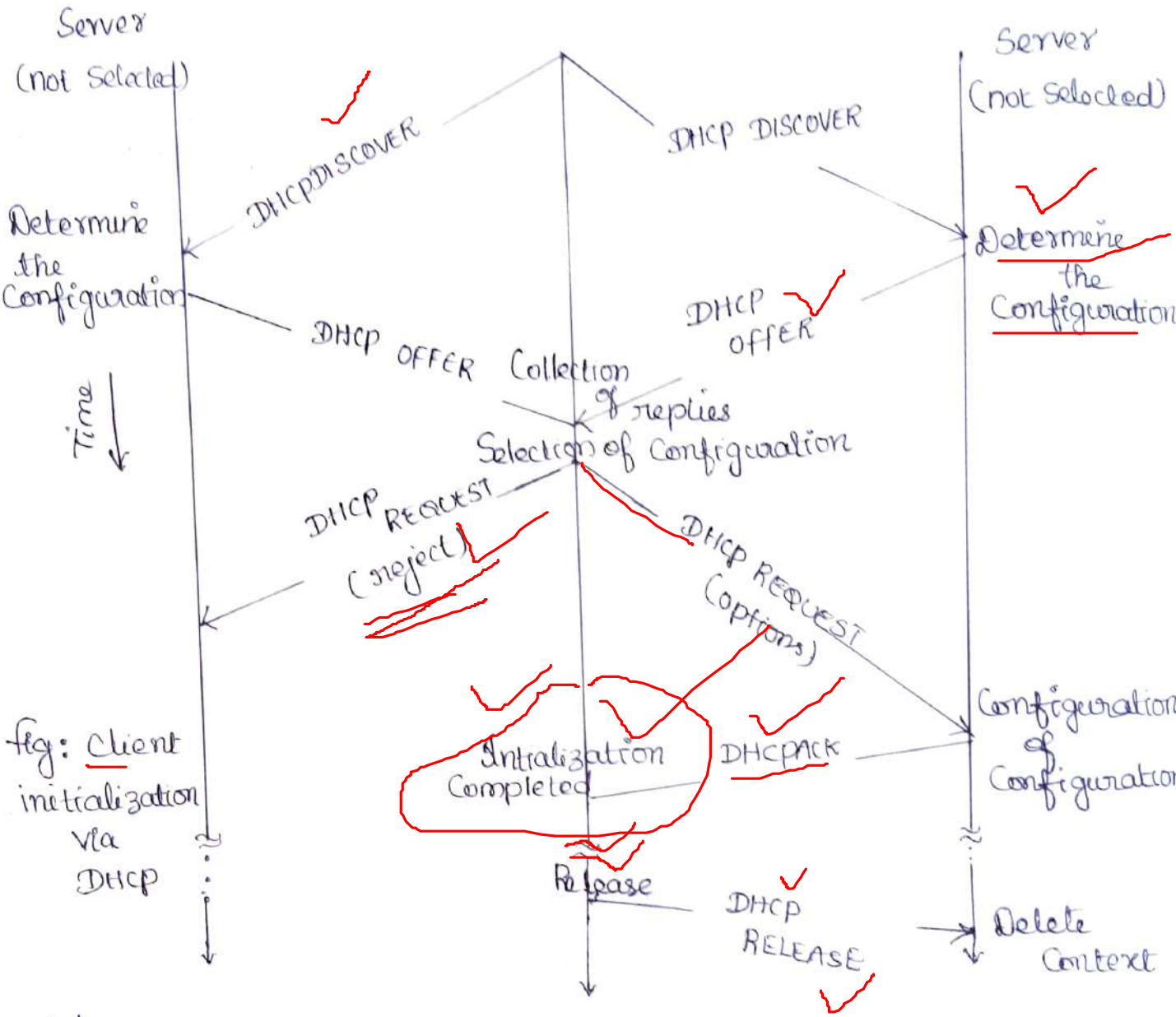


fig: Client initialization via DHCP

Advantages of using DHCP:

* DHCP is included with popular Server packages There is no additional Costs to implement DHCP

*) Centralization, Simpler management of Ip addressing.

*) Duplicate Ip addresses are prevented also preserved, DHCP Servers only allocate Ip addresses to clients when they request them.

** Disadvantages of using DHCP:-

*) The DHCP Server can be Single point of failure

in networking environments that only have one DHCP Server

*) All incorrectly defined Configuration information will automatically be propagated to DHCP clients.

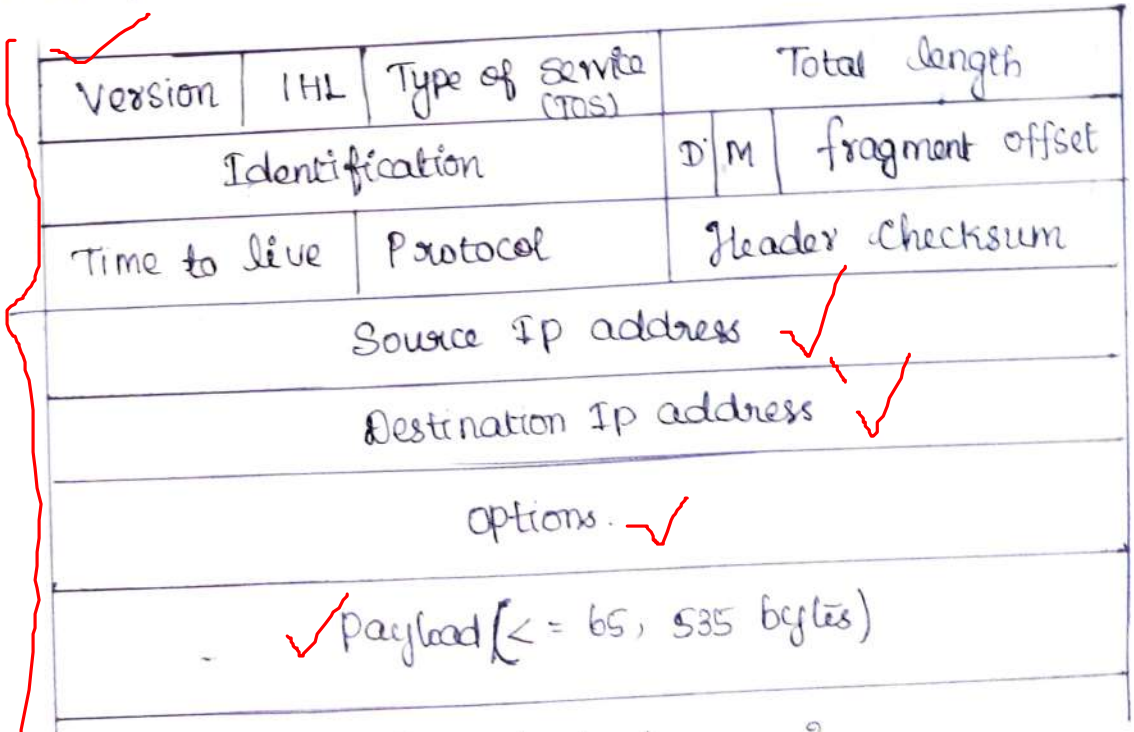
Network layer in the Internet:

Analyse all possible Soulutions to be adopted for given mobility Support in the network layer such that both delay contraints along with throughput level achieved.

(or)

Explain in detail about Network layer in the internet.

The internet protocol provided the basic for the interconnections of the internet. Ip is a datagram protocol and its packet Contain an Ip. header



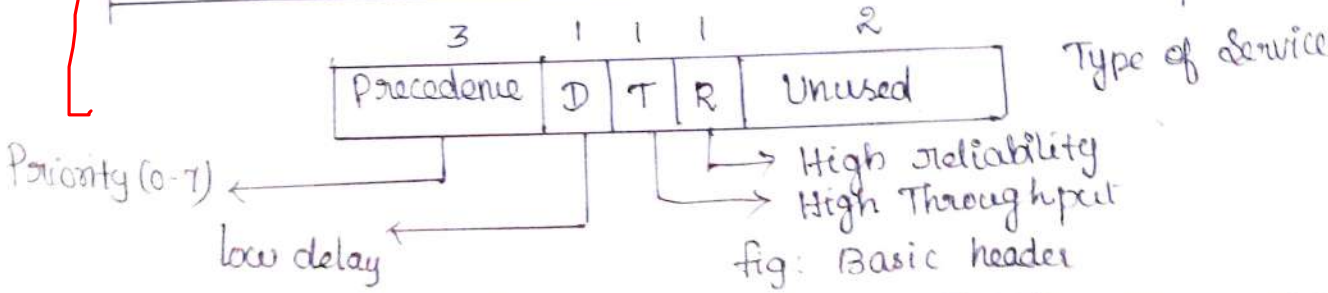


fig: Basic header

Ver : The Version field Contains the version of IPv4 or IPv6

Internet Header length :

It specifies the actual length of the header in multiples of 32 bit words.

Type of Service field :

It allows an application protocol / process to specify the relative Priority of the application data.

It is used by each gateway and router during the transmission and routing of the packets to transmit packets of higher Priority first.

Total length :

It defines total length of the initial diagram including the header and payload parts.

Identification :

It enables the destination host to relate each received packet fragment to the same original datagram.

D-bit :

Don't fragment It indicates that the packet should not be fragmented.

M-bit :

More fragment - multiple Smaller packets.

-fragment offset :

It indicates the position of the first byte of the fragment Contained with in a Smaller packet in relation to the original packet pay load.

Time to live:

It defines the maximum time for which a packet can be is transmit across the internet.

Protocol:

It is used to enable the destination Ip to pass the payload with in each received packet to the same protocol that sent the data.

Header checksum:-

⇒ It can be applied to the header part of the datagram and it is a safe-guard against corrupted packets being routed to incorrect destinations.

Source and Destination Ip address:

The source and destination internet addresses indicate the sending and recipient host.

Option field:

It is used in selected diagrams to carry additional information relating to security, source routing.

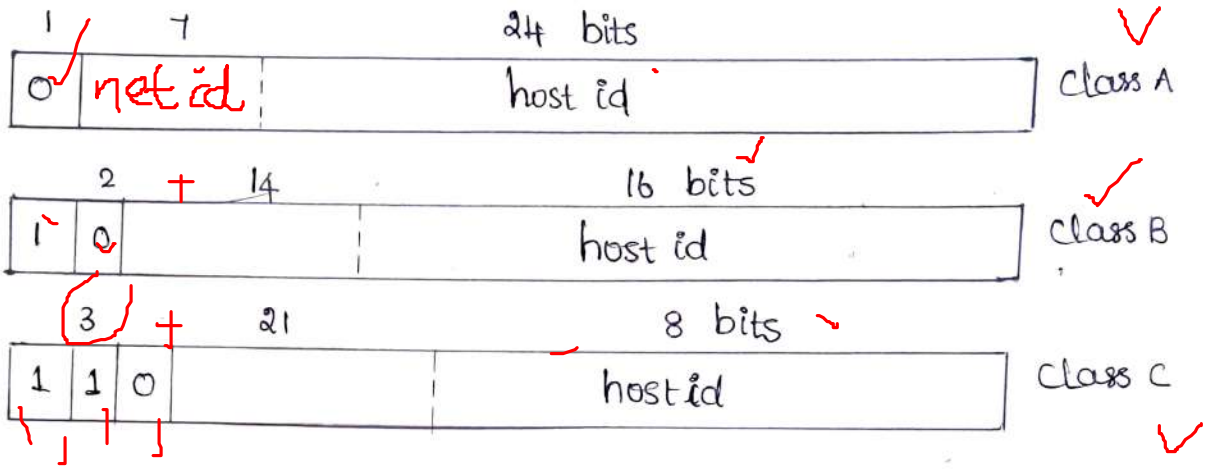
(1) Internet Address:

There are three classes of internet addresses.

1. Class A: It has 7 bits for net id and 24 bits for host id, they are used with networks having large number of hosts.

2. Class B: It has ~~14 bits~~ for net id and 16 bits for host id, they are used with networks having a medium number of hosts.

3. Class C - It has 24 bits for net id and 8 bits for host id, they are used with networks having a small number of hosts.



Look back address :-

Class A address with a net id of all 1's is used for test purposes within the protocol stack of the source host. It is known as the look-back address.

(ii) Ip adjunct protocols :-

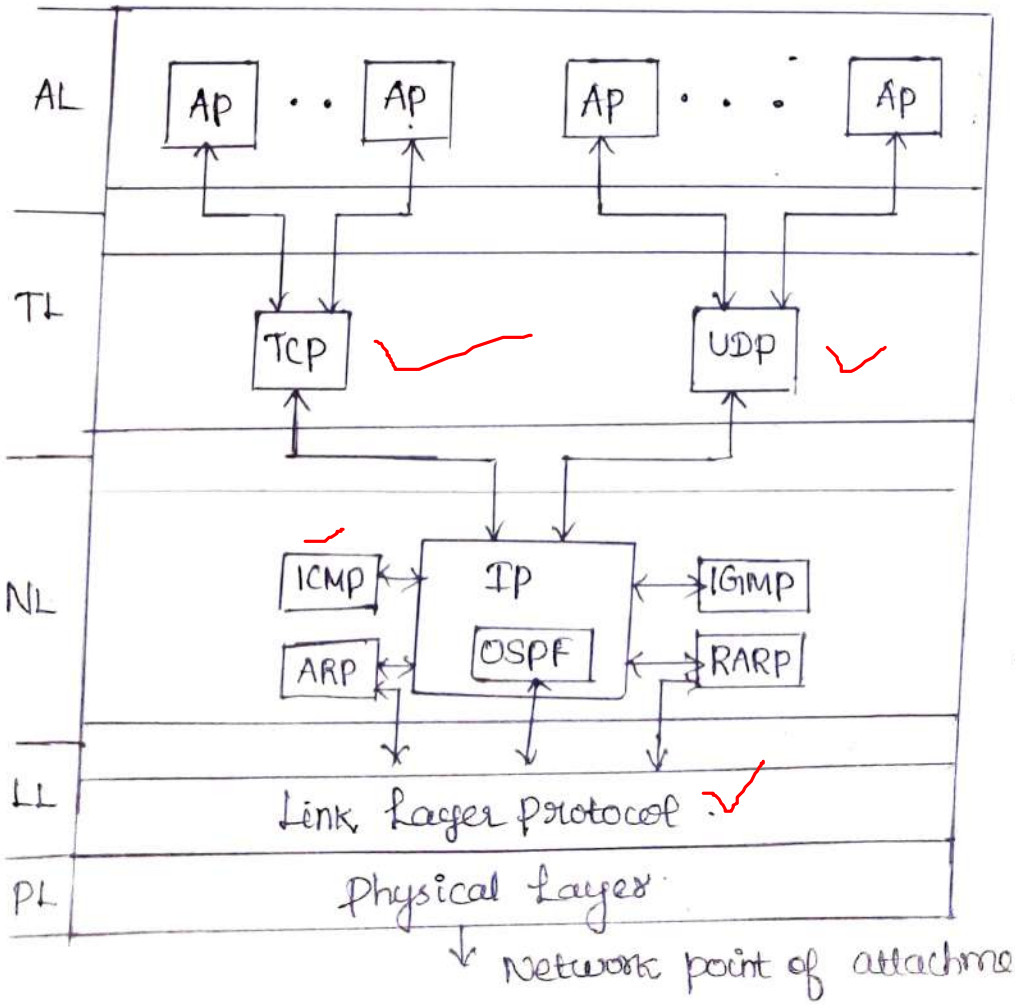


fig : Network Ip adjunct point

Address Resolution protocol (ARP) and Reverse ARP (RARP):

Two sections are used by Ip in hosts that are attached to a broadcast LAN in order to determine the physical MAC address of a hosts or gateway given its Ip address and in case of RARP.

Open Shortest path first (OSPF).

It is a routing protocol used in the global internet work Such protocols are present in each internetwork router.

Internet Group message protocol (IGMP)

It can be used with multicasting to enable a host to send a copy of a datagram to the other hosts.

Internet Control message protocol (IGMP)

It can be used by the Ip in a host or gateway to exchange errors and offer control messages with Ip in another host or gateway.

Link control protocol can run during initial link establishment and negotiates link level parameters.

Ip control protocol establishes the Ip address of the client and negotiates for the use of Tcp/Ip header compression.

Qos Support in the internet :

Qos requirements can includes a defined minimum mean packet throughput rate and maximum end-to-end packet transfer delays.

1. Integrated Services :

It has three different classes of services.

*) Guaranteed :

⇒ Specifies maximum delay and jitter and an assured level of bandwidth is guranteed.

*) Controlled Load :

⇒ predictive, no firm gurantee is provided but the flow obtains a constant level of service.

*) Best effort :

⇒ Intended for text based application.

2. Differentiated Services :

The TOS field in the Ip packet header is replaced by a net field called the differentiated service field.

*) A defined level of resources in terms of buffer space with in each router and the bandwidth of each output line is allocated to each traffic class.

Mobile Ip Session initiation protocol :

Explain in mobile Ip Session initiation protocol for mobile Ip packet delivery in mobile Ip networks ?

(or)

Explain in detail about mobile Ip Session initiation protocol :

Third orientation mobile networks are designed to provide a variety of Ip data services such as voice over Ip and instant messaging.

*) The Session initiation protocol is the key to realizing and provisioning services in Ip based mobile networks.

*) The need for mobility of future real time service independent of terminal mobility can require S/p to be seamlessly interwork with M/p operations.

The Ip address serves following purpose

→ For routing packets through the internet

→ An end point identifier for applications in end hosts.

Mobile Ip capabilities :-

1. Registration
2. Discovery
3. Tunneling

1. A mobile node uses an authenticated registration procedure to inform its HA of its COA.

2. A mobile node uses a discovery procedure to identify a prospective home agent and FA.

3. Tunneling is used to forward Ip datagrams from a home address to a COA.

SIP

~~S/p~~ is a signalling protocol used to Create modify and terminate a multimedia session over the internet protocol.

SIP

s/p network elements :-

1. User agent :

It is the endpoint and one of the most important network elements of a s/p network.

An endpoint can initiate, modify or terminate a session user agents are locally divided into two parts.

User agent client - The entity that sends a request receives a response.

User agent server - The entity that receives a request and sends a response.

2. Proxy Server :

It is the network element that takes a request from a user agent and forward it to another user. There can be a maximum of 70 proxy servers in between a source and a destination.

Stateless proxy server :

It simply forwards the message received. It does not store any information of a call or a transaction.

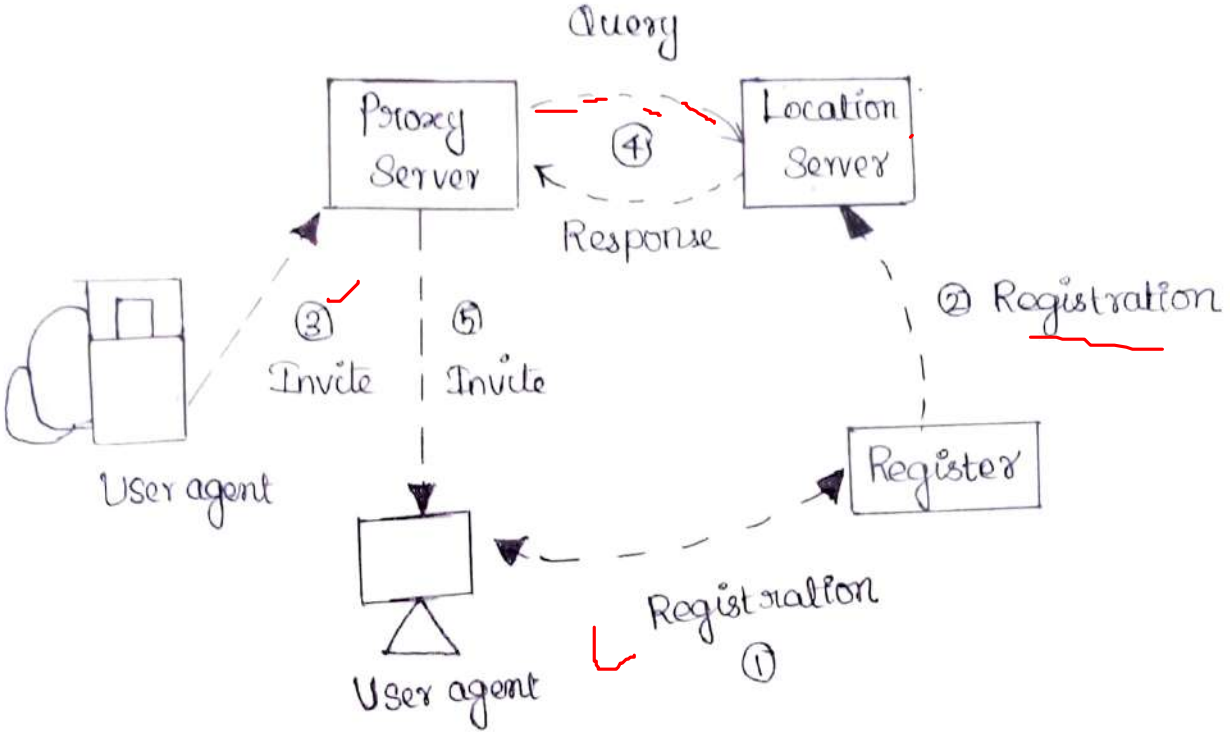
Stateful proxy server :-

This type of proxy server keeps of every request and response received and can use it in future if required.

3. Registrar Server:

It accepts registration requests from user agent and authenticate themselves with in the network.

⇒ It stores the URI and the location of users in a database to help after S/p Servers with in the same domain.



4. Redirect Server:

⇒ It receives requests and look up the intended recipent of the request in the location data base created by the registrar.

⇒ The redirect Server uses the data base for getting location information and responds with 3xx to the user.

5. Location Server:

The location Server provides information about a Caller's possible location to the redirect and Proxy Servers.

Only a proxy or a redirect server can contact a location server.

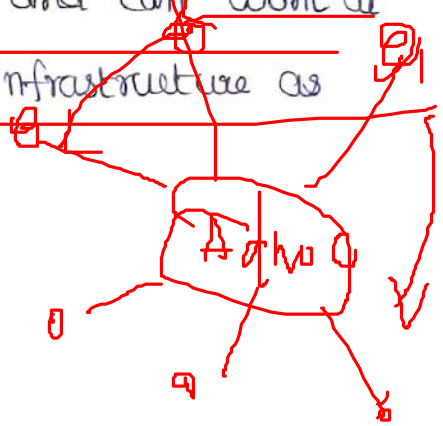
Mobile Ad-hoc networks :-

Explain in detail about mobile ad hoc networks and its characteristics?.

(or)

Explain in detail about independent infrastructure networks?

⇒ A mobile ad hoc network is a collection of independent mobile nodes that can communicate with each other via radio waves.



These networks are fully distributed and can work at any place without the help of any fixed infrastructure as access point or base stations.

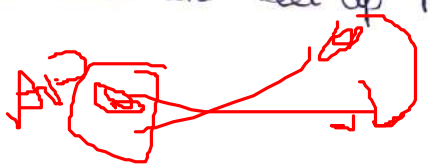
Characteristics of mobile ad hoc network :-

(i) Instant infrastructure :-

Unplanned meetings, spontaneous interpersonal communication cannot rely on any infrastructure.

(ii) Disaster relief :-

Infrastructures typically breakdown in disaster areas, no forward planning can be done and the set up must be extremely fast and reliable.



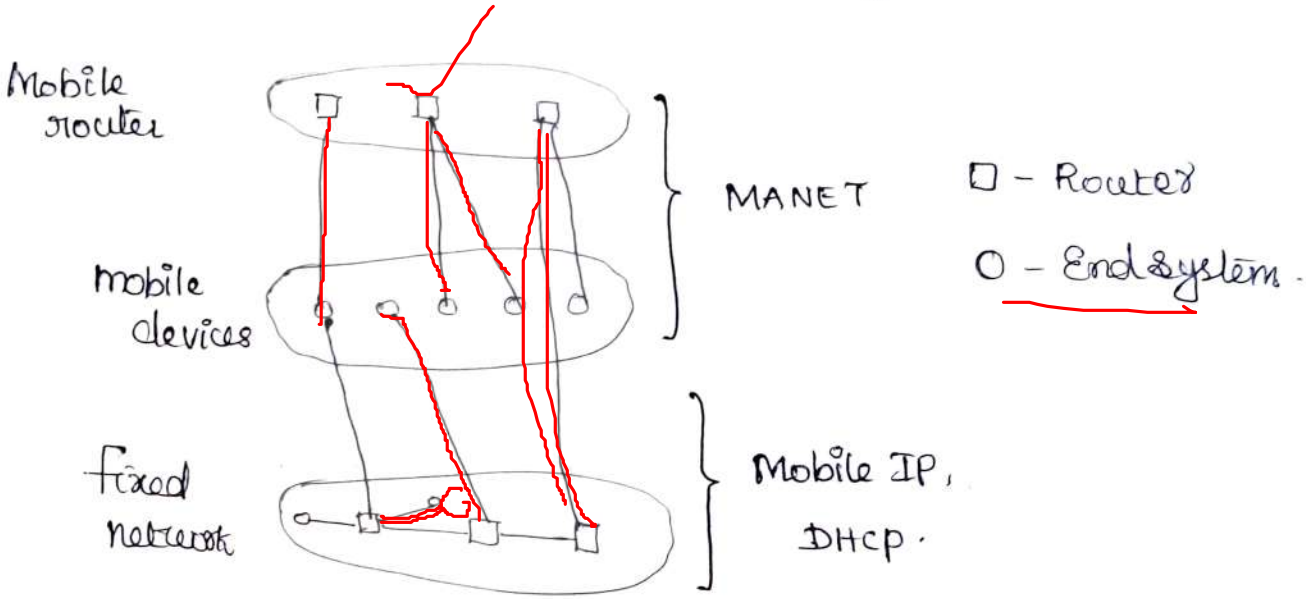
(iii) Remote areas :

Even if infrastructure could be planned ahead, it is some times too expensive to set up an infrastructure

in Sparsely populated areas.

(iv) Effectiveness

Service provided by existing infrastructure might be too expensive for certain applications. Registration procedures might take too long and Communication overheads might be too high with existing networks.



over the last few years adhoc networking has attached a lot of research interest. This has led to Creation of a working group the IETF that is focusing on mobile ad-hoc networking called MANET.

Fig above shows the relation of MANET to mobile IP and DHCP mobile devices can be Connected either directly with an infrastructure using mobile Ip for mobility support and DHCP as a source of many paramaleers, such as an Ip address.

One of the first ad hoc wireless networks was the packet radio network started by ARPA in 1973. It allowed up to 138 nodes in the ad-hoc networks and used IP packets for data transport

Routing:

Explain in detail about Routing ?

(or)

Explain routing with example network ?

⇒ Routing is needed to find a path between source and destination and to forward the packet appropriately.

In wireless networks using an infrastructure, cells have been defined with in a cell the base station can reach all mobile nodes without routing via broadcast.

In ad-hoc networks each node must be able to forward data for other nodes.

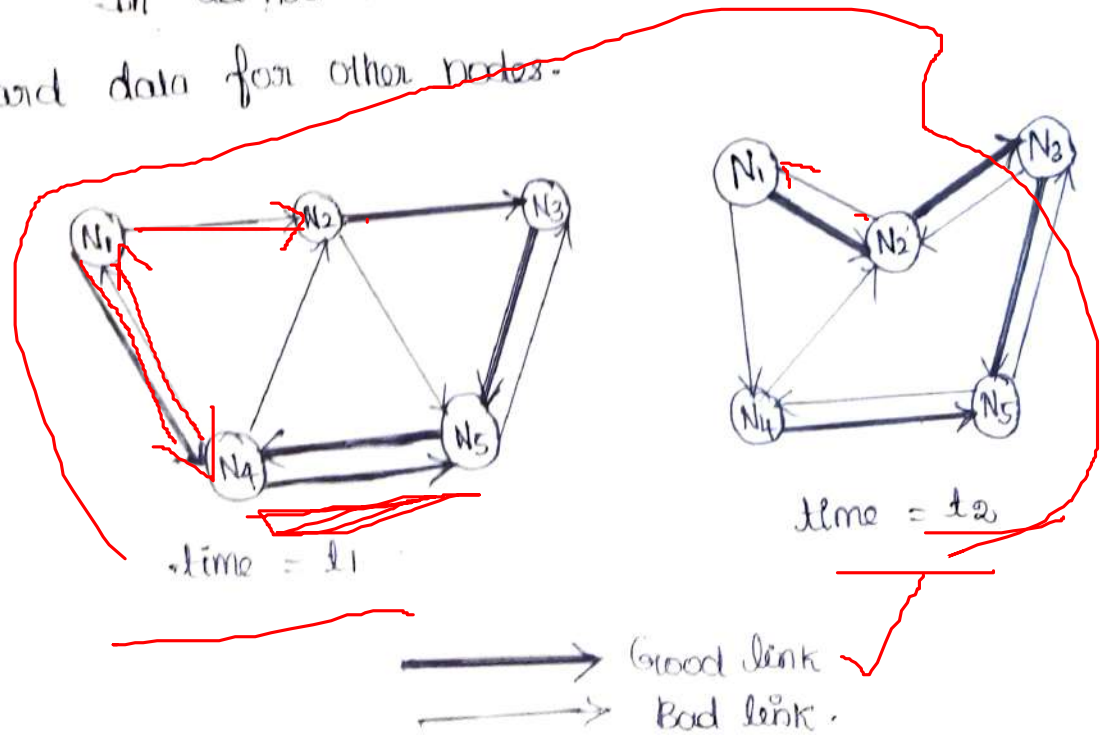


Fig: Example ad-hoc network

At a t_1 time the network topology, five node N_1 and to N_5 are connected depending on the current transmission characteristics between them.

⇒ In this network N_4 can receive N_1 over a good link but N_1 receives N_4 only via a weak link. links do not necessarily have the same characteristics in both directions.

N_1 cannot receive N_2 at the all but N_2 receives a signal from N_1 At a t_2 time, N_1 cannot receive N_4 any longer but N_4 receives N_1 only via a weak link. Now N_1 has a asymmetric but bidirectional link to N_2 that did not exist before.

→ Some fundamental differences between wired network and ad-hoc wireless networks related to routing (4 m).

(i) Asymmetric links :-

*) Node A receives a signal from node B

*) But this does not tell us anything about the quality of the connection in reverse.

*) B might receive nothing, have a weak link or even have a better link than the reverse direction.

*) Routing information collected for one direction is of almost no use of other connection.

(ii) Redundant links :-

→ In wired network redundant link to survive

link failures which additionally controlled by a network administrator.

In adhoc networks no control over the redundancy links

(iii) Interference :

In wired, network links exist only where a wire exists and connections are planned by the network administrators.

In adhoc, one transmission can interfere with another nodes can overhead the transmission of other nodes.

(iv) Dynamic topology :-

In wired network, frequent changes in topology So it valid only for a very short period of time.

In adhoc network routing tables must reflect the frequent changes in topology and routing algorithm have to be adopted.

Destination Sequence distance Vector (DSDV)

a) Explain with neat diagram and example the destination sequence distance vector routing algorithm of Ad-hoc networks ?

(or)

Explain with neat diagram DSDV algorithm

(or)

Explain with neat diagram proactive (or) table driven protocol ?

Destination Sequence distance Vector (DSDV) routing is an enhancement to distance Vector routing for ad hoc network.

It is used as routing information protocol (RIP) in wired networks. Each node changes it neighbour table periodically with its neighbours changes at one node in the network propogate slowly through the network that is step by step with every exchange.

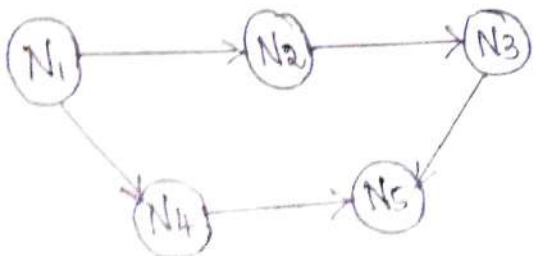
1. Sequence number:

Each routing advertisement comes with a sequence number within adhoc networks, advertisements may propagate along many paths sequence numbers help to apply the advertisements incorrect order.

2. Damping:

Advertisements containing changes in the topology currently stored or not disseminated further. A node waits with dissemination if these changes are probably unstable. Waiting time can depend on the time between the first and the best announcement of a path to a certain destination.

Example:



The routing table for N_1 node as.

Destination	Next hop	Metric	Sequence No	Instal time
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	$S_5 - 163$	$T_4 - 002$

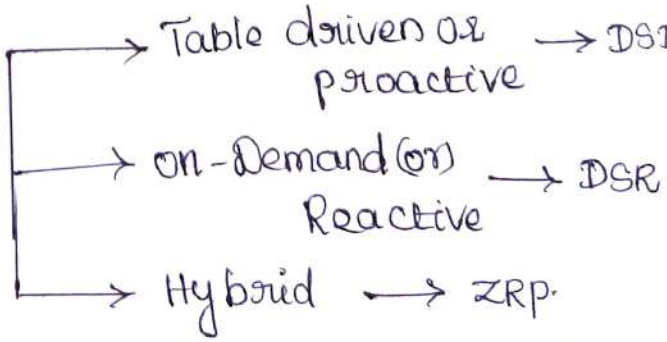
$\Rightarrow$ For each node N_1 stores the next hop toward this node, the metric (here number of hops), the Sequence number of the last advertisement for this node, and the time at which the path has been installed first. The table Contains flags and a setting time helping to decide when the path can be assumed Stable.

Give the classification of ad-hoc routing protocols.

(or)

Discuss about proactive and reactive.

Adhoc routing protocols



a) Proactive (or) Table driven:

It's attempt to maintain Consistent, up to date routing information between every pair of nodes in the network by propogating proactively, route updates

at fixed intervals As a resulting information maintained in tables eg DSDV.

b) On-demand (or) Reactive:

⇒ It's depart from the legacy of internet approach.

*) It establish a route to a destination when there is a demand for it, Usually initiated by the source node through discovery process with in the network. Once a route has been established it is maintained by the node untill the destination becomes inaccessible.

IOT: COAP [Constrained Application protocol]

Explain in detail about COAP?

(or)

Explain in detail about Constrained Application protocol?

⇒ The COAp is an application layer protocol developed by IETF Core working group.

It is designed for Constrained environments based on a REST. Style architecture, to protocol considers the Various objects in the network as resources.

⇒ COAP Protocol was designed to look like and be Compatible with hypertext Transfer protocol. (HTTP)

CoAP protocol stack :-

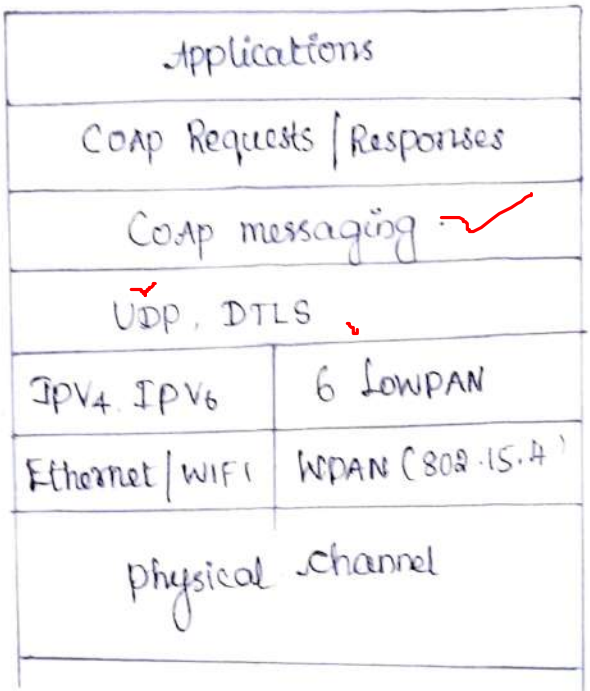


fig : CoAP protocol stack

PHY / MAC Layer :

⇒ It involves all common wireless communication technology such as IEEE 802.11, IEEE 802.15.4 (Zigbee, wireless HART).

Network / Communication Layer :

*) TCP / IP lay the foundation for the internet thus IOT communication network mainly employ TCP & UDP protocols.

*) Compared with UDP, TCP as more complex, which makes it not easy to employ on resource constrained devices. ∴, IOT use UDP protocol.

DTLS → Datagram Transport Layer Security : It achieves necessary elements for securing CoAP, like integrity, Authentication & Confidentiality also it provide end-to-end communication.

Message Layer It has been designed to deal with UDP and Synchronous switching.

It can supports 4 type of message

① CON (Confirmable)
② NON (non-Confirmable)
③ Ack (Acknowledgement)
④ RST (Reset)

a) Reliable message Transport :-

→ Keep retransmission until get Ack with same message ID (in fig 0x8c56).

→ Using default time out and decreasing counting time exponentially when transmitted CON. It recipient fail to process message, it responses by replacing Ack with RST.

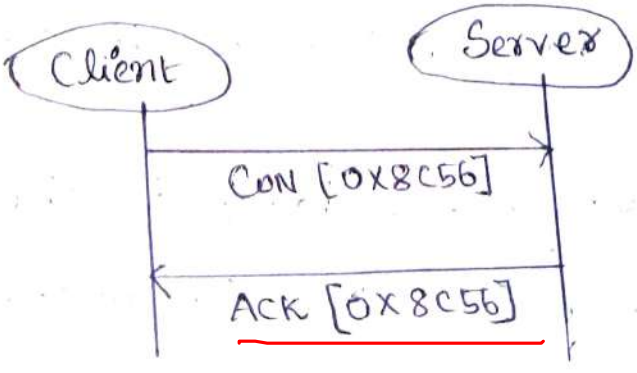


fig: Reliable message Transport

b) Unreliable message Transport:

→ Transporting with non type message. It doesn't need to be Acked but has to Contain message ID for supervising in case of retransmission

⇒ If recipient fail to process message, Server replies RST.

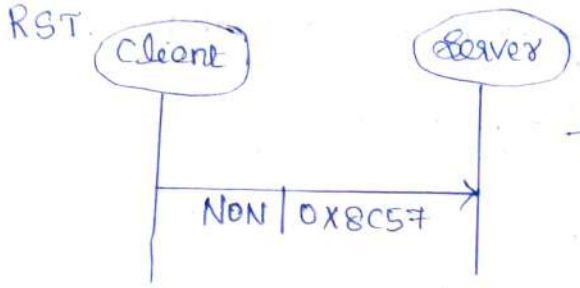


fig: Unreliable message transport

Message format:

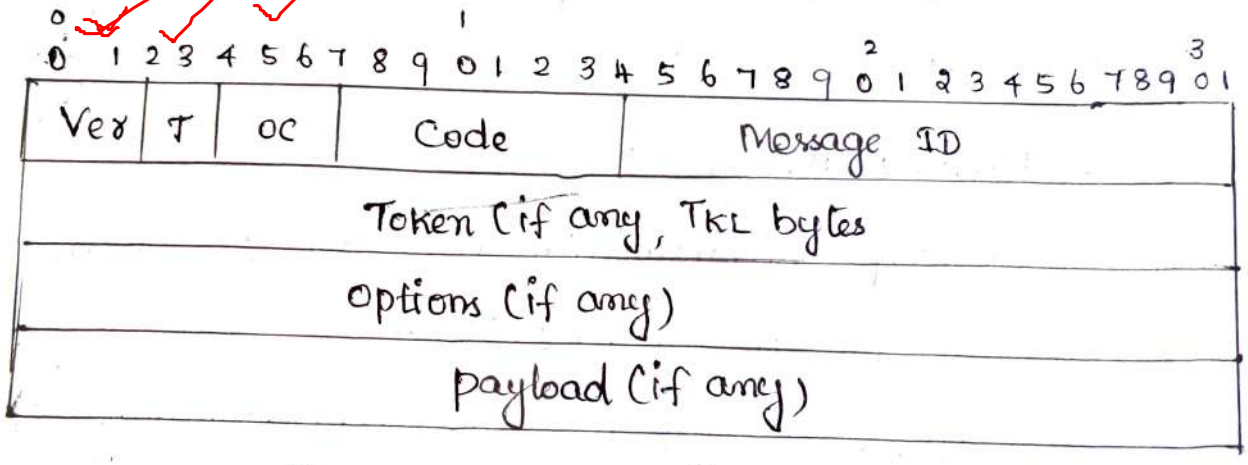


fig: CoAP message format

It Contains a fixed length 4 byte header that may be followed by Compact binary options and a payload

Ver: 2-bit unsigned integer. Indicates the CoAP Version number.

T: 2 bit unsigned integer - indicates if this message is of type Confirmable (0), Non-Conformable (1), ACK (2), RST (3).

CODE :-

8-bit unsigned integer, the request message (1-10) or response message (40-255)

Message ID :

16-bit unsigned integer in network byte order, Identifier for matching message responses.

Token (TKL) : 4 bit unsigned integer, Indicates the length of the variable length Token field (0-8 bytes).

Options :

Zero or more optional fields may follow a token, A few options like Content format, Accept, max-age, E-tag, etc.

*) Request / response Layer :-

a) Piggy-backed :-

⇒ Client sends request using CON type or NON type message and receives response ACK with Confirmable message immediately.

⇒ In fig below for successful response, ACK Contain response message identify by using token for failure response ACK Contain failure response code.

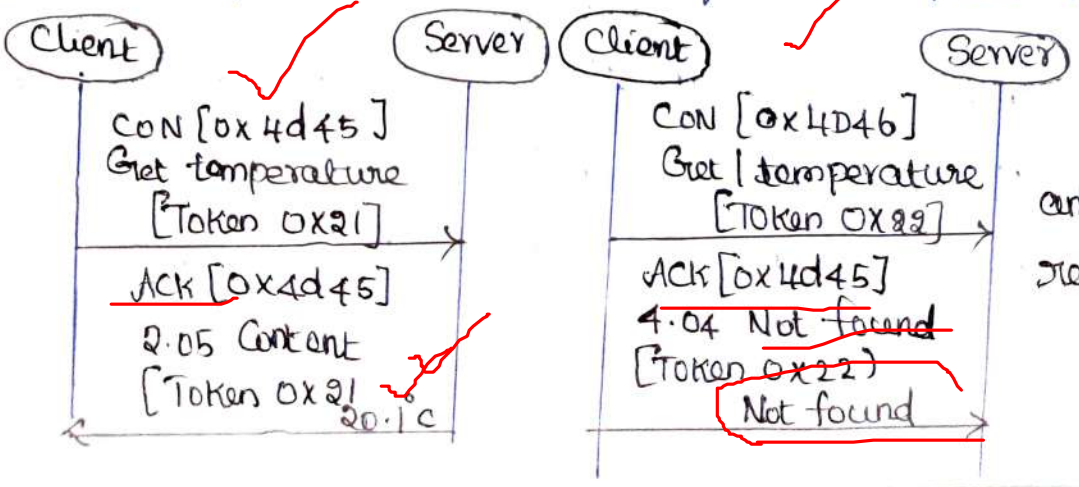


fig : Successful and failure response results of GET method.

b) Seperate response :

⇒ If Server receive a CON type message but not able to response this request immediately, it will send an empty ACK in case of Client resend of this message.

⇒ When Server ready to response this request, it will send a new CON to Client and Client reply a Confirmable message with ACK.

The ACK is just to Confirm CON message, no matter CON message carry request or response.

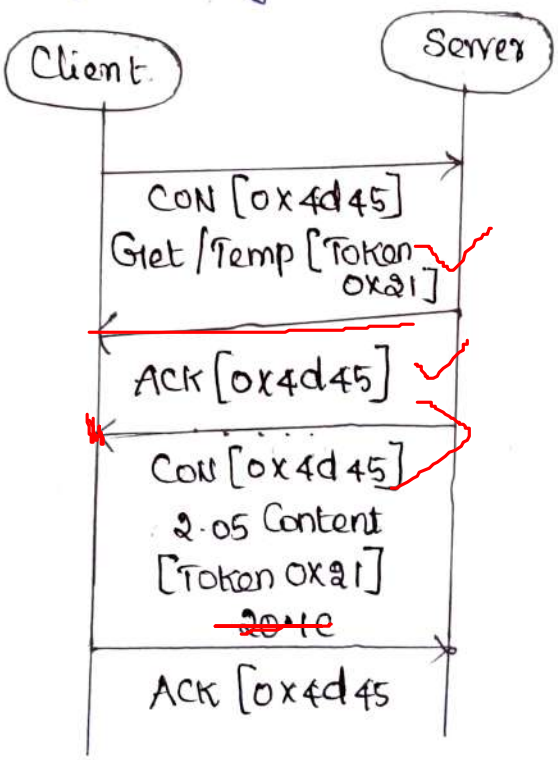


fig: A get request with a seperate response

c) Non Confirmable request and response :-

⇒ Unlike piggy-backed response carry Confirmable message in Non-Confirmable request client send. NON type message indicate that server don't need to Confirm. Server will resend a Non type message with response.

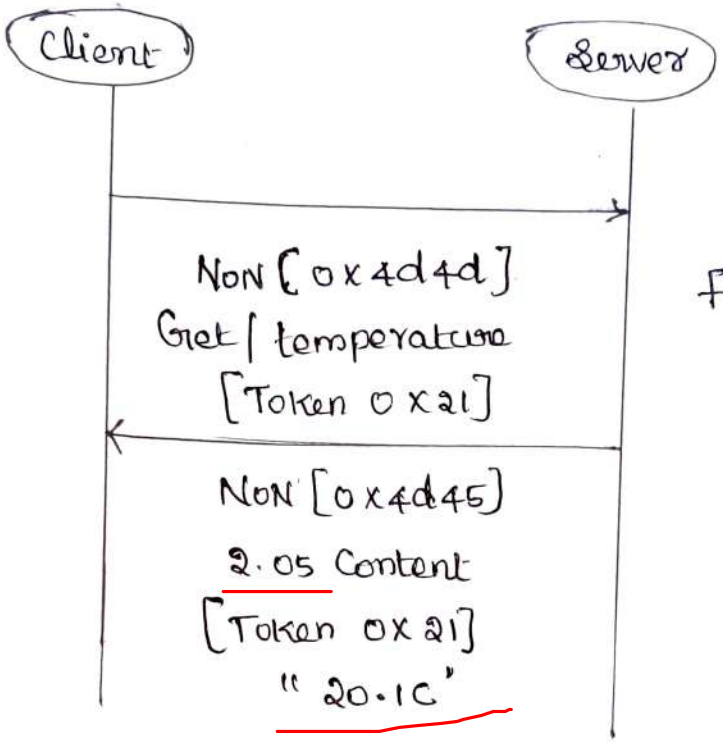


Fig: Non Confirmable request and response

CoAP features:

(i) Constrained web protocol fulfilling M2M (Machine to Machine) requirement.

(ii) Security binding to datagram Transport layer (Security DTLS)

(iii) Asynchronous message exchanges.

(iv) Low header overhead and parsing Complexity.

(v) Stateless HTTP mapping.

(vi) URI and Content type support.

UNIT : III

3G OVERVIEW

Overview of UMTS Terrestial Radio access network - UMTS Core network architecture : 3Gpp Architecture, User equipment, CDMA 2000, Overview - Radio and network Components, Network Structure, Radio network, TD-CDMA, TD-SCDMA.

OVer View of UMTS Terrestial Radio Access network :

Outline the overview of UMTS Terrestial Access Network ?

(or)

Explain the UMTS network architecture with GSM, 3G and also explain the reference architecture ?

(or)

Explain about UTRAN architecture ?

*) UMTS Network Architecture ?-

*) A Primary assumption for UMTS is that it is based on an evolved GSM Core network. This provides backward Compatibility with GSM in terms of network protocols and interfaces.

*) The Core network Supports both GSM and UMTS/IMT 2000 Services including hand off and roamening between the two.

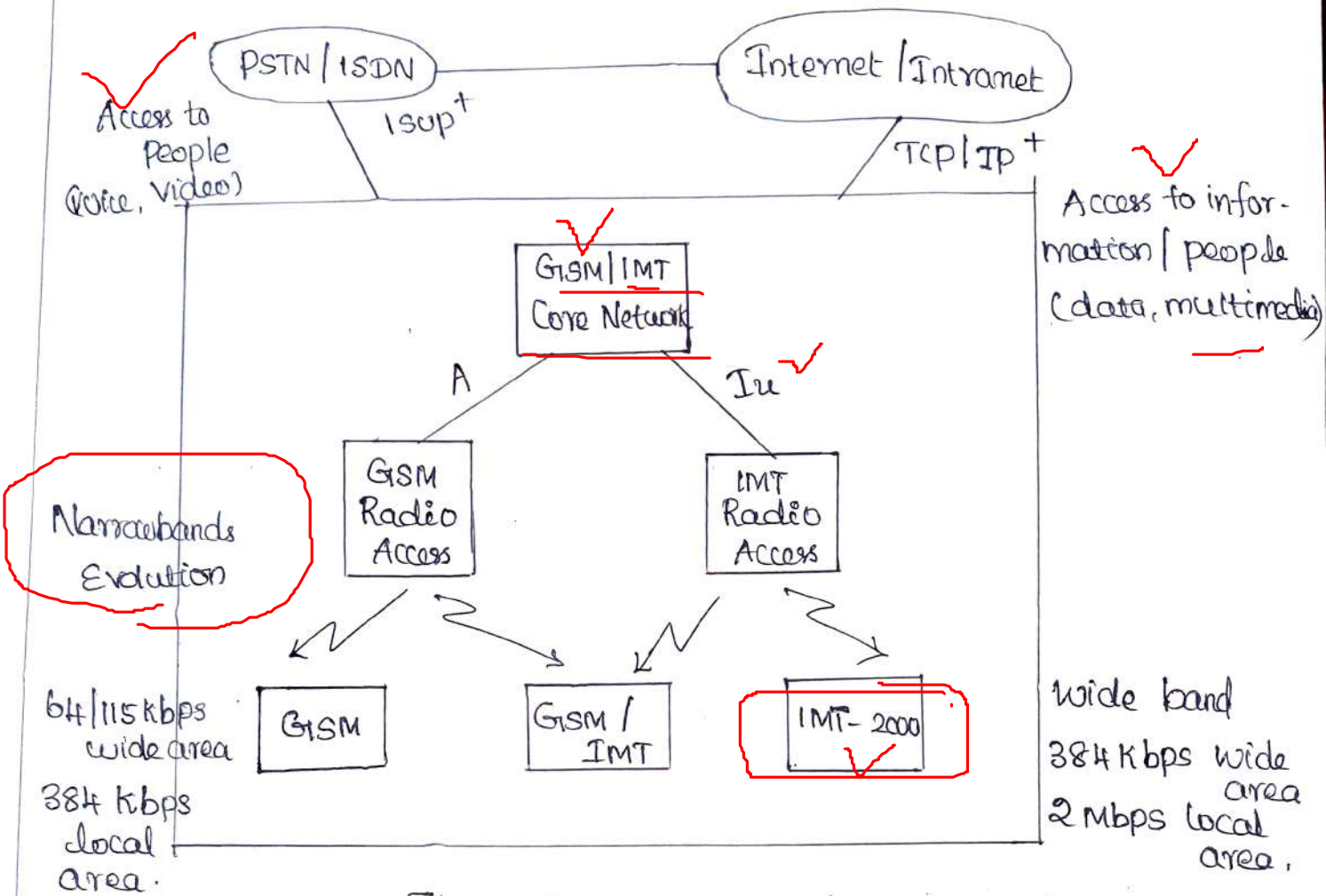


Fig: Evolution to UMTS / IMT-2000 in a GSM environment.

*) The proposed W-CDMA based UMTS Core network using a new multi vendor interface (Iu).

UMTS Terrestial Radio Access Network (UTRAN) Logical Architecture :.

The UTRAN Consists of a Set of radio network Sub Systems (RNS). The RNS has two main logical elements Node B and RNC.

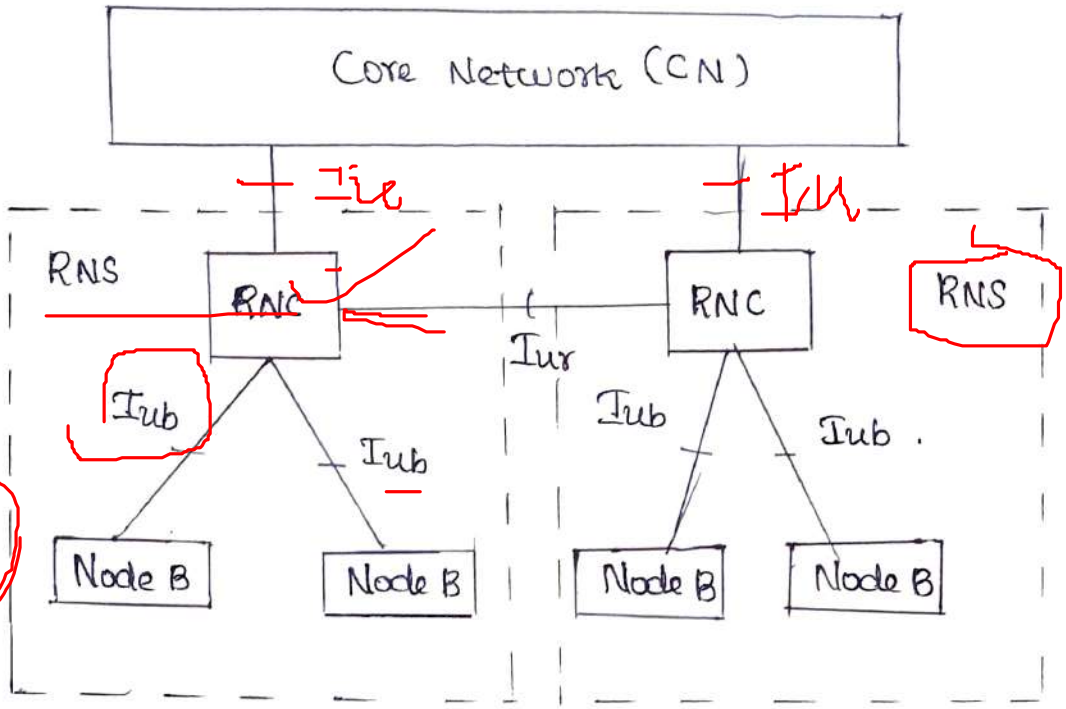


fig : UTRAN Architecture.

(i) Radio network Subsystem:

It is responsible for the radio resources and Transmission / Reception in a Set of Cells. A cell is one Coverage area Served by a broadcast channel.

a) Radio Network Controller:-

An RNC is responsible for the use and allocation of all the radio resources of the RNS to which it belongs the RNC also handles the user voice and packet data traffic. Performing the actions on the user data streams that are necessary to access the radio bearers on the user data streams.

RNC has the following responsibilities in the RNS :

*) Intra UTRAN handover
*) Frame Synchronization.
*) Radio resource management
*) Radio resource allocation
*) Frame Selection and distribution.

b) Node B :

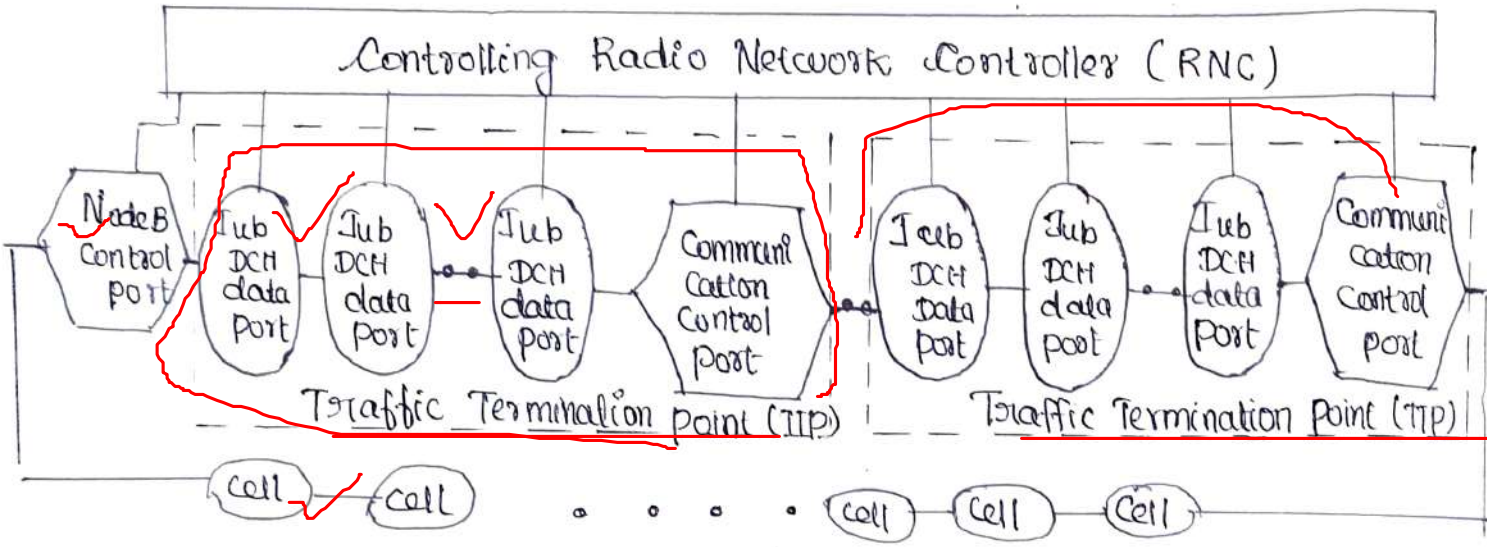


Fig : Node B logical Architecture.

It is responsible for radio transmission and reception in one or more cells to/from the user equipment.

Node B has the following responsibilities.

*) Termination of Iub interface from RNC
*) Inner and open loop power control
*) Radio Channel coding / decoding.
*) Error detection on transport Channels.
*) FEC encoding / decoding.

*) Multiplexing at transport channels and demultiplexing of coded composite transport channels.

UTRAN Interfaces :-

⇒ There are four interfaces connecting the UTRAN internally or externally to other functional entities. Such interfaces are Iu, Uu, Iub and Iur.

⇒ The Iu interface is an external interface that connects the RNC to the Core Network (CN).

⇒ The Uu is also external, connecting the node B with the user equipment.

⇒ Iub is an internal interface connecting the RNC with the node B.

⇒ Iur connects two RNCs with each other.

Explain about UTRAN logical Interfaces ?

(or)

Discuss Iu, Iur and Iub interfaces in the UMTS ?

(or)

Discuss the role of the Access link control application part in UMTS ?

⇒ The protocol structure contains two main layers ?-

1. Radio Network Layer (RNL)
2. Transport Network Layer (TNL)

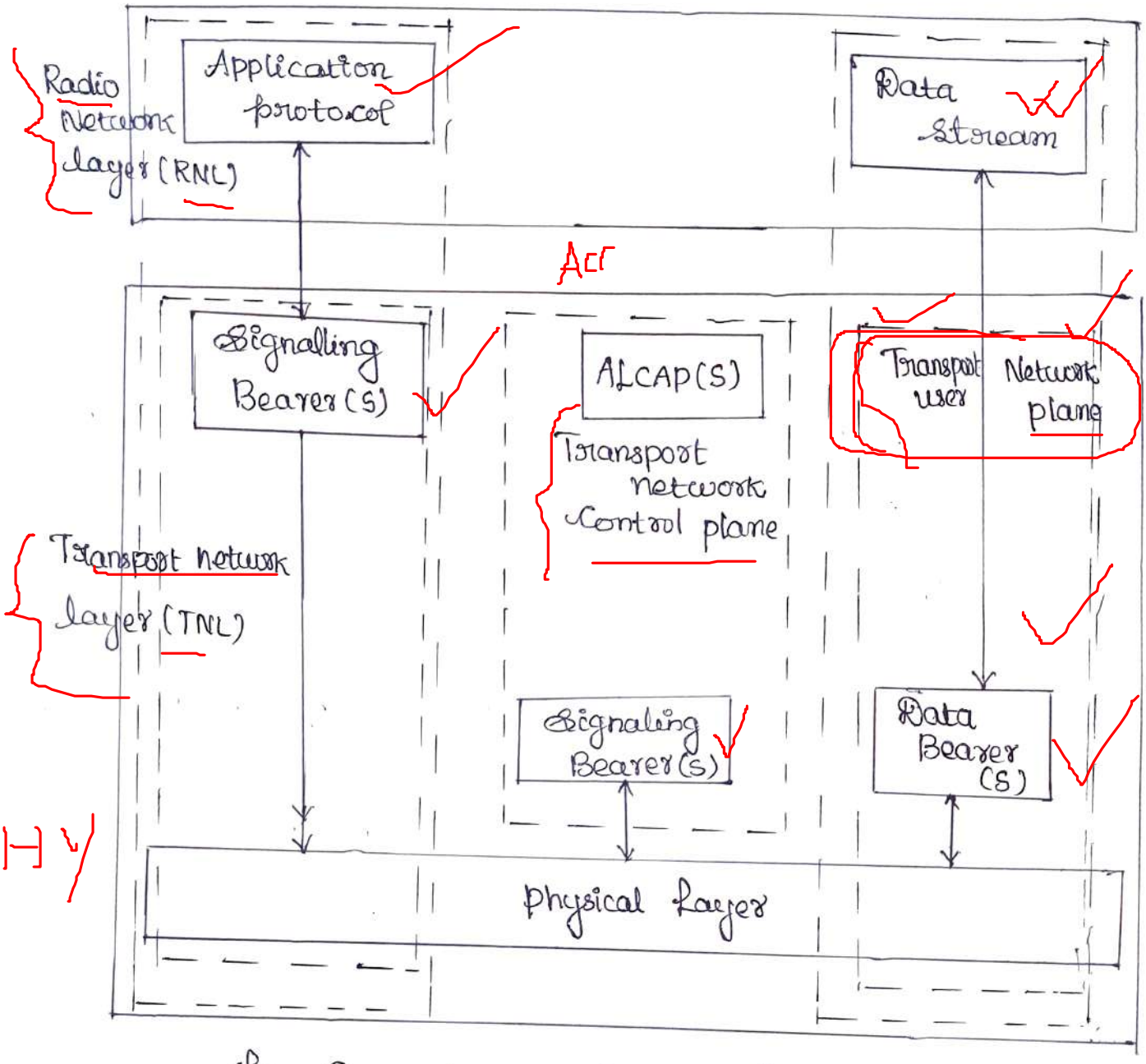


fig: General protocol model for UTRAN interfaces.

Radio Network Layer (RNL):-

* The RNL is concerned with user data and control information.
* All UTRAN related functions are visible.

Transport Network Layer (TNL):

⇒ It is concerned with the transport technologies used for the UTRAN interface.

*) Control plane :

⇒ The Control plane includes the application protocols and the signalling bearers, which transport the control information.

The application protocol used at different UTRAN interfaces are,

*) Iu-CS : Radio Access Network Application Protocol (RANAP)

*) Iu-PS : RANAP.

*) Iub : Node B application protocol (NBAP)

*) Iur : Radio Network System application protocol. (RNSAP)

*) User plane :

*) User information is carried by the user plane.

*) The user plane includes data stream (s) and data bearer(s) for data stream (s).

*) Each data stream is characterized by one or more frame protocols specified for that interface.

*) Transport Network Control plane :

⇒ It Carriers all control signalling with in the transport layer.

⇒ It does not include radio network layer information.

→ ALCAP(s) :

It contain access link control application part required to set up the transport bearers for the user plane.

⇒ The ALCAP may not be used for all types of data bearers. If there is no ALCAP signalling transaction the transport network Control plane is not required. This situation occurs when pre-configured data bearers are used.

Iu interface :

⇒ The UMTS Iu interfaces is the open logical interface that interconnects one UTRAN to the UMTS Core network.

⇒ The control plane serves to service domains in the Core network, the Circuit Switched (CS) domain and packet Switched (PS) domain.

(i) Iu Circuit Switched protocol Architecture :

⇒ The CS domain supports Circuit Switched service (eg) voice and fax. The CS domain can also provide intelligent services such as voice mail and free phone. It connects to PSTS/ISDN Network.

1.*) Radio Network Control plane :

It carries information for the general control of UTRAN radio network operation.

⇒ SCCP (Signalling Connection Control part) :

⇒ It is a network layer protocol that provides extended routing flow control, segmentation and

error Correction facilities in Signaling System 7 tele-Communication networks.

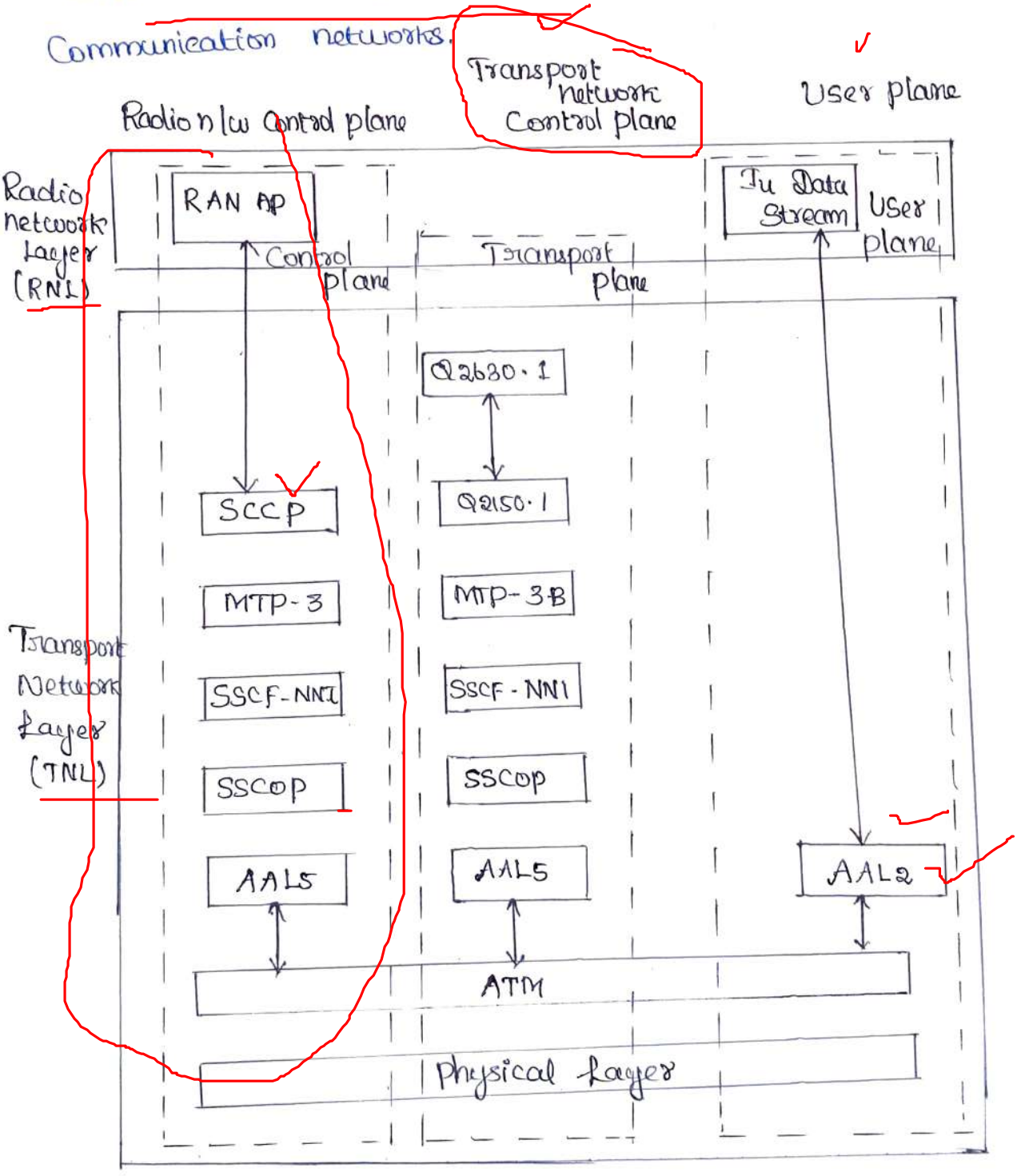


Fig: CS protocol architecture of Iu interface.

MTP3-B (Message Transfer part layer 3)

⇒ It is used for Communication in public switched Telephone networks.

*) MTP is responsible for reliable, unduplicated and in sequence transport of SS7 messages between communication partners.

-> SSCF-NNI (Service Specific Co-ordination function)

Network Node Interface in maps the requirements of above layers to the requirements of Sscop

-> SSCOP *) It is designed for signaling transport in ATM network.

-> AAL5 *) ATM Adaptation layer 5. It is used for segmenting the data to ATM cell.

2. Transport Network Control plane :

It carriers information for the control of transport network used with in Core network.

3. User plane :

It Carriers user voice and packet data information.

-> AAL2 :

It is used for the following services

*) Narrowband Speech.

*) Unrestricted digital information service.

(ii) Iu packet switched protocol Architecture :-

ps domain deals with ps services. Eg: Internet access and multimedia services. The ps domain connects to Ip network.

1. User plane :

GTP-U (GPRS Tunneling protocol - user plane part) is the multiplexing layer that provides identifiers for individual packet data flow and each flow uses UDP connectionless transport and IP addressing.

2. Transport network plane :

⇒ It is not applied to Iu-PS Interface.

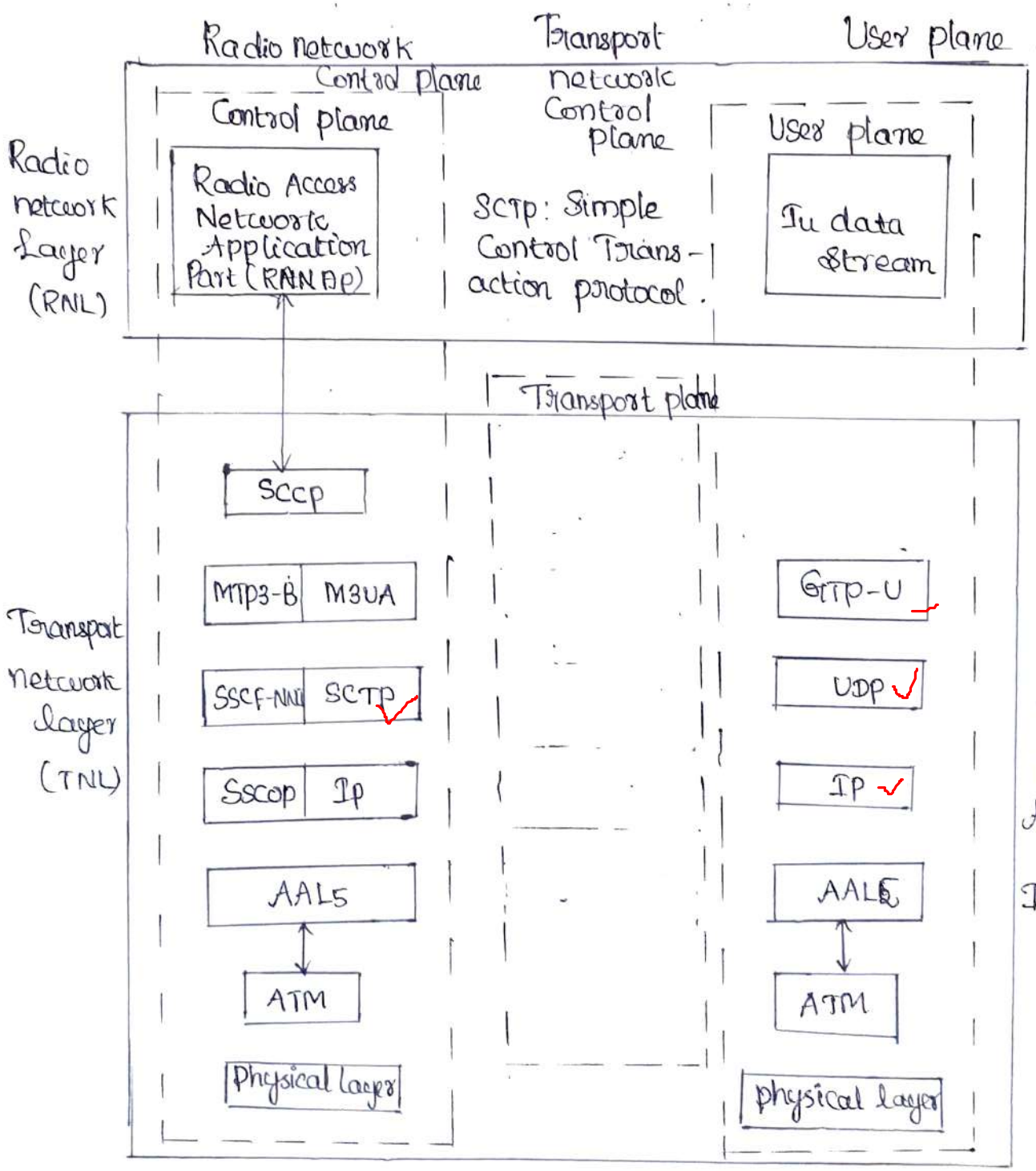


fig: PS Control Architecture of Iu interface

Radio Network Control plane:

*) The Control plane protocol Stack Consists of RANAP on the top of Signaling System 7 (SS7) protocols.

⇒ The Protocol layers are the Signaling Connection Control part (SCCP) the message transfer part (MTP3-B) and SAAL-NNI.

→ SSAL-NNI: (Signaling asynchronous transfer mode adaptation layer for network-to-network interface.

It's divided into 1) SSCF (Service Specific Co-ordination function).

2) SSCOP (Service Specific Connection oriented protocol).

3) AAL5 (ATM adaptation layer 5)

→ SCTP (Simple Control transmission protocol):

⇒ It's specifically designed for Signaling transport on the internet.

Iur Interface:

⇒ The Connection between two RNCs (Serving RNC and drift RNC)

⇒ It is used in soft handoff Scenario's. When different microdiversity streams of one Communication are supported by Node B, that belong to different RNCs.

Three different protocol planes are defined for it.

1. Radio network Control plane.
2. Transport network Control plane.
3. User plane.

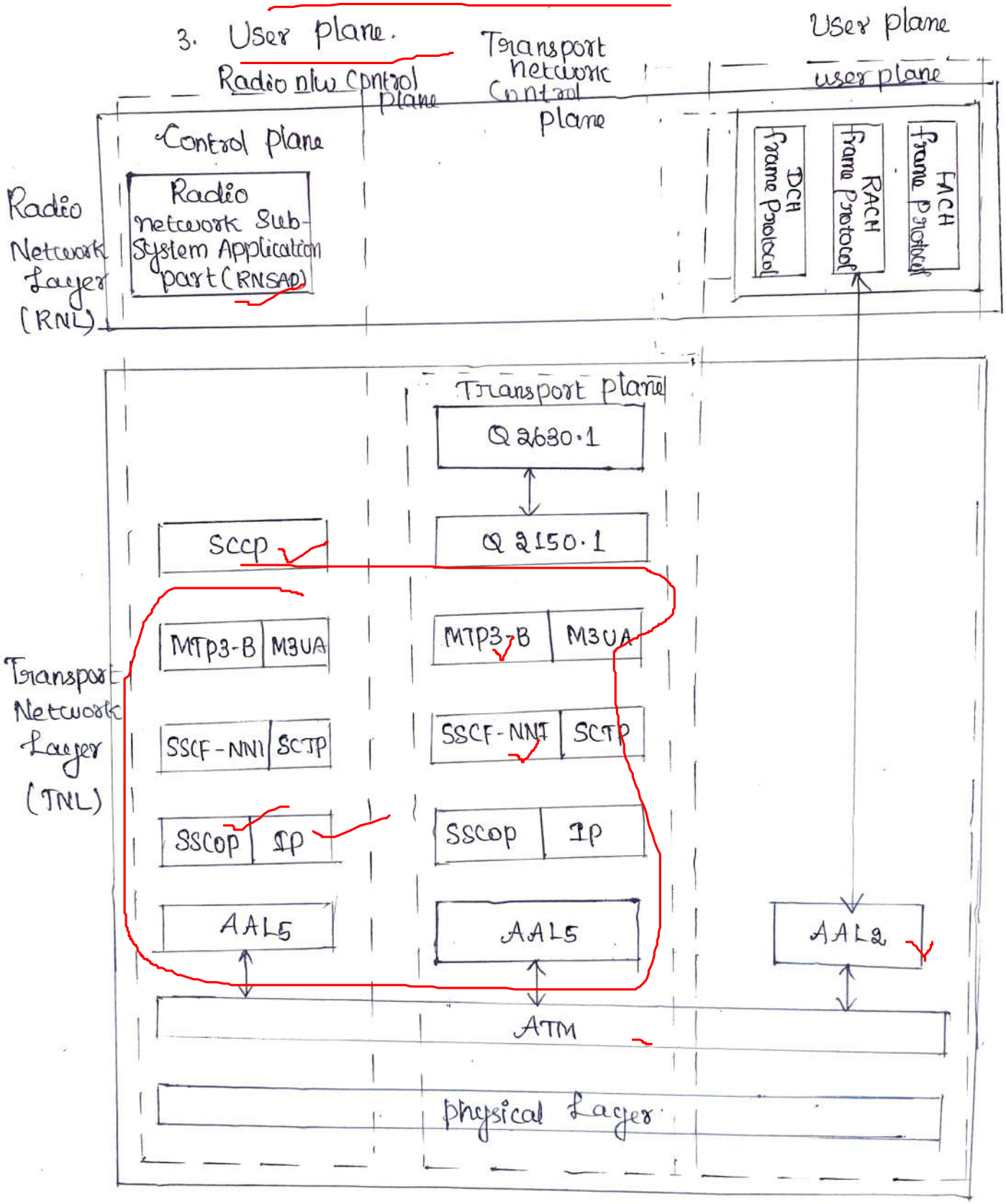


fig: Protocol Structure of Iur Interface.

① Radio Network Control plane :-

⇒ Information for the Control of radio resources in the Context of specific service request of one mobile on radio network Control plane.

RNSAP → This signaling protocol resides in the Control plane of radio network layer of Iu interface in the UMTS protocol stack.

② Transport Network Control plane :

Information for the Control of the transport network used within UTRAN on TNCP.

③ User plane :

User voice and packet information on user plane. The protocols used on this interfaces are,

(i) DCH frame protocol : (Dedicated Channel)

The data transfer takes place using a frame Protocol. The procedure belonging to this set include establishment, modification and release of dedicated channel in the DRNC due to hard and soft handover.

(ii) RACH frame protocol (Random - Access Channel)

It is a shared channel used by wireless terminals to access the mobile network for call-set up and burst data transmission.

(iii) FACH frame protocol (forward Access Channel)

Control frames used to exchange measurement and control information.

: Iur Provides the following four functions:-

① Basic inter-RNC mobility support

→ Support of SRNC relocation
→ Support of inter RNC cell and UTRAN registration area update
→ Support of inter RNC packet paging.
→ Reporting of protocol errors.

② Dedicated Channel Traffic Support.

→ Establishment, modification and release of a dedicated channel in the DRNC due to hard and soft hand off in the dedicated channel state.
→ Set up and release of dedicated transport connection across the Iur interface.

③ Common Channel traffic Support:

→ Splitting of the MAC layer between the SRNC and DRNC
→ Set up and release of the transport connections across the Iur for common channel data streams.

④ Global resources management:

→ Transfer of cell measurements between two RNCs
→ Transfer of node B timing between two RNCs.

Iub interface :-

→ The Connection between the RNC and node B is the Iub interface Radio network.

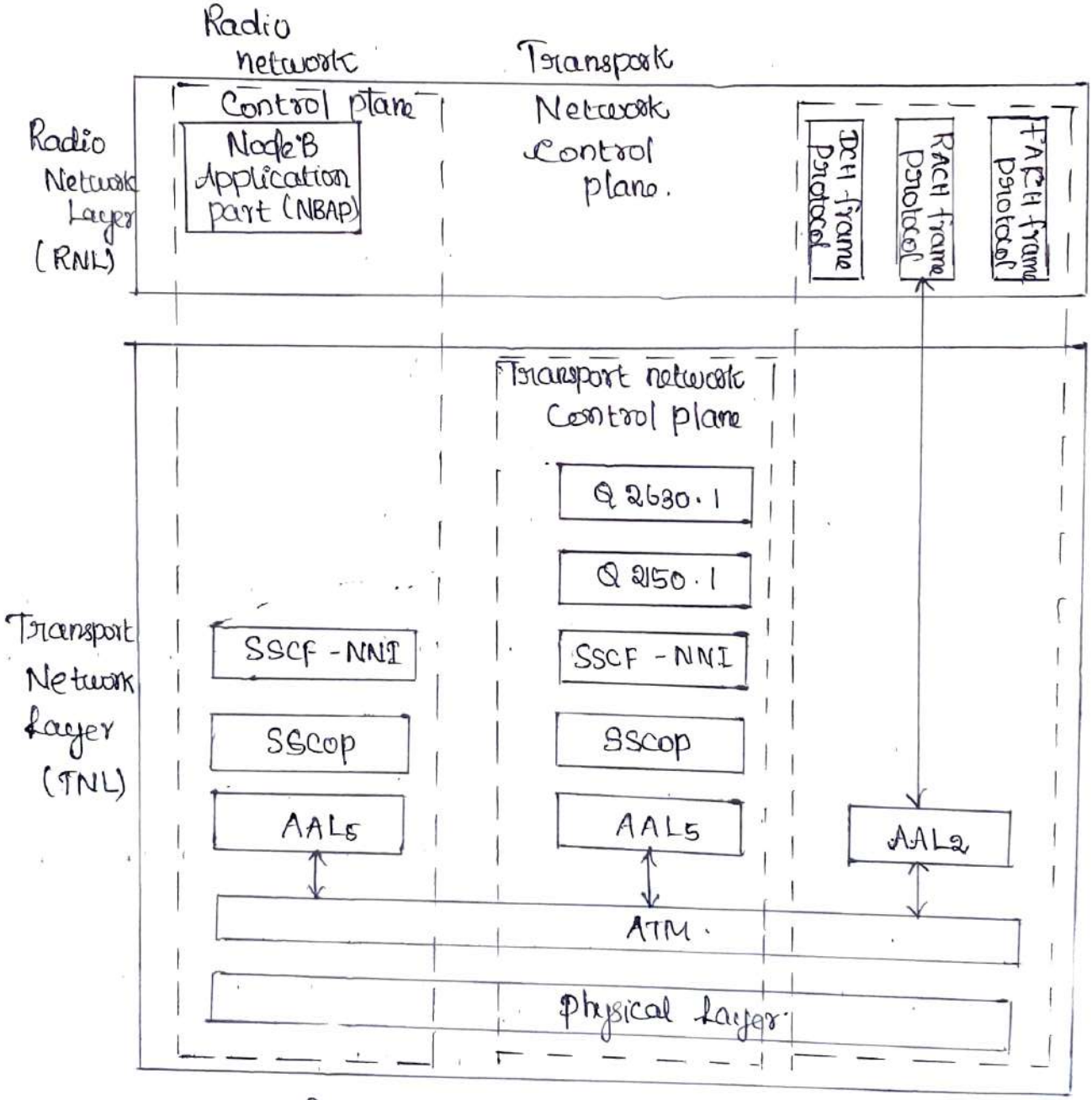


fig : Protocol structure of Iub interface.

1. Radio Network Control plane :-

Information for the general Control of node B for the radio network operation on RNCP. User CC and MM signaling on RNCP.

2. Transport Control Plane :

Information for the control of a transport network used within UTRAN or TNP

3. User plane :

User voice and packet data information on Up

The protocol used on this interface include.

1. Node B application part protocol.

→ Common NBAP → defines all the procedures for the logical operation and maintanance of node B.

→ Dedicated NBNP → It is used in the dedicated signaling link.

2. DCH frame control protocol.

3. RACH frame protocol.

4. FACH frame protocol.

When using multiple low speed links in the Iub interface node B supports inverse multiplexing for ATM.

Uu interface :

The UMTS Uu interface in the radio resource between a node B and one of its UE. The Uu is the interface through which UE accesses the fixed part of the system.

UMTS Core Network Architecture : 3Gpp Architecture :

Explain UMTS Core network Architecture ? (or)

The Core network of the UMTS is divided into three different functional areas name these areas and discuss their roles ?

(or)

Discribe in detail about UMTS 3Gpp Architecture (13)

(or)

Discuss two evolution paths for the GSM to offer 3G Services?

⇒ The UMTS Core network Consists of a CS entity for providing voice and data services and PS entity for providing packet based services.

⇒ fig shows the all entities that Connect to the Core Network - UTRAN, PSTN, the internet and logical Connection between terminal equipment (MS, UE) and

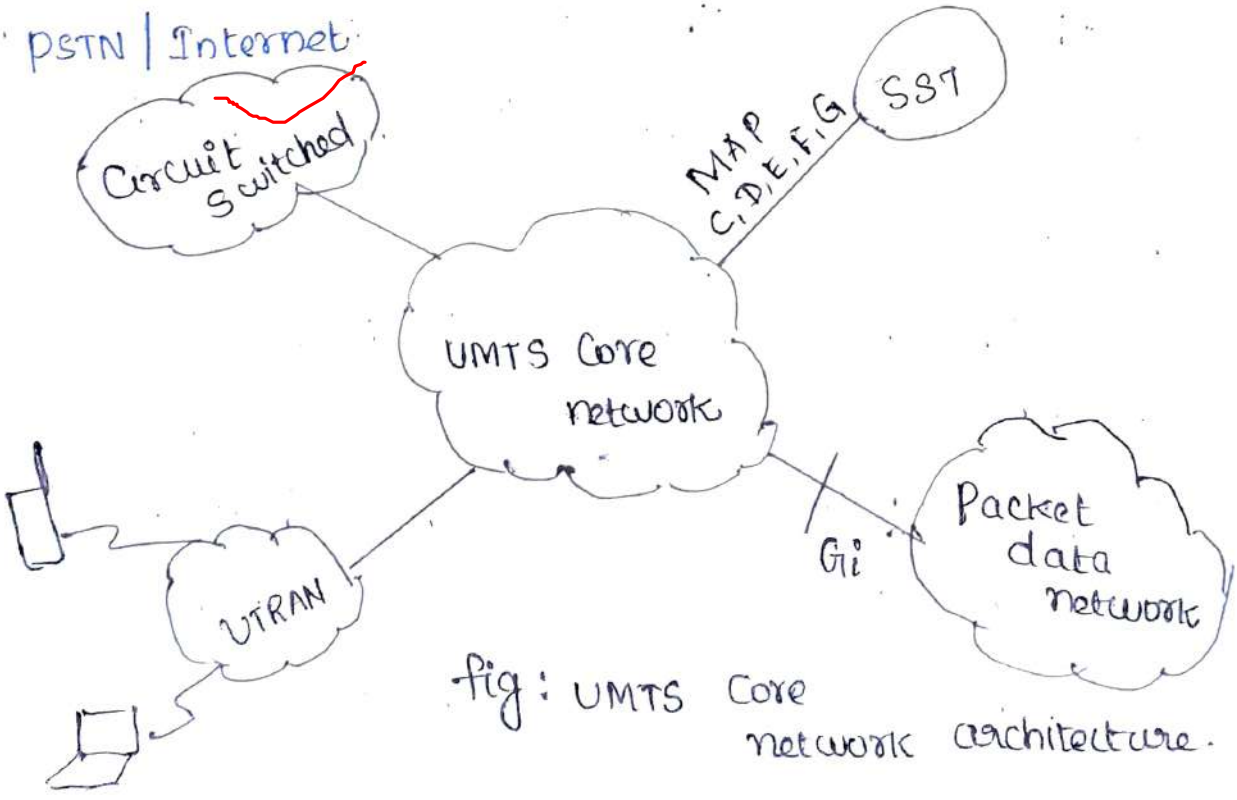


fig: UMTS Core network architecture.

3Gpp Network Architecture :

A public network administrated by a single network operator for providing land mobile services is referred to as public land mobile Network (PLMN).

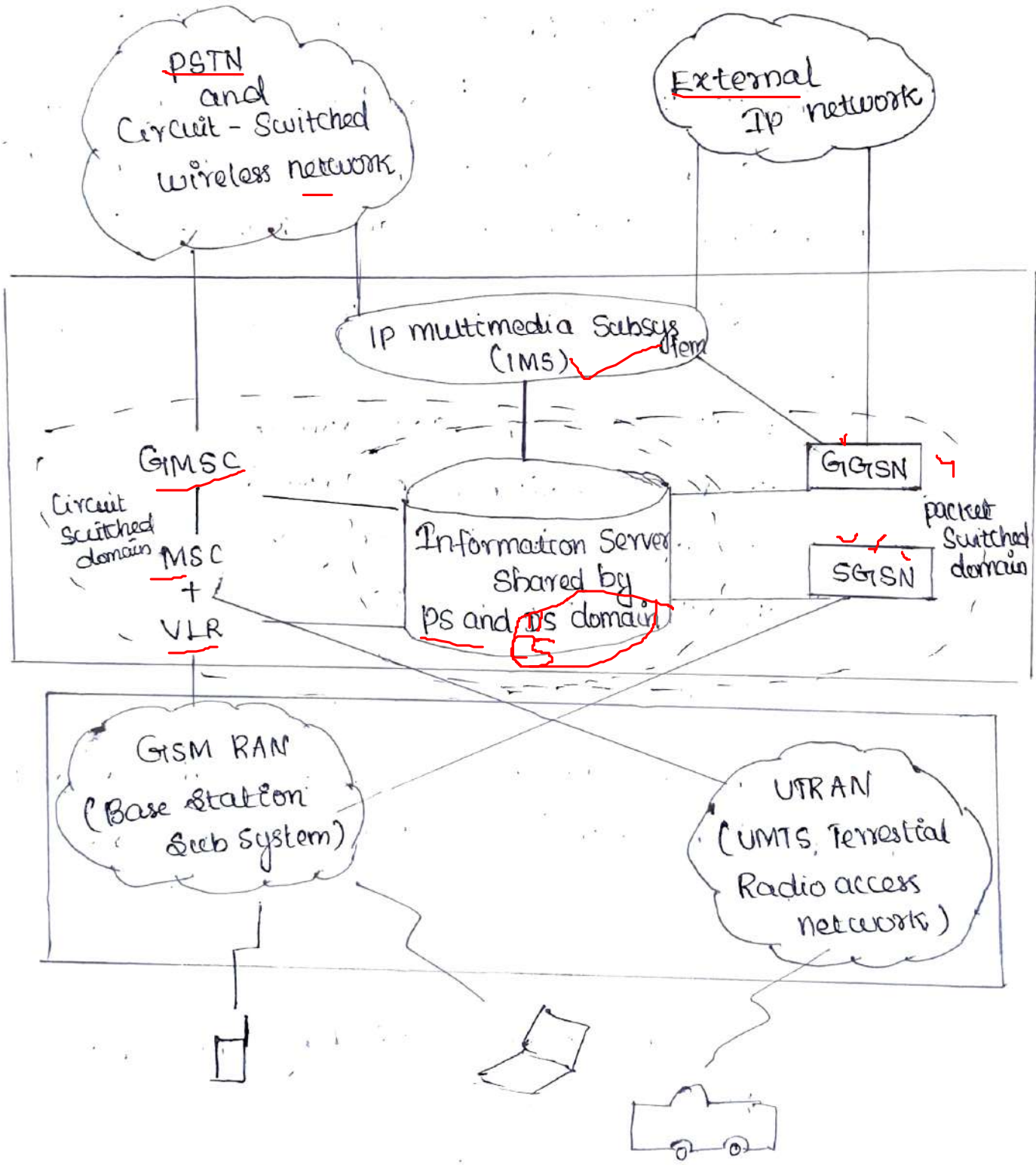


fig : 3Gpp Network Architecture.

⇒ It Consists of one or more Radio Access Networks (RAN) interconnected via a Core Network (CN).

① Radio Access Networks (RAN)

⇒ It Supports GERAN and UTRAN

⇒ GERAN is divided into Base Station Subsystem (BSS). Each BSS Consists of one or multiple Base Transceiver Stations (BTS) and Base Station Controllers.

The Core Network is divided into following functional entities.

(i) Circuit Switched (CS) domain.
(ii) packet Switched (PS) domain
(iii) Ip multimedia Subsystem.
(iv) Information Servers.

i) Circuit Switched Domain in Core network:

The CS domain Consist of all the CN entities for providing Circuit Switched Voice and data Services to mobile users.

CS domain network entities are

a) mobile Service Switching Center (MSC)
b) Gateway MSC
c) Visitor location Register (VLR)
d) Home Subscribe Server (HSS) equipment Identity Register (EIR) Authentication center (AUC)

a) MSC : It performs switching and call control functions needed to provide basic circuit switched services to mobile terminals.

In addition to perform mobility management function, location registration and hand off functions.

b) Gateway MSC (GMSC).

It is used to interface with external Circuit switched networks.

*) A GMSC is responsible for routing a circuit switched call to its final destination in external networks.

*) The switching and call control functions are separated by separate network entities.

c) Visitor Location Register (VLR)

It maintains location and service subscription information for visiting mobiles temporarily while they are inside the part of a network controlled by the VLR.

⇒ HSS & EIR, Auc shared by cs & ps domain.

(ii) packet-switched Domain in the Core Network :

⇒ The PS CN domain provides the following main functions for supporting packet-switched services.

a) Network access Control :

⇒ Determines which mobiles are allowed to use the ps domain, these functions include registration

authentication and authorization and admission control, message filtering and usage data collection.

b) Packet routing and Transport :-

→ Route user packets towards their destinations either inside the same network or external network.

c) Mobility management :.

It provides network layer mobility management functions also include tracking the location of mobile terminals.

PS CN domain consists of two main types of network nodes :

① Serving GPRS Support Node (SGSN)

② Gateway GPRS Support Node (GGSN)

① Serving GPRS Support Node (SGSN) :

→ It interconnects one or more RANs to PS CN. A SGSN performs the following specific functions.

(i) Access Control

It is responsible for the first line of control over users access to the PS CN domain.

(ii) Location management :

It tracks the location of mobiles that use packet switched services.

(iii) Route management:

It's maintaining a route to a GGSN for each mobile and to relay user traffic between the mobile and the GGSN.

(iv) Paging

⇒ The SGSN is responsible for intiating paging operation upon receiving user data destined to idle mobiles.

(v) Interface with Service Control platforms:

The SGSN is the Contact point with CAMEL (Customized Application for mobile Enhanced Logic) functions for GPRS and Ip-based services.

(2) Gateway GPRS Support Node (GGSN)

⇒ A GGSN Serves as the interface between the ps CN domain and any other packet network (e.g. Internet, Intranet, 3Gpp Ip multimedia Subsystem).

GGSN provides the following function:.

(i) Packet routing and forwarding center:

It acts as a packet routing and forwarding center for user packets.

(ii) Route and mobility management:

The GGSN maintains a route to the mobile's Serving SGSN and uses the route to exchange to user traffic with the SGSN.

(iii) Ip multimedia System (IMS):

⇒ It provides Core network entities for supporting real time voice and multimedia Ip Services.

(iv) Information Servers:

⇒ The information Servers maintain information for the network to operate and to provide service to users.

⇒ The ps and cs domain share the same information Servers.

The information Server (HSS):

a) Home Subscriber Server (HSS)

⇒ It maintains user subscription information needed by the network to control the network services provided to the users.

b) Authentication Center (AUC):

⇒ It maintains the information needed by the network to authentical each user and to encrypt the communication over the radio path.

c) Equipment Identify Register [EIR]:-

⇒ It is a logical entity that maintains the IMEIS [International Mobile Equipment Identify) of the Subscriber. It's Checks whether given UE is allowed on the network.

USER EQUIPMENT :-

Qn) Explain in detail about functional architecture of UE ?

(or)

Define UE ? What are the functional blocks in USER equipment ?.

⇒ A Mobile device in GSM is called Mobile Station (MS), which synchronous with user Equipment (UE) in UMTS.

⇒ Mobile devices are called as user equipment.

The user equipment consist of two main equipment such as,

(i) Mobile Equipment (ME)

(ii) UMTS Subscriber Identity Module (USIM).

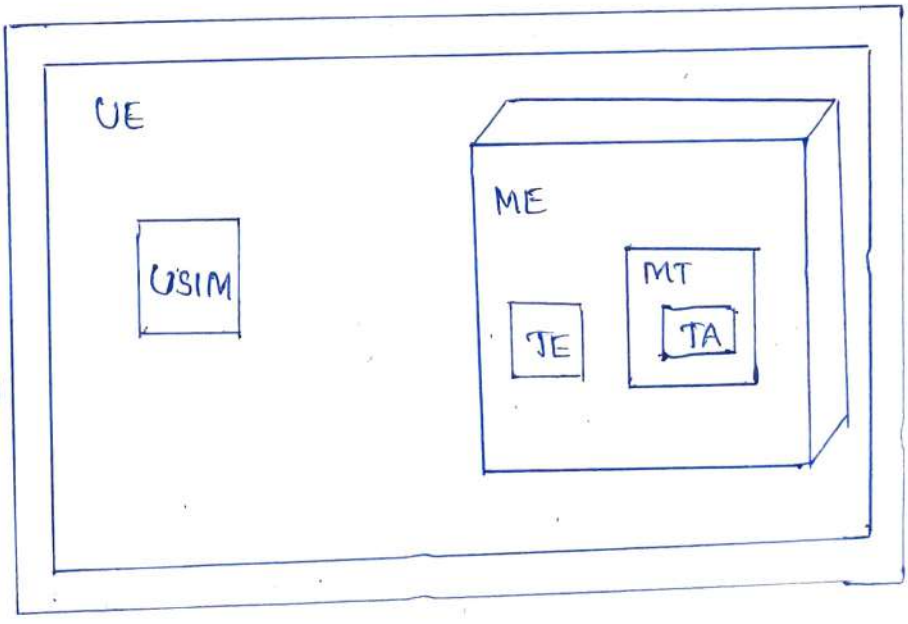


fig: functional Architecture of a user Equipment (UE)

(i) Mobile Equipment (ME)

⇒ It consists of mobile termination (MT) and Terminal Equipment (TE)

a) Mobile Termination.

⇒ It supports radio transmission and Channel management

⇒ Depending on the application an MT have a combination of different Terminal Adaptors (TA).

b) Terminal Equipment :

⇒ It is the device a user uses to access the network Services.

⇒ TE provides functions for the operations of the access protocols. eg : Laptop Computer.

⇒ It is also possible to integrate MT & TE in the same devices.

(ii) UMTS Subscriber Identity Module (USIM) :

⇒ It's developed based on the Subscriber Identity Module (SIM) used in GSM Systems.

IMSI (International Mobile Subscriber Identity).

⇒ A mobile station may be configured to access the PS domain only, The CS domain only or both the CS and the PS domains.

⇒ Each Subscriber to 3Gpp network services is assigned a globally unique international mobile Subscriber Identity (IMSI) as its permanent identifier.

⇒ A Subscriber uses its IMSI as its Common identifier for accessing ps services, CS Services or both ps and CS Services at the same time.

⇒ A Subscriber's IMSI is stored on a USIM on a mobile station

⇒ A user move its one station to another this IMSI is used to identified by the network as the same subscriber.

IMSI Structure:-

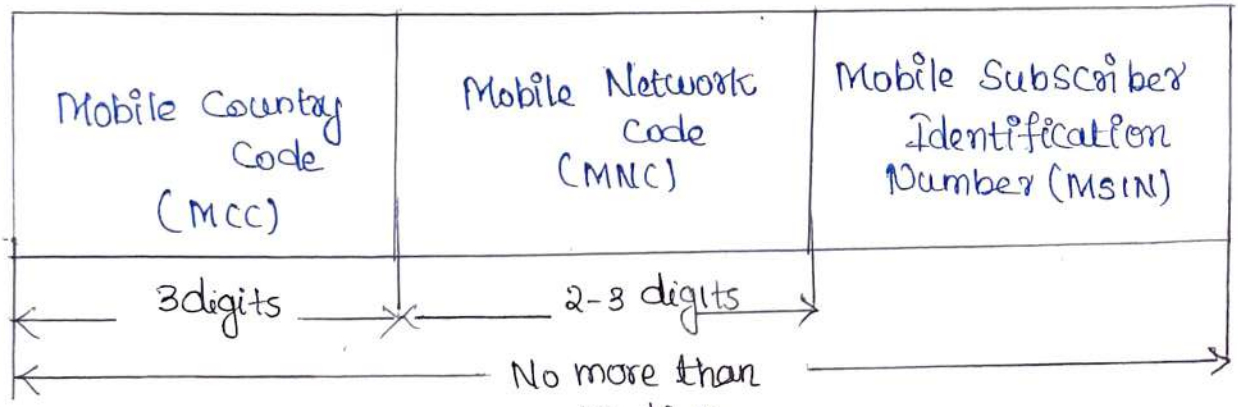


fig: Structure of International Mobile Subscriber Identity.

Mobile Country Code (MCC):-

⇒ The MCC uniquely identifies a mobile subscriber's home country.

Mobile Network Code (MNC):

⇒ It is used to identify the mobile subscriber home PLMN in the mobile subscribers home country.

Mobile Subscriber Identification Number (MSIN):

⇒ The MSIN uniquely identifies a mobile subscriber within one PLMN.

CDMA 2000 Overview :-

Qn) Discuss briefly cdma 2000 Evolution ?

(or)

Explain in detail about Cdma 2000 ?

⇒ CDMA 2000 is a unique radio and network access System. that is part of the international Mobile Tele-Communication 2000 (IMT-2000) its Collectively known as 3G Network.

*) CDMA is a high speed data and voice network Solution for low cost easy to deploy high performance services.

⇒ It can Support high volume of voice and data.

Features :-

*) Leading Performance.
*) Efficient use of Spectrum.
*) Support for advanced mobile Service.
*) It's Compatible with Ip having more flexibility and higher B.W.
*) CDMA 2000 offer the broadcast Selection of mobile devices.
*) It's designed for urban as well as rural areas.

Cdma Evolution :-

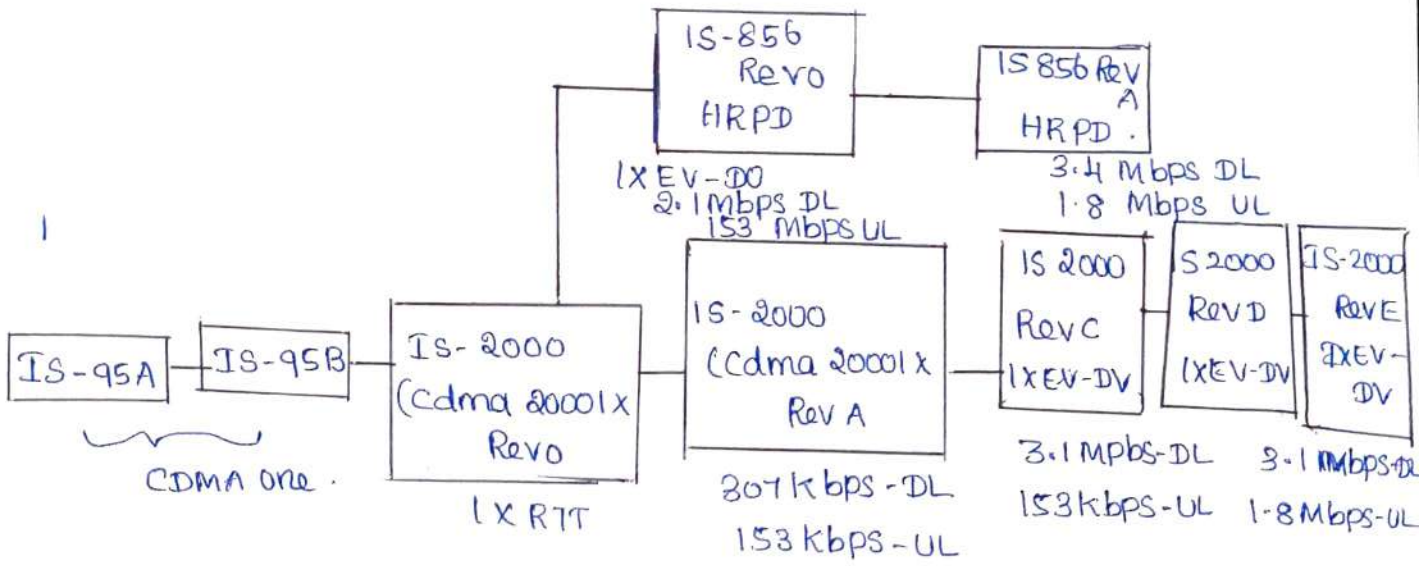


fig : CDMA Evolution.

CDMA One :

*) It is based on the IS-95A and IS-95B technology.

*) It operate the 14.4 Kbps & 1.15 Kbps.

*) It is a Second generation standard.

CDMA 20001x :

*) CDMA 20001x also referred to as CDMA 2000 1XRTT.

*) IS-2000 supports Circuit Switched voice and data rate upto 307 Kbps.

*) It provide voice capacity twice Compared to CDMA one.

CDMA 2000 1XEV-DO :

*) It is also called high data rate (HDR) is the high speed, high capacity wireless data only technology that provides upto 2.4 Mbps in a 1.25 MHz. Channel.

*) IS-856 also referred to as EV-DD (Evaluated Data only or optimised)

*) The radio channel bandwidth is same as the cdma 2000 - 1x & IS-856.

*) It will provide "always on" service supporting internet & intranet.

CDMA 2000 1XEV-DV :-

*) EV-DV (Evolution Data and Voice)

*) This system would carry both data and voice services..

*) High speed voice & data services at 3.09 Mbps.

*) Another important aspects of CDMA 2000 is that it supports not only the IS-41 system connectivity, as does IS-95 but it also supports Global system for Mobile (GSM) communications, Mobile Application part. (GSM-MAP) Connectivity requirement.

⇒ This is used to when wireless operator wanting to both wide band code division multiple Access and CDMA2000 can currently.

Advantages :-

*) Superior voice quality.

*) High speed broad band connectivity

*) Flexible spectrum allocation with excellent propagation characteristics.

*) Improved security & Privacy.

*) Lower total cost of ownership.

*) Multi mode, multi band global roaming features.

Disadvantages :-

⇒ Channel pollution : there are too many signals from cell sites in subscriber phone, but none is dominant degrading quality.

⇒ International roaming.

Applications :-

*) Wireless Internet
*) Wireless E-mail.
*) Wireless telemetry.
*) Wireless Commerce.
*) Location based service & longer stand by battery life.

Radio and Network Components:-

Qn) Explain in detail about CDMA 2000 s/m Architecture? (or) Explain in detail about Radio and networks components of CDMA 2000?

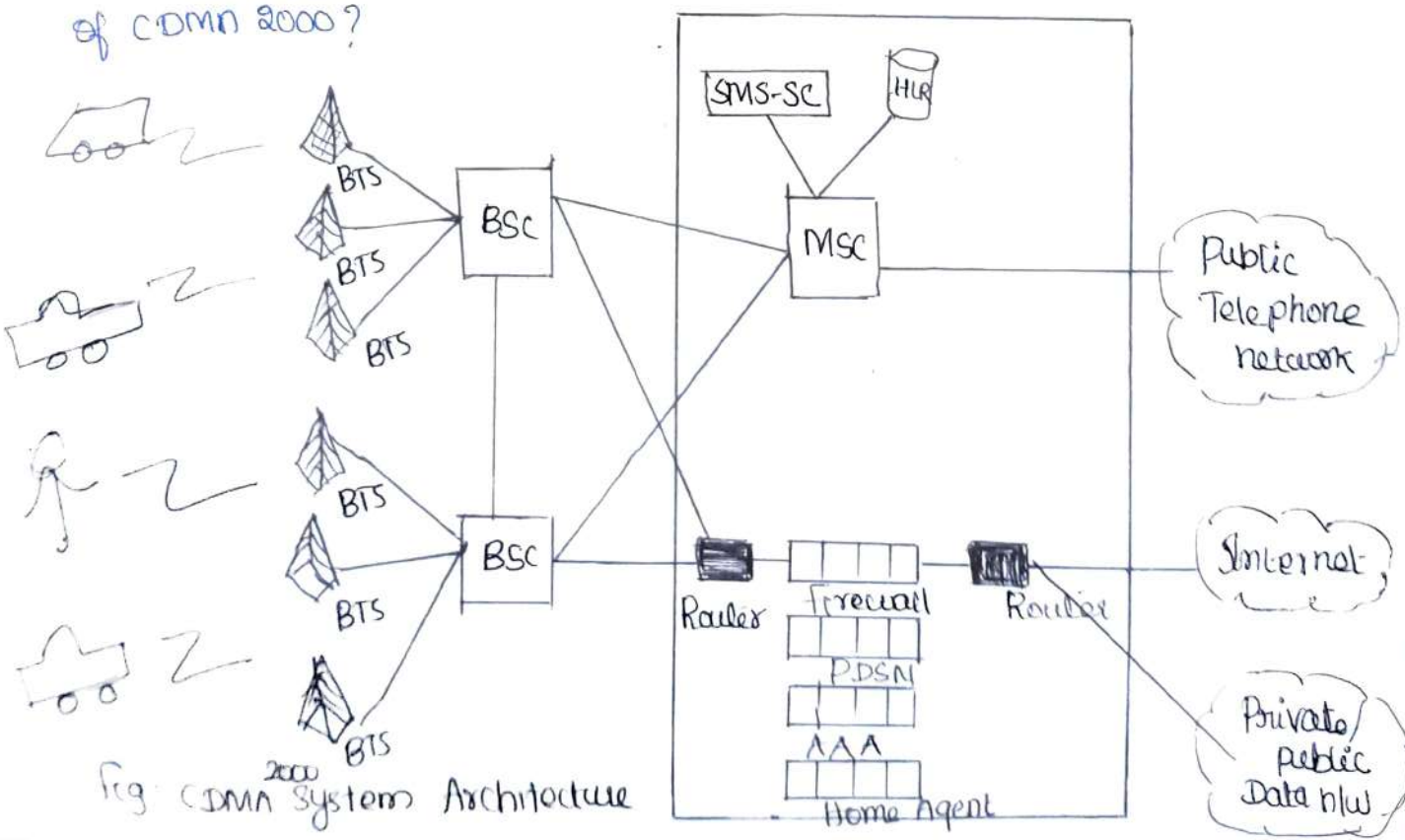


fig: CDMA 2000 System Architecture

(i) Base Transceiver Station (BTS)

⇒ It controls the interface between the CDMA 2000 network and the subscriber unit

⇒ BTs is responsible for allocating resources and both Power and walsh Codes for Consumption by Subscribers with a 1xRTT system and time slots and modulation format for 1xEVDO

*) BTs, when a new voice or packet session is initiated, it must decide how to best assign the subscriber unit to meet the service being delivered.

It also examine service requested, Consider radio Configuration the subscriber type

In IS-2000 system the following physical and logical resources the BTs must allocate when assigning resources to a subscriber.

*) The fundamental channels (FCH) (The number of physical resources available)

*) The FCH forward power (The power already allocated and that which is available)

*) The walse code required.

(ii) Base-Station Controller (BSC)

⇒ The BSC is responsible for Controlling all the BTs under its domain.

⇒ The BSC routes packets to and from the BTs to PDSN.

⇒ BSC routes Time Division Multiplexing (TDM) in Circuit Switched platforms. and routes packet data to the PDSN.

(iii) Router

⇒ It's responsible of routing packets to and from the various network elements within a CDMA 2000 System.

⇒ Also responsible for sending and receiving packets to and from the internal network to the offnet platforms.

(iv) firewall :

⇒ It is needed to ensure that security is maintained when Connecting to offnet data applications.

(v) packet Data Serving Node (PDSN) :

*) PDSN is a new Component associated with any CDMA 2000 System as Compared with CDMA one networks.

⇒ It support packet data services both 1X RTT and EVDO systems.

➡ PDSN performs the main function as :

① Establishes, maintains and terminates point-to-point protocol (ppp) sessions with the subscriber.

② Supports both simple and mobile Ip packet services.

③ Establishes, maintains and terminates the logical

links to the radio network (RN) across the radio - packet (R-P) interface.

④ Initiates authentication, authorization and accounting (AAA) for the mobile station client to the AAA Server.

⑤ Receives Service parameters for the mobile client from the AAA Server.

⑥ Routes packets to and from the external packet data networks.

⑦ Collects usage data that are relayed to the AAA Server.

Authentication, Authorization and Accounting (AAA):

⇒ The AAA provides, as its name implies authentication, authorization and accounting functions for the packet data network associated with CDMA 2000 and uses the Remote Access Dial - In User Service (RADIUS) protocol.

⇒ AAA Server main functions are.

(i) Authentication associated with point - to - point Protocol and mobile Ip Connections.

(ii) Authorization Service profile and Security key distribution and management.

(iii) Accounting.

viii) Home Agent:

It is used to tracking the location of the Mobile Ip Subscriber as it moves from one packet zone to another.

⇒ In tracking the mobile, the HA will ensure that the packets are forwarded to the mobile itself.

(viii) Home Location Register : (HLR)

⇒ The HLR performs packet data services such as store the additional subscriber information and terminal capabilities along with the traditional voice platform needs.

(ix) Visitor Location Register (VLR)

⇒ The service information from the HLR is downloaded in the VLR of the associated network switch during a successful registration process.

⇒ It is temporarily maintain location and service subscription information for visiting mobile users.

(x) MSC (Mobile Switching Center)

⇒ It performs the switching and cell control functions needed to the mobile user.

⇒ In addition to perform mobility management function, location registration and handoff functions.

Network structure :

Qn) Explain in detail about CDMA network structure ?

(or)

Explain how to CDMA network structure support 2.5G and 3G Network. Also explain the network structure of CDMA 2000 ?

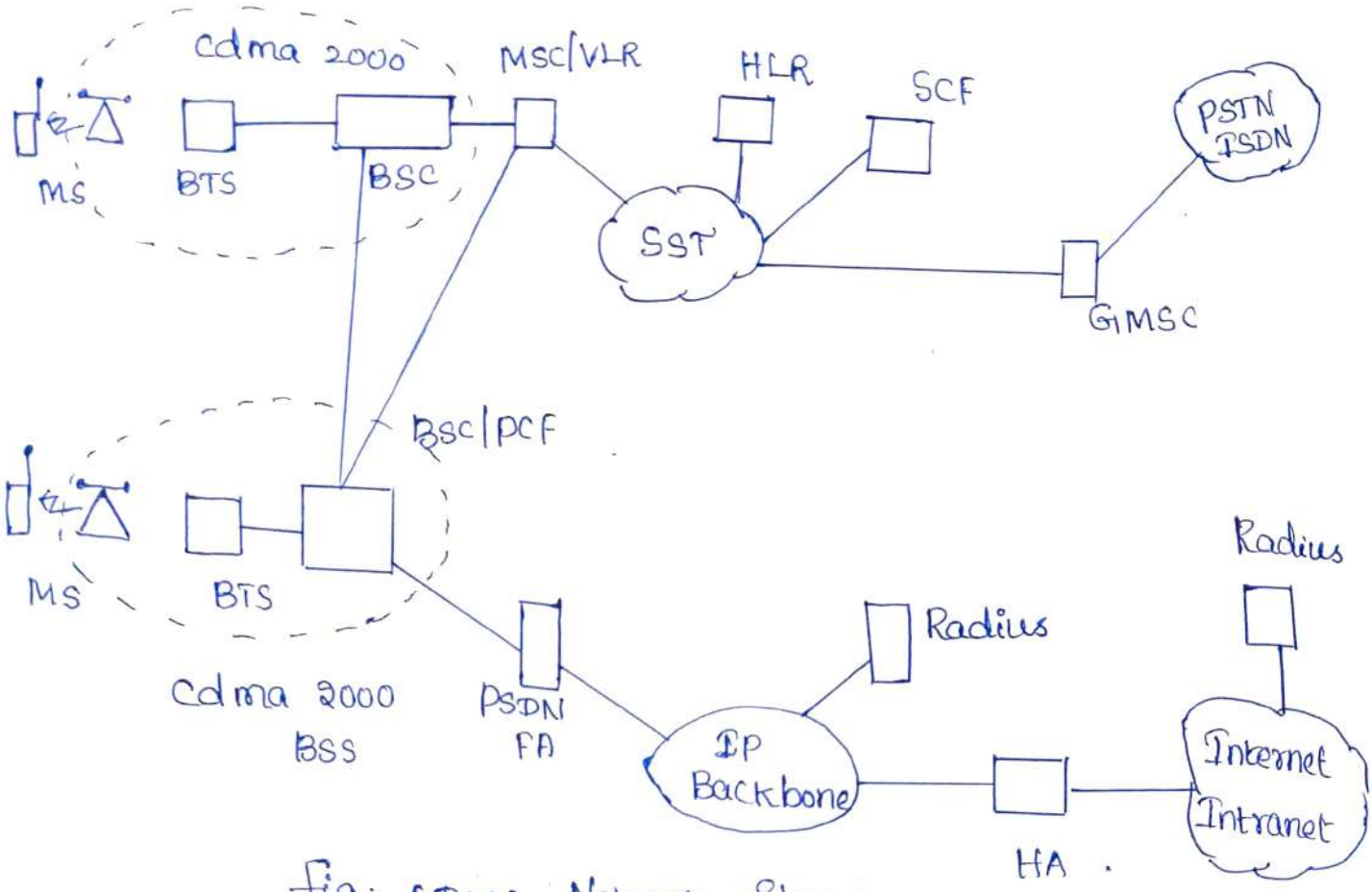


fig: CDMA Network Structure

⇒ CDMA 2000 Network architecture consists of following elements.

*) Mobile Station (MS):

→ MS is the mobile subscriber equipment, which can originate and receive calls and communicate with the BTS.

*) Base Transceiver Station (BTS):

⇒ It transmits and receive the radio signal.

*) Base Station Controller (BSC):

⇒ BSC implement the following function.

(i) Call Connection & disconnection.

(ii) Mobility management.

(iii) hard / soft hand off.

(iv) power control.

*) packet control function (PCF):

⇒ It implements the R-p Connection management. PCF can shield radio mobility for the upper layer services via handoff

packet data Service Node (PDSN):

⇒ The PDSN implements the switching of packet data services of mobile subscribers.

⇒ One PDSN can be connected many PCFs. It provides the interface between the radio network and packet data network.

Home Agent (HA):

The agent locates at the place where the mobile node also receive the registration information from MN.

*) Mobile Switching Center (MSC):

⇒ It performs switching and call control function.

Visitor Location Register (VLR)

⇒ It store the subscriber information of all the MSS in its local area.

Home Location Register (HLR):

⇒ It is responsible for storing subscription information MS location information.

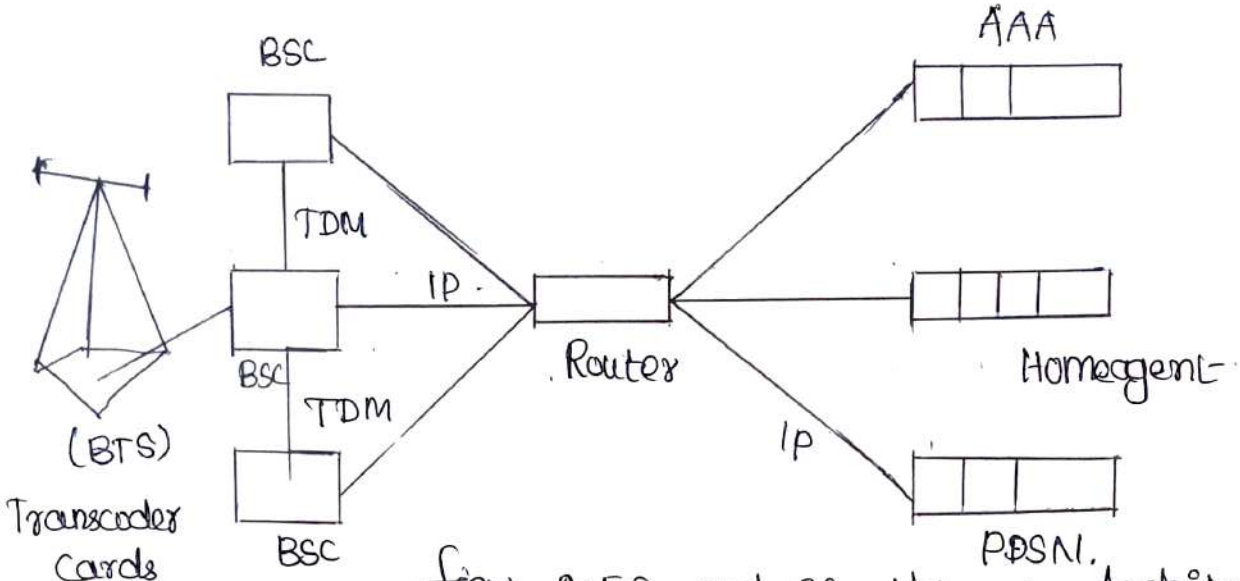


fig: 2.5G and 3G Network Architecture.

⇒ The network structure for a CDMA 2000 system that supports 2.5G and 3G and all the traditional voice elements associated with 2G wireless voice system.

⇒ Also packet network requires the additional network equipment to provide connectivity between the radio access Network & data network.

⇒ Ip network Configuration used to support 2.5G and 3G. ∴ packet network is called as Ip network. The Ip access network or the Carrier Ip network depending on the particular situation.

⇒ The numerous implementation methods are available for Configuring packet network, the three main variants in Configuring a CDMA 2000 network as follows.

① Distributed
② Regional
③ Centralized.

⇒ The Regional and Centralized Variant are Similar in Concept, except that the Centralized variant is an aggregation of several potential regional networks.

⇒ Some of the determinations for deciding on which Variant to implement are based on the following issues

(i) Service supported
(ii) Traffic Volume
(iii) Location of PDSN.
(iv) Commercial Interconnection agreement
(v) Network reliability and availability

→ other IP networks like IP multimedia service (IMS) and Voice over IP (VoIP) → It will use the distributed architecture.

Radio Network:

Qn) Explain in detail about CDMA 2000 Radio Network?

(Or)

Explain forward & Reverse Channel structure of CDMA 2000?

Or

Explain in detail Enhancement technique implemented by the CDMA 2000 Radio Network?

⇒ The radio network for a CDMA 2000 system has several enhancements over existing IS-95 / J-STD-0008 wireless systems.

⇒ These enhancements involves better power control, diver-

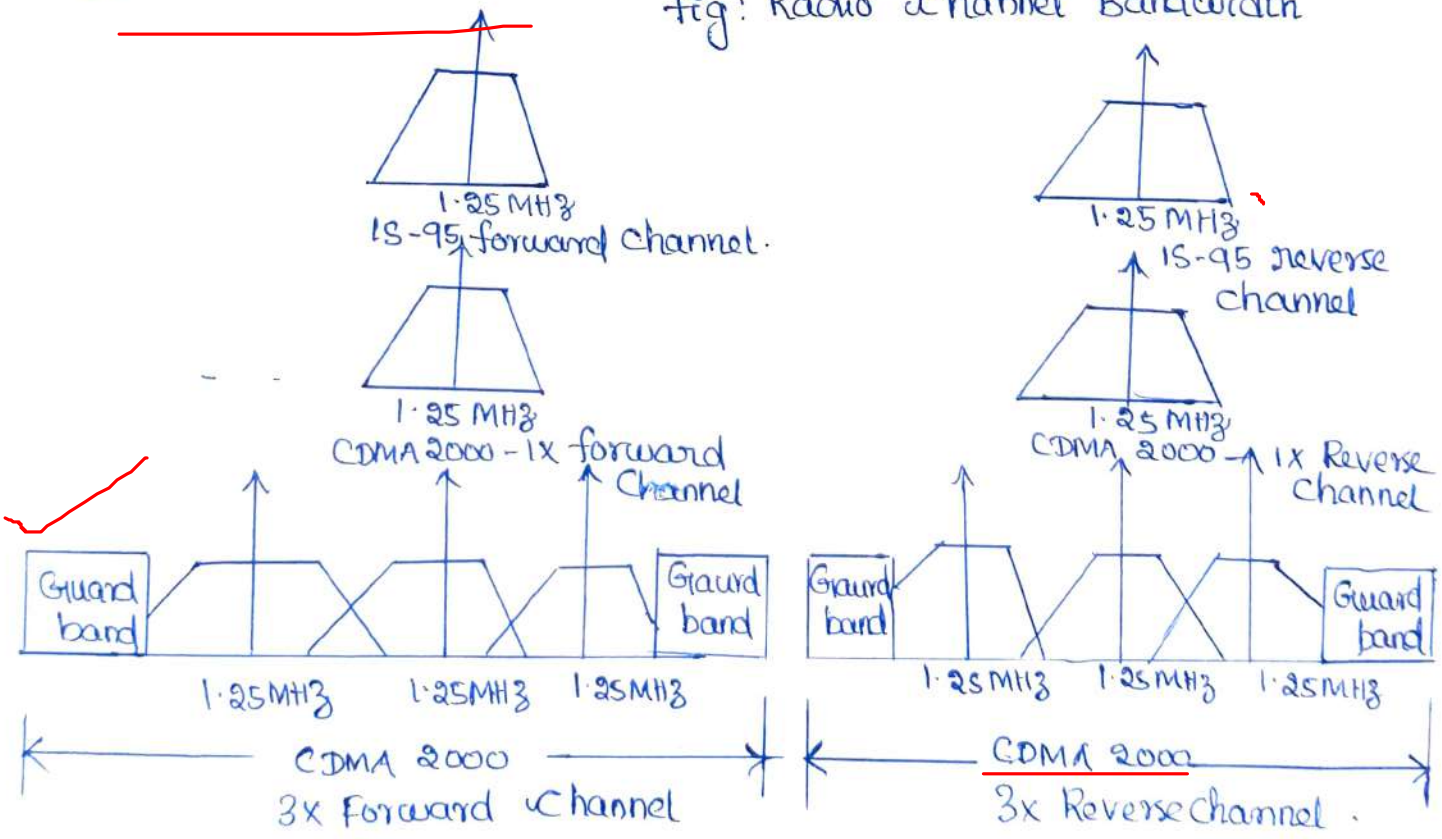
(iii) transmitting modulation scheme changes and channel bandwidth changes.

⇒ The CDMA 2000 radio system, following IS-2000 specification is designed to provide an existing cdma one.

⇒ The CDMA 2000 radio network for phase / Implementation also called CDMA 2000 1XRTT, is the same as that defined for IS-95 / J-STD-008 system where the channel bandwidth is 1.25 MHz.

⇒ A bandwidth changes in CDMA 2000 phase 2, which is referred to as CDMA 2000 - 3XRTT where multiple carrier are used.

fig: Radio Channel Bandwidth



⇒ fig above illustrate the radio carrier difference between a CDMA, IS-95, 1XRTT and 3XRTT system.

⇒ The CDMA 2000 radio access schemes has several enhancements over the existing IS-95 system as follows.

*) forward link
- → fast power control
- → QPSK modulation, dual BPSK

*) Reverse link
- → Pilot signal, to enable coherent demodulation for the reverse link.
- → Hybrid phase shift (HPS) keying spreading in the reverse link.

(i) Forward channel:

Fig below shows the forward CDMA channel structure, the Base station transmits multiple common channels as well as dedicated channel to the subscriber in their coverage area.

In forwaredchannel, F-FCH are resed for voice, F-SCH are data.

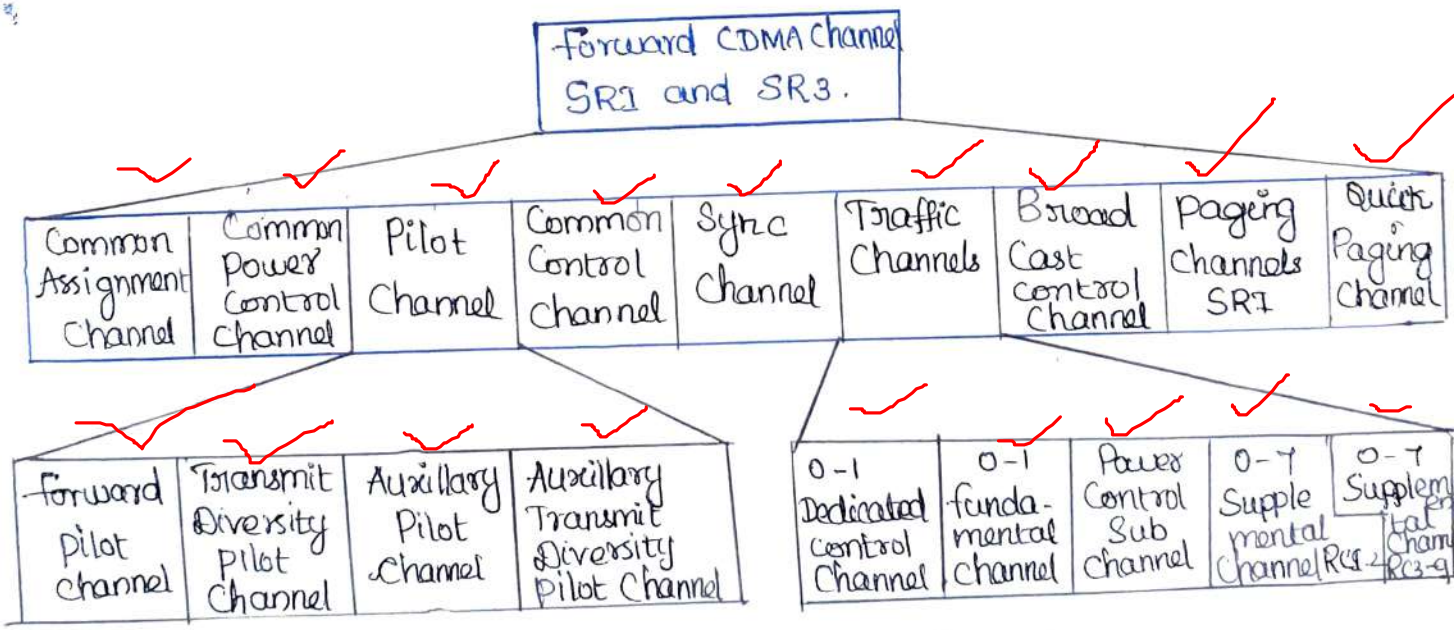


fig: forward CDMA Channel.

In this frame structure Consists of

⇒ 1 forward fundamental Channel (F-FCH)

⇒ 0-7 forward Supplemental Code channel (F-SCH) for both RC1 & RC2.

⇒ 0-2 forward Supplemental Code Channel (F-SCH) for both RC3 & RC9.

*) forward Supplemental Channel (F-SCH):

Upto two F-SCH Can be assigned to a single mobile for high speed data ranging from 9.6k to 153.6k in release.

*) Forward quick paging Channel (F-QPCH):

⇒ It enable the mobile battery life extension by reducing the amount of time mobile spends passing pages.

*) forward Dedicated Control Channel (F-DCCH):

⇒ It is used for messaging and control for data calls.

*) forward Transmit Diversity pilot Channel (F-TDPICH)

⇒ This is used to increase RF Capacity.

*) forward Common Control channel (F-CCCH)

⇒ This is used to send Paging, data messages, Signaling messages.

Reverse Channel :

Fig below shows the CDMA reverse channel received at base station.

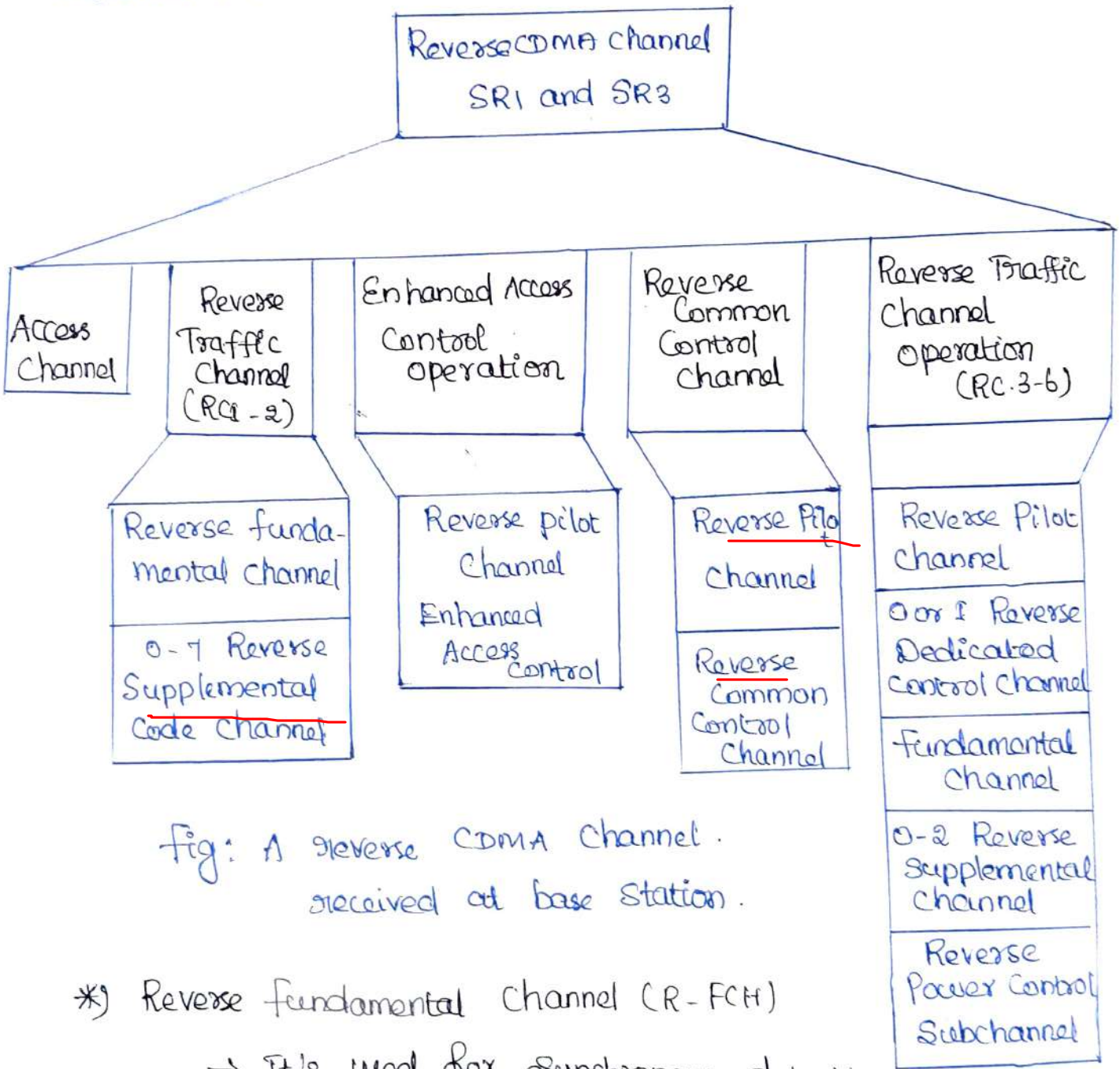


fig: A reverse CDMA channel received at base station.

*) Reverse fundamental Channel (R-FCH)

⇒ It's used for synchronous detection of voice data.

*) Reverse Supplemental Channel (R-SCH)

⇒ When the data rate more than 9.6k, a R-SCH is required and R-FCH assigned for power control

One or two R-SCH are assigned per mobile.

*) Reverse pilot Channel (R-PICH):

⇒ It provide pilot and power Control function.

*) Reverse dedicated Control Channel (R-DCH):

⇒ It is used for messaging and Control for data calls.

*) Reverse Enhanced Access Channel (R-EACH):

⇒ It is used to minimize the collisions and reduce the access channel power.

(iii) Power Control:-

⇒ Enabling better power Control of both the forward and reverse links has several advantages.

① System capacity is enhanced or optimized.
② Mobile battery life is extended.
③ Radio path impairments are properly or better compensated for
④ QoS at various bit rates can be maintained.

⇒ With any wireless system that interference limited it is important to ensure that all transmitters, whether mobile located at the Base Station, transmit at low power level while maintaining a good Communication link.

⇒ To achieve this closed loop power Control on reverse link and forward link uses reverse pilot

Channel to reduce the power.

⇒ In reverse link, outer loop power control dynamically adjust the target energy per bit per noise ratio (E_b/N_o).

⇒ It is done by measuring Frame Error Rate (FER) with target FER. if FER > target FER, mobile power up and FER < target FER mobile power down.

(iv) Walse Codes:

CDMA 2000 introduces an increase in the number of walse codes from 64 with IS-95 and 256 with 3XRTT. It's mainly used on fast-packet data rates.

TD-CDMA:

Qn) Explain in detail about TD-CDMA Architecture and Channel Structure?

(or)

Explain in detail about UMTS-TDD (or) HCR TDD Architecture with neat diagram?

⇒ TD-CDMA also referred to as HCR TDD and UMTS TDD.

⇒ The TD-CDMA RAN uses a combination of three multiple access schemes - FDMA, TDMA & CDMA.

⇒ TD-CDMA is designed to support asymmetric traffic such as IP.

⇒ TD-CDMA similar characteristics to TD-SCDMA except

that it uses a Chip rate of 3.84 Mcps, where as TD-SCDMA uses 1.28 Mcps.

⇒ In addition to TD-CDMA System is FDD-TDCDMA which has increased bandwidth.

(i) Generic TD-CDMA Architecture :

⇒ A TD-CDMA network architecture is very similar to IMT-2000 networks.

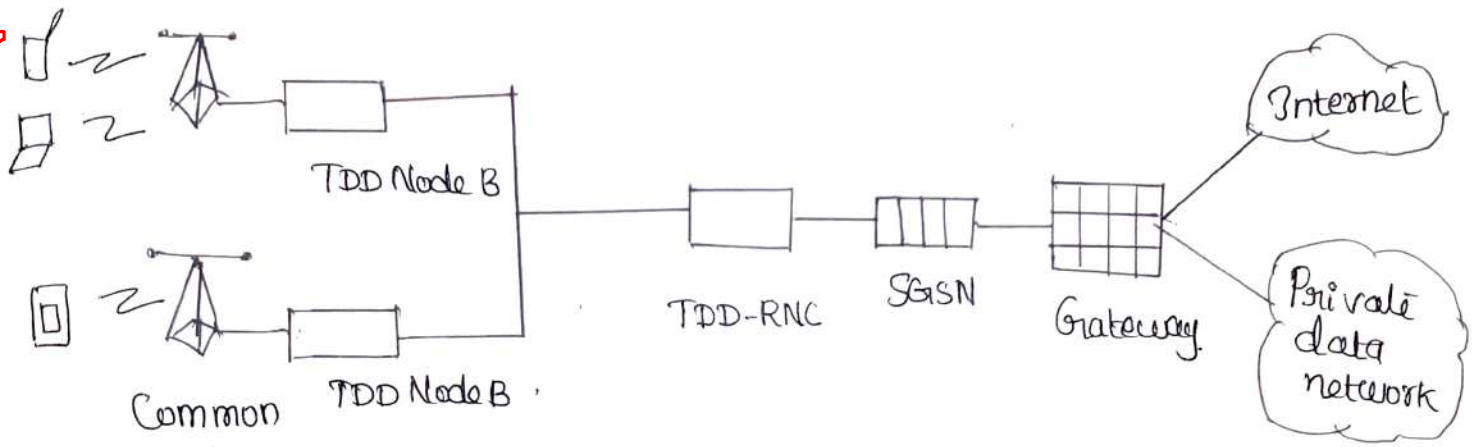


fig : TD-CDMA System Architecture.

⇒ fig above shows the TD-CDMA network that interfaces with an SGCN, enabling it to be used as a data-solution offering for a GSM/GPRS/EDGE, WCDMA or TD-SCDMA systems.

(ii) Radio Network :

*) TD-CDMA supports both Circuit and packet services and is designed primarily support the asymmetric characteristics of Ip data.

⇒ TD-CDMA uses TDD, uplink and downlink traffic share the same physical radio channel.

⇒ The uplink and downlink channel allocation can be done by the system or the operator. A minimum of one uplink and one down link always needs to be allocated per TD-CDMA Carrier.

(iii) RAN :

TD-CDMA requires 5 MHz of radio bandwidth to operate a single channel.

⇒ The channel structure for a TD-CDMA radio access uses TDMA, CDMA & FDMA.

⇒ In addition TD-CDMA uses the same chip rate, modulation and bandwidth that are used by WCDMA.

⇒ The heart of the TD-CDMA radio access is the TDD access method each radio carrier is divided into 15 time slots, each containing 16 seperate and unique codes this is shown in fig below.

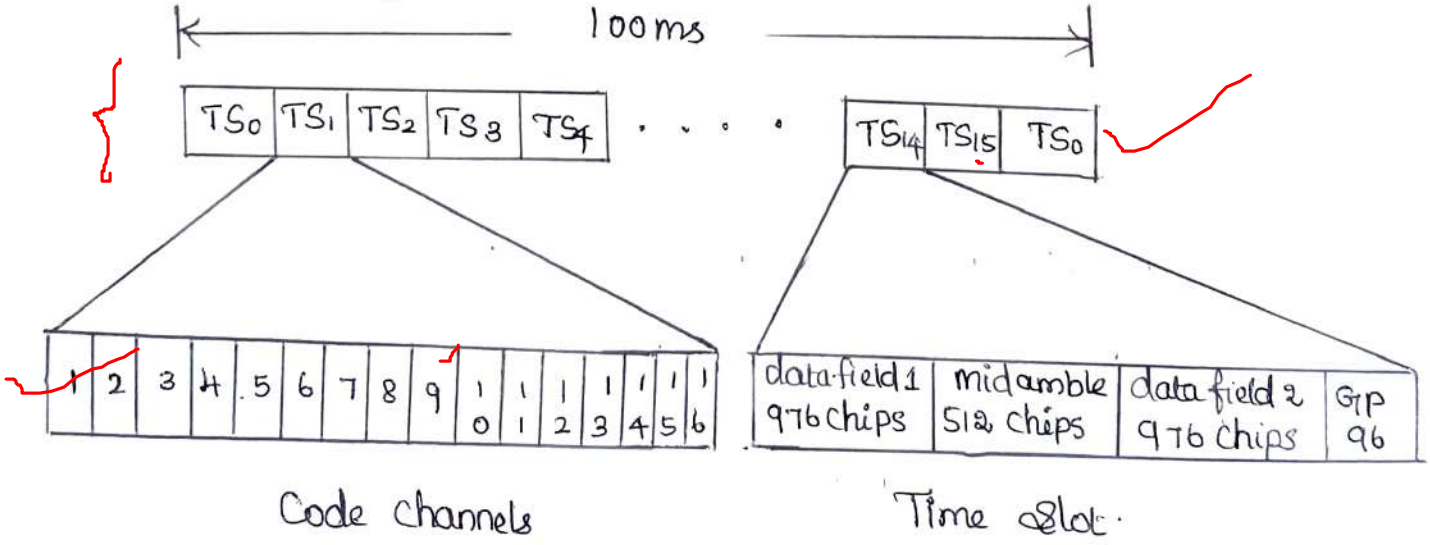


Fig : TD-CDMA channel structure.

⇒ The specific up link and down link transmissions alternate on the same radio faequency (RF) channel by allocating time slots to either the uplink or downlink with the ratio determining the relative uplink and downlink bandwidth

⇒ In TD-CDMA, Spreading, Scrambling and Channelization codes are used Spreading codes are essential element in a TD-CDMA network.

⇒ In TDD, the power control in TD-CDMA is done via a closed loop for the downlink, and for the uplink an open loop method is used.

(iv) Handover:

For the TD-CDMA systems the parameters needed in the cell selection monitoring set may include

- *) SIR
- *) path loss
- *) Interference power
- *) Received power level on BCH etc

⇒ The handover process is implemented in the mobile unit and the RNS

⇒ The RNS measures the uplink performance as well as the position information for the UE being served and uses these measurement in conjunction with defined thresholds and handover strategy to make a handover decision

TD - SCDMA :

Qn) Explain in detail about Synchronous Code division multiple Access technique.

(or)

Compare TDD & FDD, Explain Time Division Synchronous Code Division multiple Access?

⇒ In TD - SCDMA use the TDD as the radio access method has several advantages over traditional FDD networks.

① TDD has no need for paired frequencies using the same for uplink and downlink transmission.

② TDD is suitable for asymmetric uplink and downlink transmission rates, especially for Ip type data services.

③ In TDD system major attributes is its spectral efficiency with asymmetric traffic such as Ip.

(i) System Architecture :-

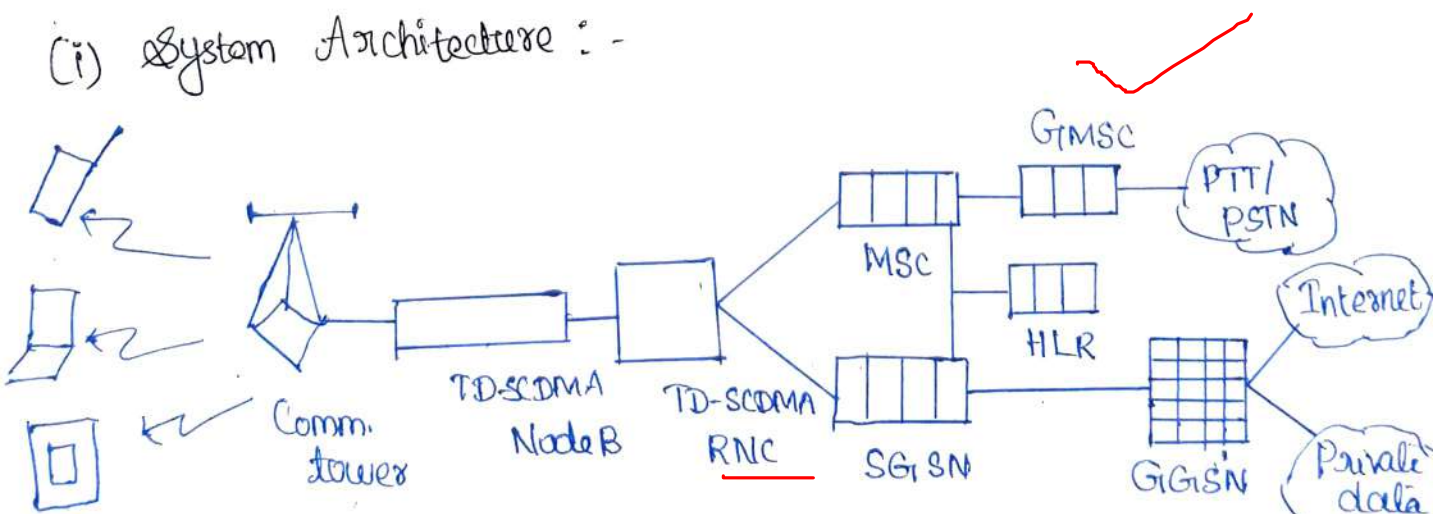


fig: TD - SCDMA System Architecture.

⇒ fig shows the general description of TD-SCDMA network that interfaces with a 3Gpp Core network only one TD-SCDMA Cell is shown other radio access systems are not shown, but they could be included easily provided that they interface at the MSC/SGSN.

⇒ TD-SCDMA uses TDD as the access method, allowing for both asynchronous and synchronous operation.

*) TD-SCDMA is a TDD network, it needs to reduce interference through a combination of interference-mitigation techniques that include the use of smart antennas and joint detection (rake receiver)

⇒ All these techniques help to reduce inferences, thereby increasing pole capacity.

⇒ TD-SCDMA supports Circuit-switched services in addition to packet (IP services). Circuit switched rates are defined as 12.2, 64, 144.4 and 2048 kbps. Packet data rates are defined as 9.6, 64, 144.4, 384 and 2048 kpbs.

(ii) Channel Structure:

⇒ The unique frame structure of the TD-SCDMA radio channel enables it to be more adaptive to network evolution.

⇒ TD-SCDMA network follows a layered approach to design and implementation.

⇒ TD-SCDMA radio resources for the uplink and downlink are allocated seperately, even though the uplink and downlink are use same carrier.

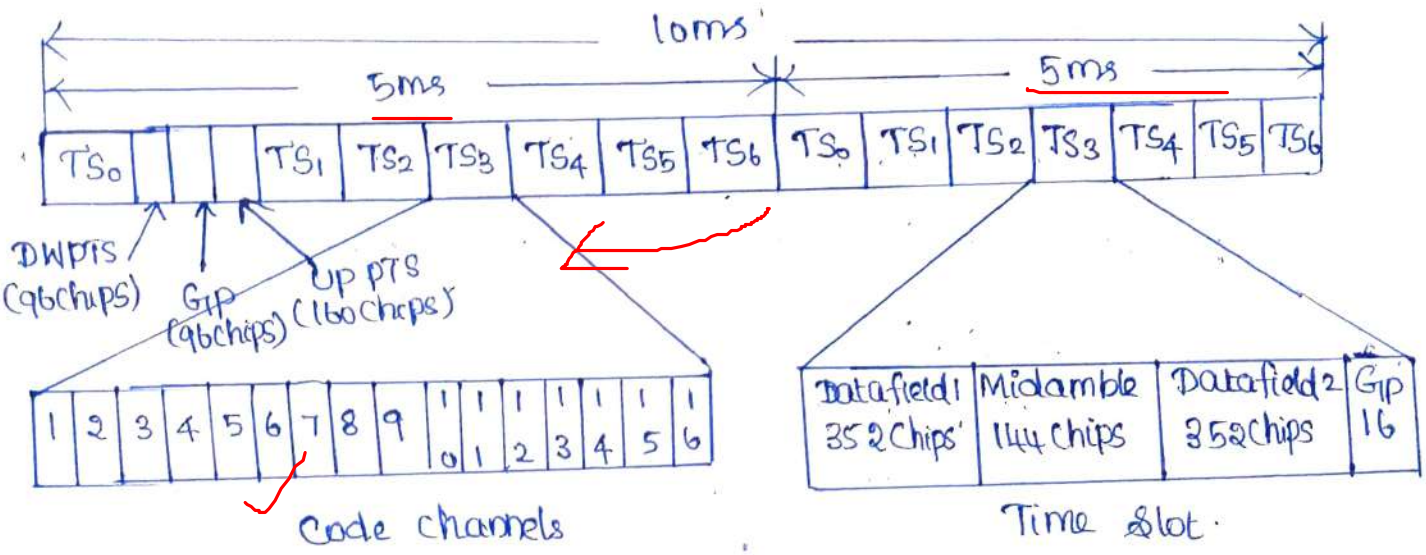


fig: TD-SCDMA Channel Structure.

⇒ fig shows the channel structure for TD-SCDMA Carrier, there are seven time slots for each TD-SCDMA Carrier.

Each of the carriers has a radio frequency that is 10ms in length as shown in fig.

⇒ The radio carrier made up of with 16 sub frames, each sub frame is made up of seven time slots.

∴ Total of 16 spreading codes are used with TD-SCDMA.

(iii) Interference - Mitigation Techniques.

⇒ It uses a combination of interference and mitigation technique that include the use of.

Smart antennas and joint detection. Synchronization and dynamic channel allocation.

All these technique reduce the interference and increasing pole capacity.

(iv) Hand over:

TD-SCDMA System, the parameters needed in the Cell Selection monitoring may include

- SIR
- path Loss
- Interference power.
- Received power level on BCH
- High speed packet data rate.

⇒ The handover process is implemented in the mobile unit and the RNS. The RNS measures the uplink performance as well as position information for the UE being served and uses these measurements in conjuction with defined thresholds and handover strategy to make a handover decision.

With neat diagram explain reference Architecture UMTS?

(or)

Explain the technique about UMTS network reference Architecture?

⇒ A UMTS System Can be divided into a set of domains and the reference points that interconnect them

fig below shows these domains and reference points.

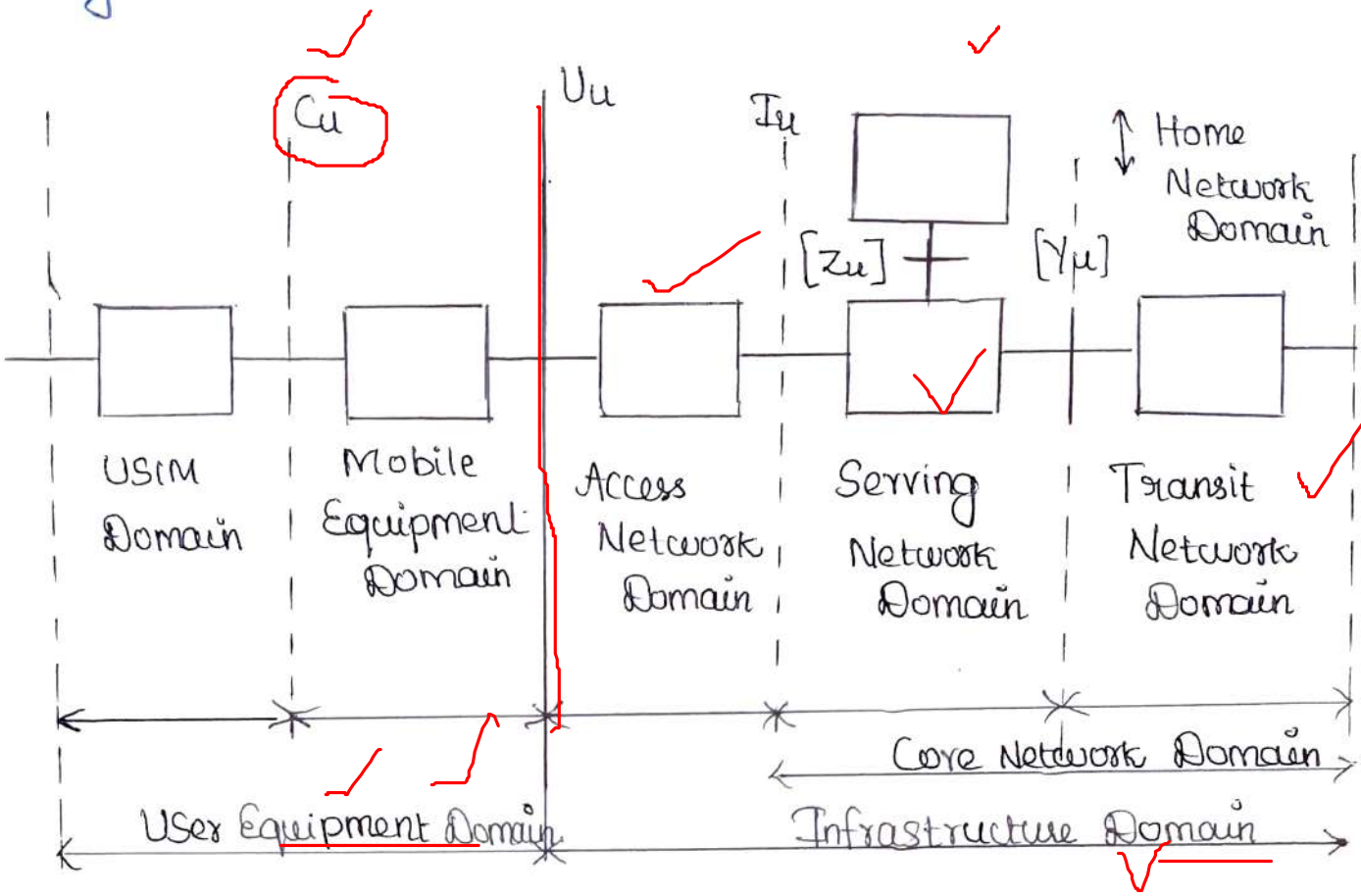


fig: UMTS domains and reference points.

*) Cu → Reference point between USIM and UE

*) Iu → Reference point between Access and Serving Network Domain.

*) Uu → Reference point between user equipment and Infra-Structure Domains. UMTS Radio Interface.

*) [Yu] → Reference point between Serving and Transit Network domain.

*) [Zu] → Reference point between Serving and home network.

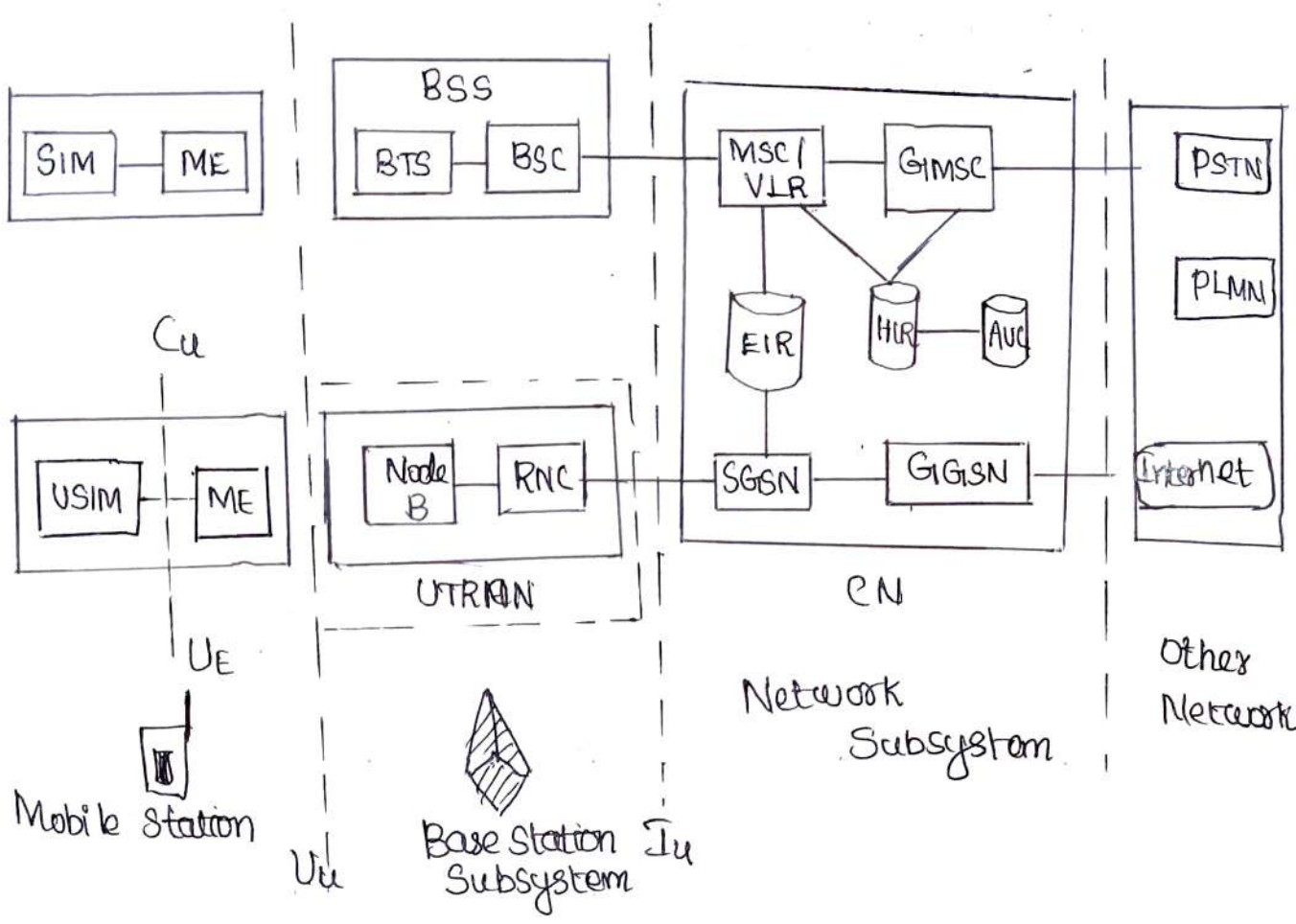
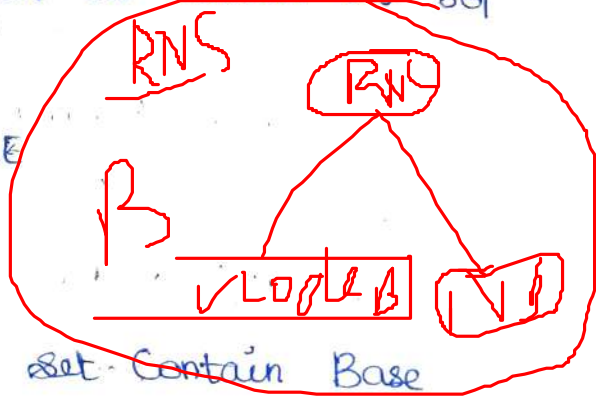


fig : UMTS - 3G reference architectures.

Mobile Station (MS) : -

In GSM (2G) mobile Station as known as 3G (user equipment)

UE → It consist of USIM & ME



Base Station Subsystem :

⇒ In GSM Basic Service set Contain Base Transceiver station (BTS) and Base Station Controller (BSC)

In UTRAN base stations as known as Node B it can controlled by Radio Network Controller (RNC)

Network Subsystem:

It's the Core Network of the System,

It consists of three,

(i) Circuit Switched domain
(ii) packet Switched domain
(iii) Information Servers.

(i) Circuit Switched Domain:-

a) MSC (Mobile Service Switching Centre):

→ It Performs the Switching and Call Control functions.

b) GMSC (Gateway MSC):

→ It is used to interface with external Circuit Switched Networks, also routing to the Calls in external networks.

c) VLR (Visitor Location Register):

→ It maintain user location and service subscription information.

(ii) packet Switched Domain:

a) SGSN (Serving GPRS Support Node):

⇒ It is used to interconnect one or more RAN to PS CN. It performs Access Control, location management, Route management paging.

b) GGSN (Gateway GPRS Support Node)

⇒ It is used to interface between ps Core Network to any other packet network.

⇒ It performs packet routing and mobility management.

(iii) Information Servers:-

a) HLR (Home Subscriber Server)

⇒ It maintain user Subscription information needed by the network.

b) AUC (Authentication Center)

⇒ It maintain the information needed by the network to authenticate each user and to encrypt the Communication over the radio path.

c) Equipment Identity Register (EIR)

⇒ It maintain International Mobile Equipment Identity of the Subscriber.

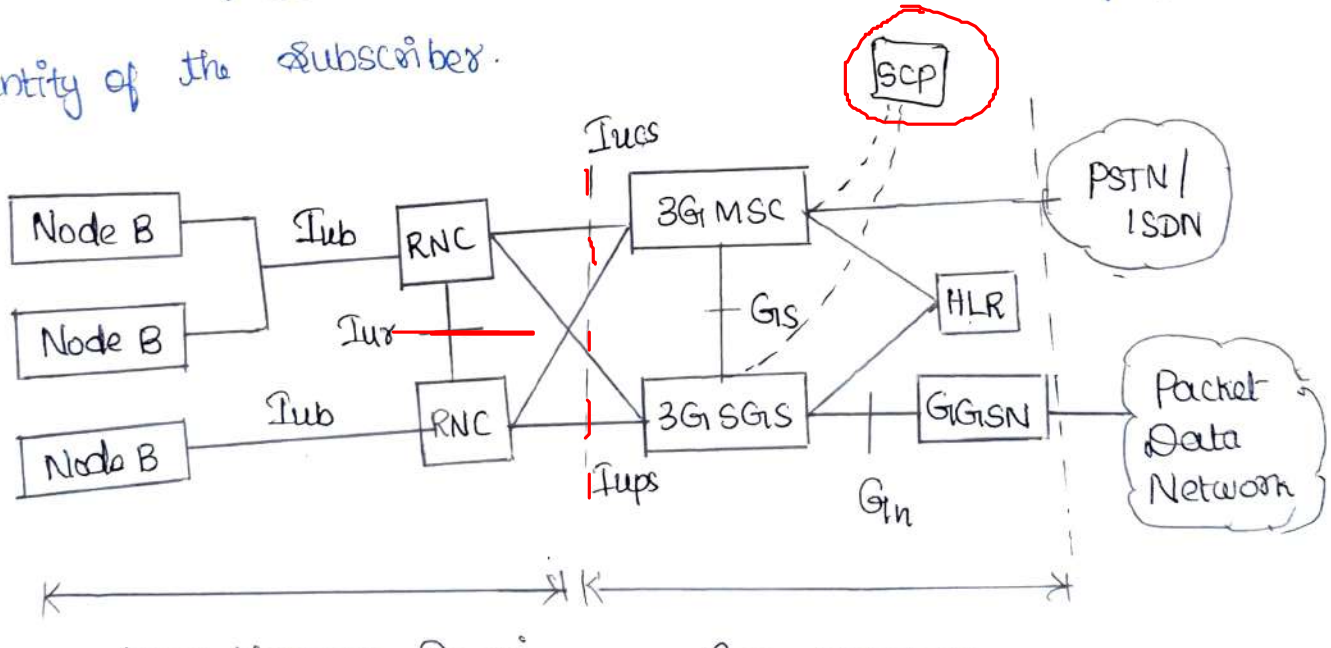


fig: Simplified UMTS Network reference model.

⇒ fig above the simplified mapping of functional entities to the domain model. This reference model

⇒ does not represent any physical architecture.

⇒ The Iu is split into two logical interferences, 'Iups Connecting the packet switched domain to the access network.

⇒ Iucs Connecting the Circuit switched domain to the access network

Iur ⇒ It logically Connect two RNCs.

Qn) Describe the channel structure in UMTS Terrestial Radio?

(or)

Explain in detail about channel structure in UTRAN?

⇒ UMTS terrestial radio access network has an access stratum and Nonaccess stratum.

⇒ access stratum includes air interface and provides function related to OSI layer 1, layer 2 and layer 3.

⇒ Non-access stratus Communication between user Equipment (UE) Core Network (CN) and layer 3.

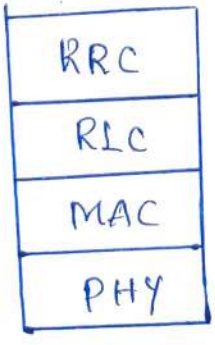


fig: OSI layer model and air interface protocols.

*) Physical layer:

It performs the following function.

→ forward Error Correction, but interleaving and rate matching

⇒ Signal measurements.

⇒ Modulation, spreading, demodulation, despreading of physical channels.

*) Medium Access Control: (MAC)

⇒ It is responsible for efficiently tranfering data for both real time (CS) and non real time (PS) services to the physical layer.

MAC is responsible for

⇒ Selection of appropriate transport format with in a predefined.

⇒ Priority handling between data flow of a user as well as between data flows from several uses.

*) Radio link control (RLC)

It sets up a logical link over the radio interface and is responsible for fulfilling QoS requirements.

⇒ Segmentation and Assembly of the packet data unit

⇒ Transfer of user data

⇒ Error Correction through retransmission

⇒ Sequence Integrity.

Radio Resource Control (RRC):

⇒ It broadcast system information, handles radio resources and controls the requested QoS.

The RRC layer offers the following services.

→ General Control (GC) Service used as an information broadcast Service.

→ Notification (NT) Service used for paging and notification of selected UE.

→ Dedicated Control (DC) Service used to establish/release a connection and transfer messages.

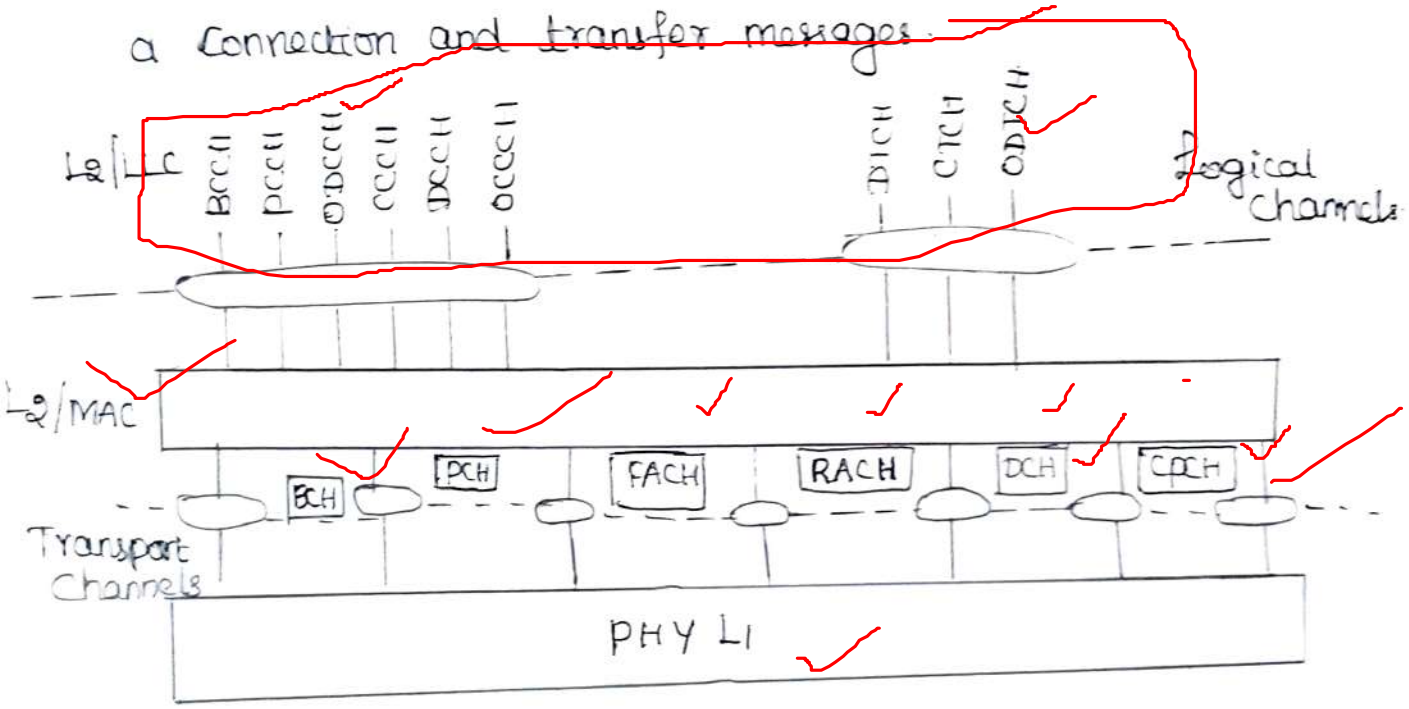


fig: UTRAN Channels.

UTRAN channels divided into three

(i) Logical Control channels

(ii) Logical traffic Channels

(iii) Common transport Channels.

(i) Logical Control Channels in UTRAN

a) Broadcast Control channel (BCCH): It provides broadcasting & Control information.

b) paging Control Channel (PCCH). It's used to transfer page information

c) Common Control Channel (CCCH):

⇒ It is bidirectional Channel to transfer Control information between network and mobile.

d) Dedicated Control Channel (DCCH):

⇒ It is a point-to-point bidirectional Channel to transmit delicated information between mobile network.

e) ODMA Common Control Channel (OCCCH):

⇒ Bidirectional Channel to transmit Control information between mobiles.

f) ODMA dedicated Control Channel (ODCCH):

⇒ Point-to-multipoint bidirectional Channel to transmit dedicated Control information between mobiles.

(ii) Logical traffic Channels in UTRAN:

a) Dedicated traffic Channel (DTCH):

⇒ Point-to-point dedicated to one mobile to transfer user information.

b) ODMA traffic Channel (ODTCH):

Point-to-point channel dedicated to one mobile to transfer user information between mobiles.

(iii) UTRAN Common transport Channels:

(a) Broadcast Channel (BCH): broadcast cell specific information transmitted over the entire cell with low fixed bit rate.

b) Forward access channel (FACH):

⇒ Transmitted over entire cell or only part of the cell.

c) paging channel (PCH):-

⇒ Transmit the physical layer signal, the Paging indicator, to Support efficient sleep mode procedure.

d) Random access channel (RACH):

⇒ Received over the entire cell, characterized by a limited size data field.

e) Common packet channel (CPCH):

⇒ Contention based random access channel used for transmission of bursty data traffic.

f) Downlink shared channel (DSCH):

⇒ DL channel shared by several mobiles, associated with a DCH.

UNIT : IV

INTERNETWORKING BETWEEN WLAN's and WWANS

Internetworking objectives and requirements, Schemes to Connect WLANs and 3G Networks, Session Mobility, Internet working Architecture for WLAN & GPRS, Multichannel multipoint Distribution System. System Description, Local multipoint distribution Service.

Internetworking Objectives and Requirements :

Qn) What are the requirements for interworking between a wireless wide Area Network (WWAN) & WLAN?

(or)

Explain in detail about internetworking objectives and requirements?

Internetworking objectives :-

⇒ The main objectives of interworking is to allow independant WLAN and 3Gpp (WWAN) standards.

⇒ It extend of interdependence between these standards should be minimized or localized at the point of inter Connection.

⇒ A user is availing 3Gpp services and is using a WLAN device, it must be made possible to use 3Gpp facility without hardware / software upgrades.

⇒ 3Gpp services must be made available to the end user without any additional expenditure on his side.

Requirements for interworking :-

(i) Common billing and customer care :-

⇒ It provides a common bill and customer care to the subscriber but otherwise requires no real interworking between the WLAN and 3Gpp data networks.

(ii) 3Gpp based access control and charging :-

⇒ To enable a mobile subscriber to use his (SIM/USIM) to avail the WLAN services. Authentication, Authorization and Accounting (AAA) is required for WLAN uses to access 3Gpp data networks.

(iii) Access to 3Gpp based packet switched services :-

⇒ To enable WLAN subscribers to use 3Gpp based packet switched services, This allows WLAN uses to access 3Gpp data services in both 3Gpp and WLAN networks.

(iv) Service Continuity :-

⇒ The goal is to allow seamless service Continuity across the 3Gpp and WLAN systems.

The service Provider should be smooth across both

3Gpp and WLAN Systems without Compromising on quality and totally avoiding disruptions.

(v) Access to 3Gpp Circuit - Switched Services:

⇒ The goal of this requirements is to allow the 3Gpp operator to offer access to Circuit Switched Services such as Voice Calls from the WLAN systems.

Schemes to Connect WLANS and 3G Networks:

Qn: Discuss briefly the various ways to achieve interworking between a WWAN and a WLAN ?

(or)

Explain in detail about Schemes to Connect WLAN & 3G networks.

⇒ Interconnecting Schemes can be Categorized as three approach

*) Mobile Ip approach (loose coupling)
*) Gateway approach
*) Emulator approach (tight Coupling)

① Mobile Ip approach (Loose Coupling):

⇒ This mechanism can be implemented in the mobile nodes and installed on the network devices of 3G and WLANS.

⇒ This approach provides Ip mobility for roaming between 3G and WLANS.

⇒ It requires installing mobile Ip devices such as home agent (HA) and a foreign agent (FA) in both networks. and terminal devices should also implement mobile Ip features.

⇒ The user device requires sending the registration back to its home network, packet delay and loss are also a problem for hand offs.

⇒ This approach suffers from the triangular routing between networks if mobile Ip does not support route optimization.

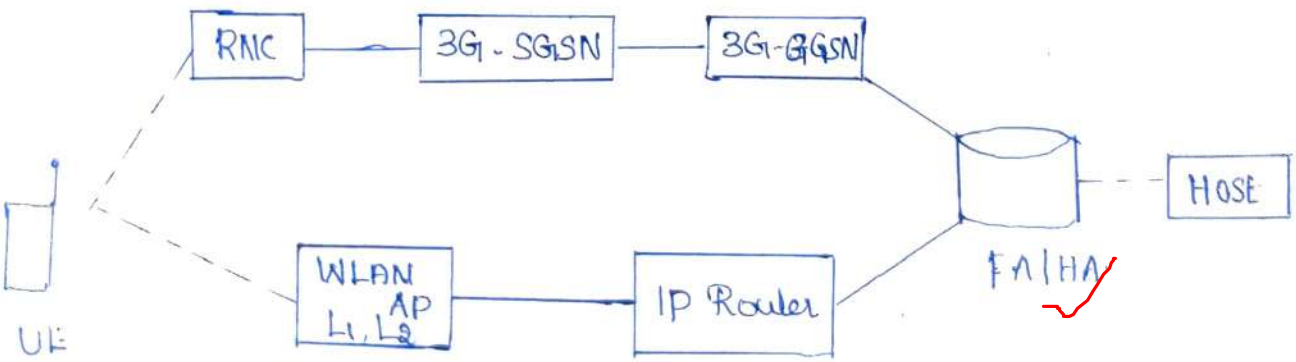


fig: Architecture of mobile Ip approach

UE : User Equipment

AP : Access point

RNC : Radio Network Controller

3G - SGSN : 3G Serving GPRS Support Node

3G - GGSN : 3G Gateway GPRS Support Node

FA : Foreign Agent HA : Home Agent.

(2) Gateway Approach

⇒ The Gateway Approach introduce a new logical node to connect two wireless networks.

⇒ The new node is located between the two networks and act as an internal device.

⇒ It exchange the information between the two networks, Converts Signals and forwards the packets for the roaming users.

⇒ It aims to seperate the operation of two networks, which implies the two networks are peer-to-peer, and can handle their subscriber independently.

⇒ With the two network operator having a roaming agreement, the logical node helps two networks offer intersystem roaming.

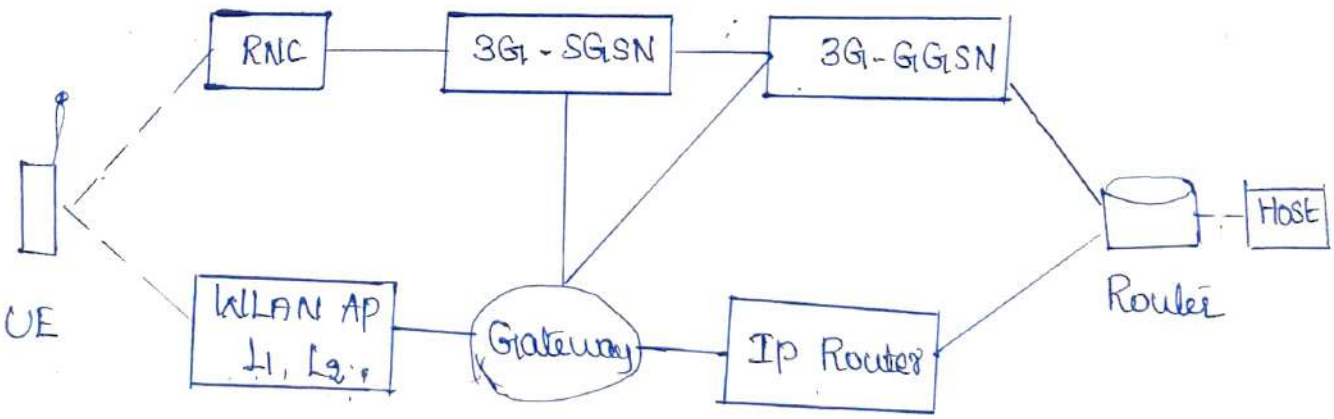


fig: Architecture of the gateway approach

Advantage:

*) Two networks can be operated independently, Packets for roaming users go three the node without processing by mobile Ip. ∴ delay and loss during handoff can be minimized.

③ Emulator Approach (tight Coupling):

*) This is also called as tight Coupling. It uses WLAN as basic access in the 3G networks.

⇒ It also replaces 3G basic accesses by WLAN layer1/ layer 2.

⇒ The Access point (AP) of WLAN could be viewed as 3G network Controller. It is like a Serving GPRS Support node ~~Saf~~ SGSN respectively.

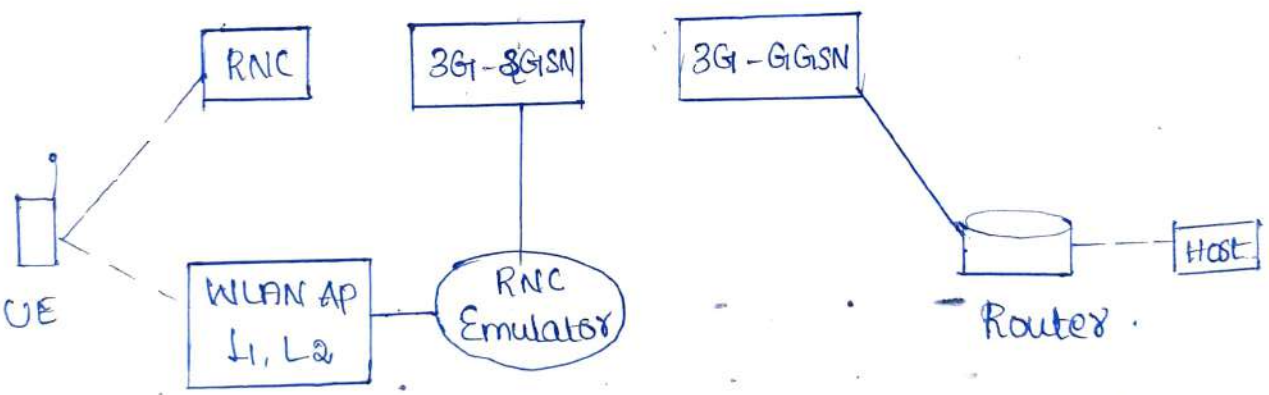


fig: Architecture of emulator approach.

Advantage:

*) The main use of emulator approach is that mobile IP is not needed. The 3GPP Core network takes care of packet routing and forwarding processes.

*) The packets loss is reduced to a significant level. Delay is also minimized.

Disadvantages:

⇒ It has less flexibility because of the tightly coupled networks arrangement.

⇒ The gateway GPRS support node (GGSN) is the only point to the Internet. hence all the packets have to travel first through this node.

⇒ GGSN acts as a bottleneck at same point of time.

Session Mobility :-

Qn: Give the short notes about session mobility?

(or)

Define session? Explain in detail session Mobility?

⇒ Session is defined as a flow of Ip packets between the end-user and an external entity.

∴ When there is a flow of packets in a networked environment session mobility enables easy roaming

eg: FTP or HTTP session

Consider a mobile device capable of connecting to the data network through WLANs and 3Gpp networks.

⇒ The end-user is connected to the data network and is in session flow through one access network say a WLAN.

⇒ As the user moves out of the coverage area of the WLAN, the end devices detect the

failing WLAN Coverage and seamlessly switched the flow to the 3Gpp network.

⇒ The end-to-end session remains unaffected. Typically no user intervention would be required to perform the switch over from WLAN to 3Gpp.

⇒ When the user moves back into the Coverage of the WLAN System, the flow is handed back to the WLAN.

Internetworking Architecture for WLAN and GPRS:

Qn: Discuss about internetworking Architecture for WLAN and GPRS?

(or)

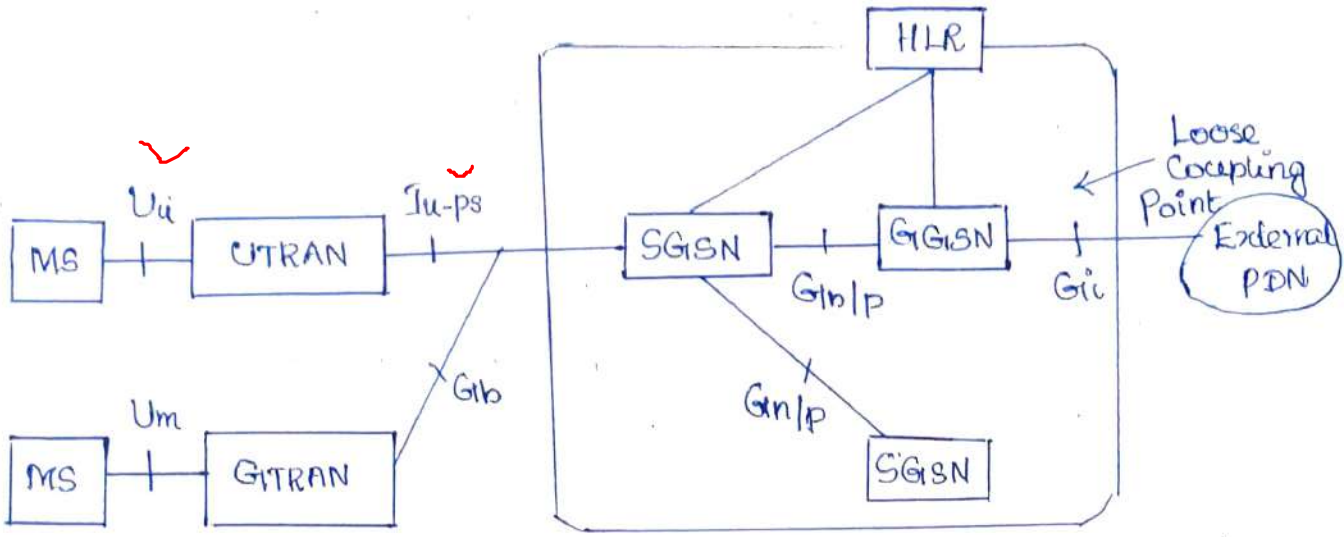
Explain in detail about internetworking Architecture for WLAN and GPRS?

⇒ In Internetworking of WLAN and other Cellular Standards like GPRS aims to provide high quality Circuit Switched Voice Service to the mobile users. The different characteristics of Cellular network interacts with the wireless local area networks (WLANS)

*) Two Generic approaches for interworking.

(i) loose Coupling.

(ii) tight Coupling.



MS : Mobile Station

UTRAN : UMTS Terrestial Radio Access Network.

GITRAN : GPRS Terrestial Radio Access Network

SGSN : Serving GPRS Support Node.

GGSN : Gateway GPRS Serving Node.

HLR : Home Location Register

PDN : packet Data n/w

fig: GPRS reference diagram with WLAN Coupling points.

(i) Tight Coupling :

In Tight Coupling WLAN is Connected to the 3Gpp (GPRS) Core network (or) any other radio access networks (RAN), such as GPRS RAN and UMTS terrestrial RAN (UTRAN).

*) WLAN data traffic goes through the GPRS Core network before reaching the external packet data networks.

⇒ With tight coupling the WLAN is connected to either Gb or Iu-ps reference points.

⇒ In tight coupling approach, 3GPP system based access control and charging is used. This requires AAA for subscribers in the WLAN to be used on the same AAA procedure used in the GPRS system.

Advantages :-

⇒ The advantages of tight coupling architecture between IEEE 802.11 WLANs and GPRS are the following,

(i) Seamless Service Continuation across WLAN and GPRS

⇒ The users are able to maintain their data sessions as they move from WLAN to GPRS and vicevers. For services with tight coupling quality of service (QOS) requirements, seamless service continuation is subject to WLAN QOS capabilities.

(ii) Reuse of GPRS AAA

(iii) Reuse of GPRS infrastructure (eg subscriber data bases, billing systems) and protection of cellular operator investment

(iv) Common provisioning and Customer Care

(v) Increased Security, since GPRS authentication and ciphering can be used on top of WLAN ciphering.

vi) Support of lawful interception for WLAN Subscribers.

(ii) Loose Coupling :-

In Loose Coupling WLAN · Utilizes the subscriber data bases in the GPRS network but features no data interfaces to the GPRS Core network.

*) The loose coupling architecture between the GPRS and the WLAN at the Gi reference point is indicated.

*) This means, WLAN bypasses the GPRS network and provides direct network data access to the external packet data networks (PDNs).

Advantage :-

⇒ It is used in SIM or USIM based authentication and billing.

⇒ In this approach a Subscriber can reuse the SIM Card or USIM Card to access a set of wireless data services over a WLAN.

System Description with tight Coupling :-

Qn: Explain in detail about tight Coupling System Configuration?

(or)

Discuss tight Coupling architecture between the IEEE 802.11 WLAN & GPRS

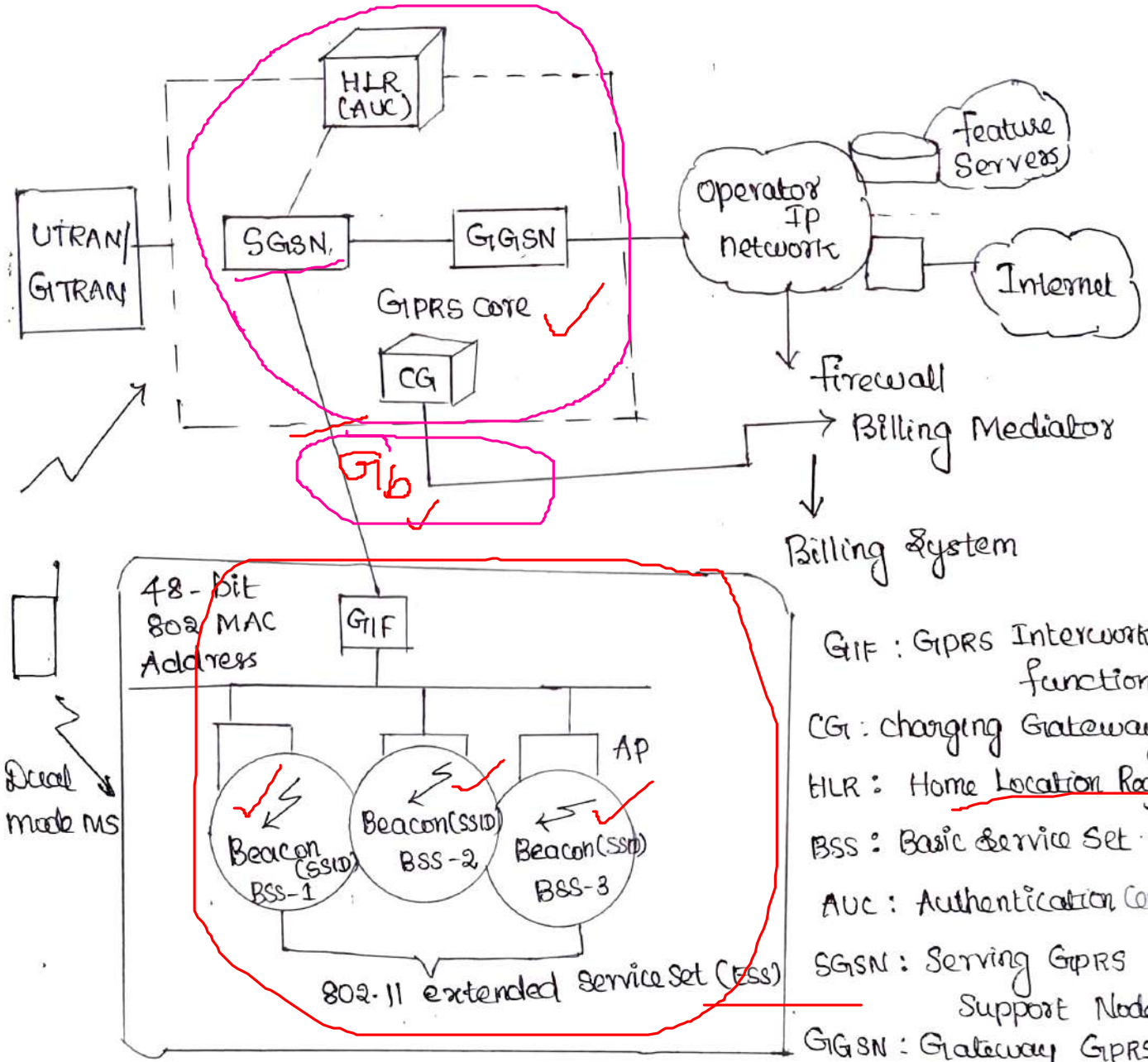


fig: WLAN - GPRS integration with tight Coupling system configuration.

WLAN Network :-

* WLAN, one or more Ap Connected to the distribution system.

*) APs behave like base stations and mobile exchange data only with APs. The service area of an Ap is called a basic service set.

⇒ More number of BSS together form a Extended Service Set (ESS)

GPRS Core network:

*) The WLAN network Connect to the GPRS Core network through the Standard Gib interface.

*) From the Core network point of view, the WLAN is Considered as other GPRS routing areas (RAS) in the System.

*) The GPRS Core network does not identify the difference between an RA with WLAN radio technology and One with GPRS radio technology.

GIF:

⇒ The key functional element to the System is the GPRS interworking function (GIF), which is Connected to a distribution System and to an SGSN via the Standard Gp interface.

⇒ It provide a standardized interface to the GPRS Core network and to virtually hide the WLAN.

⇒ When a mobile station is outside the WLAN area, its WLAN interface is in passive scan mode, that is it scans a specific frequency band and searches for a beacon signal. When a beacon is received the service set identifier (SSID) is checked and compared against a Pre-Configured SSID.

⇒ The SSID Serves as a WLAN identifier and can help mobiles attach to the Correct WLAN.

⇒ When an MS detects a valid SSID, it performs the typical authentication and association procedures. It then enables its WLAN interface and further signalling is carried over this interface.

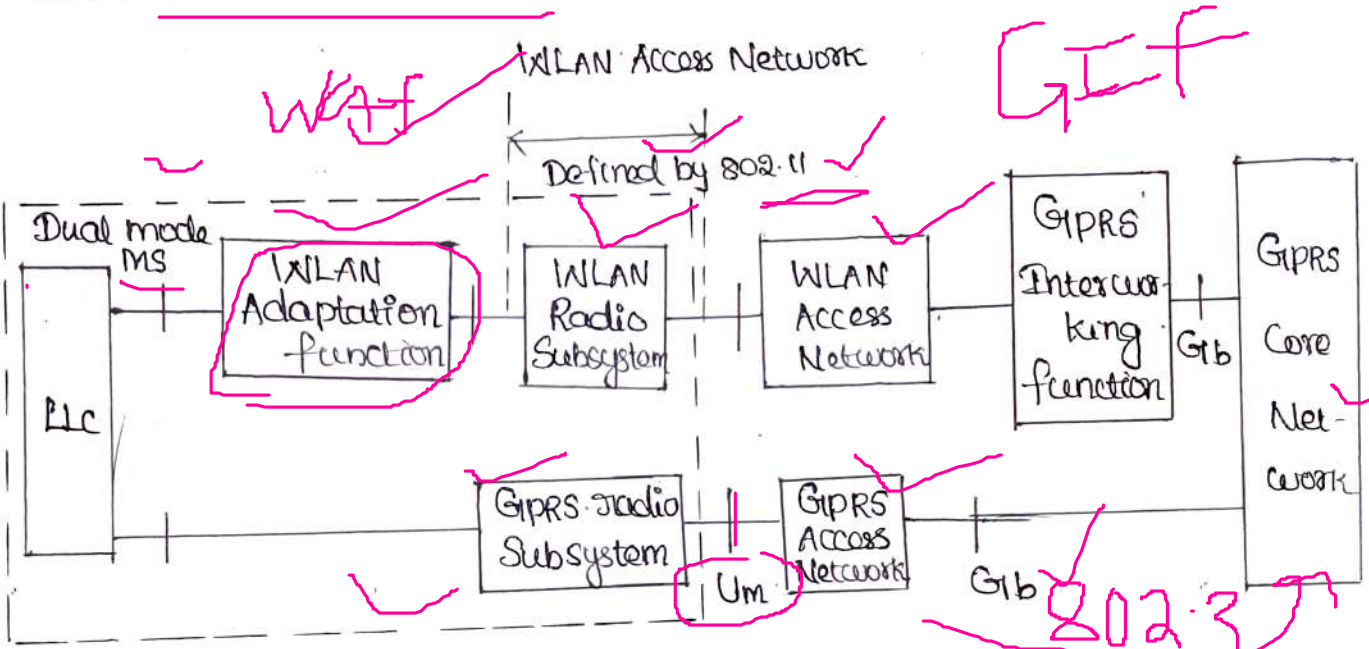


fig: Tight Coupling over Gb interface a reference diagram.

⇒ Mobile Stations are dual mode, that they support both GPRS and WLAN access in a Seamless fashion.

⇒ System mobility is achieved by means of the routing area update (RAU) procedure which is the Core mobility management procedure in GPRS.

⇒ When mobile enter into a WLAN area RAU procedure take place and Subsequent GPRS Signalling

and user data transmission carried over WLAN interface.

⇒ Similarly When the mobile exist WLAN area, another RAU Procedure take place and the GPRS interface is enabled and used to carry further data and signalling traffic.

⇒ In fig The MS has two radio subsystem, one for GPRS access and another for WLAN access.

WAF (WLAN Adaptation function):

⇒ It identifies when the WLAN radio subsystem is enabled and informs the LLC layer, which subsequently redirects signalling and data traffic to the WLAN.

LLC:

GPRS protocols are used, Subnet work dependent Convergence protocol (SNDCP), GPRS Mobility Management (GMM) and session management are used in both the GPRS and WLAN.

*) ~~Below~~ fig shows that the MS supports two radio subsystems for transporting GPRS signalling and user data.

*) The first interface is implemented with GPRS specific radio link Control (RLC) MAC and physical layers.

*) The second interface is implemented with 802.11 specific MAC and physical layer.

⇒ These two interfaces provide two alternative means for transporting LLC packet data units. (PDUs)

⇒ When the MS is outside a WLAN area, LLC PDUs are transmitted over the GPRS interface. (Um).

WAF :

⇒ These two interface switching is performed using WAF and completely transparent to the user and upper GPRS layer.

*) It operates in both MS & GIF

⇒ It provides an adaptation function for interworking between LLC and 802.11 MAC (in the mobile) and between 802.3 MAC and BSSGP (in GIF).

GIF :

The GIF also implements the GPRS protocols specified on Gb interface frame relay (FR), network service (NS) and base station subsystem GPRS protocol (BSSGP)

AP :

The AP implements the 802.11 and 802.3 protocols and a simple interworking function that provides bridging between them.

(ii) WLAN Adaptation function :

⇒ The WAF is implemented in every dual mode MS & GIF.

WAF Provides the following function

(1) It signals the activation of the WLAN interface when a mobile enters a WLAN area. It also signals the change of RA to GMM when a mobile enters a WLAN area and gets associated with an AP

(2) It supports the GIF / RAT discovery procedure, which is initiated by MS in order to discover the MAC address of GIF & RA Identity (RAI) of the WLAN

(3) It transfer uplink LLC PDUs from MS to the GIF by using the transport services provided by the 802.11 MAC It also transfers downlink LLC PDUs from the GIF and in the MS.

(4) It supports QoS by implementing transmission schedu-ling in the GIF and in the MS

(5) It transfers the temporary logical link identifier (TLLI) and QoS information in the WAF header. The TLLI is a temporary MS identifier used by the LLC layer for addressing purposes.

Encapsulation scheme :

⇒ The encapsulation scheme used in the uplink direction as well as the format of a WAF PDU are shown in fig.

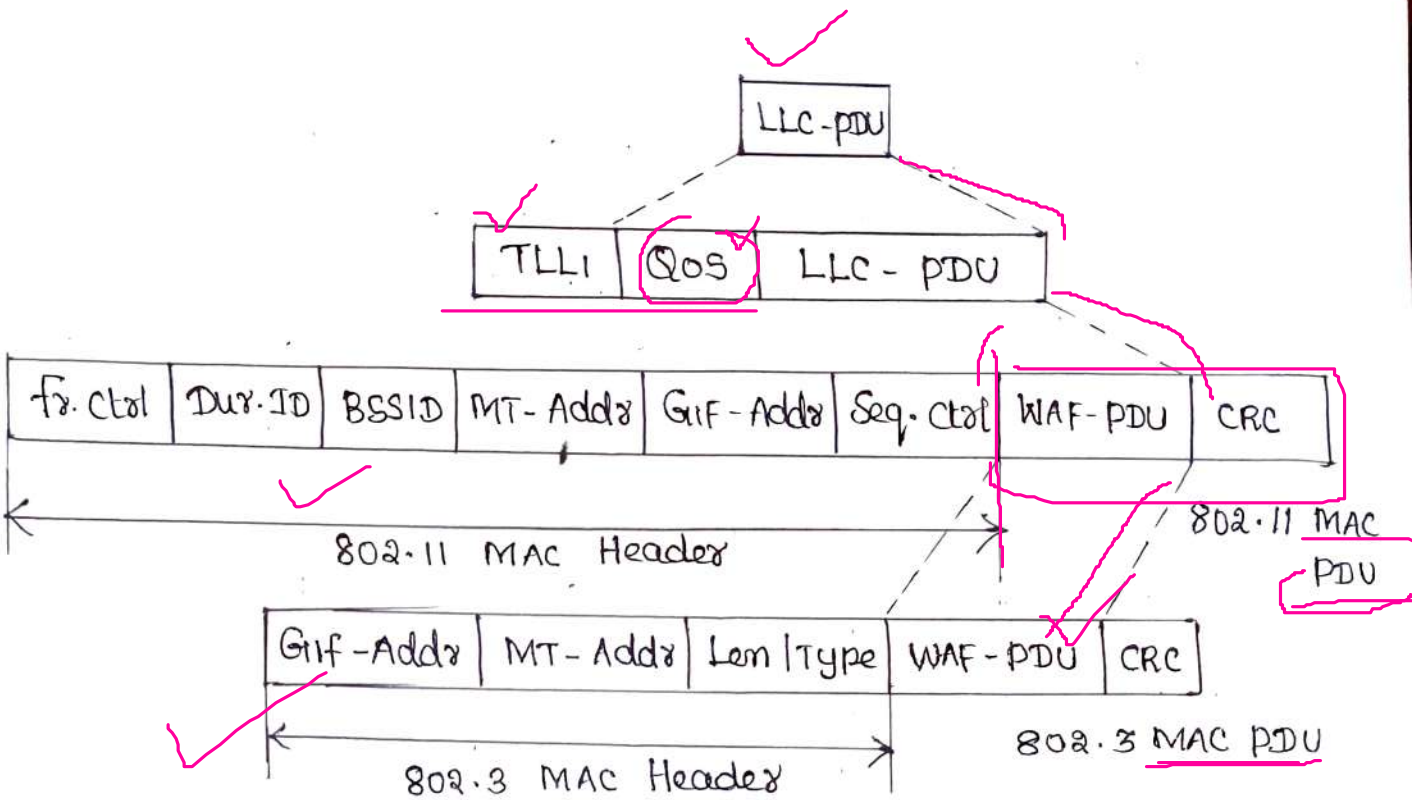


Fig: The encapsulation scheme

WAF PDU:

*) Each LLC PDU is encapsulated into a WAF PDU, which includes the TLLI and QoS in the header.

TLLI → Temporary MS identifier used by the LLC layer for addressing purposes.

The TLLI is used by the GIF to update an internal mapping table that correlates TLLI with 802 MAC address.

⇒ The correlation between TLLI & 802 MAC address is used for forwarding downlink LLC PDUs received on the Gb interface to the correct mobile on the WLAN.

QOS :

⇒ In the uplink direction, QOS contain the following attributes

*) Peak throughput
*) Radio priority
*) RLC mode

⇒ These QOS attributes are primarly used for Scheduling in the MS & GIF.

⇒ In downlink direction QOS may be empty, since there is no need to transfer any QOS parameters to the mobile

⇒ IEEE 802.11 & IEEE 802.3 MAC headers encapsulated in the WAF - PDU

(iii) GIF / RAI Discovery Procedure :

It's carried out immediately after an MS enters an 802.11 WLAN area and gets associated with an AP

⇒ The WAF in the MS initiates this Procedure :

(i) To discover the 802 MAC address of GIF. All uplink LLC PDUs are subsequently transmitted to this MAC address

(ii) To discover the RAI that corresponds to the WLAN network.

(iii) To send the MSs IMSI Value to GIF.

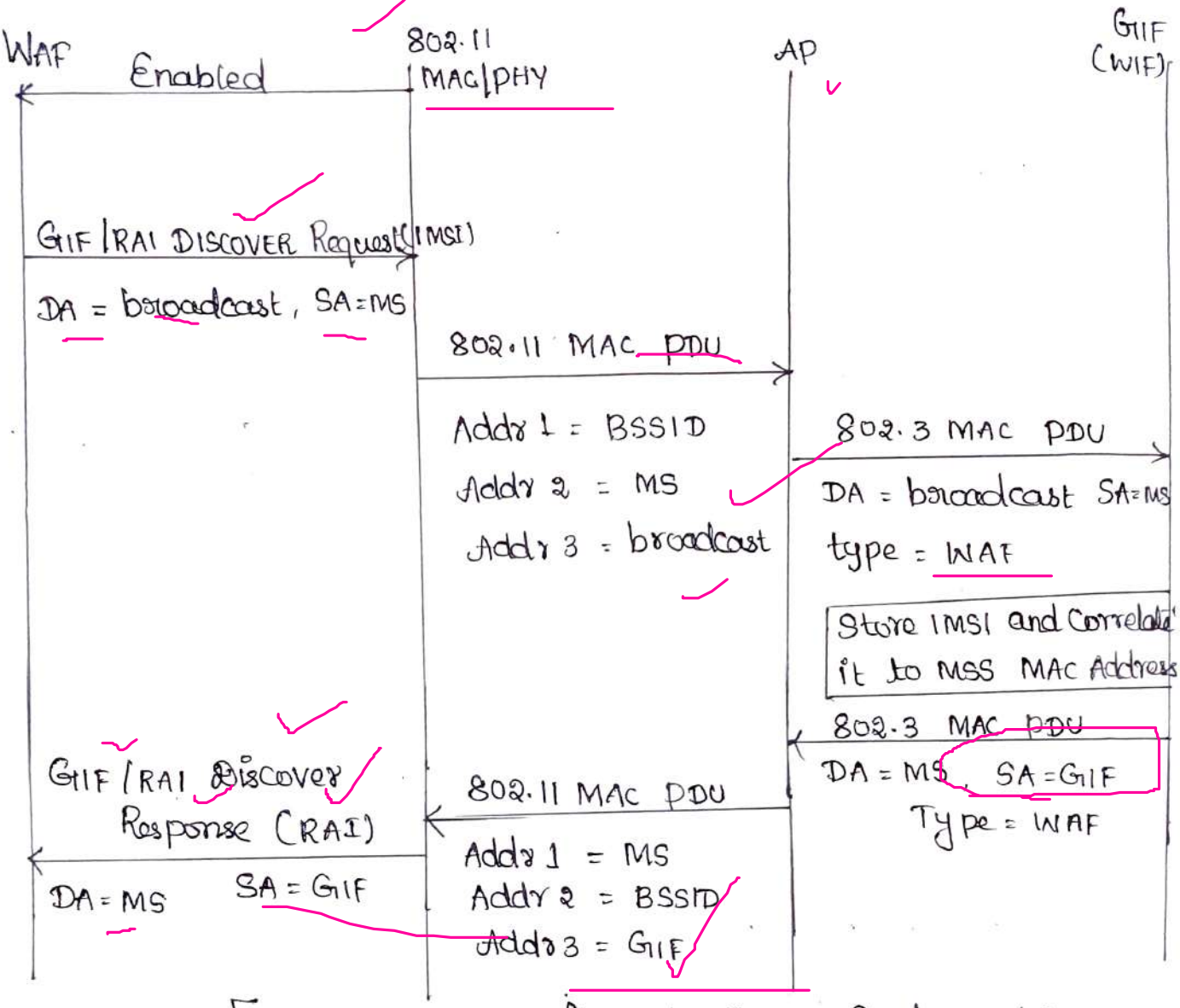


Fig: Signalling flow during a GIF/RAI discovery Procedure.

Fig shows the signalling flow during the GIF/RAI Procedure:

① The Procedure is initiated after the 802.11 MAC layer is enabled.

② WAF layer in the MS sends a request to 802.11 MAC to transmit a PDU with a source address (SA)

equal to MS's MAC address and a destination address equal to broadcast.

⇒ This PDU is a GIF/RAI discover request message that includes the IMSI Value of the MS.

③ The 802.11 MAC layer transmits an 802.11 MAC PDU with the Appropriate address information (designated Addr 1, Addr 2, Addr 3) this PDU is directed to the AP with identity BSSID.

④ The AP broadcast this message to the MS and finally received by GIF, which associates the IMSI with the MSS 802.11 MAC Address.

⑤ The MS receives this response, stores the GIF address and the RAI and notifies the GMM layer that the current GPRS RA has changed.

⑥ WAI in the GIF responds with GIF/RAI discover response that include the RAI of the WLAN.

System Description with Loose Coupling:-

Q) Discuss loose Coupling architecture between the IEEE 802.11 WLAN and GPRS? (13m)

(or)

Explain in detail WLAN GPRS integration using loose Coupling?

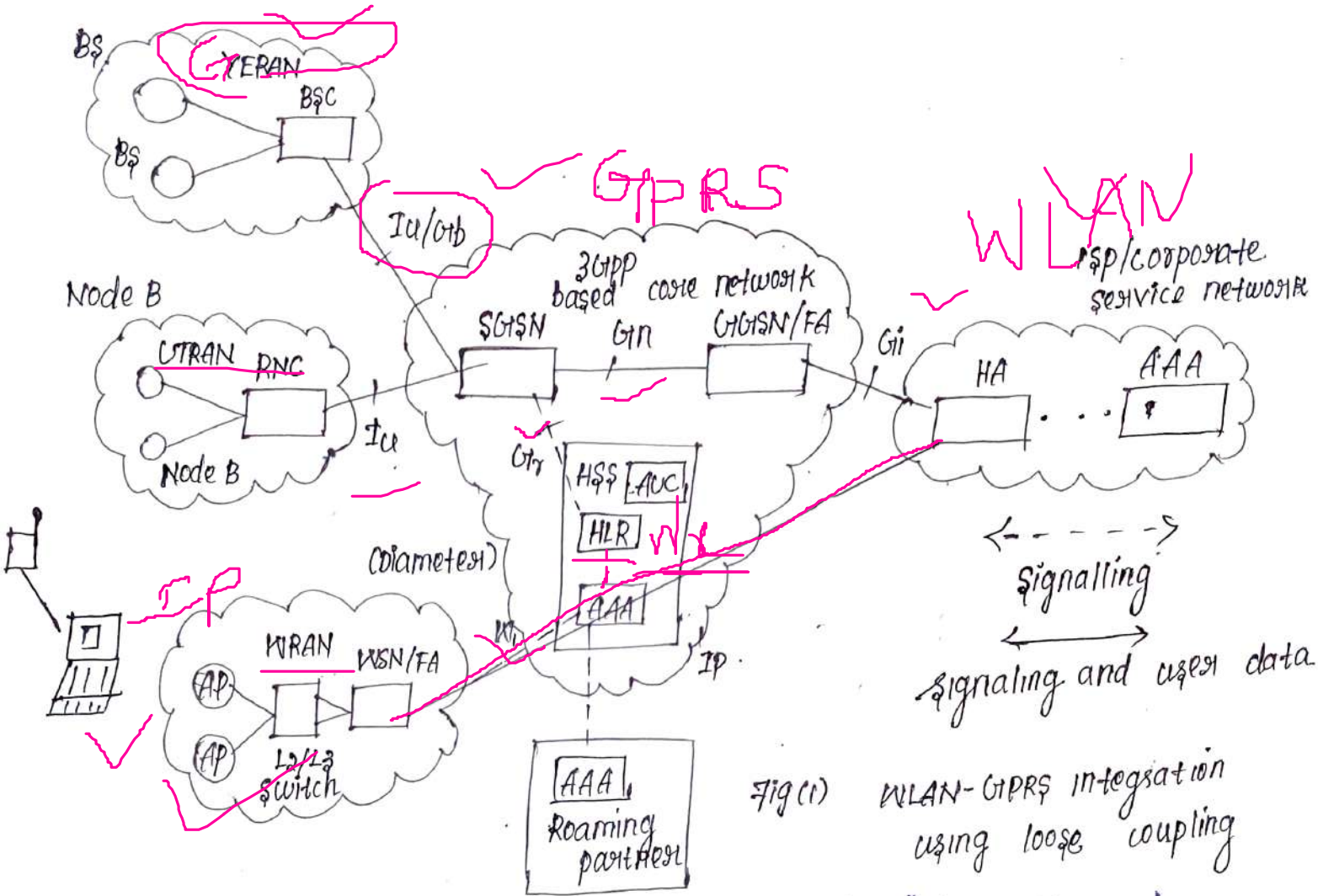


Fig (1) WLAN-GPRS integration using loose coupling

⇒ The loose coupling that provides interworking between GPRS and WLAN at the Gi interface.

⇒ The WLAN data traffic does not pass through the GPRS core network but goes directly to the operators IP network.

*) This architecture supports the integrated billing, via the billing mediator in a common billing system.

*) Loose coupling utilizes standard IETF-based protocols for authentication accounting and mobility.

*) The WLAN access network connects to the GPRS data network like a different type of radio access network

for interworking, which commonly support RADIUS/ DIAMETER protocols in the WLAN access network.

In this approach some new interfaces are used:

1) Wx interface:

In fig (1) using Wx interface. This interface connects the AAA server with HLR/HSS.

⇒ The AAA server retreives the authentication vectors over this interface form the HLR/HSS, also retrives the WLAN access related subscriber information.

*) It is similar to the mobile application part (MAP) Gr interface defined between SGSN and HLR/HSS. This interface is based on MAP or DIAMETER protocol.

2) Wb/Wr interface:

This interface connects the WLAN access network with the visited 3Gpp data network or the home 3Gpp data network. The Wr interface transports authentication, authorization, charging related information.

3) Wn interface:

This interface transports tunneled WLAN user data towards the packet data gateway in the home network.

In Wn ~~method~~ interface two methods of tunneling used.

(i) Establish Secure tunnel between the WLAN access network and the packet data gateway. This method is called network based tunneling as the WLAN user is not involved.

(ii) Establish direct Secure tunnel between WLAN user Client and the packet data gateway. This method is called Client based tunneling.

4) Wf interface:

⇒ This interface Connects the AAA Server with the 3Gpp Charging Control function or Charging gateway function

⇒ The charging data is Collected by the AAA Server from either the packet data gateway over the Wm interface or the Wb interface from the WLAN network or both. This interface is based on DIAMETER or GPRS tunneling protocol (GTP).

5) Wo interface:

This interface Connects the AAA Server with 3Gpp on-line charging System for Credit Control Checks for the WLAN Capable User. This is based on DIAMETER Protocol.

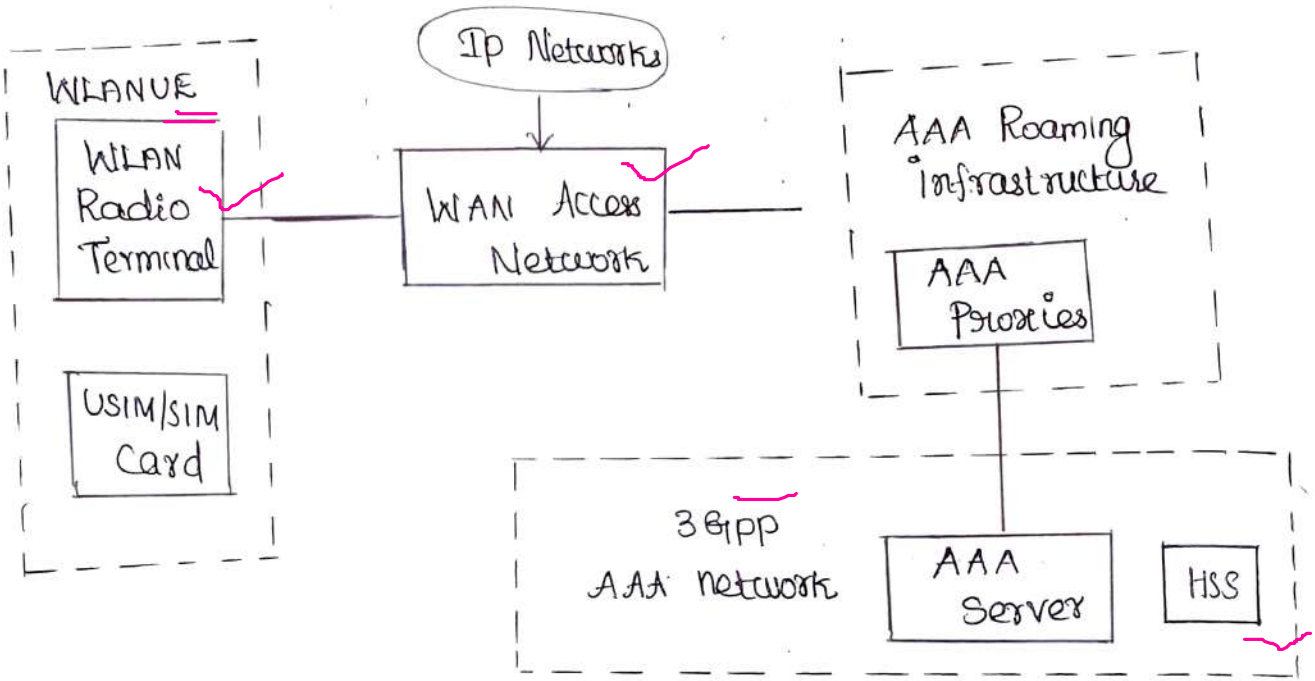
6) Wm interface:

⇒ This interface Connects the AAA Server with the packet gateway for transport charging, tunneling. This interface is based on DIAMETER protocol.

7) Wi interface :

This interface connects the packet data gateway with the packet data network.

(i) Authentication :



HSS : Home Subscriber Server.

AAA : Authentication, Authorization, Accounting.

UE : User Equipment

fig: WLAN System architecture reusing the 3Gpp Subscription.

⇒ Where the GPRS operator owns the WLAN, the operator will reuse SIM based authentication or 3Gpp-based USIM authentication for UMTS Subscriber within the WLAN Environment.

⇒ To reused 3Gpp Subscription, 3Gpp interworking WLAN terminals will need access to UICC Smart Cards

With SIM/USIM applications.

*) A WLAN equipped with a SIM/USIM smart card is called WLANUE.

→ Given the need for dual-mode (WLAN-Cellular) UEs, SIM/USIM will be available in those UEs. The fig above shows the architecture of interworking WLAN access reusing 3GPP USIM/SIM an HSS.

SIM based authentication over WLAN

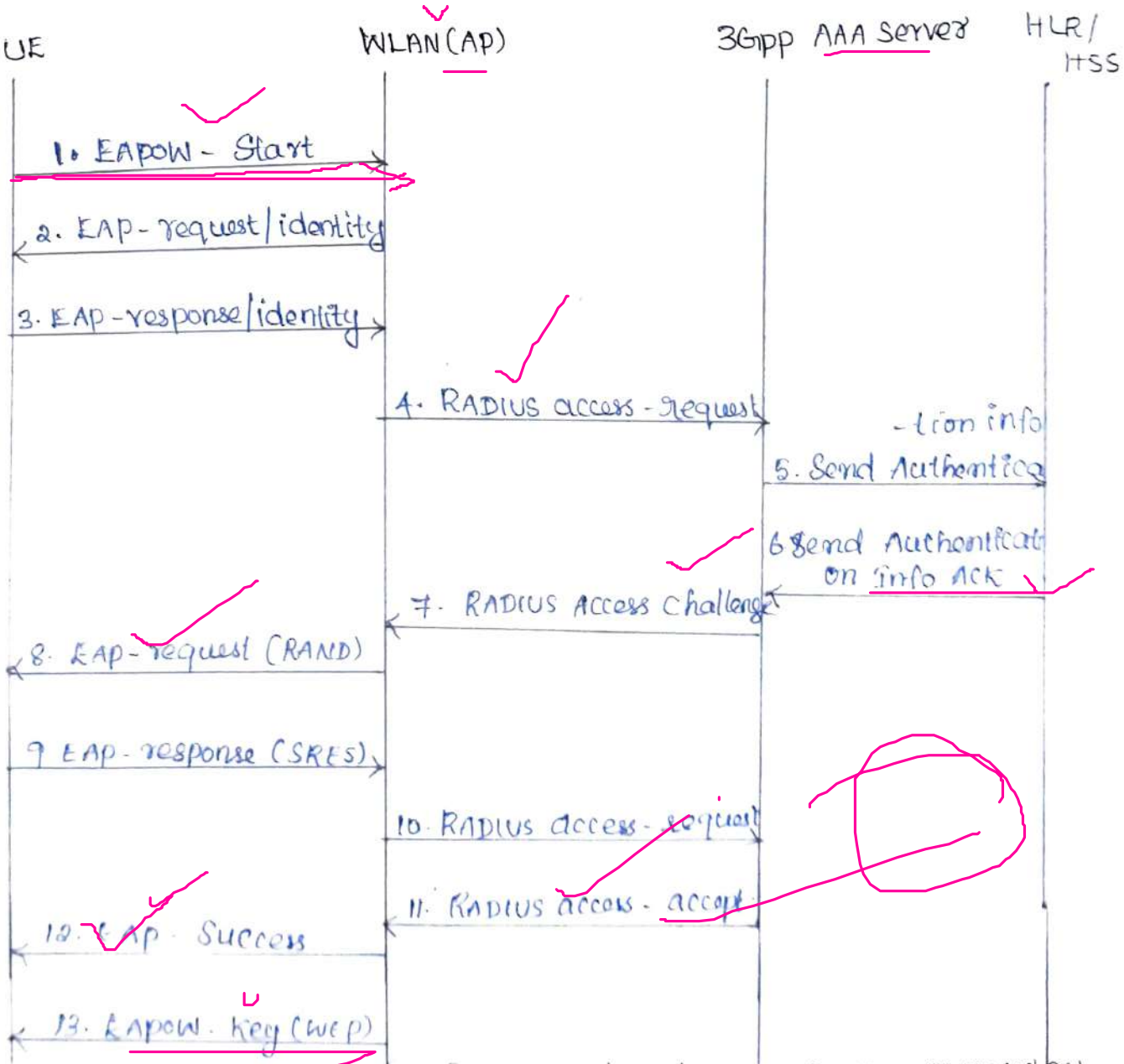


fig SIM based authentication over WLAN

Step 1 :

The authentication process starts after the UE has associated with an AP. The UE Sends an EAP-over WLAN (EAPoW) Start message to trigger the initiation of 802.1x authentication.

EAP → It is used to Perform authentication of the UE, passing the Subscriber identity, SIM based authentication data and encryption Session Keys.

Step 2 & 3 :

The identity of the UE is obtained with Standard EAP - Request / Response message.

Step 4 :

Ap initiates a RADIUS dialog with the access gateway by Sending an Access - Request message that Contains the identity reported by UE.

In SIM based authentication, this identity includes the IMSI Value stored in the SIM Card. The access gateway uses IMSI and other information included in the identity (ie domain name) to derive the address of HLR/AAS that Contain Subscription data for the particular UE.

Step 5 & 6 :

The access gateway retrieves one or more Authentication Vectors from the HLR/HSS. These Could be either UMTS authentication Vectors or GSM authentication Vectors.

In both cases a random Challenge, RAND and an expected response, XRES is included in every authentication Vector.

Step 7 & 8:

The random challenges sent to the UE, which runs the authentication algorithm implemented in the USIM card and generates a challenge response Value (SRES).

Step 9 & 10:

SRES is transferred to the access gateway and Compared against the corresponding XRES Value received from the HSS.

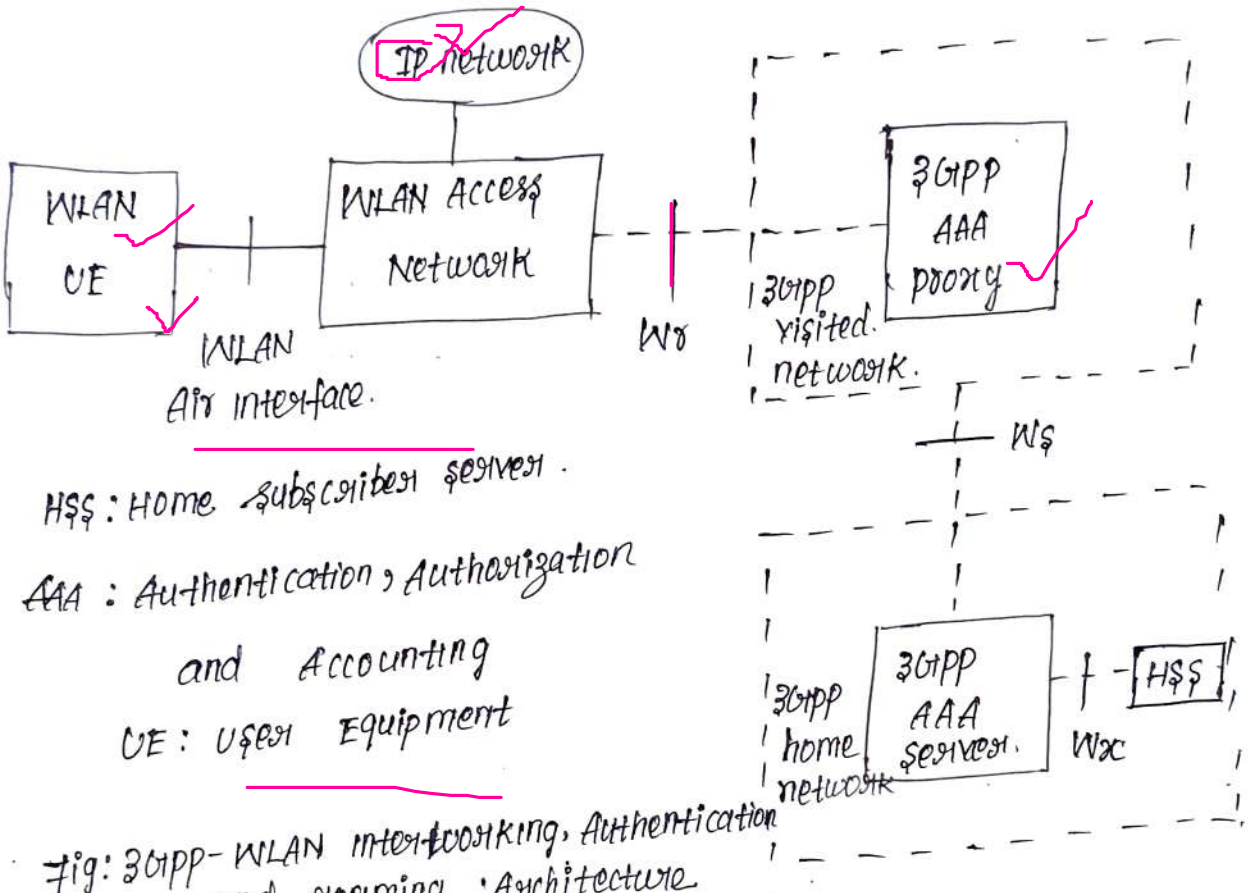
Step 11:

If these Value match, a RADIUS Access-Accept is generated in Step 11. Otherwise a RADIUS Access-Reject is generated. This instructs Ap to authorize the 802.1X port and allow Subsequent data packets from the UE.

Step 12 & 13:

The AP transmits a standard EAp-Success message and Subsequently an EAPoW-key message for configuring the Session key in the UE.

Authentication and roaming Architecture :-



HSS : Home Subscriber server.

AAA : Authentication, Authorization and Accounting

UE : User Equipment

Fig: 3GPP-WLAN interworking, Authentication and roaming Architecture

*) The WLAN access Network is Connected to a 3GPP AAA Proxy via the Wr reference point.

⇒ The Wr reference point is used for authentication and key agreement signalling, and the protocols in this reference are extensible authentication Protocol (EAP) over DIAMETER or RADIUS.

*) The 3GPP AAA Proxy forwards authentication signaling between WLAN access network and the 3GPP AAA server over the Ws reference point.

*) The 3GPP AAA Server Verifies if the Subscriber is authorized to use WLAN.

*) The authorization information and authentication vectors needed in the authentication protocols are stored by the HSS.

*) The 3GPP AAA server retrieves this information over the Wx reference point.

*) After the user has been successfully authenticated and authorized for network access, the WLAN access network grants UE access to an IP network.

(ii) User Data Routing and Access to Services:

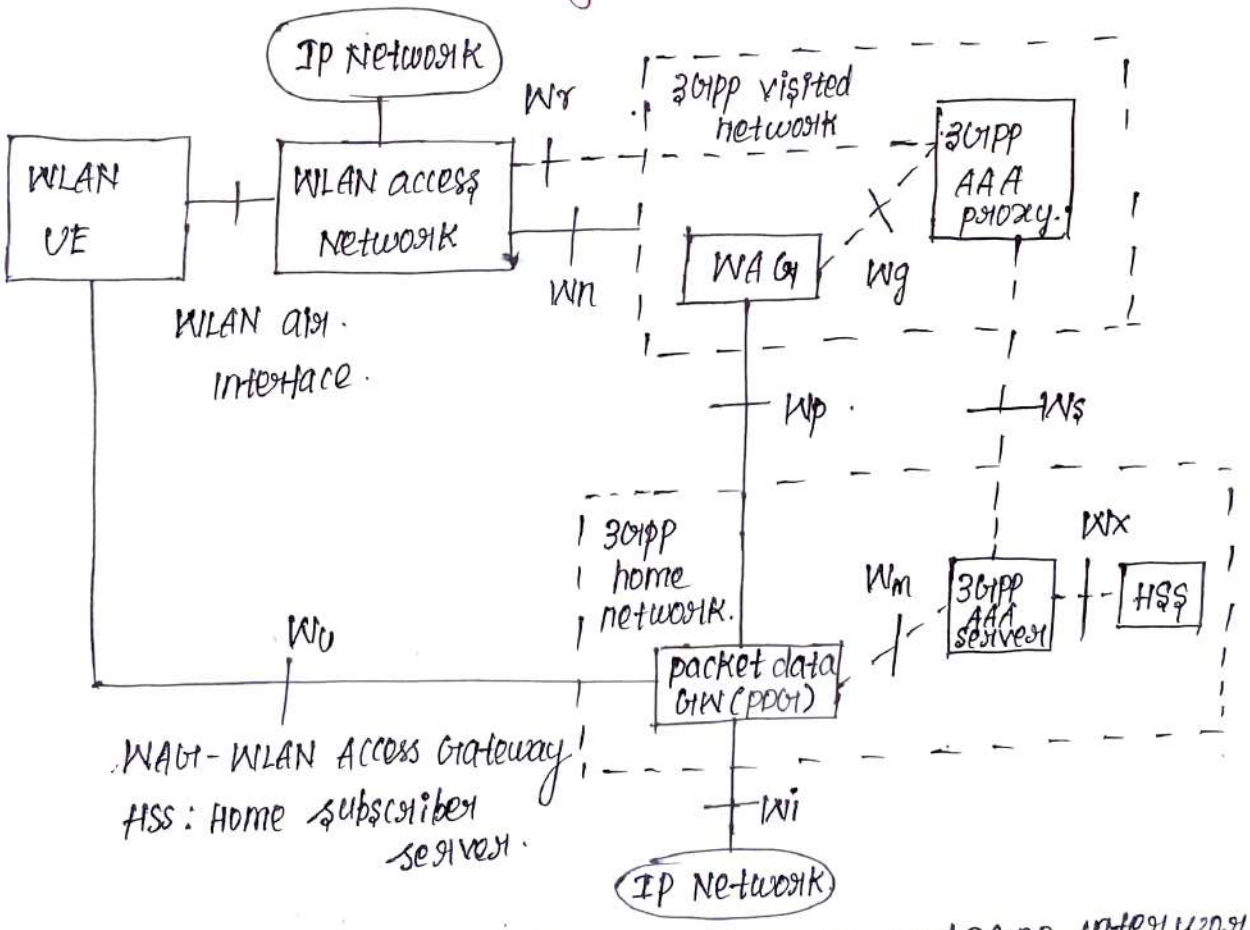


Fig: user data routing in WLAN and 3GPP interworking.

*) The IP network selection is based on a parameter called WLAN access point name (WAPN) similar to the APN parameter used in GPRS.

*) The UE, indicates the desired IP network with W-APN,

*) The network authorizes the request, or verifies that the user has the right to use the W-APN.

*) After selecting the IP network, appropriate tunnels are established to route the user data to the selected IP network.

*) The tunnel is terminated in the home operator packet data Gateway (PDG). The PDG is similar to the GGSN used in GPRS.

*) The Wi reference point between the PDG and the remote network is similar to the Gi reference point used between GGSN and the remote IP networks in GPRS.

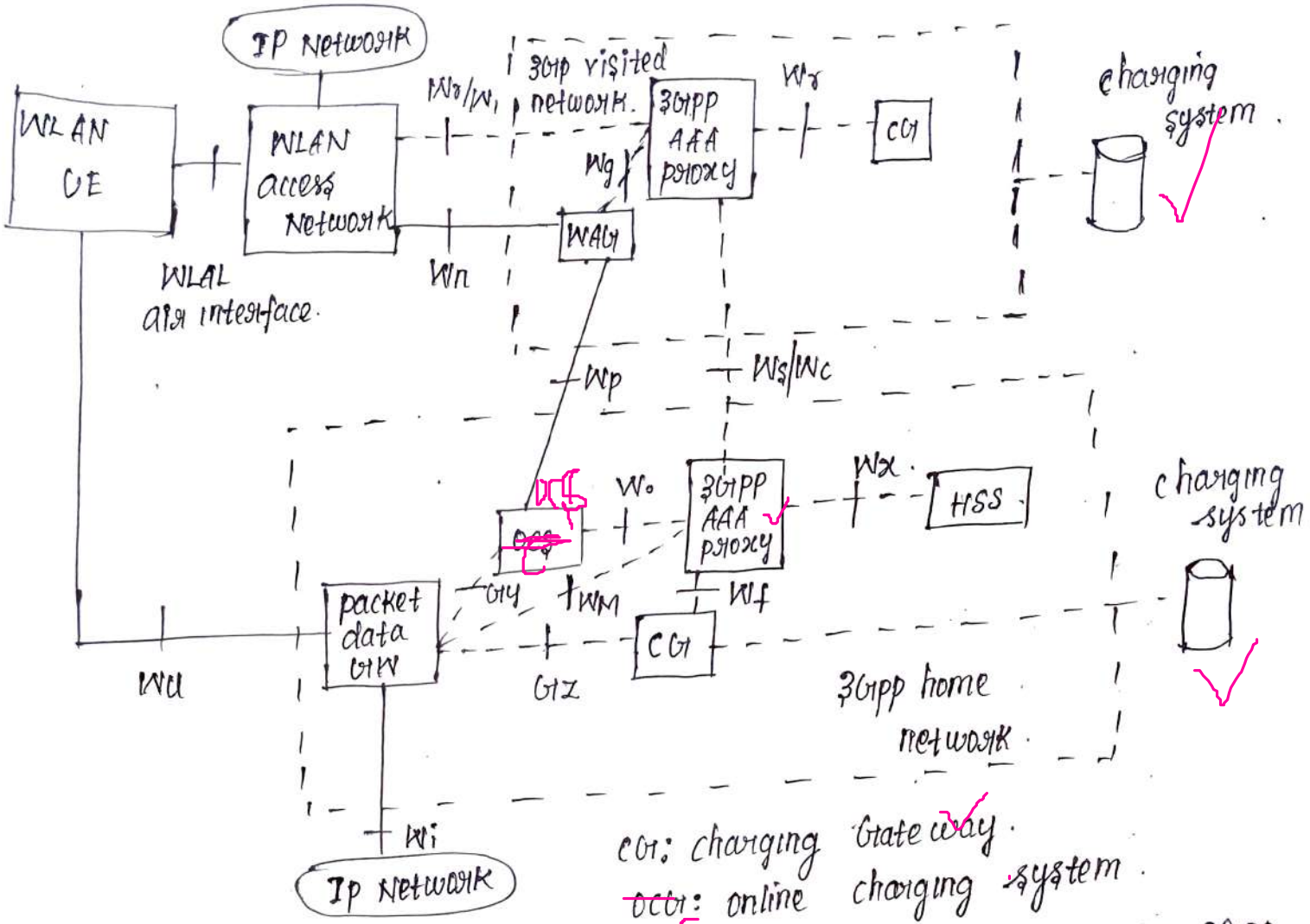
*) In the visited 3GPP network, the WLAN access gateway (WAG) is required to implement tunneling.

*) The reference points Win, Wp, Wu and Wi are used to convey the user data plane, and Wg and Wm are used for control.

iii) 3GPP based Charging for WLAN:

*) Charging information about WLAN is collected at the WLAN access network and forwarded to the 3GPP visited and home networks.

*) The AAA server in the home 3GPP network authorizes each user's access to a WLAN.



CGI: charging Gate way.

OCS: online charging system.

Fig: charging infrastructure and reference points in the 3Gpp WLAN interworking architecture.

*) Before authorizing a prepaid user to access the WLAN for direct internet access, the 3Gpp AAA Server makes a credit reservation from the User's prepaid amount in the OCS (Online Charging System) over the Wo reference point.

*) 3Gpp AAA Server monitors the received accounting information from the WLAN access network.

*) At the termination of the WLAN Connection, the 3Gpp AAA Server returns any unused Credit back to the OCS.

*) After authorization to access the WLAN Connection, access network is Completed, a user specific accounting session is established between the WLAN access network and the 3Gpp home network.

⇒ accounting session:

It is established with standard AAA accounting signaling, and the reference point for this signaling is Wb

*) After the establishment the WLAN Collects accounting information and reports it to the 3Gpp AAA Server over the Wb reference point.

* PDG:

All associated IP flows traverse through the PDG, more accurate and service specific charging information can be collected at the PDG.

*) for the charging of the traversing IP flows, the PDG is also connected to the OCS by the Gy reference point and to the CG (Charging Gateway) by the Gz reference point.

*) At the establishment of IP flow via the PDG, the PDG requests Credit for IP flow charging from the OCS over the Gy reference point in a similar way as the 3Gpp AAA Server does over the Wb reference point for WLAN access charging.

iii) Session Mobility:

* Mobile IP is used to provide session mobility across GPRS and WLAN

→ When the UE moves from GPRS to WLAN, it performs a mobile internet protocol (MIP) registration via the FA that resides in the WLAN.

→ FA Completes the registration with the HA to be used for a forwarding address for the packet destined to the UE.

⇒ FA then associates the CoA with that of the UE and acts as a proxy on behalf of the UE for the life of the registration.

⇒ UE retains its Ip Address when it moves from the WLAN to GPRS.

Local Multipoint Distribution Services: (LMDS)

Explain in detail about LMDS Configuration /

(or)

Discuss briefly local multipoint distribution system (LMDS)

⇒ It is the new stationary broadband wireless access technology based on the millimeter micro frequencies - 2.4GHz and above.

LMDS:

Local it indicates that the propagation characteristics of signals in this frequency using limit potential Coverage are

Distribution refers to the distribution of signals, which may Consists of Voice, data, Internet and Video.

*) Service implies the relation between the operator and Customer the Services offered through an LMDS network are entirely dependent on the operator's Choice of bussiness.

Fig: below shows the example of the LMDS configuration:

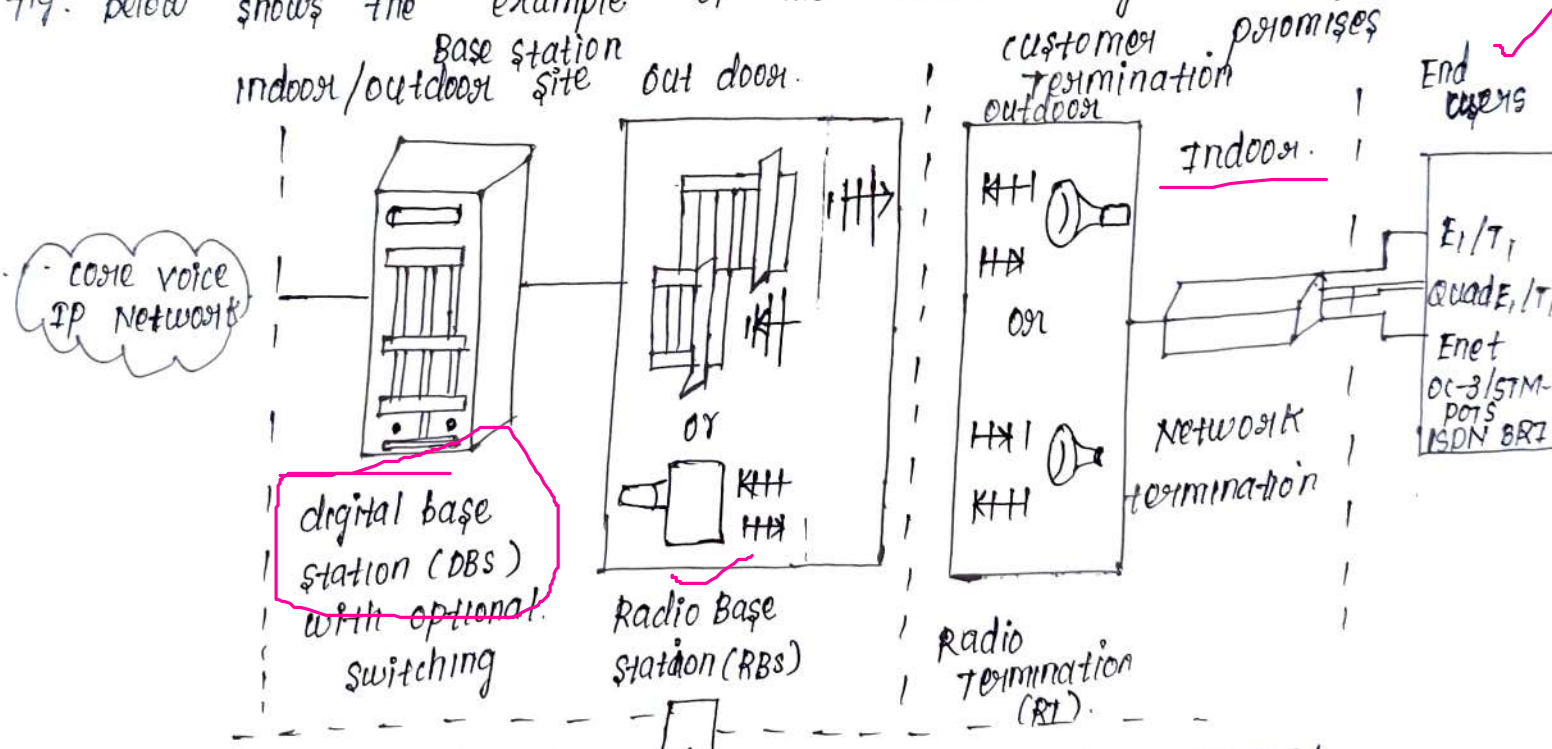


Fig: Examples of LMDS configuration.

*) LMDS is an ideal Candidate for integrating voice and data in new multitenant buildings.

*) Antenna at the end user site located with in 3 to 5 km of an operator two-way LMDS Cell, the access technology Can deliver large bandwidth.

*) LMDS transmission are Strictly Line of Sight

*) LMDS Services are permitted at a number of frequencies 24 GHz, 28 GHz, 31 GHz, 38 GHz, 40 GHz

⇒ The 28 GHz region has a spectrum allocation of 1.3 GHz

→ The 28 GHz region has a spectrum allocation of 1.3 GHz

*) The capacity of 28 GHz LMDS consist of three bands 27.5 to 28.35 GHz, 29.10 to 29.25 GHz, 31.0 to 31.5 GHz.

*) LMDS include multiple virtual private networks for corporations and government agencies or ATM telephony and streaming video, including video broadcasting.

~~*) LMDS include multiple virtual private networks for~~

*) LMDS, a data access scheme can be FDMA, TDMA or CDMA

→ data rate is 45 Mbps.

Advantages :-

*) Lower entry/deployment costs than wireline.

*) Ease/speed of deployment.

*) Fast realization of revenue.

*) Scalable architecture.

*) Cost effective network maintenance, management operations.

*) IEEE 802.16.2 standard focuses on fixed broad band wireless access (BWA) system.

It covers 2 to 66 GHz frequencies detailed emphasis on 3.5, 10.5 and 23.5 to 43.5 GHz.

The following are present IEEE 802.16 standards.

→ P802.16a : 2 - 11 GHz licensed band, addresses point-to-multipoint BWA, OFDM, and single carrier system.

⇒ P802.16b : License-exempt bands, 5-6 GHz, wireless high speed unlicensed metropolitan area network (HUMAN), OFDM

⇒ P802.16.2 : focuses on 2-11 GHz frequency band and the Co existense of BWA System.

Multichannel Multipoint Distribution System :-

Explain in detail about MMDS System for digital Video and wireless internet?

(or)

What is the multichannel multipoint distribution System (MMDS). Compare it with LMDS?

*) MMDS is new technology for wireless access - Internet.

*) MMDS signals have longer wavelength, can travel farther without losing significant power.

*) MMDS signals not blocked easily by objects.

*) Repeater stations can be used to redirect MMDS signals.

*) MMDS, a transmitting tower placed at a high elevation can reach customers with in a 35-mile radius who have receiving dishes on the side of roof of the building.

*) MMDS has narrow Spectrum allocation (2.5 to 2.7 GHz)

*) Data rate of MMDS are 0.5 to 3 Mbps.

*) The access Schemes are FDMA, TDMA, OFDM, CDMA

*) MMDS are line-of-sight system, but a non-LOS system is possible.

*) The network topology for MMDS can be either point-to-point or point-to-multipoint.

*) Transmission power upto 1 to 100 Watt range.

*) MMDS favored cell architecture is a single large microcell

*) In large cell, the 2.5 GHz frequency band requires large antennas which are not well received consumer client receivers or smaller antennas with a very broad beam.

*) In single cell MMDS, the available bandwidth is limited to the frequency band licensed, which is equal to or less than 200 MHz.

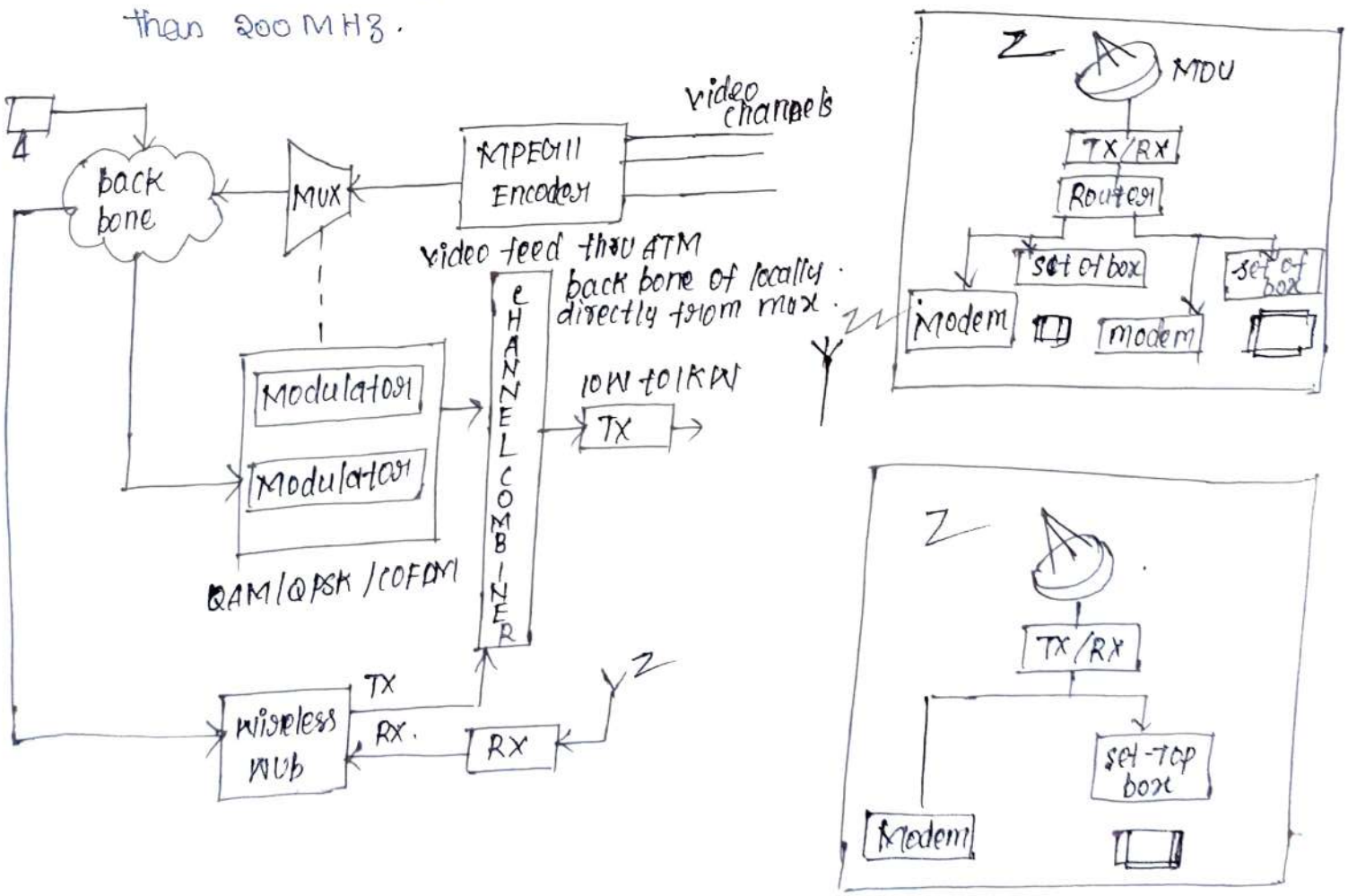


Fig: Typically MMDS system for digital video and wireless internet.

Comparison of LMDS versus MMDS :

Feature	LMDS	MMDS
Frequency range	28 - 31 GHz (US) 2 - 42 GHz (rest of world)	2.5 – 2.7 GHz
Propogation Characteristics	Good for medium range, LOS, ≤ 5 miles, free space attenuation.	Good for short range LOS ≤ 35 miles, free space attenuation.
favored cell Architecture	multiple, small microcells	single, large microcell
Impact of cell architecture	Large bandwidth available which can effectively be increase by decreasing cell size.	Limited bandwidth availability due to no. frequency re use.
Ability to support 2-way system architecture	Well suited due to small cell size, large bandwidth, and highly directive antenna	Limited due to bandwidth antenna Characteristics and Propogation characteristics.
Fading pathology	Long range and broad antennas beams ensure significant multipath	Short range and highly directive antennas mean little or no multipath.
Range	upto 5 miles	upto 35 miles
Data rate	Typically upto 45 Mbps, burst rate up to 311 Mbps	Typically 0.5 to 3 Mbps
Access schemes	FDMA TDMA CDMA	FDMA TDMA OFDM. CDMA.
Target Market	Large and medium enterprises	Residential, small enterprises.
Customer premises Equipment Costs	High	Low to Medium.

Qn: Compare Tight and Loose Coupling architecture for interworking between IEEE 802.11 WLAN and GPRS?

(or)

Distinguish with Tight and Loose Coupling architecture?.

Tight Coupling	Loose Coupling
1. The WLAN is Connected to the 3Gpp (GPRS) Core network in the same way as any other radio access network such as GPRS RAN and UTRAN.	1. WLAN is deployed as an access network Complementary to the GPRS Core network.
2. WLAN data traffic goes through the GPRS core network before reaching external data packets.	2. WLAN by passes the GPRS network and provides direct network data access to the external packet data networks.
3. In Tight Coupling the WLAN is Connected to Gb or Iups reference Points.	3. In Loose Coupling architecture between the GPRS and the WLAN Gi reference point is indicated.
4. 3Gpp System based access Control and Charging is used.	4. This approach use SIM or USIM based authentication and billing.
5. The different networks would Share the same authentication, Signaling transport and billing infrastructure.	5. different mechanisms and protocols can handle authentication billing and mobility management
6. Tightly Coupled network Support Service Continuity to other access network during handover, thus loose coupled scheme has long hand over latency and packet loss	6. loosely Coupled network Cannot Support Service Continuity to other access network during handover.

Tight Coupling	Loose Coupling.
7. Access to Core GPRS Services such as Short message Service (SMS), location based Services and multimedia messaging Services. (MMS)	7. With this approach, a Subscribes Can re use the SIM Card or the USIM Card to access a Set of wireless data Services over a WLAN.
8. Reuse GPRS Accounting	8. Billing mediator to provide common accounting.
9. A new interface in the SGSN might be required Specifically for Connecting to WLAN.	9. EAP-SIM based authentication as used.

Q. What is the WLAN adaptation function (WAF) in tight Coupling architecture? Discuss briefly?

(or)

Discuss in detail about WLAN adaptation function in tight Coupling architecture.

⇒ The WAF is implemented in every dual mode MS & GIF WAF provides the following functions.

1. Signals the activation of the WLAN interface when a mobile enters a WLAN area.
2. It Supports GIF/RAI discovery Procedure which is initiated by MS in order to discover the MAC address of GIF/RAI of the WLAN.
3. It transfers uplink LLC PDU from MS to the GIF

by using the transport services provided by the 802.11 MAC. It also transfers downlink LLC PDUs from the GIF and in the MS.

4. It supports QoS by implementing transmission scheduling in the GIF and in the MS.

5. It transfers the temporary logical link Identifier (TLLI) and QoS information in the WAF header.

Encapsulation Scheme:

⇒ The encapsulation scheme used in the uplink direction as well as the format of the WAF PDU are shown in figure.

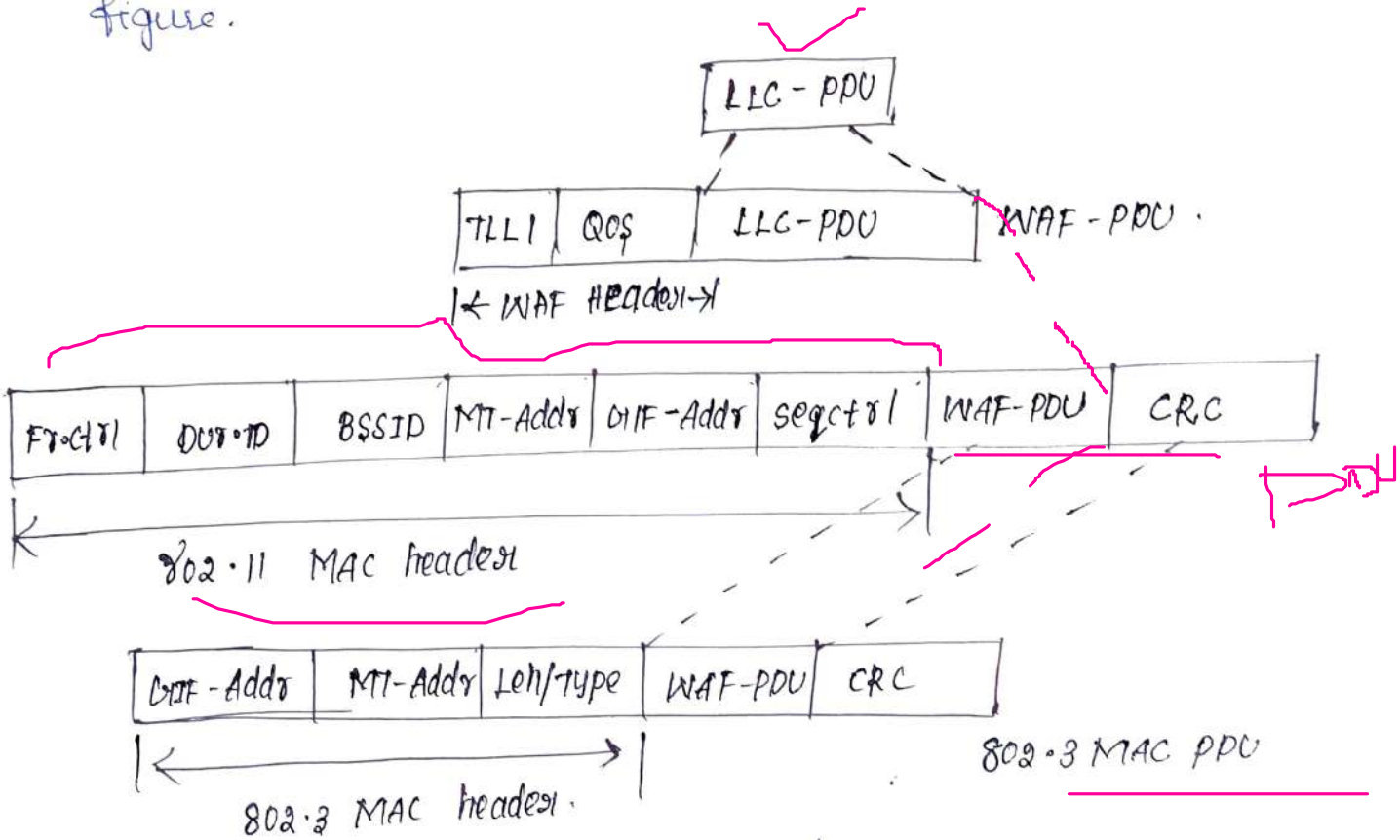


Fig: encapsulation scheme.

WAF PDU:

Each LLC PDU is encapsulated into a WAF PDU, which include the TLLI and QOS in the header.

TLLI → Temporary MS idententifier used by the LLC layer for addressing purposes.

The TLLI is used by the GIF to update an internal mapping table the correlates TLLI with 802 MAC address.

The correlation between TLLI & 802 MAC address is used for forwarding downlink LLC PDU received on the Gb interface to the correct mobile on the WLAN.

QOS:

→ In the uplink direction, QOS contain the following attributes,

*) Peak throughput
*) Radio Priority.
*) RLC mode.

These QOS attributes are primarly used for scheduling in the MS and GIF.

→ In the downlink direction QOS may be empty since there is no need to transfer any QOS parameters to the mobile.

*) IEEE802.11 & IEEE802.3 MAC header encapsulated in the WAF-PDU.

Qn: Discuss the GPRS interworking function (GIF) / routing area update RAU discovery procedure in tight coupling architecture? (or)

GIF / RAU

Explain in detail about signalling flow during a GIF/RAI discovery procedure.

⇒ It is carried out immediately after MS enters an 802.11 WLAN area and gets associated with an AP.

The WAF in the MS initiates this procedure:

(i) To discover the 802 MAC address of GIF. All uplink LLC PDUs are subsequently transmitted to this MAC address.

(ii) To discover the RAI that corresponds to the WLAN network.

(iii) To send the MSS IMSI value to GIF.

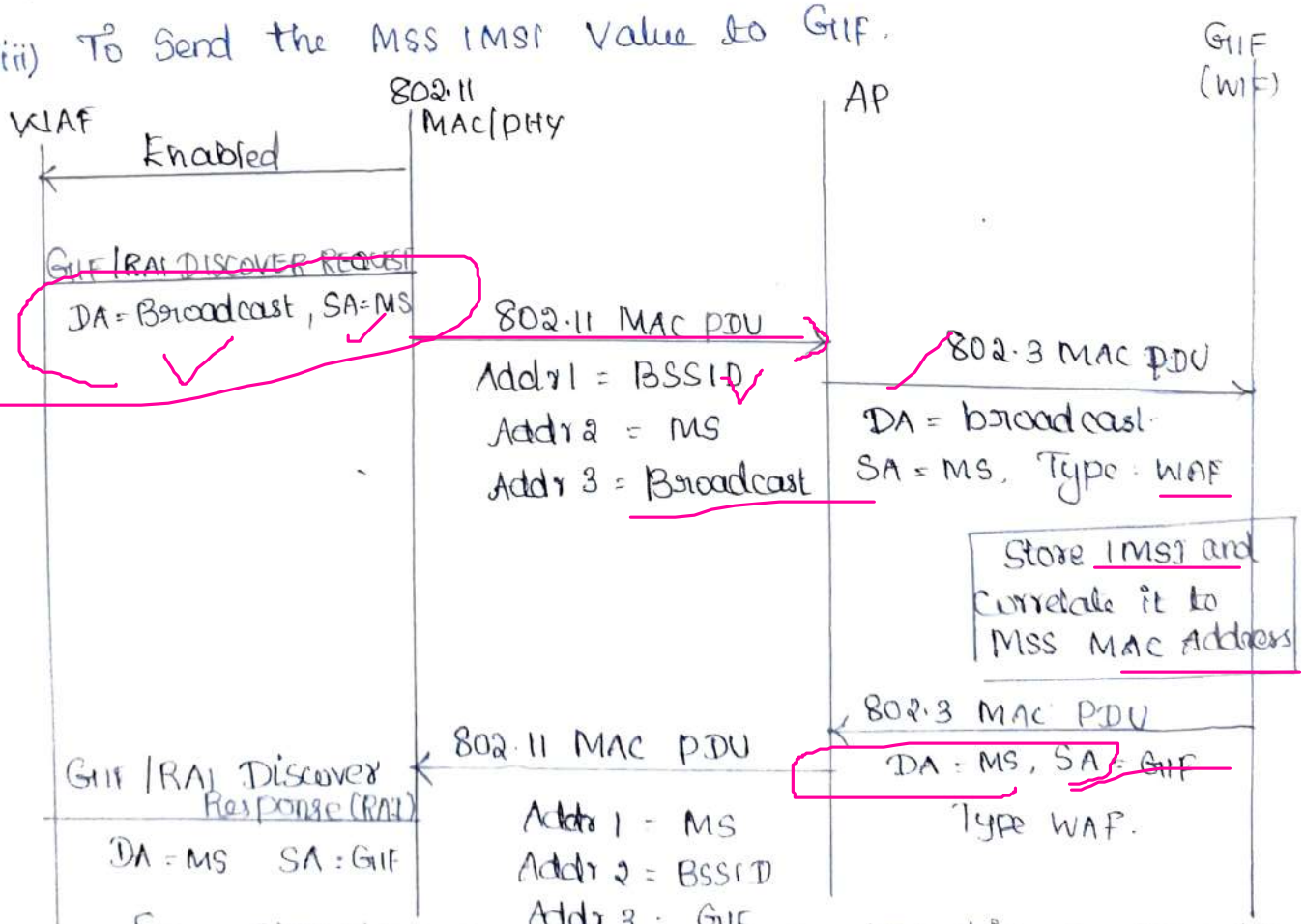


Fig: Signaling flow during a GIF/RAI discovery procedure

① The Procedure is initiated after the 802.11 MAC Layer is enabled.

② WAF layer in the MS Sends a request to 802.11 MAC to transmit a PDU with a Source Address (SA) equal to MS MAC address and a destination address equal to broadcast

This PDU is a GIF/RA/ discover request message that includes the IMSI value of the MS.

③ The 802.11 Layer transmits an 802.11 MAC PDU with the appropriate address information (designated Addr 1, Addr 2, Addr 3) this PDU is directed to the Ap with identity BSSID.

④ The Ap broadcast this message to the MS and finally received by the GIF, which associates the IMSI with the MSS 802.11 MAC address

⑤ The MS receives this response, Stores the GIF address and the RAI and notifies the GMM layer that the current GPRS RA has changed

⑥ WAF in the GIF responds with GIF/RAI discover response that include the RAI of the WLAN.

UNIT - 5

4G & Beyond

Introduction - 4G vision - 4G features and challenges - Application of 4G - 4G Technologies; Multicarrier modulation, Smart antenna techniques, IMS Architecture, LTE, Advanced Broadband Wireless Access and Services, MVNO.

INTRODUCTION

⇒ Mobile Communication Systems revolutionized the way people Communicate, jointing together Communications and mobility. Recent advancements in Covering the internet and mobile radio is accelerating the demand for 'internet in the pocket.

⇒ Mobile networks going multimedia, potentially leading to an explosion in throughput from a few kilobytes (SMS) to few kilobytes (MMS) to several 100kbps for Video Content.

⇒ Diverse wireless transmission technologies such as local multipoint distribution service (LMDS), Digital Video Broadcasting (DVB), DAB and multichannel multipoint Distribution Services (MMDS) for fixed Wireless access.

⇒ IEEE Standards are extending from the enterprise world into public and residential domains.

⇒ A long way in remarkably short time has been achieved in the history of wireless Evolution of wireless access technologies is about to reach its fourth generation (4G).

⇒ 4G mobile systems mainly Concentrate on seamless integration of existing wireless technologies including WWAN, WLAN and Bluetooth, while 3G simply focuses on developing new standards and hardware.

⇒ The 4G systems will encompass all systems from various networks, public to private operator-driven broadband networks to personal areas, and ad hoc networks.

⇒ The 4G systems will be interoperable with 2G and 3G systems as well as with digital broadcasting system

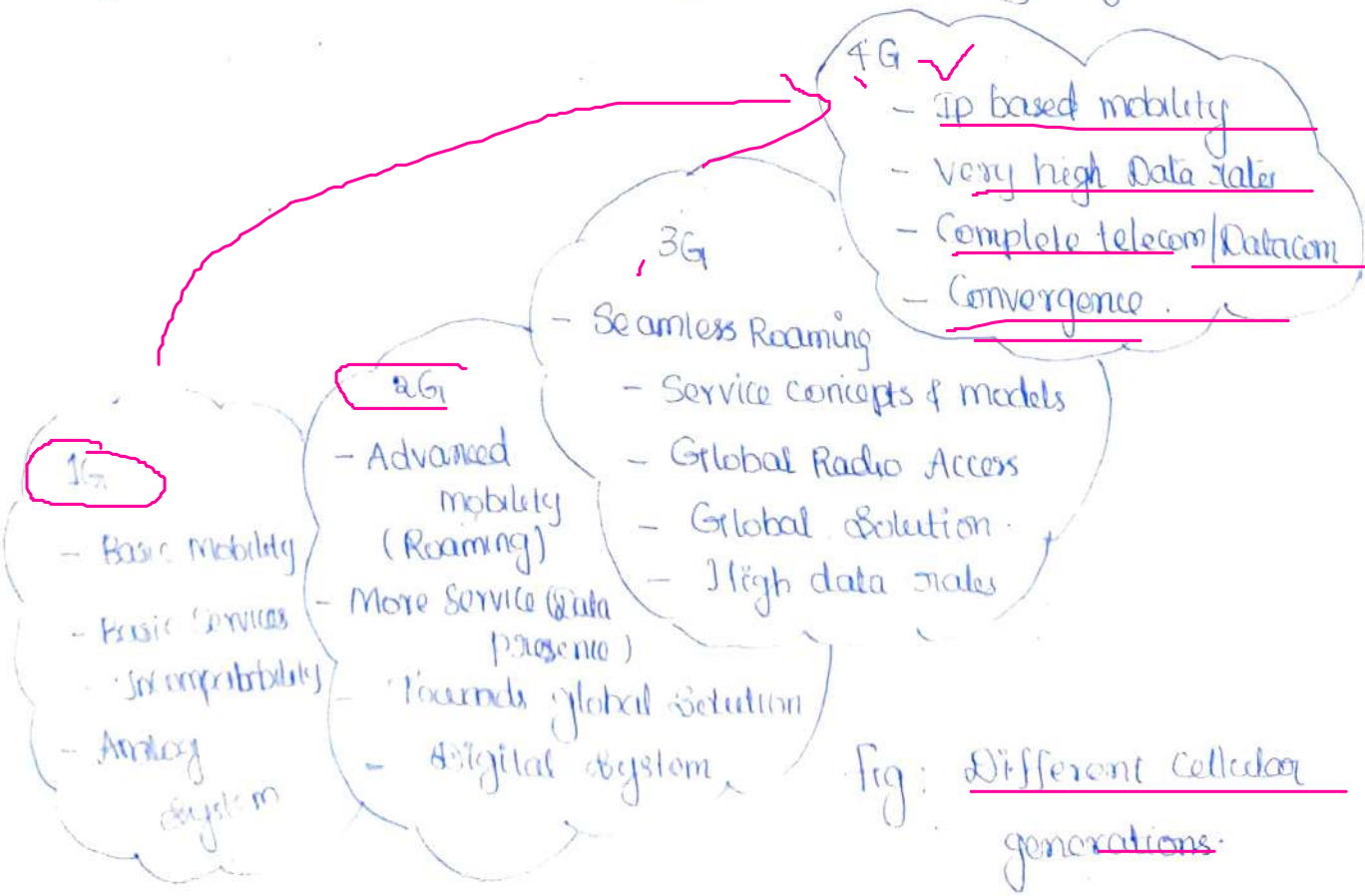


Fig: Different Cellular generations.

4G can be described in a nutshell as a integration of different advanced technologies to satisfy demands.

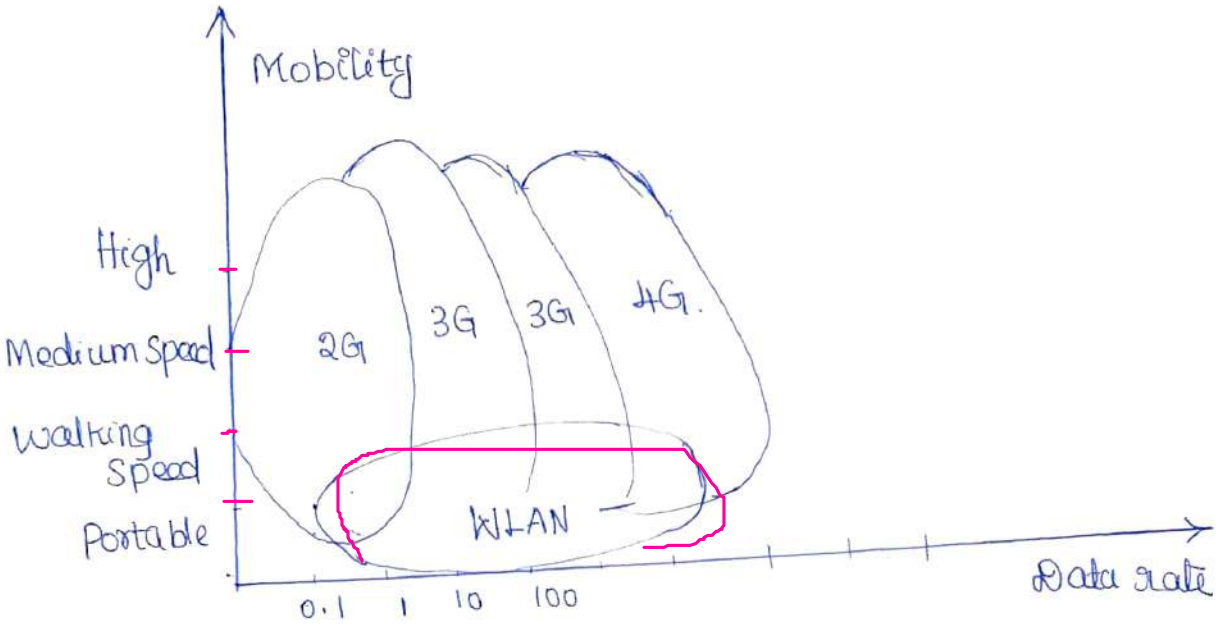


fig: Data VS Mobility in wireless Standards

⇒ The 4G intends to integrate from Satellite broad band to high altitude platform to cellular 2G and 3G systems to wireless local loop (WLL) and Broadband wireless Access (BWA) to WLAN, and wireless personal Area Networks (WPANs) all with Ip as the integrating mechanism.

Comparision of key parameters of 4G with 3G

Sl.No	Detail	3G includes 2.5G (EDGE)	4G
1.	Architecture	Wide area cell based network	Hybrid (Integration of WLAN) (wifi, Blue tooth)
2.	Speed	3.84 Kbps to 2 Mbps	20 to 100 Mbps

Sl. No	Detail	3G includes 2.5G (EDGE)	4G
3.	Frequency band	1.8 to 2.4 GHz	2 to 8 GHz.
4.	Bandwidth	5 to 20 MHz	2 to 8 GHz
5.	Switching	Both circuit and packet	All digital with packetized voice
6.	Access Technique	WCDMA - CDMA	OFDM and multi Carrier CDMA.
7.	Component design	Optimized Antenna design	Smart antenna, Softwar defined multiband and wide band radios.
8	Ip (Internet protocol)	IPV 5.0	All Ip (IpV 6.0)
9.	Mobile top Speed	200 km/hr	200 km/hr.
10.	Services and Applications	CDMA 2000, UMTS, EDGE	LTI and Advanced.
11.	peak upload rate	5 Mbps	500 bps
12.	Forward Error Correction	Turbo Codes are used for FEC	Concatenated Codes used for FEC

4G VISION

⇒ 4G Systems are designed for Providing wide Variety of new services right from high quality Voice to high definition Video high data rate wireless channel.

Definition 4G can be defined as MAGIC.

⇒ Mobile multimedia
⇒ Anytime Anywhere
⇒ Global mobility Support.
⇒ Integrated wireless Solution
⇒ Customized personal Service.

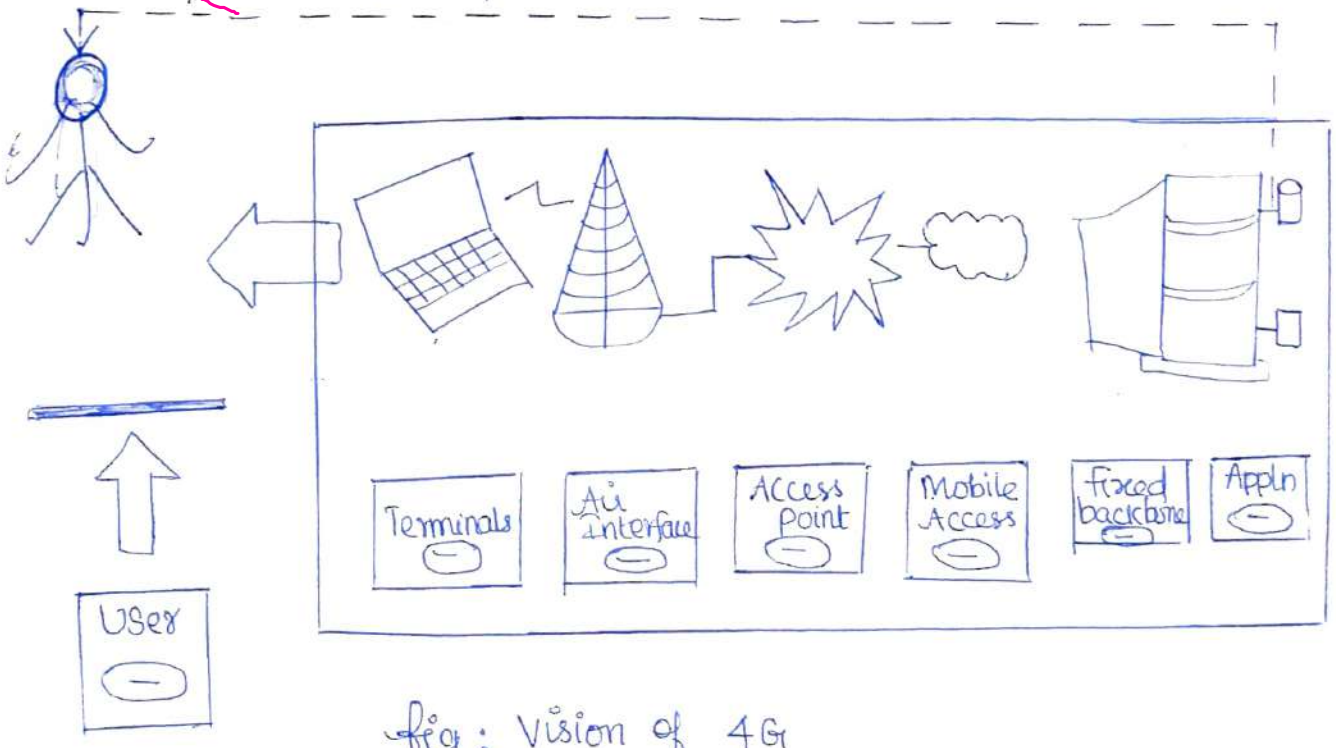


fig: Vision of 4G

⇒ 4G Systems Supports both the next generation mobile Services as well as support fixed wireless networks. The 4G Systems are about Seamlessly

integrating terminals, networks and applications to satisfy increasing user demands.

⇒ The key infrastructure of 4G is to access information anywhere, any time with a seamless connection to a wide range of information and services data, pictures videos and so on.

Seamless Connections :-

The future 4G systems will consists of a set of various networks using Ip as common protocol.

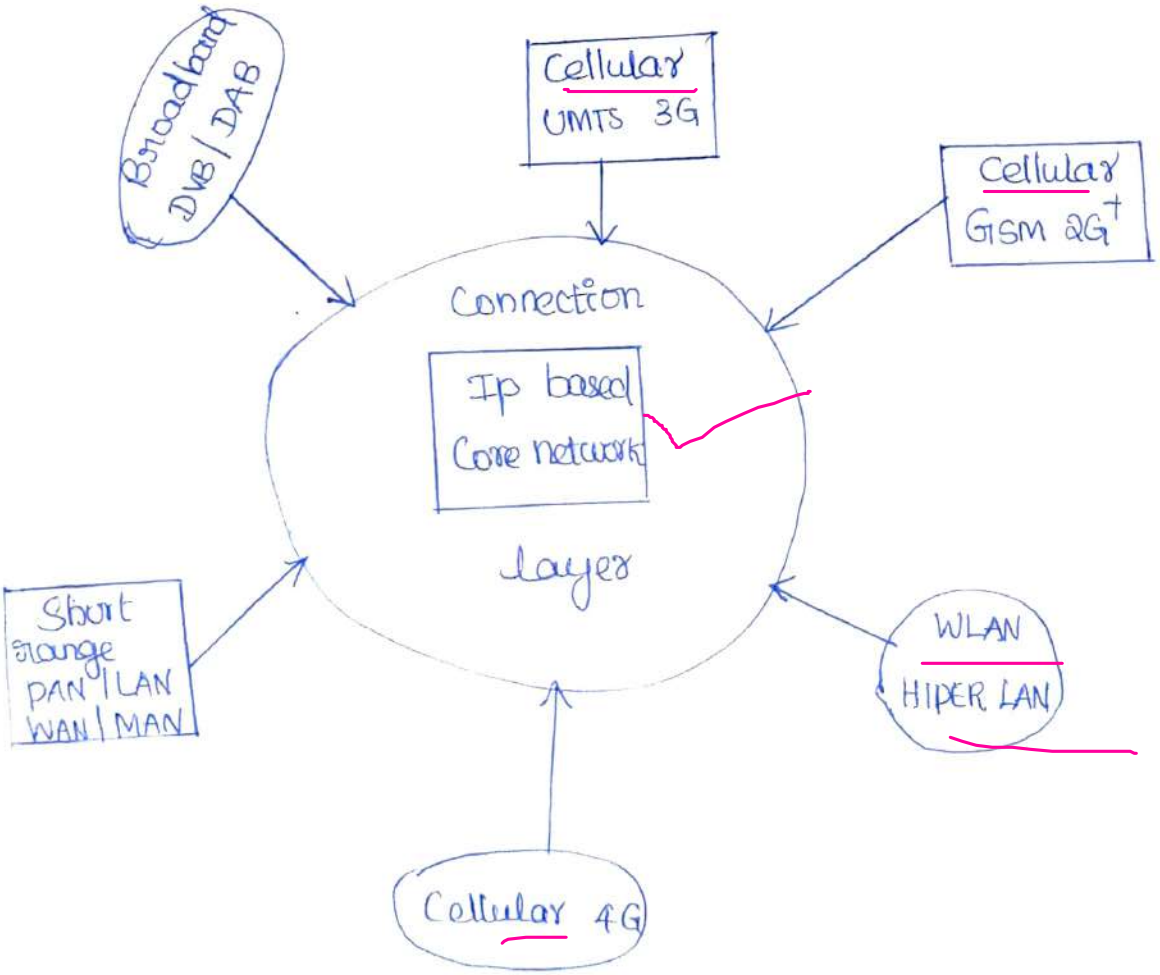


fig: Seamless Integration in Ip.

PAN – Personal Access Network

LAN – Local Area Network

WAN – Wide Area Network

DVB – Digital Video Broadcast

DAB – Digital Audio Broadcast

MAN – Metropolitan Area Network

WLAN – Wireless LAN

UMTS – Universal Mobile Telecommunication System

⇒ 4G systems will have high data rate, broad bandwidth and smoother handoff to ensure seamless service across a multiple wireless systems and networks. To satisfy increasing user demands 4G systems seamlessly integrate terminals, networks and applications.

Unlike 3G, 4G is Ip based (ie) every user connected to internet will have an Ip address

Features and Challenges of 4G:

Features:-

The following are some of the features of 4G system

*) High Usability : anytime anywhere

*) Support for multimedia and with any technology service

*) Personalization

*) Integrated services

Ip based Heterogeneous:-

4G networks will be all Ip-based heterogeneous networks that will allow users to use any system at any time and anywhere.

Telecom, Data and multimedia services:

⇒ 4G systems provides Telecom, data and multimedia services with high data rates and reliability. Also a low per bit transmission cost is maintained.

Personalized services:

4G networks provides personalized services. These systems will also provide facilities for integrated services, users at the same time.

⇒ Adhoc networks and multi hop networks

⇒ Provides global ecosystems with inherent mobility

⇒ Better scheduling and call admission control.

Challenges of 4G:

⇒ The first successful field trial for 4G was Conducted in Tokyo, Japan on June 23rd 2005. NTT DoCoMo was successful in achieving 1 Gbps real time packet transmission in the downlink at a moving speed of about 20kmph. Several such attempts have been made in the past by several companies in different parts.

The main challenges are classified into three.

(i) Based on mobile station

(ii) Based on system

(iii) Based on service.

(i) Based on Mobile Station:

*) Multimode User Terminals

*) Wireless System Discovery and Selection.

(ii) Based on System

⇒ Terminal mobility

⇒ Network Infrastructure and QoS Support.

⇒ Security and privacy.

⇒ Fault Tolerance and Survivability.

(iii) Based on services :-

- multiple operators and Billing system.
- personal Mobility.

(i) Mobile Station based Challenges:-

a) Multimode User terminals:

Challenge:

In order to access different kinds of service and technologies, the user terminals should be able to configure themselves in different modes. This eliminates the need for multiple terminals.

Proposed Solution:-

*) Adaptive techniques like Smart antennas and Software radio have been proposed for achieving terminal mobility.

⇒ The most promising way of implementing multimode user terminals is to adopt the Software radio approach.

(b) Wireless System discovery and selection:

Challenge:

⇒ The main idea behind this is the user terminal should be able to select the desired wireless system. The system could be LAN, Gps, GSM etc.

Solution:-

One proposed solution for this is to use Software radio approach where the terminal scans for the best available network and then it downloads required

Software and Configure themselves to access the particular network.

(ii) System based Challenges:

a) Terminal Mobility

Challenge.

⇒ In order to provide wireless services at anytime and anywhere terminal mobility is a must in 4G infrastructure

⇒ Terminal mobility allows mobile clients to roam across geographic boundaries of wireless networks

There are two main issues in terminal mobility

*) Location management ✓
*) Handoff management ✓

⇒ With location management, the system tracks and locates a mobile terminal of possible Connection

⇒ Handoff management maintains ongoing communications when the terminal roams.

Solution:

Signalling mechanisms and fast handoff mechanisms

(b) Network Infrastructure & QoS:-

⇒ Unlike previous generation networks (2G and 3G) 4G is an integration of IP and non-IP based ✓

system prior to 4G, QoS designs were made with a particular wireless system in mind. But in 4G networks QoS designs should consider the integration of different wireless networks to guarantee QoS for the end-to-end services.

c) Security & Privacy:

The security challenge with Ip networks is one of the most significant factors that slows down the further adoption of network technologies. An end-to-end system approach to security is required in next generation wireless networks including:

*) plat-form hardening
*) User/operator authentication, authorization and auditing.
*) Secure protocols, Communication and data storage
*) Software and Configuration integrity
*) Secure network management, Control & Signalling
*) End-point Compliance
*) Network perimeter protection & interior protection
*) unsolicited traffic protection.

⇒ To overcome the security and privacy issues, approaches can be followed.

*) To modify the existing Security and Privacy methods, so that they will be applicable to heterogeneous 4G networks.

*) To develop new dynamic reconfigurable, adaptive and light weight mechanisms whenever the currently utilized strategies cannot be adopted to 4G networks.

(iii) Service based Challenges:

a) Personal Mobility:-

In addition to terminal mobility, personal mobility is a concern in mobility management. personal mobility concentrates on the movement of users instead of user terminals and involves the provision of personal communication and personalized operating environments. Mobile-agent based infrastructure is one of the widely used solution.

(b) Charging and Billing:-

In the 4G network environment, multiple service Providers will be involved during a session, when the users roam from one service provider network to one or more other service provider networks. Hence there is a need of more charging agreements between the service providers in order to allow roaming during a session in order to get a continued service as far as a customer is concerned.

(c) Fault Tolerance and Survivability:-

⇒ The fault-Tolerant designs should Consider power Consumption, User mobility, Qos management, Security, System capacity, and link error rates of many different wireless networks. To improve network Survivability in different layers, three classes of strategies are proposed.

They are:-

⇒ Prevention

⇒ Network design and capacity allocation

⇒ Traffic management and restoration.

Application of 4G:-

Few of the applications of 4G wireless technology are given.

Virtual Presence:

Even under circumstances when the user cannot be online, the required services will be provided without interruption at all times through 4G.

Virtual Navigation:-

⇒ With the expected high data rates of 4G, it will be possible to maintain and provide a database of all cities, Countries and remote places for user access as Virtual navigation.

Tele Medicine:

⇒ 4G will support multi-user Video Conferencing thus enabling remote health monitoring of patients by number of doctors in real time.

(ie Video Conference assitance for a doctor at any time and any where).

Tele-geo Processing applications:

⇒ User can get simultaneous information about anything from weather to traffic through instant satellite mapping which is a combination of GIS (Geographical Information System) and Gps (Global positioning System).

Gaming:

⇒ High-Speed multi-user gaming will be possible with the adoption of 4G.

Cloud Computing:

⇒ Safe and Secure Cloud Computing options unlike those being currently employed.

Crisis detection and Prevention:

⇒ Disasters, both natural and man-made bring down Communication especially being a hurdle in rescue operations with 4G, it is expected

that in case of such crisis, it will be easier to restore Communication at a fast rate.

Education : Distance education is a Variable option nowadays for many students. 4G will provide them with real-time class room experience. This will Provide beneficial in Coming days as it can be instrumental in reducing infrastructure demands of universities and colleges to accomodate the rising number of students.

TECHNOLOGIES USED IN 4G :

⇒ The following are the Varices technologies in 4G They are.

*) Multicarrier Modulation (MCM)
*) Smart Antenna Techniques
*) OFDM - MIMO Systems.
*) Adaptive Modulation and Coding with Time Slot Scheduler.
*) Cognitive Radio.

Multicarrier Modulation (MCM) :

⇒ Multicarrier modulation (MCM) is a derivatives of frequency division multiplexing. Varices derivative of multicarrier systems are used currently

in Digital Audio and Video broadcasting (DAB/DVB) and in DSL (Digital Subscriber line) modems.

MCM - Baseband Process & FFT:

Multicarrier modulation is a baseband technique that uses parallel equal bandwidth sub channels to transmit information and generally implemented with Fast fourier Transform methods.

MCM - Advantages:

⇒ Better performance in Intersymbol Interference Environment.

⇒ Avoidance of single frequency Interference.

MCM - Drawbacks:

*) MCM increases the peak to average ratio of signal.

*) To overcome the ISI a cyclic extension (guard bit) is to be added to data.

Difference (D):

The Difference (D) of the peak to average ratio between MCM and a single carrier system is a function of number of sub carrier (N).

i.e $D(dB) = 10 \log N$

Operation:

Let Q_b is the original length of block and the channels response is of length Q_c, the cyclically

extended symbol has a new length $Q_b + Q_c - 1$. The new symbol of length $Q_b + Q_c - 1$ sampling periods has no ISI.

In the MCM receiver, only Q_b samples are processed and $Q_c - 1$ samples are discarded which results in a loss in SNR Ratio.

$$(SNR)_{Loss} = 10 \log \frac{Q_b + Q_c - 1}{Q_b} \text{ (dB)}.$$

MCM for 4G:

Two types of MCM for 4G are

*) Multicarrier Code Division Multiple Access (MC-CDMA)

*) Orthogonal frequency Division Multiplexing (OFDM with TDMA).

OFDM with TDMA and MC-CDMA:

⇒ In OFDM with TDMA, the users are assigned time slots to transmit and receive data.

⇒ MC-CDMA uses Quadrature phase shift keying (QPSK) for modulation where as OFDM-TDMA uses high level modulation like QAM for all sub carries.

⇒ IFFT is responsible for pulse forming and modulation. Finally to decode the transmission, a receivers needs only to implement FFT.

OFDM - Sub Channels :

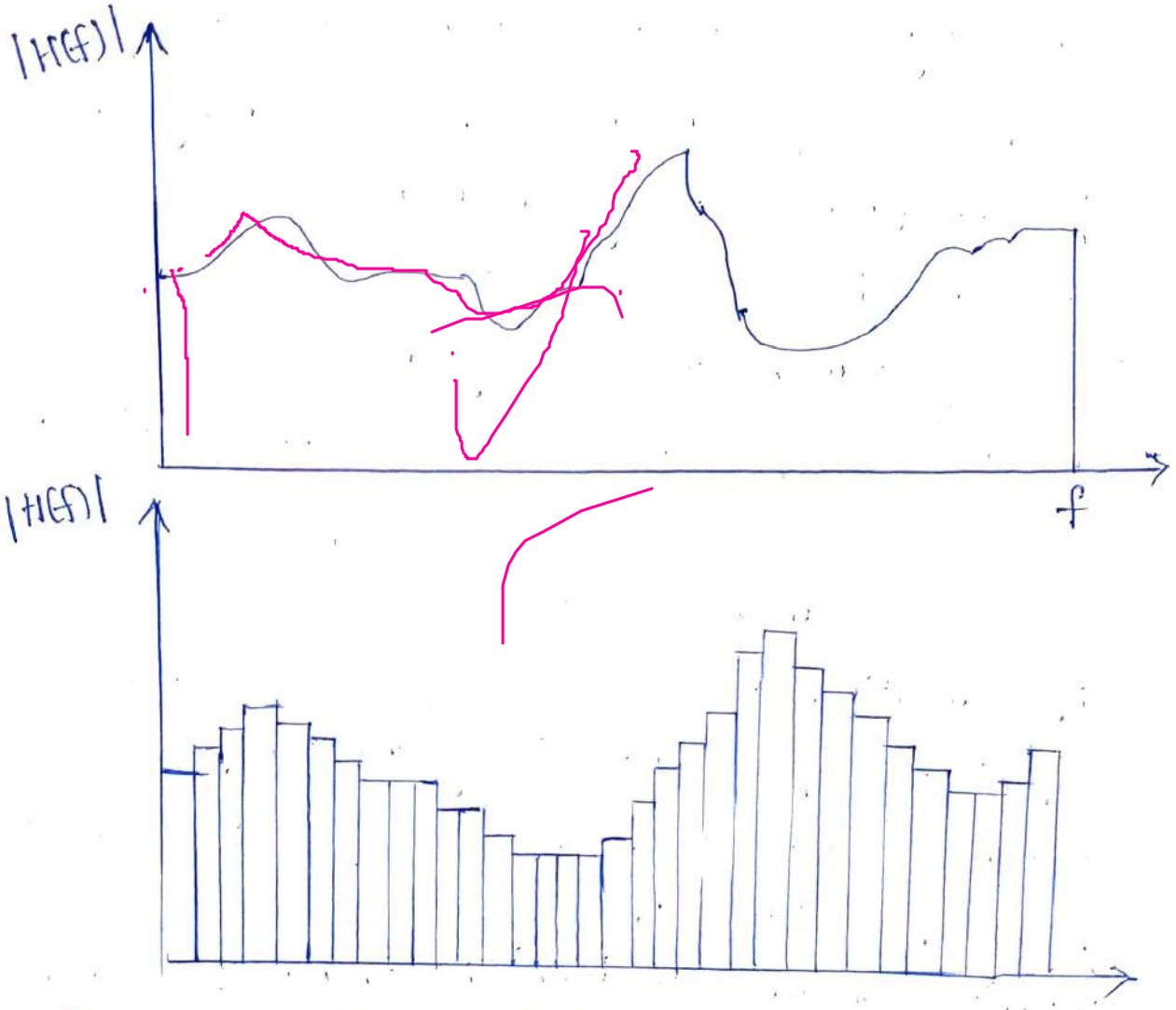


fig: Broad Channel divided into parallel narrow band Channels.

SMART ANTENNA TECHNOLOGIES (or) TECHNIQUES :-

⇒ A smart antenna is a multi-element antenna where the signals received at : improve the performance of the wireless system.

Design of smart antenna systems combines the technologies of antenna design, signal

Processing and hardware implementation. A smart antenna is therefore either phased or adaptive array that adjust to the environment. That is for adaptive array, the beam pattern changes move and for the phased array the beam is steered or different beams are selected as desired. User moves. The early smart antenna systems were designed for use in military applications to suppress interfering or jamming signals from the enemy.

Smart antenna techniques, such as multiple input multiple output (MIMO) systems extends the capabilities of 3G and 4G systems to provide customers with increased data throughput for mobile high speed data application. MIMO systems use multiple antenna at both the transmitter and receiver to increase the capacity of the wireless channel.

Benefits of Smart Antenna Technology :-

a) Reduction in Co-channel Interference

b) Range Improvement

c) Increase in Capacity.

d) Increase in Transmitted power.

e) Reduction in Hand off

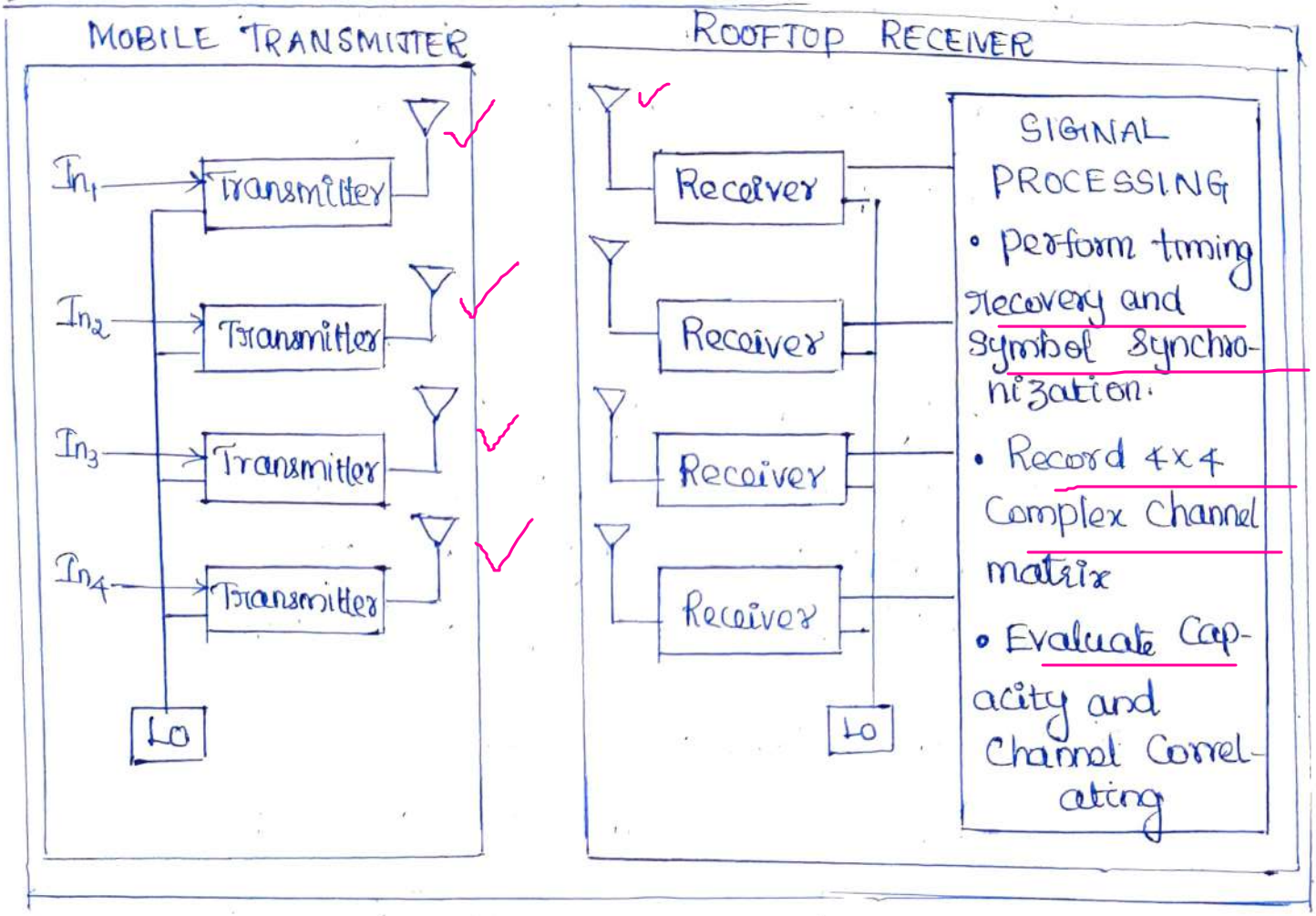
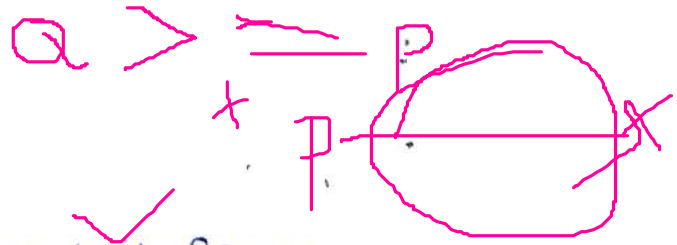


fig: MIMO system.

MIMO systems transmit different signals from each antenna simultaneously in the same bandwidth and seperated at the receiver.

⇒ four antenna present at transmitter and receiver which have potential to provide four times the data rate of a single antenna system without an increase in transmit power or bandwidth MIMO techniques, support multiple independent channels in same bandwidth provided the multipath environment is capable.

Now let us see four cases in which the number of transmitting antennas is p and receiving antennas is q. where $q >= p$.



They are

⇒ Single - Input, Single output (SISO)

⇒ Single - Input, Multiple - output (SIMO)

⇒ Multiple - Input, Single - output (MISO)

⇒ Multiple - Input, Multiple - output (MIMO)

a) Single - Input, Single output (SISO)

⇒ There is one input and one output in the radio channel hence it is called "Single Input Single output". If the channel bandwidth is B, the transmitter power is P_T, then signal at receiver has average SNR of (SNR_0).

⇒ Here the Shannon limit on channel capacity C is,

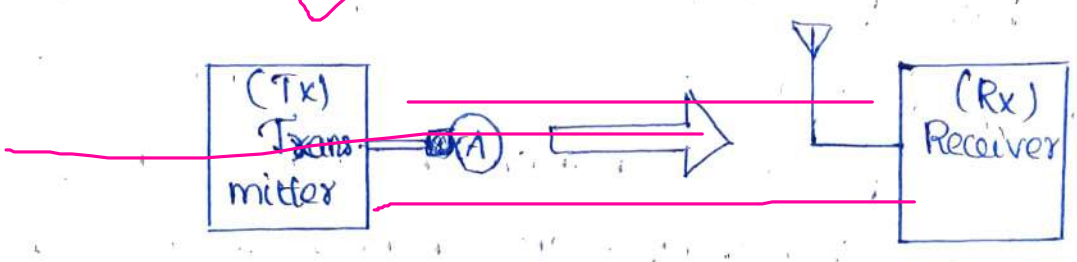


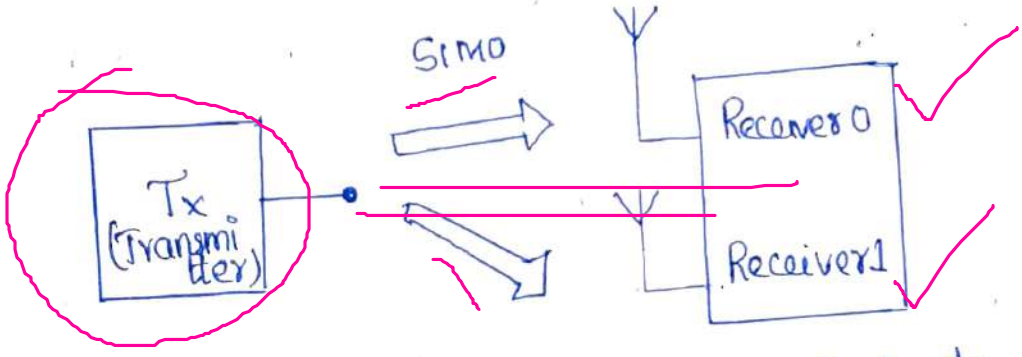
fig: Single - Input, Single - output

$$C \simeq B \log_2 (1 + SNR_0)$$

b) Single - Input, Multiple Output (SIMO):

⇒ The SIMO Configuration of the radio channel should look fairly familiar to most radio planners, and is known as receiver diversity. The input to the channel is a single transmitter signal that feeds two receiver paths.

⇒ Depending on the multipath fading and the correlation between two receiver antennas, gain is achieved in the form of fading resistance.



⇒ The gain of this method depends greatly on multipath environment and how efficient the receiver is in utilizing the micro diversity environment. If the signals received on the antennas have an average of the same amplitude, then they can be added coherently to produce an Q^2 increase in signal power considering Q antenna's at the receiver.

⇒ The capacity for this channel is approximately equal to,

$$C \simeq B \log_2 [1 + Q \times SNR_0]$$

The overall SNR will be,

$$SNR = \frac{Q^2 \times (\text{Signal power})}{Q \times (\text{noise})} = Q \times SNR_0$$

C) Multiple Inputs, Single Output (MISO):

⇒ The MISO configuration of the radio channel is a type of transmit diversity. It is used for LTE, Space frequency Block Coding (SFBC) and is applied to the radio system in order to make the radio channel more robust and add more fading resistance.

⇒ Here we have p transmitting antenna, The total power is divided into 'p' transmitter branches. When the signals are added coherently at the receiver antenna, We get p-fold increase in SNR given by,

$$SNR = \frac{p^2 [\text{Signal power}/p]}{\text{noise}}$$

$$= p \times SNR_0$$

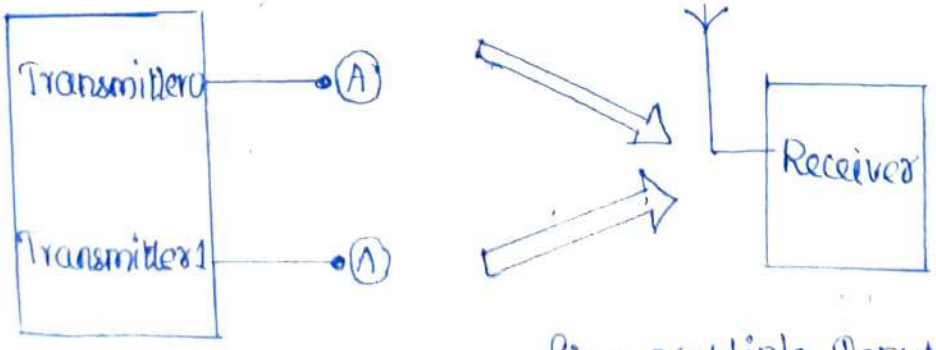


fig: multiple Input single output

d) Multiple Inputs, Multiple Outputs (MIMO)

⇒ MIMO represents multiple individual, Parallel data streams that are carried on the air interface. The decoding of both data streams (2x2 MIMO) is possible to Scattering (short reflections).

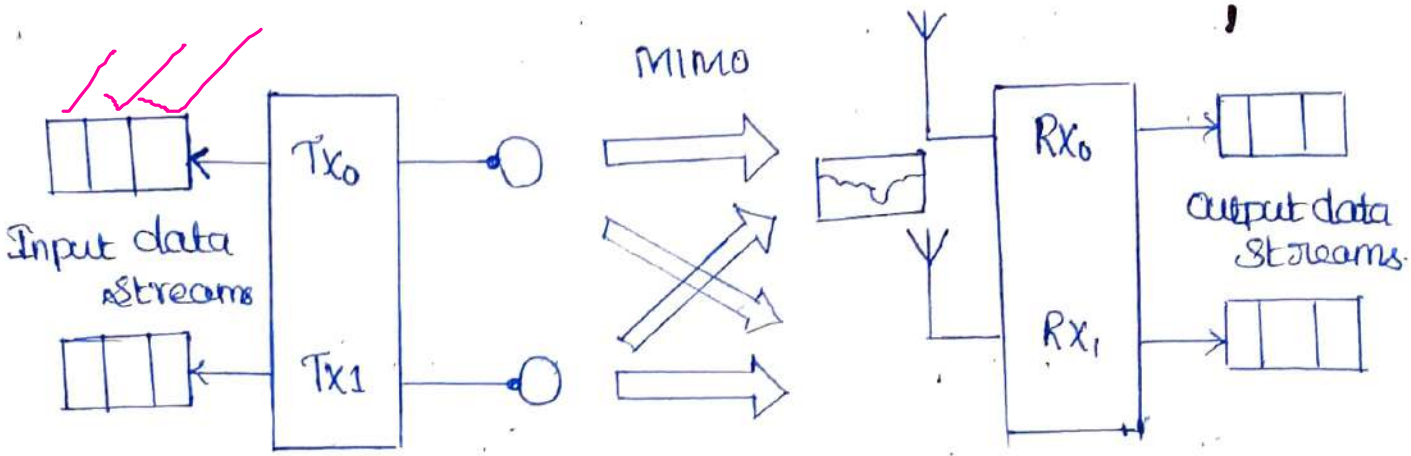


fig: Multiple Input, Multiple Output

⇒ The channel capacity 'C' is given by;

$$C = B\log_2(1 + P \times Q \times SNR_0)$$

When there are p channels (p transmitting antennas), the total capacity of the system is

$$C = PB\log_2\left(\frac{1}{P} + \frac{Q}{P} \times SNR_0\right)$$

IMS Architecture :

Introduction :-

⇒ Many successful services are available today on the internet including e-mail, web-browsing

Chat, and audio and Video downloading / Streaming Internet telephony and multimedia Communication services, Some of the latest to be launched, are already being proposed by Microsoft MSN, AOL and Skype.

IMS - Ip multimedia subsystem Standardized by the telecommunications world is a new architecture based on new Concepts, new technologies, new partners and ecosystem.

⇒ IMS provides real-time multimedia sessions (voice session, Video Session, Conference session, etc) and non real time multimedia sessions (push to talk, Presence, instant messaging) over an all Ip network.

⇒ IMPS targets Convergence of Services Supplied indifferently by different types of networks: fixed, mobile, Internet. IMS is also called Multimedia NGN (Next Generation Network).

MNGN

⇒ IMS deployment is a Strategic decision not a network technology decision. It can be taken either by a traditional Service provider in the Context of repositioning its business on Ip Services

or by any entity that would decide to start an activity in Ip. Services even without owning an access or transport network.

⇒ The Ip multimedia Subsystem (IMS) is a reference architecture defined by the 3rd generation partnership project (3Gpp) for delivering Communication services built on the Internet protocol.

⇒ Along with providing a framework for evolving from classic circuit switch (CS) to packet switch (PS) telephony, IMS is lauded for its Openness and well defined hierarchical structure.

⇒ The Ip multimedia Subsystem Standards details the Core network functionality required to provide multimedia communication services, identifying the distinct elements responsible for delivering each features and documenting a well-defined set of reference interfaces to each Component.

⇒ IMS enables operators to prevent Vendor lock-in and select 'best-of-bread' components for each operational features, while still guaranteeing their interoperability and interworking.

⇒ Acquisition of the basics of IMS architecture and standards in particular Specification of specific protocols and interfaces such as SIP, Diameter

Cops, and the knowledge of the Vendors solutions already available are essential for any stakeholder - network or service provider, telecommunications vendor, or customer that wants to be an actor in the emerging business of value added Ip services.

ARCHITECTURE:

⇒ The IMS (Ip Multimedia Subsystem) vision is to integrate mobile / fixed voice communications and Internet technologies, bringing the power and wealth of internet services to mobile and fixed users. It allows the creation and deployment of Ip-based multimedia services in the 3G networks.

⇒ IMS can enable Ip interoperability for real-time services between fixed and mobile networks and so holds the promise of seamless converged voice / data services; services transparency and integration are key features for accelerating end-user adoption. Two aspects of IMS are of fundamental importance to deliver these features.

*) Ip-based transport for both real-time and non-real-time services.

*) Introduction of a multimedia call model based on Sip (Session Initiation protocol).

The IMS will provide :

⇒ A multi-service multi-protocol, multi access, IP based network - Secure, reliable and trusted services.

⇒ Multi-Services : Any type of services may be delivered by a Common QoS enabled Core network.

⇒ Multi-access : diverse access networks (WiFi, WiMAX, UMTS, CDMA2000, xDSL, Cable etc). Can interface with IMS.

IMS An enabler for Service providers to offer :

⇒ Real-time and non real-time, Communication Services between peers, or in a client-Server Configuration.

⇒ Mobility of Services and mobility of users (Nomadicity)

⇒ Multiple Sessions and Services Simultaneously over the Same Connection.

Layers of the IMS Architecture :

⇒ The IMS architecture as defined by the 3Gpp standards in an all-packet Core network that Creates an access-agnostic environment to deliver a wide range of multimedia Services that a user can access using any devices or network Connection. Leveraging the SIP protocol, IMS Supports IP-to-IP Sessions over any wire line Connection (e.g Wi-Fi, GSM or CDMA). The IMS infrastructure allocos a carrier to interwork between the TDM and IP networks to provide a Seamless Services experience.

(a) Access layer:

⇒ IMS is access independent. In case of mobile, it can be GPRS, EDGE (also called enhanced GPRS), UMTS or wireless LAN. 3Gpp UMTS R5 focuses on EDGE and UMTS accesses. 3Gpp UMTS R6 adds I×LAN. 3Gpp2 assumes cdma 2000 accesses. Fixed service providers will apply IMS to ADSI and Cable network accesses.

(b) Transport layer:

⇒ It is an All-Ip network that consists of Ip routers (edge and Core Ip routers).

Connectivity layer = Access Layer and Transport Layer.

(c) Session Control layer:-

⇒ Comprises network Control Servers for managing Calls or establishing sessions and modifications. The two main elements of this layer are the CSCF (Call Session Control function) and the HSS (home Subscriber Server).

⇒ Some times called the SIP Server., the CSCF Performs end-point registration and routing of the SIP signalling messages to the application Server related to a particular services. In addition the CSCF interworks with the access and transport layer to guarantee QoS for all services.

(d) Application layer :-

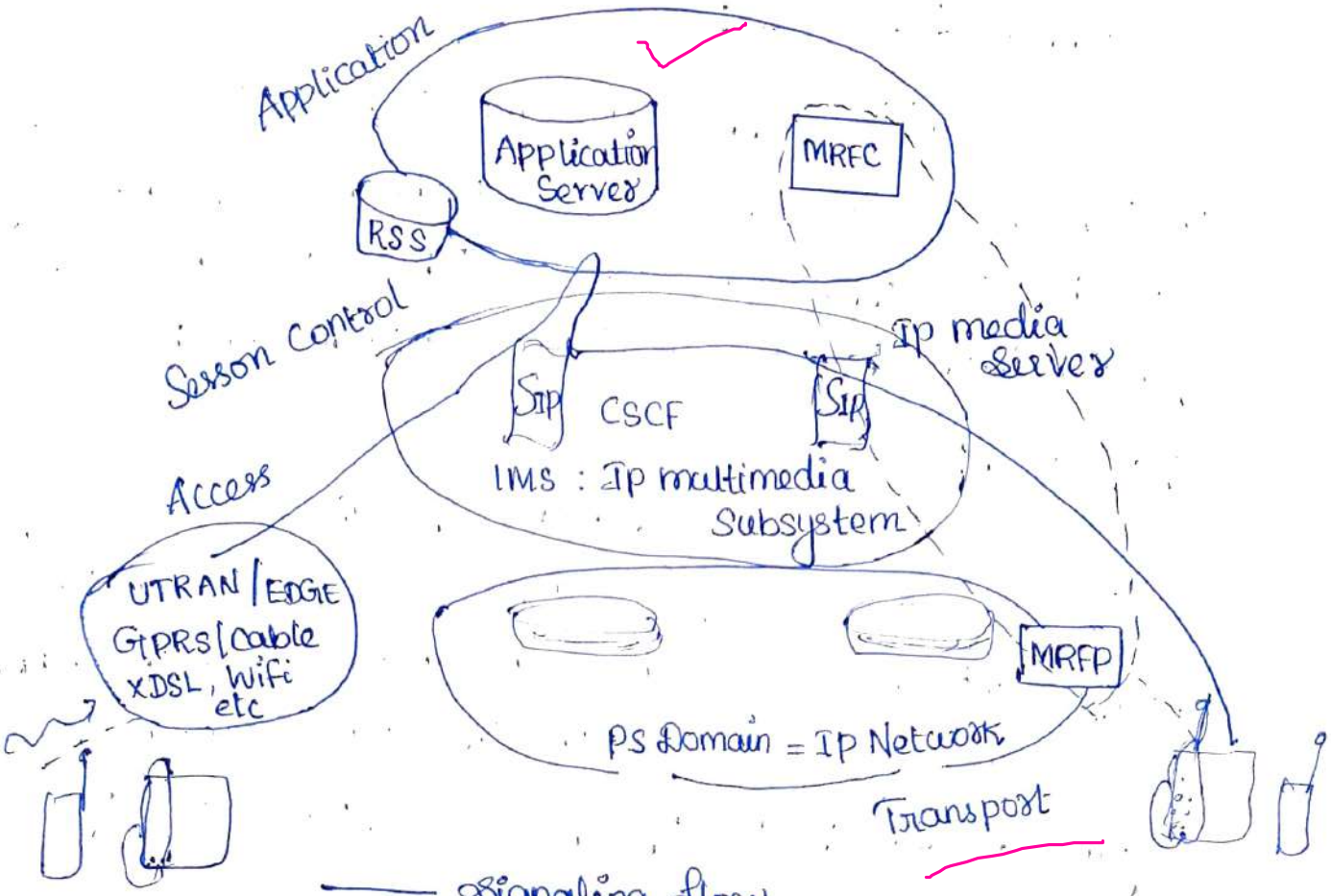
⇒ Utilizes application and Content Servers to provide Various Value - added Services. At the heart of this layer are the AS (application Server), MRFC (multimedia resource function Controller), and the MRFP (multimedia resource function processor).

⇒ The AS is responsible for the execution of Service - Specific logic, for example call flows and user interface interaction Switch Subscribers, while the MRFP - more Commonly known as the Ip media Server - provides adjunct media processing for the application layer

⇒ Through the media Server, a Service Provider can deliver Various non - telephony Services (e.g., push - to - talk) as well as Speech - enabled Services, Video Services, and other more mainstream Services such as Conferencing, Prepaid Card and Personalized ring - back tones. Control and application layers are access and transport independent so that a uses can access to his/her IMS Services from any access.

Underlying Concepts of the IMS Architecture :

⇒ A Set of requirements has been introduced for the design of IMS.



—— signaling flow

- - - - - Media flow

CSCF :- Call State Control function

PS : packet Switched.

UTRAN : UMTS Terrestrial Radio Access Network.

GPRS : General packet Radio Service

EDGE : Enhance Rate Rates for Global Evolution

MRFC : Multimedia Resource function Controller.

MRFP : Multimedia Resource function Processor.

Ip Connectivity :-

⇒ A fundamental requirement is that a client has to have Ip Connectivity to access IMS services. In addition, it is required that IPV6 is used.

2) Access Independence :

The IMS is designed to be access-independent so that IMS services can be provided over any IP connectivity networks (e.g., GPRS, WLAN, broadband access x DSL, etc). Release 5 IMS specifications contain some GPRS-specific features. In Release 6 (e.g GPRS) access-specific issues are separated from the core IMPS description.

3) Ensures quality of service from IP multimedia services.

*) Via the IMS, the terminal negotiates its capabilities and express its QoS requirements during a session Initiation protocol (SIP) session set up or session modification Procedure.

*) The terminal is able to negotiate such parameters as: Media type, Media type bit rate, packet size, Packet transport frequency, bandwidth, etc.

*) After negotiating the parameter at the application levels, the terminals reserve suitable resources from the access network.

4)*) IP policy control for ensuring correct usage of media resources.

⇒ IP policy control means the capability to authorize and control the usage of bearer

traffic intended for IMS media, based on the signaling parameters at the IMS Session. This requires interaction between the IP Connectivity access network and the IMS.

5) Secure Communication :

The IMS Provides at least a similar level of security as the Corresponding GPRS and GSM networks. The IMS ensures that users are authenticated before they can start using services, and users are able to request privacy when engaged in a session.

6) Charging arrangements :

The IMS architecture allows different charging capabilities to be used, Particularly, off-line (post paid) and on-line (pre paid) Charging.

7) Support of roaming :-

The roaming features makes it possible to use services even though the user is not geographically located in the service area of the home network.

8) Interworking with other networks :-

To be a new, successful communication network technology and architecture, the IMS has to be able to connect to as many users as possible. Therefore the IMS supports communication with PSTN, ISDN, mobile and internet users.

9) Service Control

IMS provides all the network with all the information about the services the user has subscribed to, so that standardized mechanisms are used to enable the network invoking the user's services.

10) Service development

IMS provides service capabilities for multi-media service development. presence, conferencing, instant messaging. Push-to-talk are examples of service capabilities.

LTE NETWORK ARCHITETURE AND PROTOCOL

Long Term Evolution (LTE) has been designed to support only packet switched services. It aims to provide seamless Internet protocol (IP) connectivity between User Equipment (UE) and the packet Data Network (PDN), without any disruption to the end user's application during mobility.

⇒ While the term "LTE" encompasses the evolution of the universal mobile telecommunications system (UMTS) radio access through the evolved UTRAN (E-UTRAN)

⇒ E-UTRAN is accompanied by an evolution of the non-radio aspects under the term "System Architecture Evolution (SAE)". Which includes the Evolved packet Core (EPC). Together LTE and SAE comprise the Evolved packet System (EPS).

EPS uses the concept of EPS bearers to Route IP traffic from a gateway in the PDN to the UE. A bearer is an IP packet flow with a defined Quality of Service (QoS) between the gateway and the UE

Overall Architectural overview :-

EPS provides the user with IP Connectivity to a PDN for accessing the Internet, as well as for running services such as voice over IP (VoIP). An EPS bearer is typically associated with a (QoS)

Multiple bearers can be established for a user in order to provide different QoS Streams or Connectivity to different PDNs for example, a user might be engaged in a voice (VoIP) call while at the same time performing web browsing or FTP download.

A (VoIP) bearer would provide the necessary QoS for the voice call, while a best effort bearer would be suitable for the web browsing or FTP session.

The network must also provide Sufficient security and privacy for the user and protection against false use.

Architecture Model:-

Below figure shows the overall network architecture, including the network elements and the standardized interface. At a high level, the network is comprised of the CN (EPC) and the acces network E-UTRAN

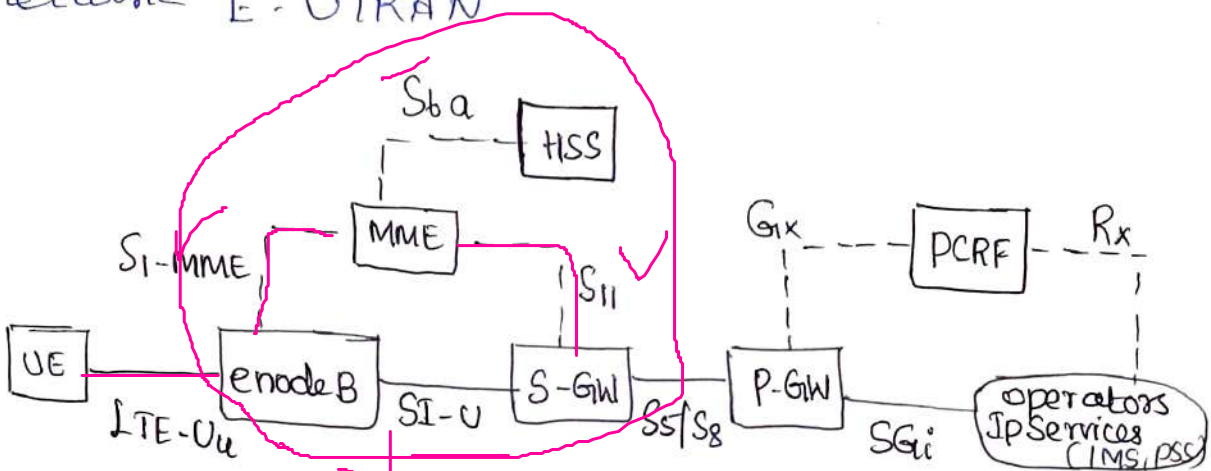


fig: The EPS network element

Functional Split between E-UTRAN and EPC:-

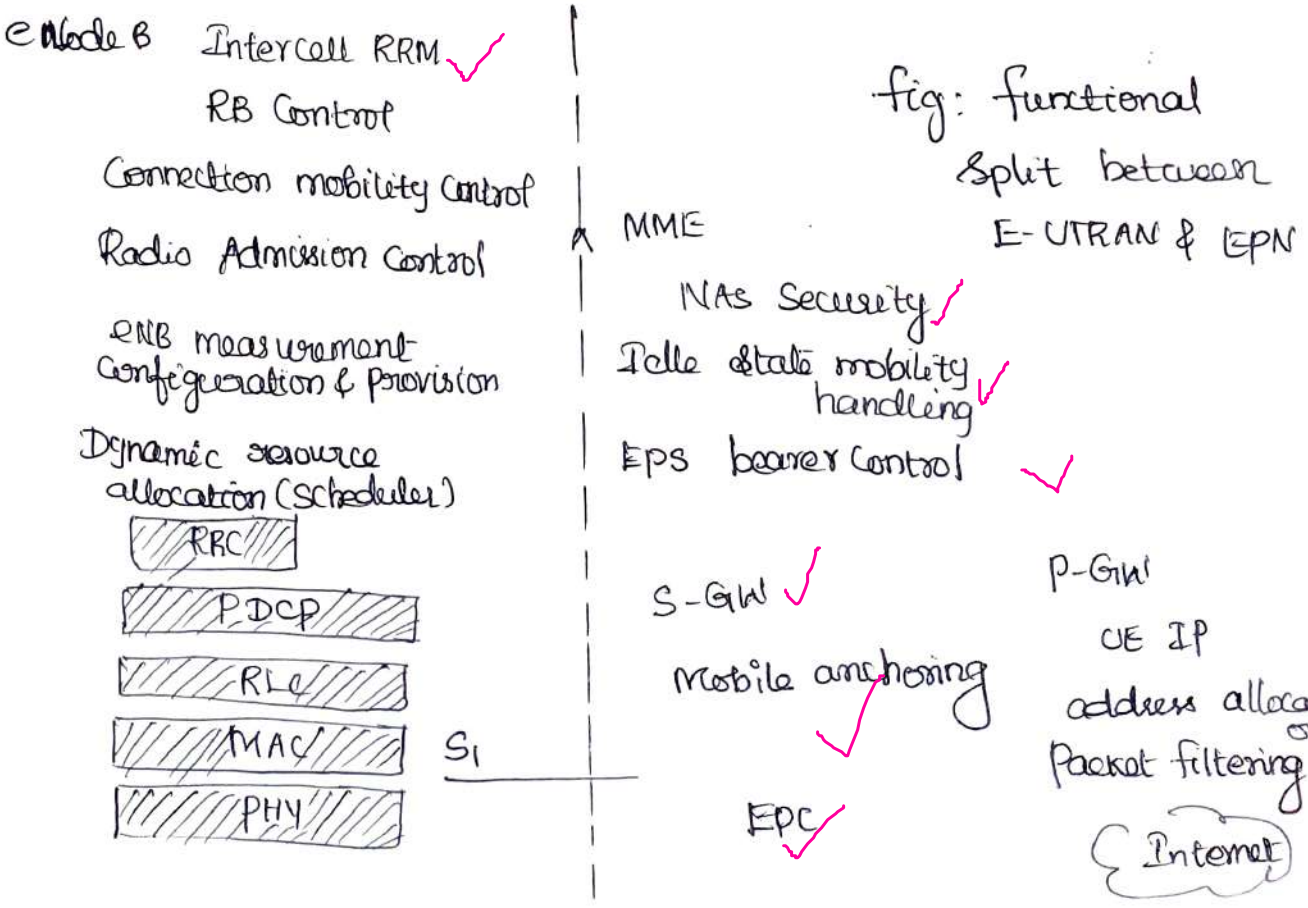


fig: functional Split between E-UTRAN & EPN

The Core Network :-

The Core network (Called Epc in SAE) is accountable for the overall Control of the UE and establishment of the bearers CN consists of many logical nodes, the access network is made up of essentially just one node, the evolved node B (enode B) which connects to the UEs

The main logical nodes of the EPC are :

* PDN Gateway (P-GW)
* Serving Gateway (S-GW)
* Mobility Management Entity (MME)

In addition to these nodes, Epc also include other logical nodes and functions such as the Home Subscriber Server (HSS) and the policy Control and Charging Rules Function (PCRF) Since the Eps only provides a bearer Path of a certain (Qos) Control of Multimedia applications

* PCRF - The policy Control and Charging Rules Function is responsible for policy control decision-making as well as for Controlling the flow-based charging Functionalities in the policy control Enforcement function (PCEF), which resides in the P-GW, The PCRF Provides the Qos

authorization (Qos class identifier [QCI] and bit rates) that decides how a certain data flow will be treated in the PCEF and ensures that this is in accordance with the user's subscription profile.

* HSS - The Home Subscriber Server contains users SAE subscription data such as the EPS - subscribed QoS profile and any access restriction for roaming. It also holds information about the PDNs to which the user can connect. This could be in the form of an access point name (APN) or a PDN address of the MME to which the user is currently attached or registered. The HSS may also integrate the authentication center (AUC), which generate the vectors for authentication and security keys.

* P-GW - The PDN Gateway is responsible for IP address allocation for the UE as well as QoS enforcement and flow-based charging according to rules from the PCRF. It is responsible for the filtering of downlink user IP in to the different QoS-based bearers. This is

Performed based on traffic flow templates (TFTs)
The p-GW performs QoS enforcement for guaranteed bit rate (GBR) bearers. It also serves as the mobility anchor for interworking with non-3GPP technologies such as CDMA 2000 and WiMAX networks.

* S-GW - All user IP packets are transferred through the Serving Gateway, which serves as the local mobility anchor for the data bearers, when the UE moves between eNode Bs. It also retains the information about the bearers when the UE is in the idle state and temporarily buffers downlink data while the MME initiates Paging of the UE to reestablish the bearers. In addition the S-GW performs some administrative functions in the visited network such as collecting information for charging and lawful interception. It also serves as the mobility anchor for interworking with other 3GPP technologies such as General Packet Radio Service (GPRS) and UMTS

MME - The Mobility Management Entity (MME) is the control node that processes the signaling between the UE and the CN. The protocols running between the UE and the CN are known as the Non Access Stratum (NAS) protocols.

The main functions supported by the MME can be classified as.

i) Functions related to bearer management - This includes the establishment, maintenance and release of the bearers and is handled by the Session management layer in the NAS protocol.

ii) Functions related to Connection management:. This includes the establishment of the Connection and Security between the network and UE and is handled by the Connection or mobility management layer in the NAS Protocol layer.

Mobile Virtual Network operation (MVNO)

A mobile virtual Network Operator (MVNO) is an entity, who offers telecommunications services similar to a mobile network operator (MNO) however the MVNO does not own any radio frequency Spectrum.

Instead the MVNO enters into an agreement with a mobile network operator, who has radio frequency Spectrum. Depending on the type of MVNO, it will either buy bulk access to the network services from the mobile network operator at discounted rates (wholesale agreement)

and then set its own proposition and retail prices as it will enter into a reseller agreement with the mobile network operator.

MVNOs can afford to mark down their retail prices to a certain extent because they do not have to pay radio Frequency Spectrum licenses and they have no infrastructure to build or maintain. Because MVNOs have low overhead, they can spend aggressively on marketing to increase their chances of selling minutes to Consumers.

MVNOs can be classified in to the following Categories

* Business MVNO provides Custom-made Services to business.
* Discount MVNOs provides low call rates to Certain market Segments.
* Life Style MVNOs Focuses on a niche market demograph
* Advertising-Funded MVNOs Builds revenues through advertising to provides Free voice text and content to various Subscribers.
* Ethnic MVNOs provides long-distance Calling Service

There are Several reasons why mobile operators permit MVNOs on networks For example mobile operators generally find it hard to Serve

all Customer Segments, MVNOs can implement Specific marketing to tackle targeted Consumer Groups. Most of the mobile operators have Capacity Segment needs and provides in new areas Such as 3G. MVNOs help ensure better network utilization

MVNOs also help mobile operators target Customers with Spececial Service requirements They provide low operational costs for mobile operators grow average revenue per user and Solve difficult issues regarding how to deal with Fixed mobile Convergence MVNOs are also more able to try experienced applications and projects.