Network Security

Unit-1

Network Devices :-

1) Repeater :- It make weak signal strong upto a prefixed value not more than it.
It is used to regenerate signals. Bit by Bit regeneration is done by repeater. Regenerating signal maintain signal strength.
→ Works on Physical layer.

2) Hub → It is used to send the data packet to all the devices connected. Different devices will be connected to control unit called Hub.
→ Works on Physical layer & is not intelligent.
Types :-
(i) Active Hub :- Needs power supply. It is a multipoint repeater with capacity of regenerating signals.
(ii) Passive Hub :- It is just a connector which connects wires comming from devices.

3) Bridge :- used to interconnect two different n/w of same protocol. It is intelligent device because it work on MAC address. It works on DDL.

4) Switch :- It is intelligent device. It is similar to repeater with additional facilities. It will only send good and correct data packets to ports. If packets contains error then it will be ignored by switch. It perform error checking means good datapackets will be send to

correct port and data packets with error is not forwarded.
It comes in 8 port, 16 port & 58 ports.

5) Router :- It will collect the data and send it to different port based on IP address. Router use different routing algo to send the data and it will select the best routing algo path for sending the data.

6) Gateway :- It passes data from one n/w to other n/w which are holding in different protocol.
It passes data to N/w of different network models like OSI and TCP. It is also known as protocol conversion.

7) NIC :- Network Interface Card is a n/w adapter to connect computer to n/w. It is installed in computer to establish a LAN. The cable act as a interface b/w computer and router. It is a layer 2 device which means it work on both Physical & Data Link layer.

* Types of Switch :-
(i) Store and forward switch :- The switch buffer and verifies each frame before forwarding it. It is slow but reliable.
(ii) Cut through switch :- It reads only upto the frame added before forwarding it to n/w and no error checking is done.
(iii) fragment frame switch :- Retains features of both store and forward switch and cut through switch. It checks frames for 64 bytes.

Devices used in each layer

1. PL :- Hub, Repeater, Cables, Fibres
2. DLL :- Bridge, Modems, N/w Card, 2 layer switch
3. NL :- Router, B Router, 3 layer switch
4. TL :- Firewalls, gateway
5. SL :- Gateways, firewall, PC's
6. PL :- Gateways, firewall, PC's
7. AL :- Gateways, firewalls, PC's, all end devices like PC, phone, servers, etc.

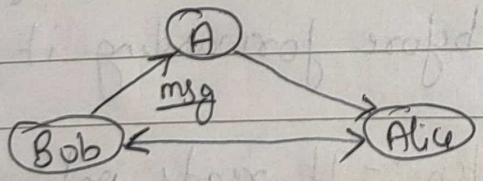
Security Attacks in n/w :-

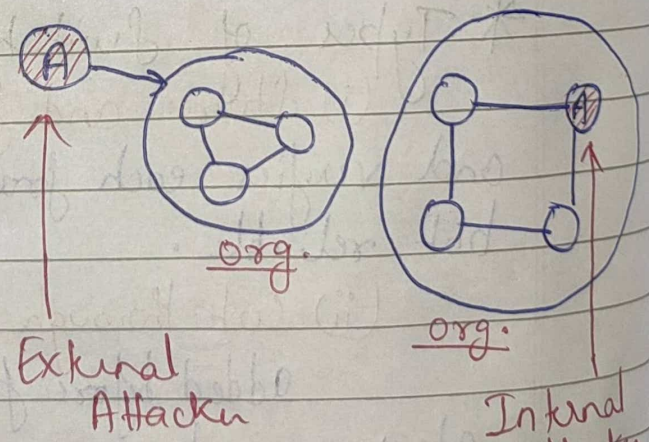
- Passive Attack
  - → packets are not modified
  - → information pattern going to be collected
- Active Attack
  - → modification is done

types :-

(i) External (ii) Internal

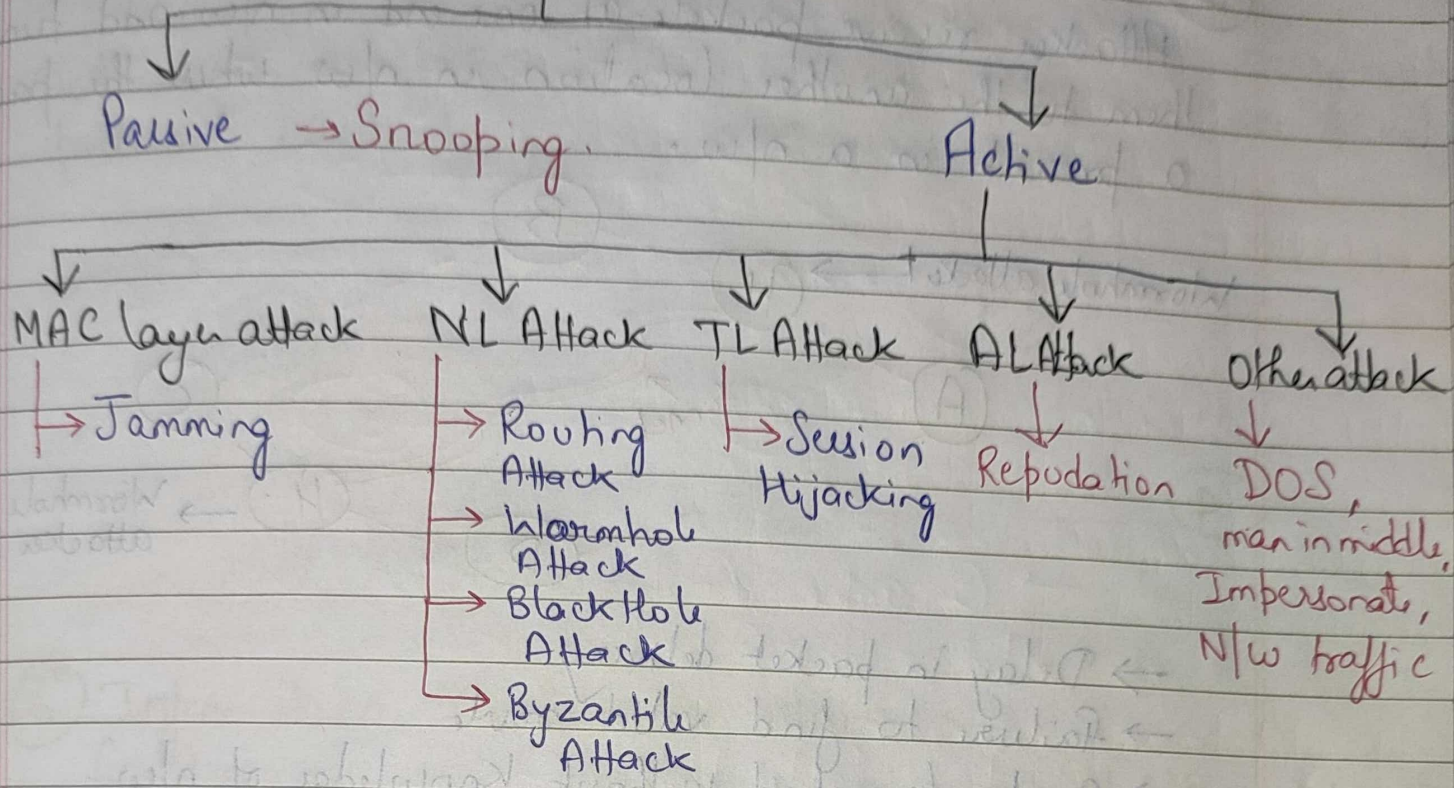
Snooping :-





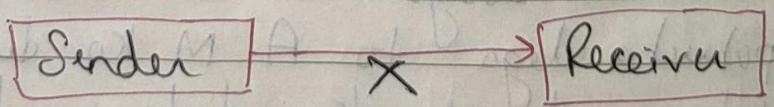
* Human is weakest to get attacked.

Attacks



① Snooping Attack :- (Replay Attack) :-
It involves intruder listening to a traffic b/w a machine or n/w. If traffic contains password, an unauthorized user can excess the n/w and read confidential data.
Eg → Keylogger, man-in-middle, N/w Snooping, Packet capture / Sniffer, Telephone wire tapes.

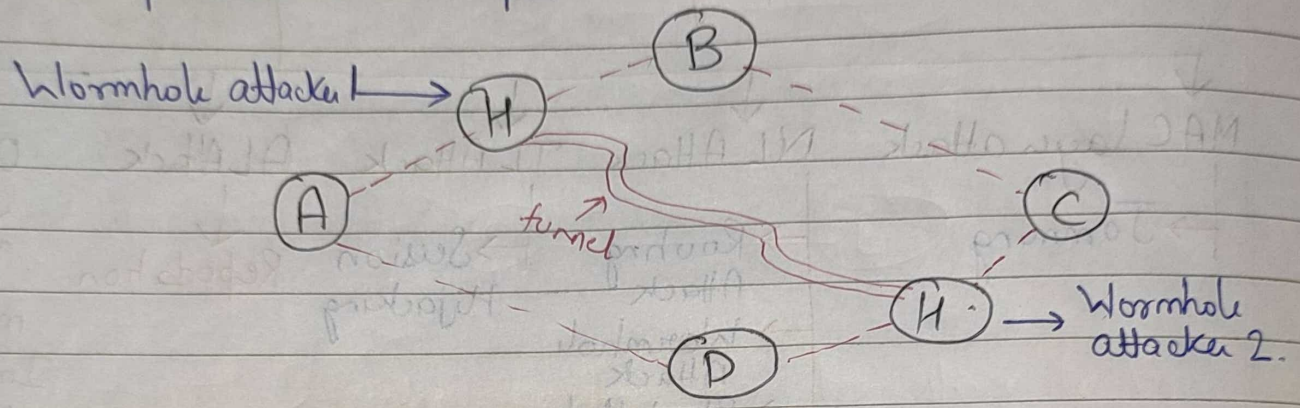
② Jamming :- It is a attack in which a attacker transfer interfering signals on a wireless n/w intentionally. As a result, it decreases the signal to noise ratio at the receiver end.



Types of Jammer :-
1) Proactive
2) Reactive
(iii) Function Specific
(iv) Smart Hybrid

(3) Wormhole Attack :-

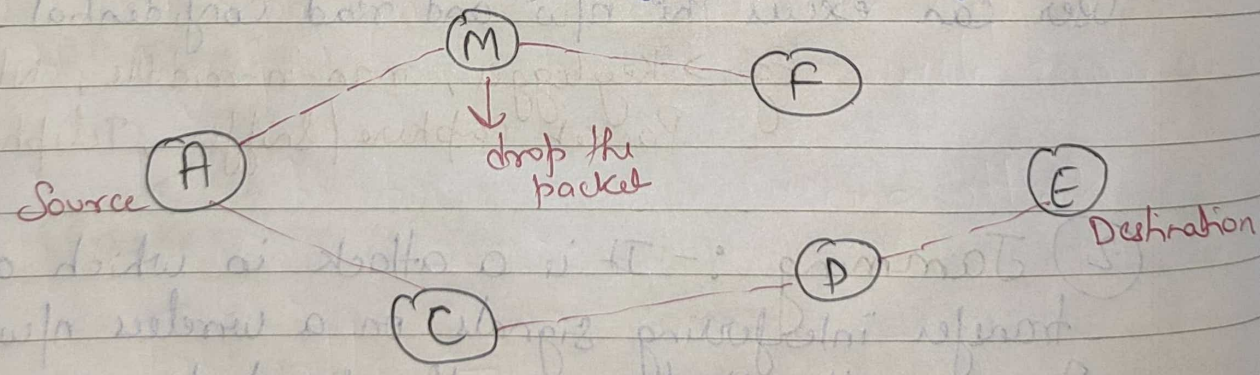
Attacker receive packets at one end in n/w and tunnel them to the another location in n/w where the packet a present in a n/w.



→ Delay in packet delivery
→ failure to find valid route
→ Can be launched without knowledge of n/w.

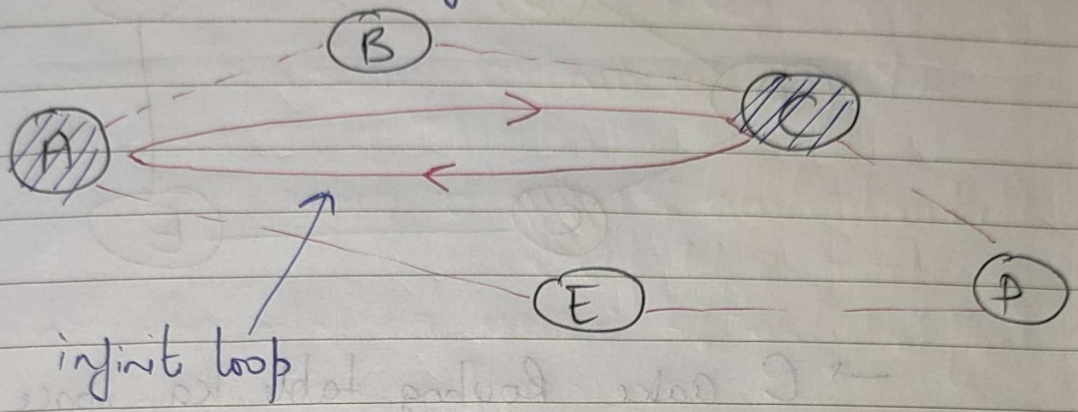
(4) Blackhole attacks :-

A malacious node falsely advertise good path to the destination node, during path finding process.

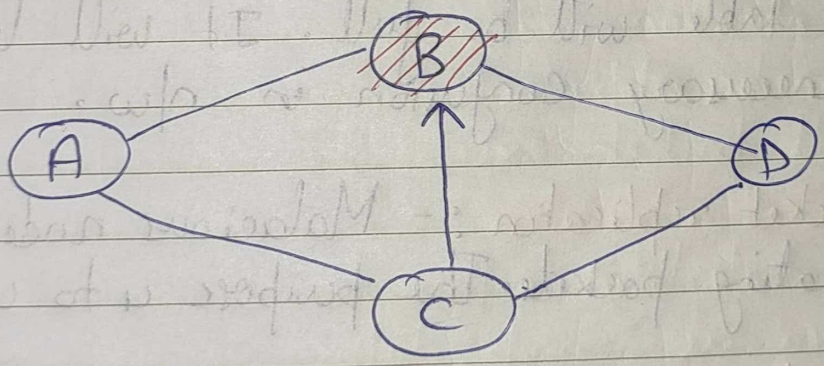


M bolega ki wo bas 2 skp me E tak pahucha dega to A M ko de dega packet qki uske route se km distance pad rha h.

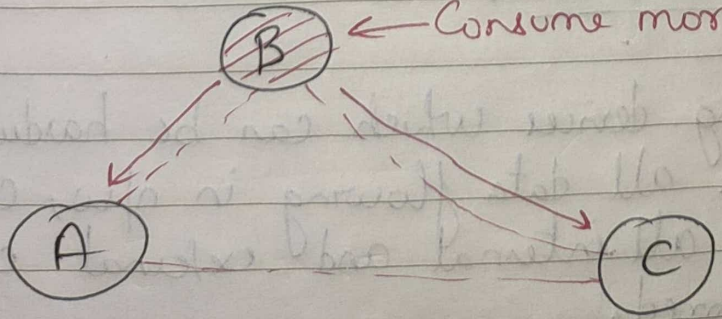
(5) Byzantile Attack :-
Comparise nodes works in collaboration and carry out acts such as creating routing loops, packets on non-optimal path and selectively droping the packets.



(6) Information Disclosure attack :-
Compromise node may leak important file or confidential file to unauthorized node.

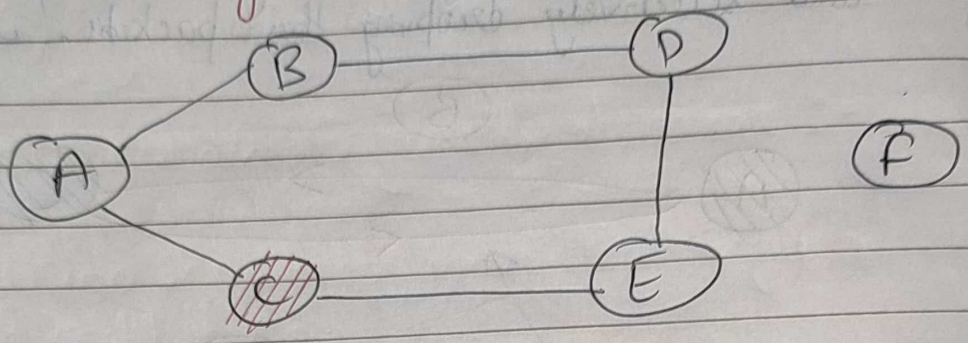


(7) Resource Consumption attack :- In this, malacious node try to consume or wast the resources.



(8) Routing attack :- These are various attack on routing protocol.

(i) Routing table overflow :-



→ C aake Routing table ka space le lega jisse ek valid node F include nhi ho payega.

(ii) Routing table poisoning :-
In this malicious node will send false info and again table will be full. It will lead to unnecessary confusion in n/w.

(iii) Packet replication :- Malacious node keep on replicating packets. The purpose is to waste resources.

(iv) Route cache poisoning (v) Rushing attack.

Firewalls :-

→ Networking devices which can be hardware or software.
→ It monitors all data flowing in n/w, checks for virus and all internal and external communication gets monitored.

Types of firewall :-

1) Packet filter routing firewall
2) App level gateway firewall
3) Circuit level gateway firewall.

Unit-2

IP Security :- It is a capability that can be added to either current version of IP (IPv4, IPv6) by means of additional headers.

IPSec contain 3 functional areas :-

Authentication :- how to prove that info is comming from right place.

Confidentiality :- ensures no info gets leaked to any unauthorised user.

Key-management :- it manages keys b/w sender and receiver, we use mathematical computation to generate key so that it become difficult to unlock.

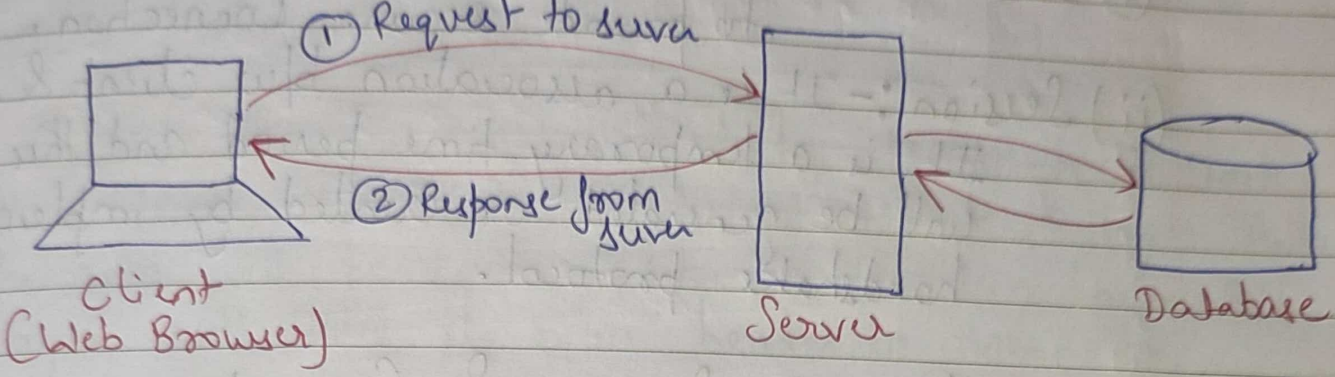
* Authentication make use of HMAC (Hash-MAC). It can be applied to entire original packet of IP or to all packet except IP header.

* Confidentiality is provided by an encryption format known as encapsulation security payload.

Application of IPSec :- It provides the capability to secure communication across a LAN (private) and public MAN and across internet.

Unit-4

Web Security :-



* Two protocols used for ensuring Web security are HTTP & HTTPS.

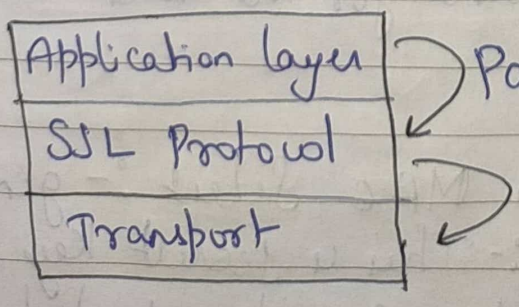
Secure Socket Layer :-

It provide the security for the data transfered between web browser and server. It is a Internet Protocol for secure exchange of ~~too~~ information ~~in~~ between the browser and server.

It provides security at transport layer. It is situated b/w application layer & transport layer.

SSL protocol is implemented by different protocols :-

(i) SSL Record protocol
(ii) Handshake protocol
(iii) Change Cipher Specification
(iv) Alert protocol.



For implementing SSL protocol we need to understand 2 important concept :-

(i) Connection :- It is the transport b/w client and server to provide secure Connection.

(ii) Session :- It is a association b/w client & server. It is a temporary time period and this session will be generated or created by implementing handshake protocol.

* Parameters of Session & Connection :-

(i) Session State parameters :-

→ Session identifier
→ Peer Certificate (Eg. X.509)
→ Compression method (lossless) → optional
→ Encryption Algorithm (AES, DES, DDDES, etc)
→ Master Secret (nothing but a secret key shared b/w client & server).
→ Is resembled (flag value).

(ii) Connection State parameters :-

→ Server and client Random :- These are bytes sequence which are associated with connections.

→ Server Write MAC Secret :- This is a MAC generated by the server for the data and data is send by the server.

→ Client-Write MAC Secret :- generated by client.
→ Server Write key :- This is secret key used by Conventional encryption and it is send by server.

→ Client Write key :- Send by client
→ Initialization Vector (IV) :- It is data or value which is used to perform modes of operation.
→ Sequence No.

SSL :- This is implemented by SSL Protocol Stack. It is above the TCP and below the HTTP layer. When the data will be coming from Application Layer, SSL layer will add its own header in data.

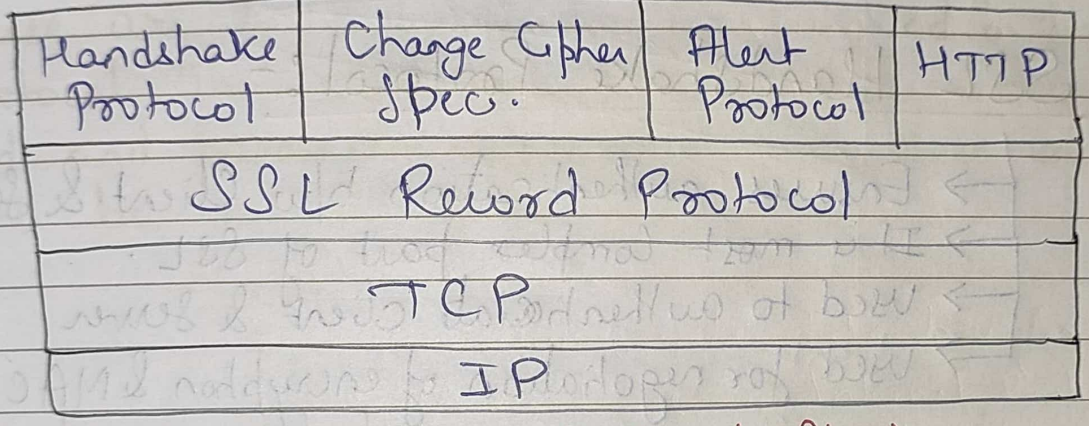
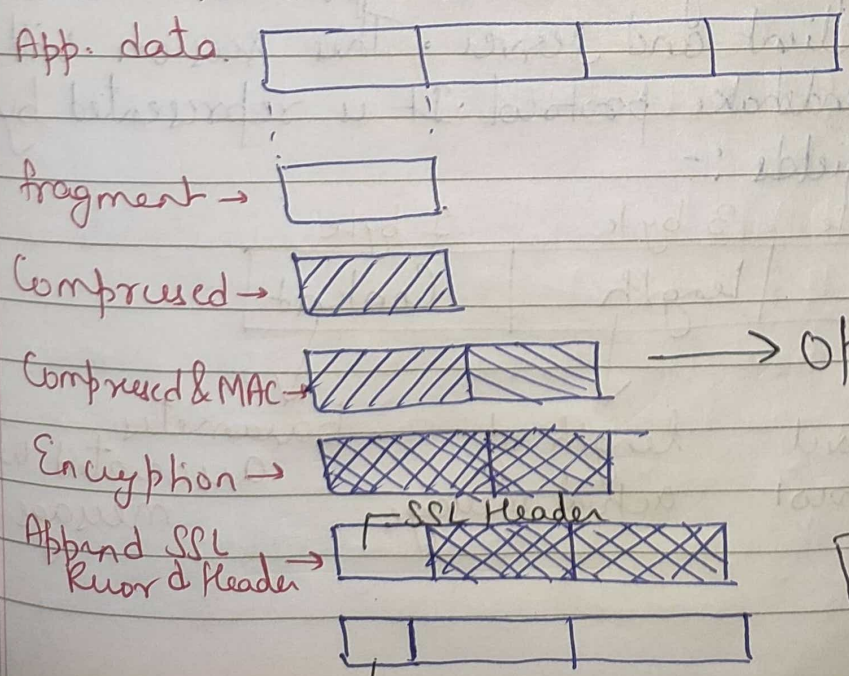
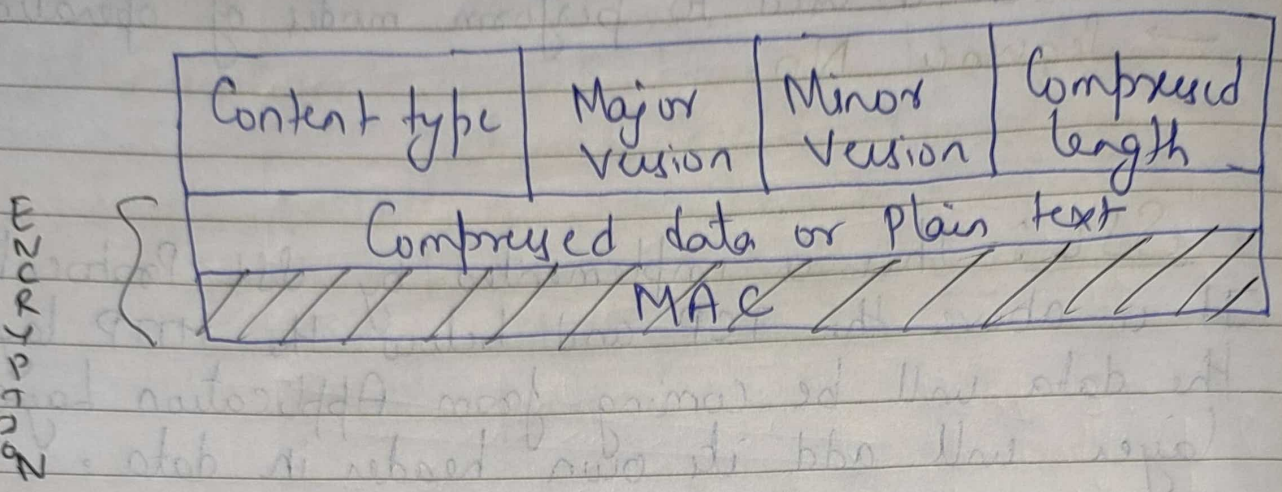


fig. SSL Protocol Stack

SSL Record Protocol :-



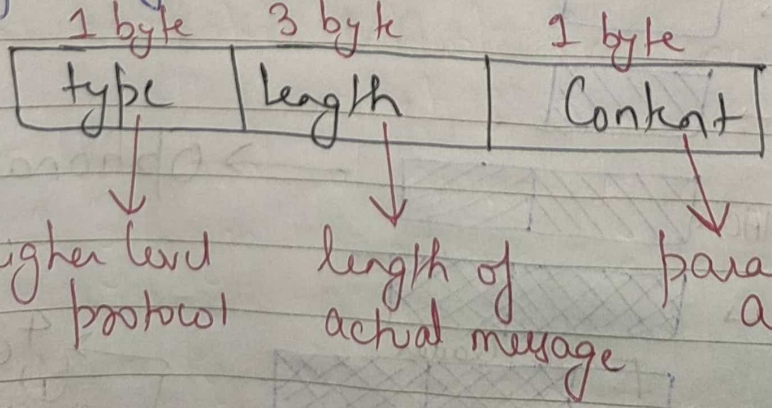
SSL Record Header :-



SSL Handshake Protocol :-

- → Ensures authentication b/w Client & Server
- → It is most Complex part of SSL.
- → Used to authenticate client & Server
- → Used for negotiation of encryption & MAC Algorithm
  - encryption → DDDES, DES, AES
  - MAC → MD-5, SHA-1

The main purpose of handshake protocol is to establish the session b/w client and server. This session will be generated by handshake protocol. It is represented by following 3 fields :-



Message @ involved in Handshake Protocol :-

→ Client Hello
→ Server Hello
→ Certificate X-509
→ Server key exchange
→ Server Done
→ Client-key Exchange
→ Certificate-verify
→ finished

These are the different message involved in handshake protocol. The length of the message will be the record field and parameter associated with these message will be in 3rd field.

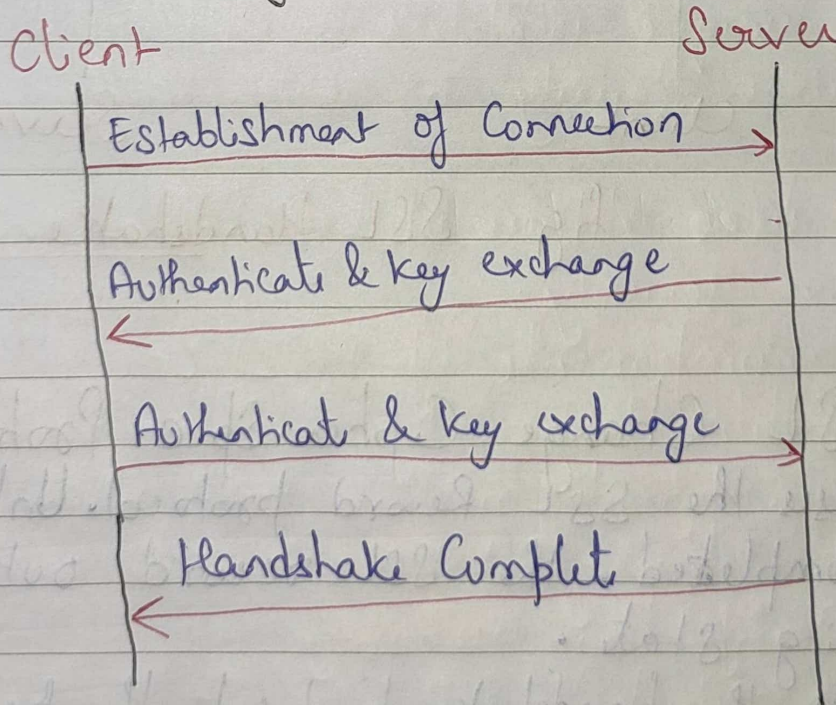


fig. Working of SSL Handshake protocol.

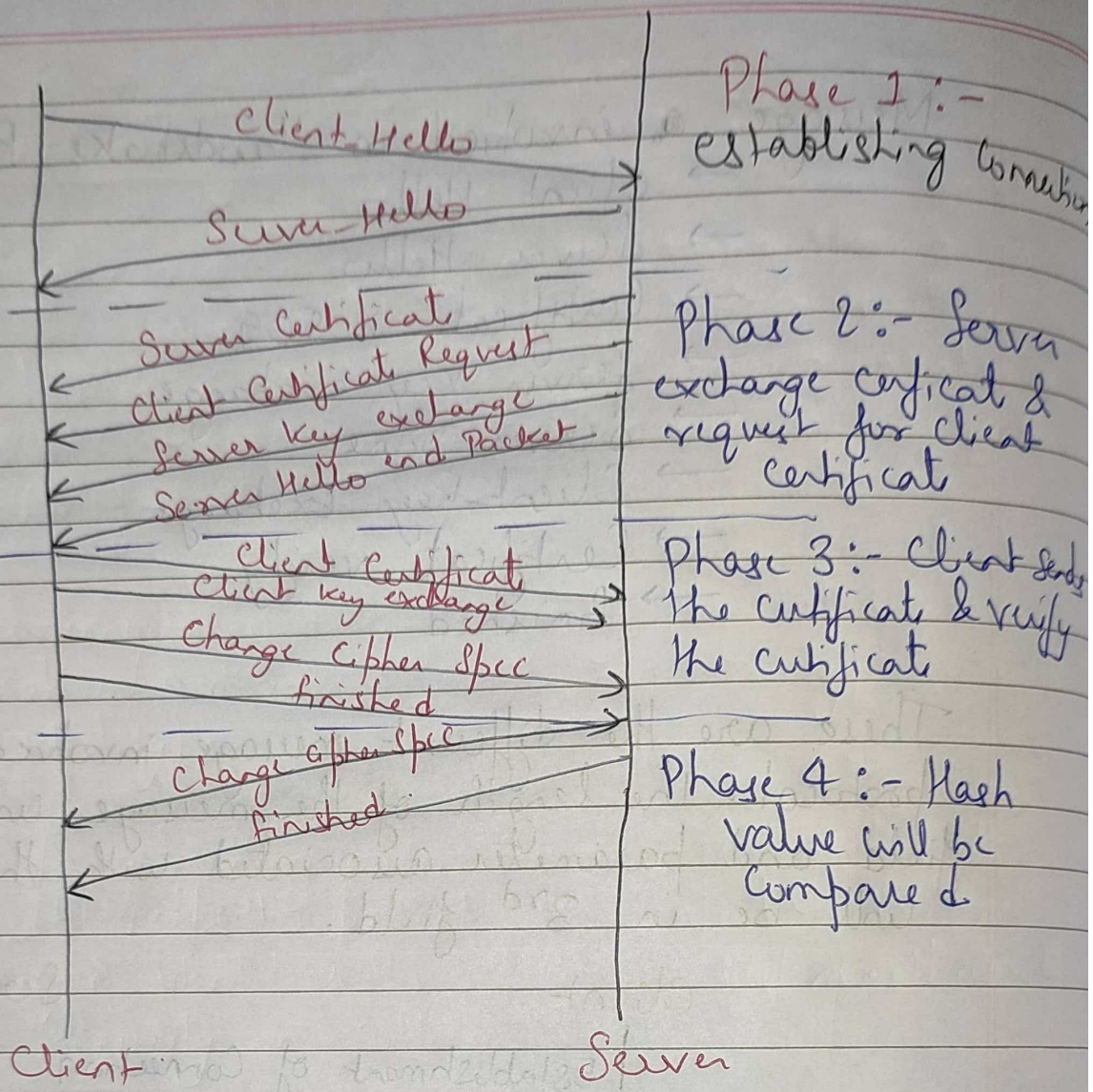


fig: SSL Handshake Protocol

SSL Change Cipher Spec Protocol :-

→ It uses the SSL Record protocol. Unless the handshake is completed, the SSL record output will be in pending state.

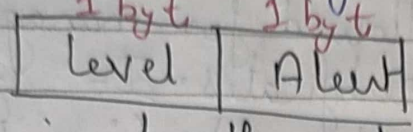
→ After the handshake protocol, the pending state is converted into the current state.

→ Change cipher protocol consist of a single message which is 1 byte in length and can have only one value.

→ Its purpose is to cause the pending state to be copied into the current state.

Alert Protocol :-

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contain 2 bytes.



The label is further classified into 2 parts :-

(i) Warning :- This alert has no impact on the connection b/w sender and receiver.

(ii) fatal error :- This alerts break the connection b/w sender and receiver.

Warning :-
- → Unexpected_message
- → Bad_record MAC
- → Decompression
- → Handshake failure
- → Ilegal_parameter

Remainder of Alert :-
- → close_notify
- → no_certificate
- → bad_certificate
- → unsupported_certificate
- → certificate_revoke
- → certificate_expired
- → certificate_unknown.

SET (Secure Electronic Transaction)

* Used to secure transaction between customer & merchant.
* Aim is to protect (i) Personal info. (ii) financial info

Info < Payment info, order info.

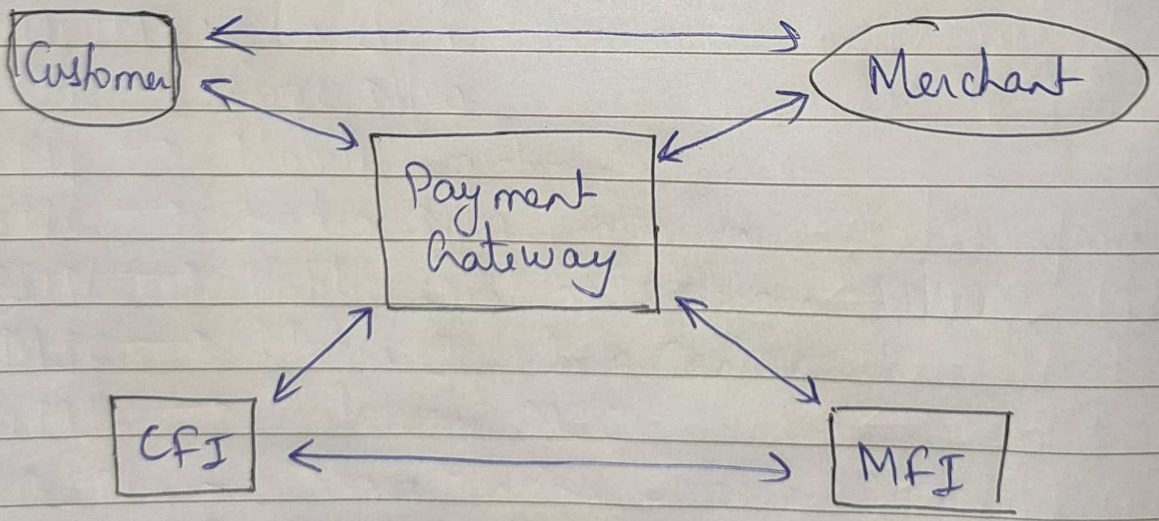
Set Services :-

① Confidentiality :- (of your data)
② Integrity :- (should not have data alteration)
③ Cardholder Authentication :- (card is valid or not)
④ Merchant Authentication :- (able to accept the card)

SET

* It is a system or electronic protocol to ensure the integrity and security of a transaction conducted on Internet.
* E-commerce website implemeate this protocol to ensure electric payment made by debit card is secure.
* SET Blocks out all personal details on card, preventing hackers and the data from accessing or stealing card holder info.
* SET is not a payment gateway but a security protocol which uses aspect of PKI to address privacy, authenticity & security.

* The primary goal of SET protocol is to protect credit/debit card transaction as they take place over the internet. It also helps to authenticate user - with digital certificate.
* A general scenario of electronic transaction includes clients, payments gateway, client financial inst, merchant and merchant financial inst.



Participant of SET :-

Set includes following participants :-

1. Cardholder → (Customer)
2. Merchant → (Seller)
3. Issuer → (CFI)
4. Acquirer → (MFI)
5. CA → Authority that follow certain standards and issuing certificate (x.509) to all participants.

Set functionality :-

1. Provide Authentication :-
   Types :- 1. Cardholder / Customer
   2. Merchant
2. Provide Message Confidentiality
3. Provide Message Integrity.

Requirements of SET :-

1. has to provide mutual authentication (i.e customer auth. by confirming is the customer intended user or not and merchant auth.)

2. Secure SET also needs to prove inter operability and make use of best security mechanism.

3. Has to keep PI and OI confidential by appropriate algorithm.

Public Key Infrastructure :-

It is a standard followed for managing, storing and revoking the digital certificates. It follows asymmetric key cryptography (i.e two different keys are going to be used here one for encryption and other for decryption).

PKI includes message digest (integrity), digital signature (Authentication/non-repudiation) and encryption service (confidentiality).

PKI is the governing body behind issuing digital certificate. It helps to protect confidential data and gives unique identities to users and system. Thus it ensures security in communication.

PKI uses a pair of key Public and Private key to achieve security.

Components of PKI :-

(i) Public key certificate (also refferd as digital certificate or SSL certificate).
(ii) Private key tokens
(iii) Certification authority
(iv) Registration authority
(v) Certificate managment System

(i) Digital Certificate :- It is a small file stored on computer or electronic device. The file extension for digital certificate is ".cir".
→ It establish relation b/w user & public key.

→ Digital certificate must be issued by a trusted third party or entity.
→ It can be connected on the id card issued to person.
→ People uses this ID card such as driving licence, passport to prove their identity. A digital certificate does the same basic thing in electronic world. But with 1 difference. Digital certificate are not only issued to people, but they can be issued to computers softwares or anything else that need to provide integrity in electronic world.
→ It is based on ITU Standard X.509 which defines a standard certificate format for public key certificate. Hence digital certificate are sometimes refered as X.509 certificate.

(ii) Certificate Authority :- CA digitally signs the entire information and includes digital signature in certificate.
→ Anyone who needs the assurance about the public key and associate information of client he carries out the signature validation procedure using CA's public key.

Unit - 5

GSM (Global System for Mobile Communication)

→ It is a digital cellular technology used for transmitting mobile devices. It uses 4 different frequency bands of 850 MHz, 900 MHz, 1800 MHz and 1900 MHz.

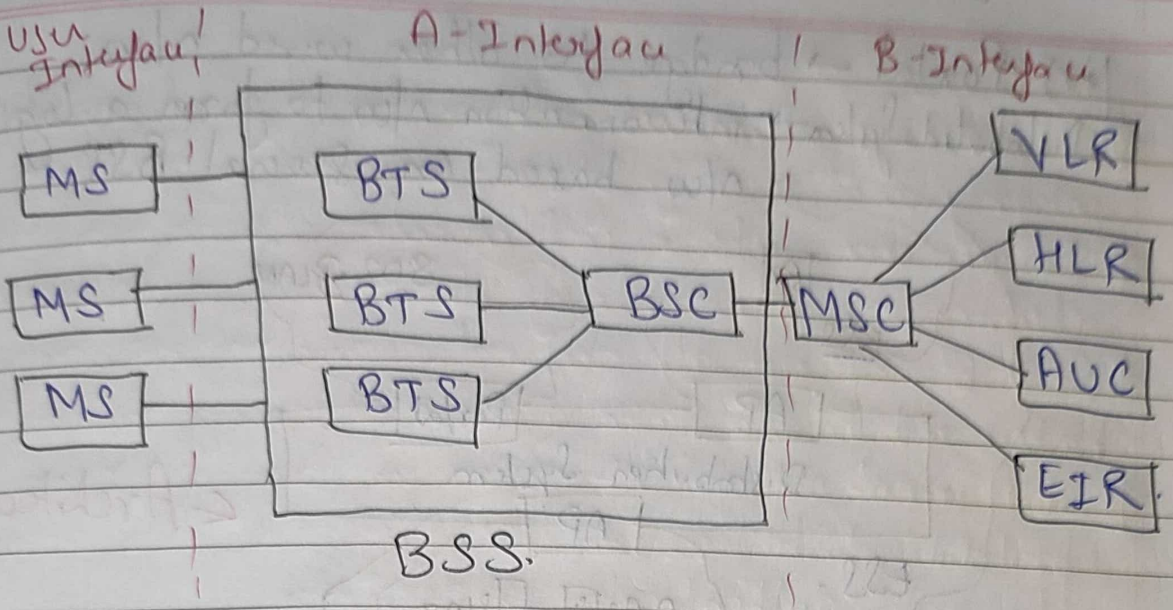
→ It uses concept of FDMA and TDMA.
→ It is having 4 different sizes of cells which are used in GSM technology :-
(i) Macro → In this size of cell, base station is installed
(ii) Micro → In this size, antena height is less than avg. roof level.
(iii) Pico → Small cells diameter of few meter
(iv) Umbrella → It covers the shadowed regions.

* Feature of GSM :-

→ Good voice Quality → Support international roaming.
→ Ability to support multiple handed devices
→ Low service cost → ISDN Compatibility.
→ New features & services can be integrated easily.

GSM Architecture :-

MS → Mobile Station
BTS → Base transiver Station
BSS → Base Station Subsystem
MSC → Mobile Switching Center
EIR → Equipment Identity Register.
VLR → Visitor Location Register
HLR → Home Location Register
AUC → Authentication Code



IEEE 802.11 Architecture (Wifi)

↓

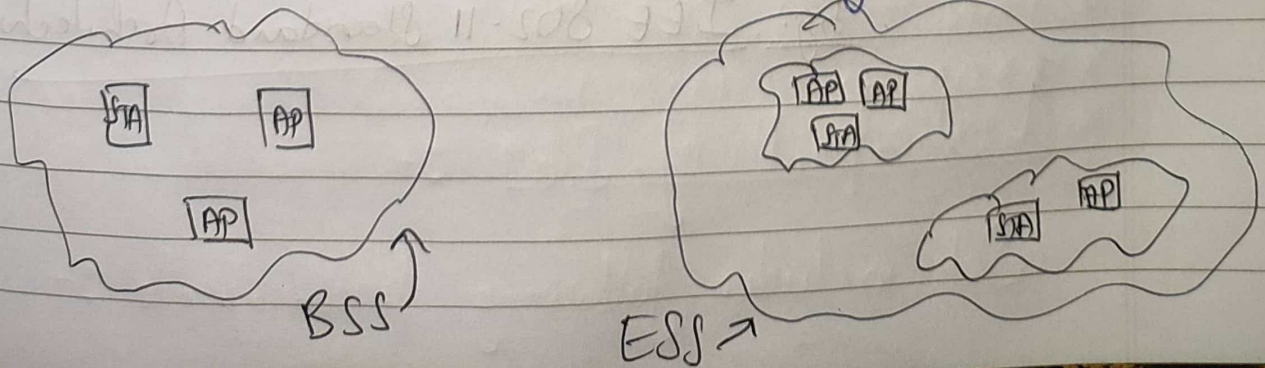
2 types of Services

- BSS (Basic Service Set)
- ESS (Extended Service Set)

→ Wireless N/w :- Those n/w which provides communication without the use of wires.

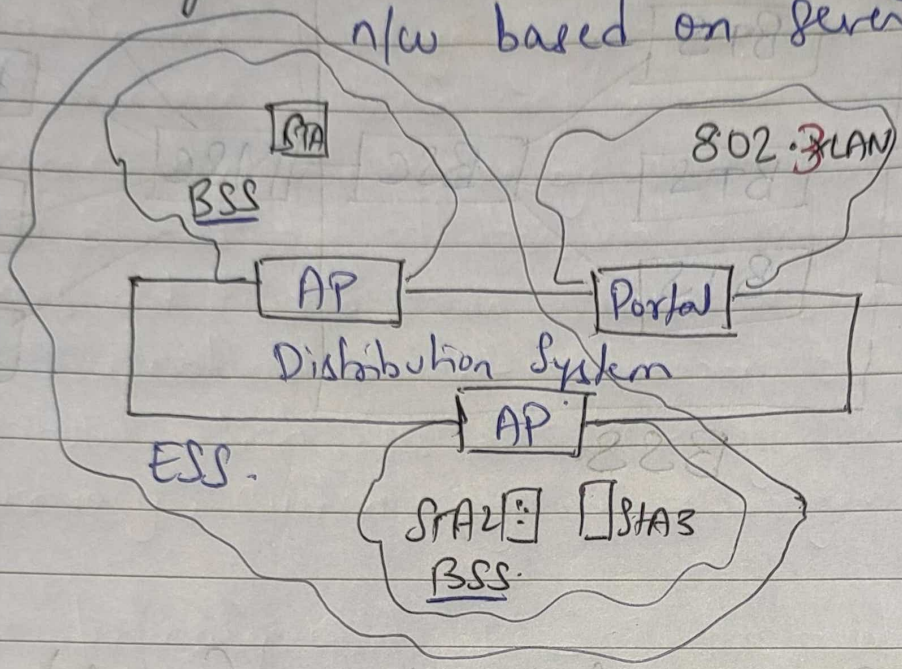
Components :-

(i) STA → (Station) → mobile nodes
(ii) Access point (AP) → Stations are connected to access pt.
(iii) BSS → Stations + AP with same radio coverage.
(iv) ESS → Several BSS connected through AP.

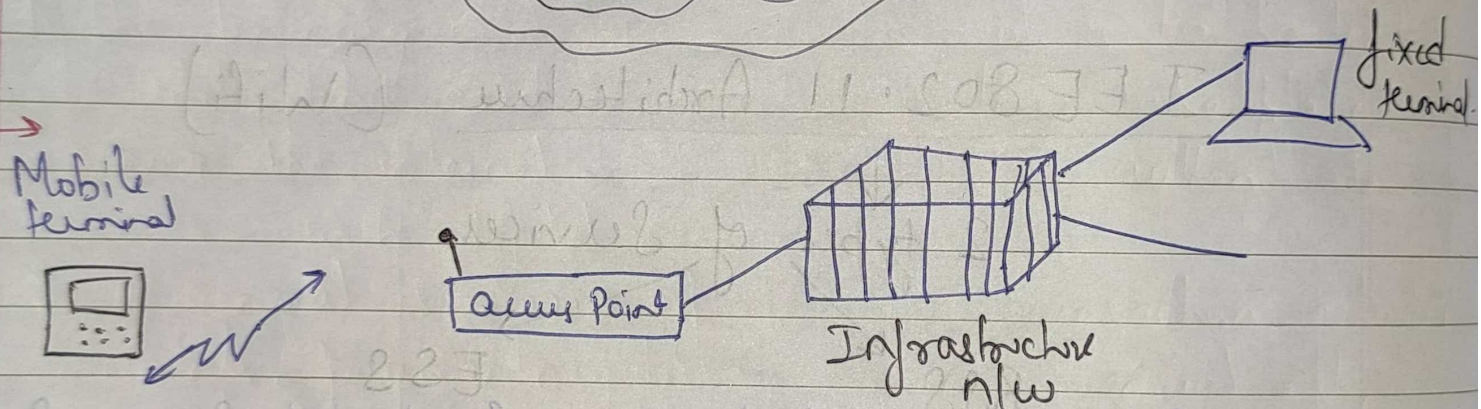


(iv) Portal → bridge to other wired n/w

(vi) Distributed System → interconnection n/w to form a logical n/w based on several BSS.



← Architecture



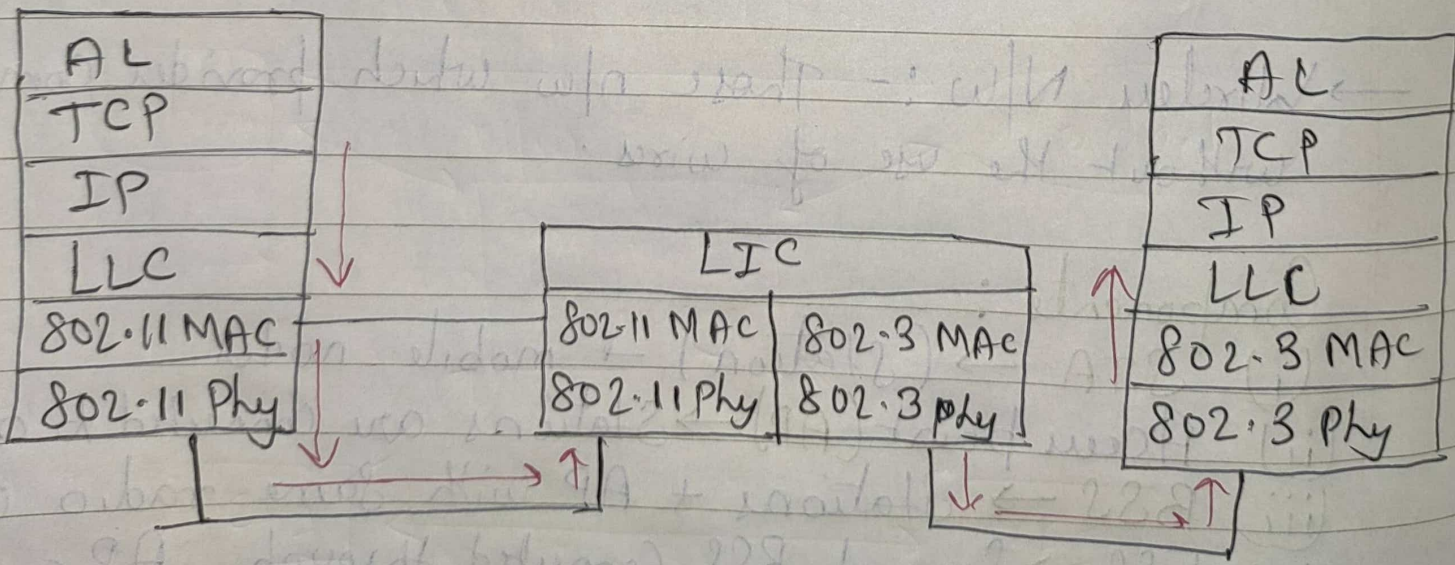


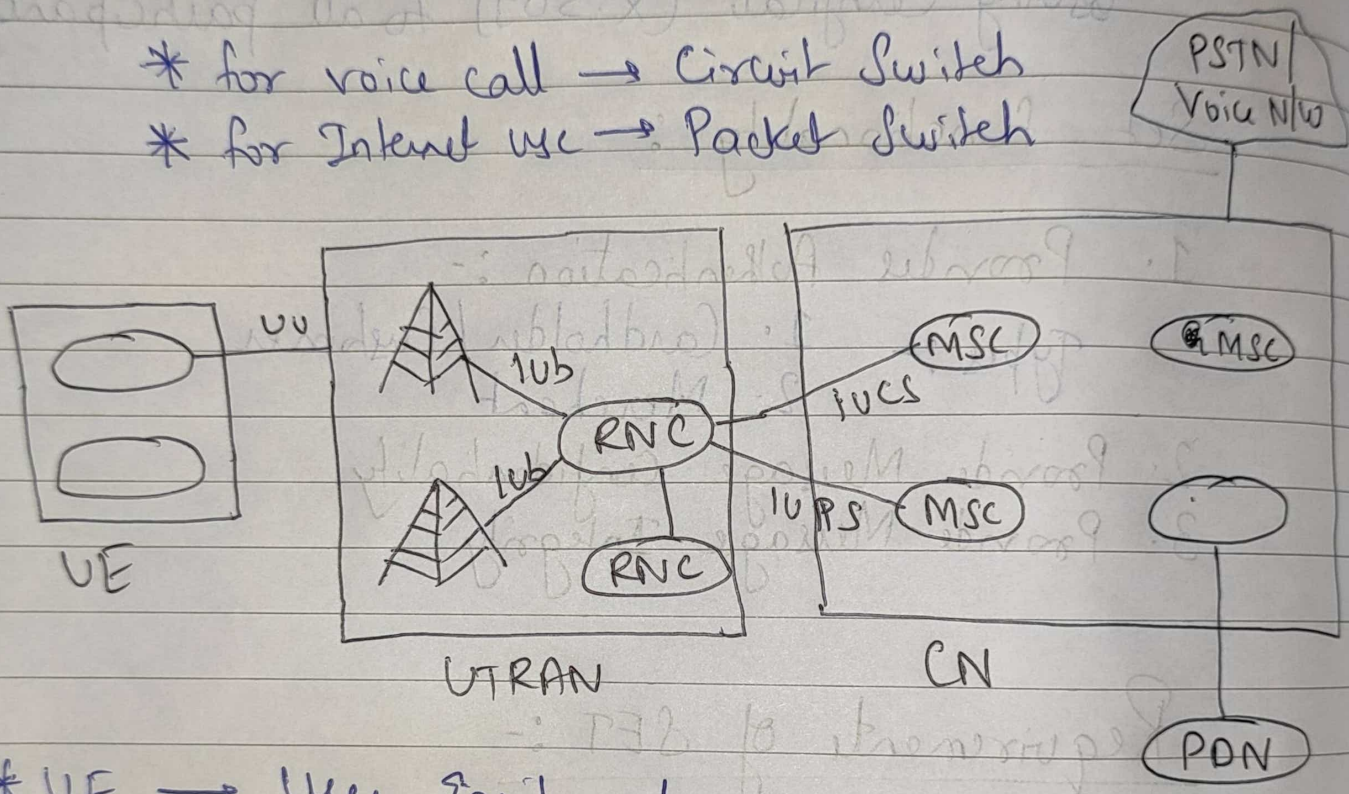
fig: IEE 802.11 Standard Architecture

UMTS :-

Universal Mobile Telecommunication System.

→ It is a 3rd gen broadband mobile cellular system based on GSM. It uses packet and circuit switch transmission.

* for voice call → Circuit Switch
* for Internet use → Packet Switch



* UE → User Equipment
* USIM → User Sim
* CN → Core N/W
* ME → Mobile Equipment
* RNC → Radio N/W Controller
* PSTN → Public Switch Telephonic N/W
* MSC → Mobile Switching Centre
* GMSC → Gateway MSC.
* SGSN → Service GPRS Support N/W
* PDN → Packet data N/W
* UTRAN → UMTS terrestrial radio acces N/W.
* GGSN → Gateway for GPRS Support N/W.