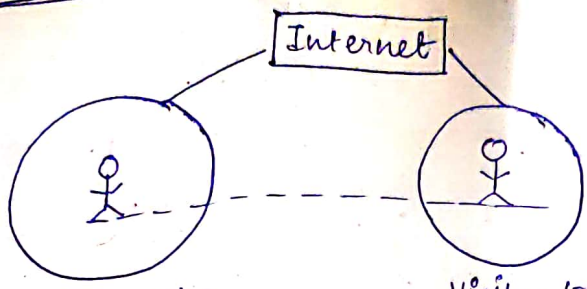
Mobile IP :



When a device moves from its home N/W to foreign N/W (i) normal IP routing cannot be used to send/receive data packets.

(ii) The active sessions in its home N/W gets closed which ~~is~~ is undesirable.

Soln : Mobile IP.

↳ Even if the device moves from one N/W to another, the IP address of the device remains the same i.e. IP address of the device is made permanent during that time the device is connected to the internet.

∴ No session is lost/terminated.

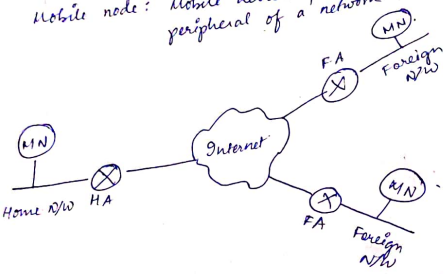
→ Components of mobile IP :

i) Home agent (HA)
ii) Mobile node (MN)
iii) Foreign agent (FA)

Agent ⇒ Router

Scanned by CamScanner

Home agent : Router connected to home network.
Foreign agent : " " " foreign "
Mobile node : Mobile devices present in the peripheral of a network.



Care-of-address
Current location of an MN which moved from its home N/w to a foreign N/w in the foreign N/w is the care-of-address of the MN.

→ Working of mobile IP :

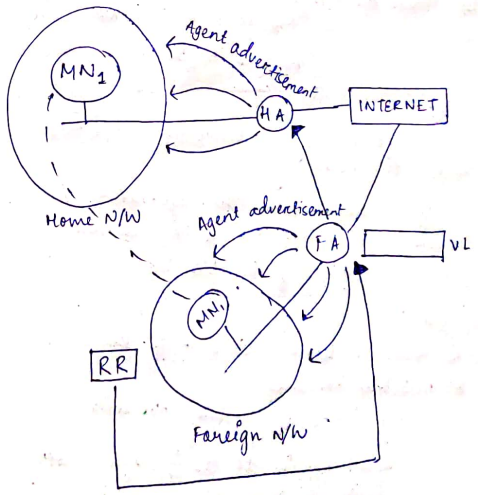
Phases involved in working of mobile IP :
i) Agent discovery
ii) Registration
iii) Tunneling

Agent discovery
When a mobile device is just added to a network, it does not know its home agent, so it needs to discover it.
Also, when a mobile device moves to a foreign network, it does not know its foreign agent which it needs to discover.

Registration
The current location (care of address (COA)) of a mobile which moved from its home N/w to a foreign N/w must be registered in both home N/w and foreign N/w.

Tunneling
- The home N/w creates a tunnel when a mobile device moves from home N/w to foreign N/w
- Tunnel is needed so that the active sessions of the mobile device should not terminate. The services must continue.
The data packets from home N/w must reach the mobile device in the foreign N/w.

(I) Agent Discovery :



Scanned by CamScanner

(II) Registration

* Wheren foreign agent advertises itself and the mobile node is now in the foreign N/W, then the mobile node understands that it has left its home N/W and has come to a foreign N/W

* The mobile node makes a "registration request" using its IP address, security key, information from foreign agent advertisement.

* MN keeps the registration request in its pending list and sends to the foreign agent.

* Foreign agent then validates the registration request
  - ↳ whether the MN is authenticated
  - ↳ " " " has come to this N/W before
  - ↳ " " " belonged to the foreign N/W

  etc.

  Then the foreign agent sends the registration request to home agent.

* Home Agent then confirms the registration of the mobile node i.e. both HA & FA now know the care-of-address (COA) of the MN.

Then HA

* a) creates a tunnel to COA of the MN.
  b) mobility binding
  ↳ association of mobile node with its COA.

* Then, home agent replies to the foreign agent that the MN of its N/W has come to the foreign N/W, so add the MN in the visitor's list of foreign N/W.

* Then the FA validates the reply (checks if the reply is from the same agent to which it had sent request for registration)

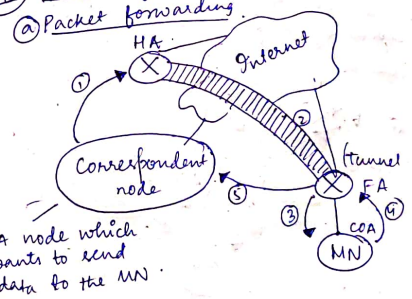
* After successful validation, the MN is added to the visitor's list of the foreign N/W.

* The reply is then sent to the MN from FA ~~and~~. (So, now the MN knows that its registration request has been successful)

Note: The mobile node must re-register itself before its registration lifetime finishes

(III) Tunneling:

(a) Packet forwarding



Currently, MN has moved from home N/W to foreign N/W and agent discovery & registration has been completed.

* Correspondant node sends the data packet to HA initially (as it does not know that MN has moved to a foreign N/W)

* Then, HA knows that the received packet is meant for MN.

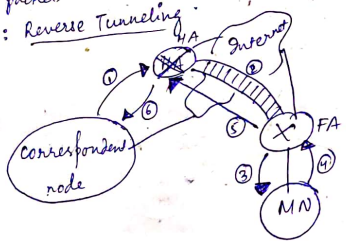
Scanned by CamScanner

* HA encapsulates all the data packets and sends to the FA via the tunnel. At the FA, the encapsulated packet is decapsulated and original data packets are retrieved and sent to MN.

* If MN needs to send data to correspondent node, the data packets to are sent to FA which directly sends the data to the correspondent node.

Problem:
The correspondent node expects a response from some N/W but gets packets from another N/W (not the one to which it sent the data packets)
So, many times, the correspondent node discards the packets received by it from other N/W.

Soln: Reverse Tunneling.



→ DHCP :

(Dynamic Host Configuration Protocol).

Need for DHCP

Assigning IP address to a huge no. of system manually is impractical.

∴ We configure the IP address of the system dynamically.

Working of DHCP

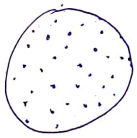
DHCP maintains a table which is of dual nature.
↓ some part is static
↘ rest is dynamic

MAC	IP
M_1	I_1
M_2	I_2

Static - Web servers, Email servers, file servers.

MAC	IP	Lease time
M_3	I_3	10 min
M_4	I_4	12 min
M_5	I_5	7 min

dynamic
↳ unless the host in a N/W has requested for an IP address, the host is not given an IP address.



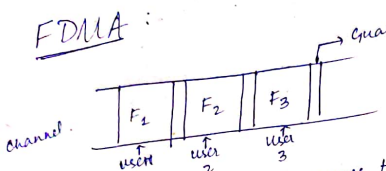
Pool of IP addresses

After the lease time expires, a renew request is sent by the S/W of the host internally. otherwise the IP is pulled out and added to the pool.

If renew request is not sent, possibilities are:
a) The host no more require IP address.
b) The host was idle in the lease time.

Scanned by CamScanner

FDMA :



Many users might want to access the channel at the same time.

↳ If all the users are given access to the channel in total, collisions might occur which is undesirable.

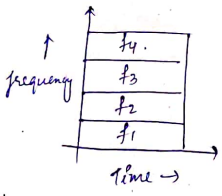
↳ Efficient method to allow multiple access i.e. more than one user can access the channel at the same time :

i) FDMA
ii) TDMA
iii) CDMA

FDMA

↳ channel is divided ~~into~~ based on frequencies
i.e. channel is divided into various frequencies.

* Guard bands are used to reduce interference between two frequencies in the channel



Disadv.

* There is still chance of cross-talk even though guard bands are used.

↳ Application : Satellite communication.

TDMA :

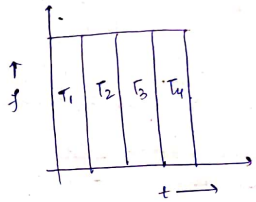
↳ Time slots
(each user is given a time slot)

↳ the users (stations) can transmit in the given time slot only. (interference is reduced greatly)

↳ Application : Radio systems.

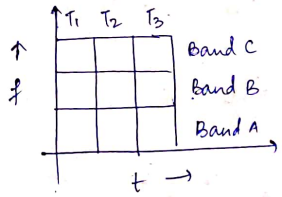
↳ Access to full length frequency of channel.

↳ No guardbank required for the wideband system



↳ Generally, the frequency in TDMA is divided into sub-bands.

↳ carrier frequency.

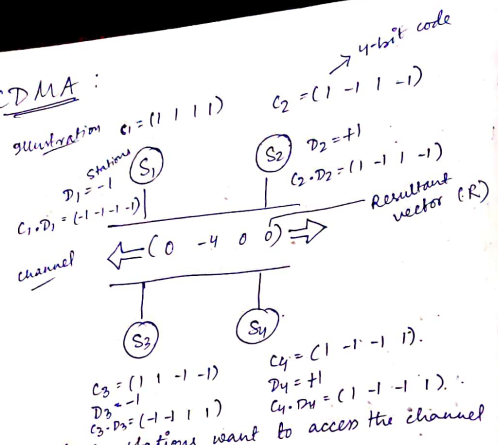


* Within T_1, first A will transmit, then B and then C.
(Usability is increased i.e. now the bandwidth is used by 3 stations which was earlier used by only one station)

efficiency ↑
performance ↑.

Scanned by CamScanner

CDMA :



The four stations want to access the channel.

* Each station is given a unique code.
* The codes are assigned based on 2 conditions which must be satisfied by every pair of code.

i) Multiplication of codes of two station must result in '0'. (corresponding terms → different)

$$C_1 \times C_2 = (1\ 1\ 1\ 1)(1\ -1\ 1\ -1)$$
$$= (1\ -1\ 1\ -1)$$
(sum of terms) $= 0$

ii) Multiplication of code of a station by itself must result in the total no. of station which ~~want to access the channel~~ are involved in the N/W.

$$C_4 \times C_4 = (1\ 1\ 1\ 1)(1\ 1\ 1\ 1)$$
$$= (1\ 1\ 1\ 1)$$
$$= 4.$$

D : Data bit that is sent
D. ↳ 0 (-1)
↳ 1 (+1)

S_i wants to send D_i. $(1 \le i \le 4)$.
So, the code which is sent over the channel is
$C_1 \cdot D_1 + C_2 \cdot D_2 + C_3 \cdot D_3 + C_4 \cdot D_4$ (Encoding)
$= (-1\ -1\ -1\ -1) + (1\ -1\ 1\ -1) + (-1\ -1\ 1\ 1)$
(odd corresponding terms) $+ (1\ -1\ -1\ 1)$
$= (0\ -4\ 0\ 0)$

Decoding

R_i wants to receive data sent by S_i.

$$R_1 = (C_1 \cdot R) / \text{no. of stations}$$
$$= ((1\ 1\ 1\ 1) \cdot (0\ -4\ 0\ 0))/4$$
$$= -4/4 = -1.$$

$$R_2 = (1\ -1\ 1\ -1) \cdot (0\ -4\ 0\ 0)/4$$
$$= 4/4 = 1$$

$$R_3 = (1\ 1\ -1\ -1) \cdot (0\ -4\ 0\ 0)/4$$
$$= -4/4 = -1.$$

$$R_4 = (1\ -1\ -1\ 1) \cdot (0\ -4\ 0\ 0)$$
$$= 4/4 = 1.$$

Scanned by CamScanner