* TDMA

→ different frequencies at same time

→ different frequencies separated by time division.

- This pattern is called Fixed TDMA

→ Fixed TDM.

- Time slots were divided.
- The sender will send data in a particular time slot, at the time receiver will receive at the same time slot.

- Again MAC will helps in dividing the time slot

total pattern will repeated after 10ms.

each time slot - 417 μs.

uplink - 2nd 12 slots.

downlink 1st 12 slots.

- disadvantages:

- If no data is not sent, though time slot is provided then there is a waste of Bandwidth, & Frequency.

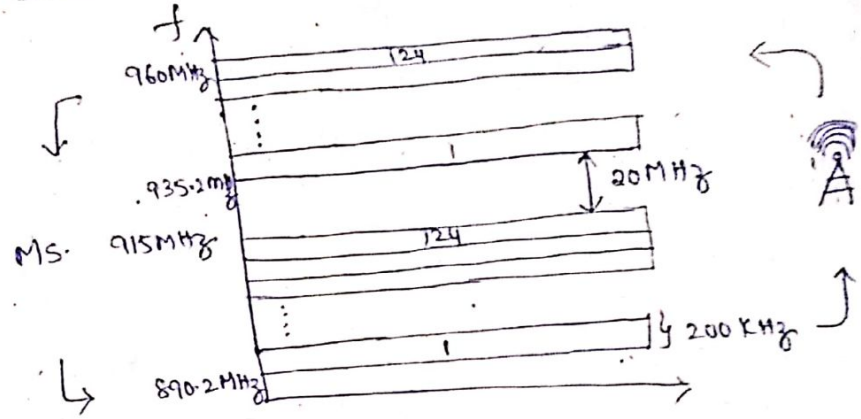
- while accessing some data, if it exceeds the division ti, it has to wait till the next division comes to the station

Scanned by CamScanner

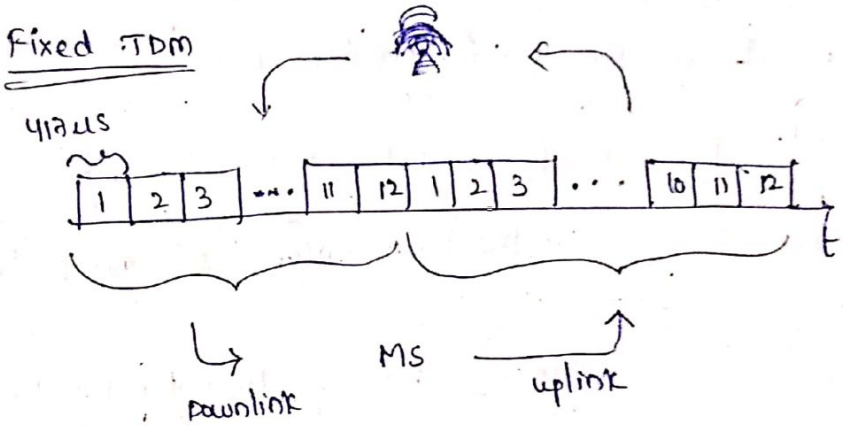
classical Aloha

- ~~Pure~~ Aloha
- slotted Aloha

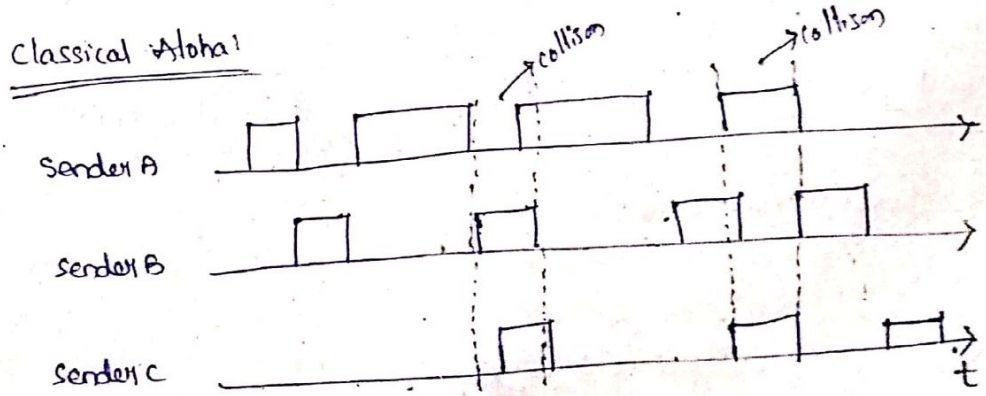
FDMA



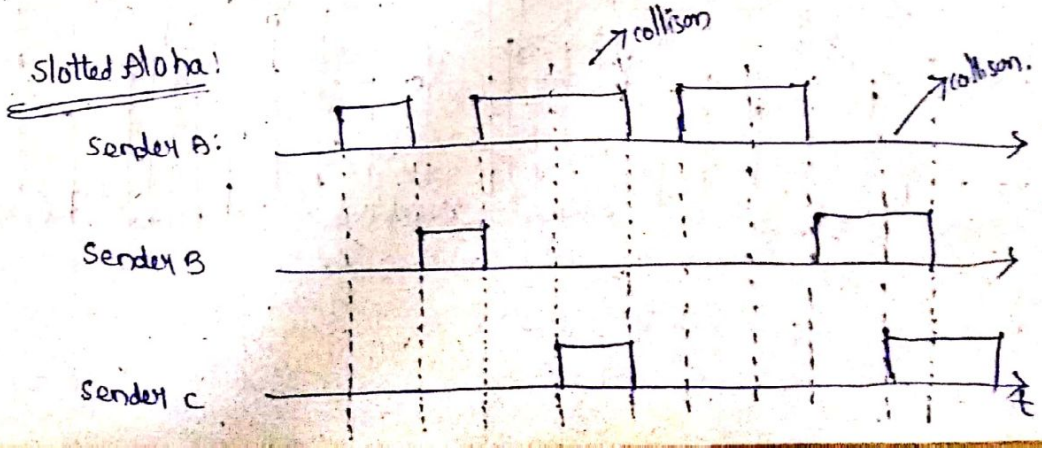
Fixed TDM



Classical Aloha!



Slotted Aloha!

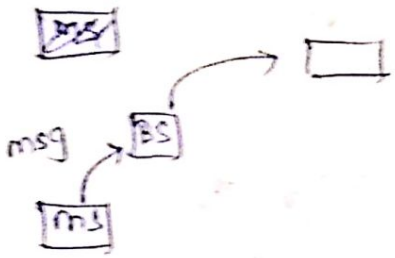


Scanned by CamScanner

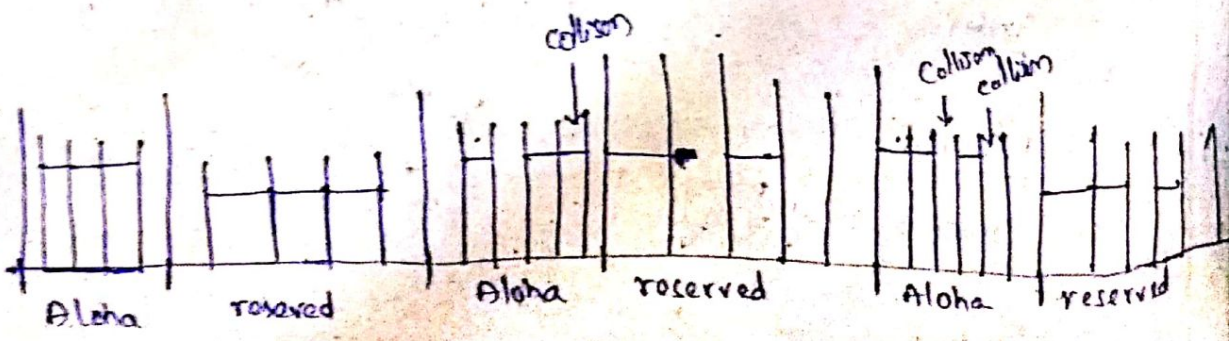
27/08/15

DAMA : Demand Assigned multiple access.

→ The station who ever want to send data, it will demand for collison free transmission



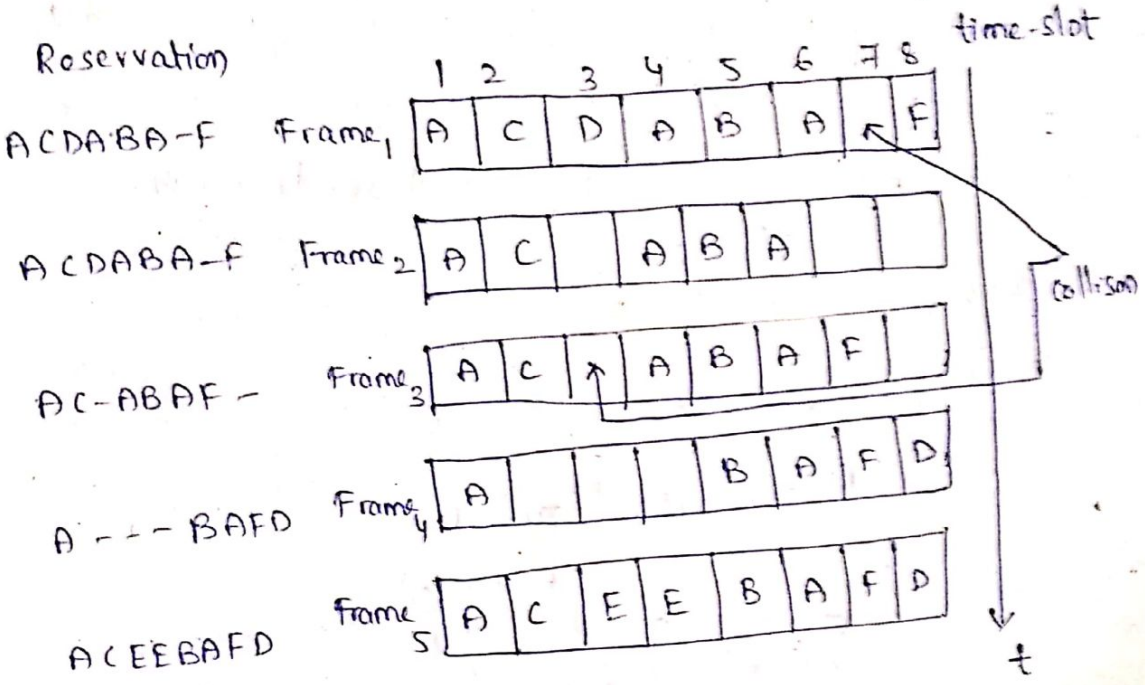
- It reserve time.
- at time of reservation collisions may take place
- but during transmission no collison takes place
- After reservation, satellite control will send back a list to all the base stations, all the base stations will accept the list
- If collision occurs during any time slot; then it will not be allocated to any station.
- This is called "Explicit Reservation" it is also called as "Reservation Aloha"



Scanned by CamScanner

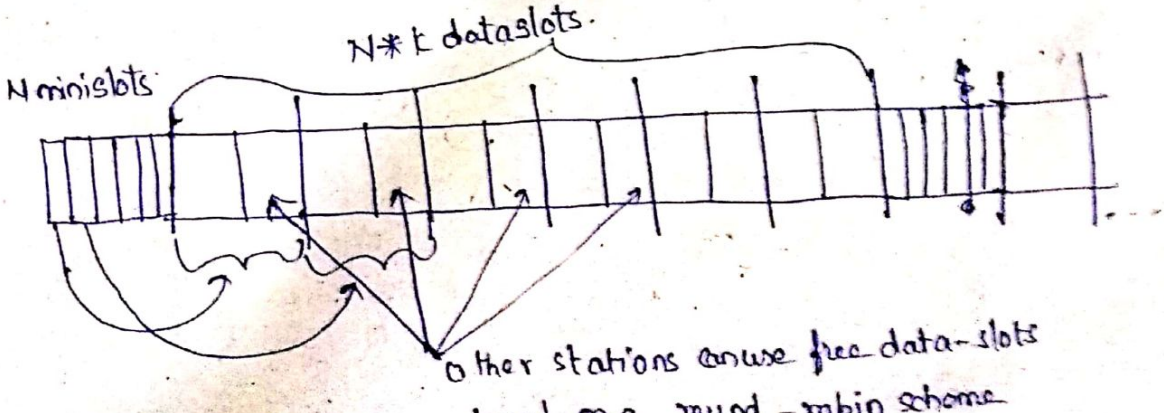
PRMA: Packet Reservation multiple Access

- In this a single time slots will form a frame.
- here also reservation takes place
- According to message size, future slots are also be reserved.
- The request to satellite → short request



Reservation TDMA:

- 6 slots will become 1 Frame,
- each time slot divided into two
- here unused mini slots be given to other stations.



Eg: N=6, k=2.

Scanned by CamScanner

multiple access with Collision Avoidance (MACA):

- It is a simple technique which avoid collison without use of TDMA / FDMA / CDMA etc.

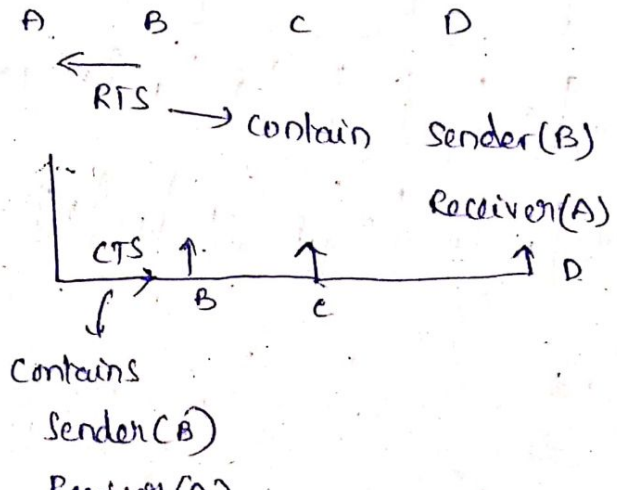
→ RTS - Request to send.

→ CTS - clear to send

which station receives RTS, then only those stations are allowed to send.

- This helps to avoid collisons in hidden terminals.

- En Exposed terminal.



29/08/19

Scanned by CamScanner

23/08/23

Mobile IP

→ Mobile internet protocol

Goals:

- until there is a link layer connection to mobile Ip.
  It should provide dissconnection less data transfer.

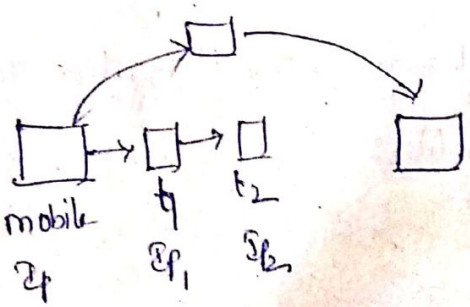
Prefix 244.13.12/24 → physical subnet of server

- Assumptions

  * DHCP - Dynamic host configuration protocol.
  - If any device moving from one place to another, in order to get connected, allocate different mobile Ip by using DHCP.
  - problem here → mobile there is a lot of mobile Ip.

* - DNS is used here, which will store all Ip addresses and routing table

  problem DNS takes some time to update the routing table



* Tcp - Transmission control protocol

  Tcp will transwer, data, but when Ip address changes, Tcp connection get disconnection.

Scanned by CamScanner

Tcp - send based on socket pair.

(source, port).

↵

→ Ip changing also gives packet losing,

when Ip is changed then Routing doesn't know where to route, it sometimes drop so, data lost.

Requirements of new mobile Ip:

Assignment (1)

- Compatability
- Transparency
- Efficiency / scalability
- Security

Compatability: It should integrate with the previously designed services.

- They haven't changed the connectivity
- It enhanced the efficiency of Routers, Switches without changing h/w (or) s/w.

Transparency: Internal transfer of data / Routing is not known to the end users. [no transparency] here.

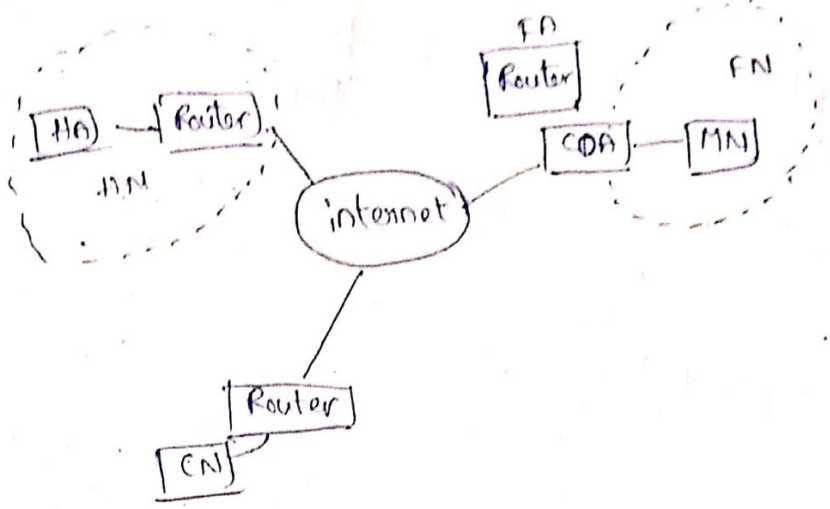
Security: Security will be given by Encryption & decryption by the end-routers

Scanned by CamScanner

3/09/19

Entities & Terminology:

- mobile node (MN)



Foreign Agent

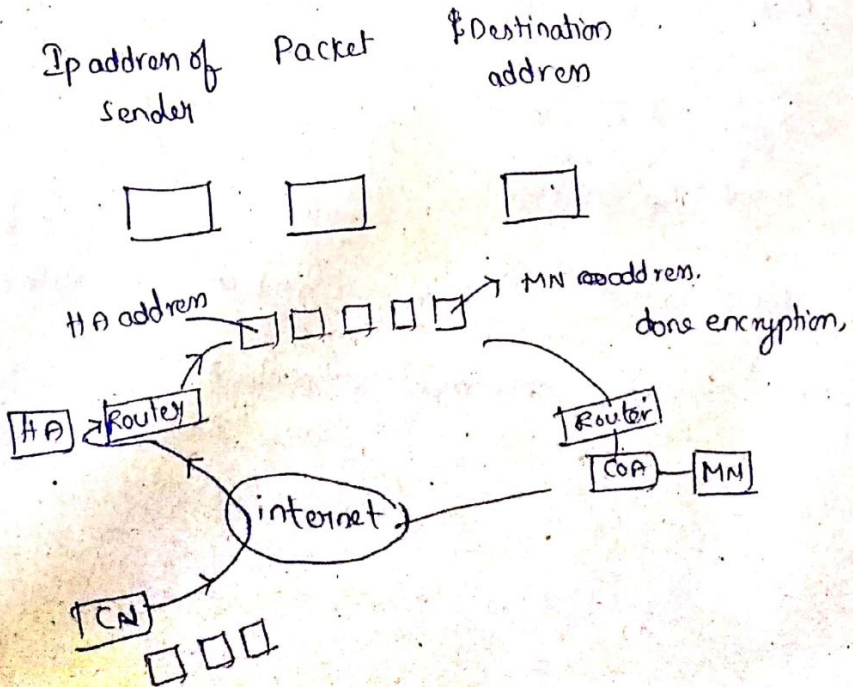
CoA - c/o address.

without passing through CoA, no packet will reach and get out from MN

→ 2 types

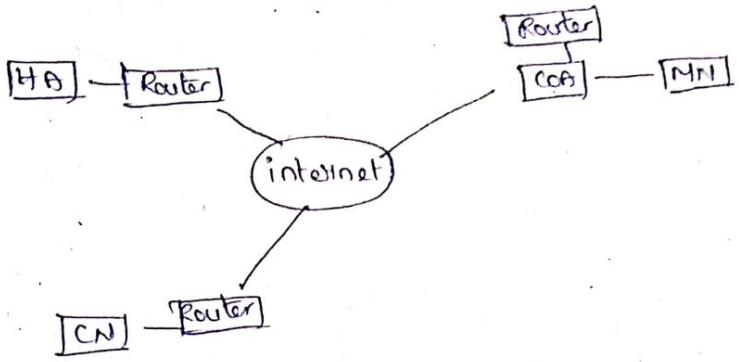
- foreign agent CoA
- co-located CoA

- correspondent-node (CN)



Scanned by CamScanner

- Foreign agent CoA
- co-located agent CoA



Foreign agent CoA → CN to HA
HA to MN

co-located agent CoA → CN to internet
internet to MN using
DHCP & DNS
- without getting enter into CoA

Agent discovery:

MN goes from H

- Agent solicitation
- Agent Advertisement

All HA & FA advertise themselves and make advertise

ICmp - internet control message protocol

type - 9

code - m

checksum

address

lifti

Rou

Pre

mobile

type

length

Sequ

Scanned by CamScanner

type - 9 default

code - may be 0 or 16 if 0 mobile to other
16 - mobile to mobile

checksum — 16th bit 1's complement

address - all the original address of the mobile nodes

lifetime - advertising life time
- how much longer it has to be displayed

Router address

preference level.

mobile extension.

type = 16 default

length - can be anything

Sequence number : How many advertisements has done,

- How much time the mobile node is present in that current location

R - set ⇒ Though having temporary IP, still have to register with CN

B - If HA(B) F-n, have mobile no of MN, It is saying I am busy, so don't come int my n/w.

H - mobile node is in H location

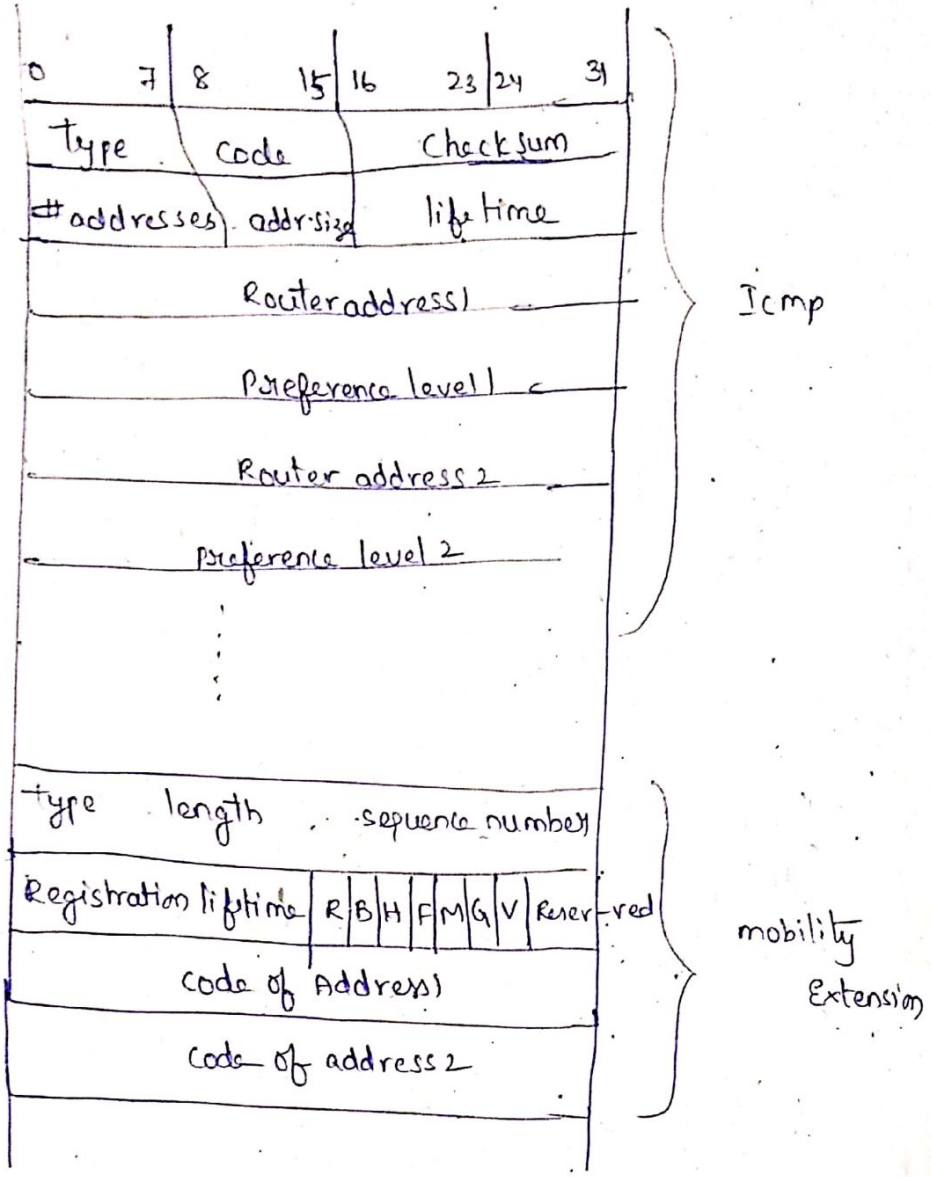
F - mobile node is in the Foreign location

m - It is performing routing

G = generic routing algorithm

V = 0

Scanned by CamScanner

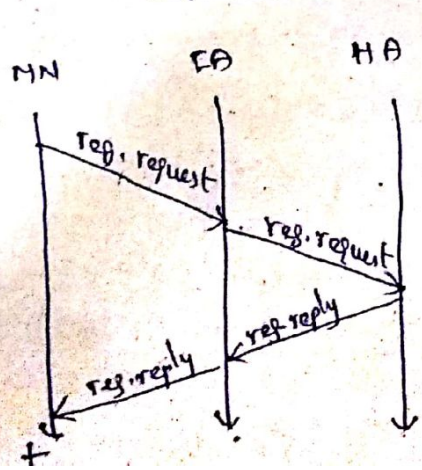


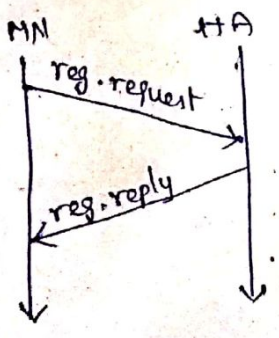
Type - set to 9

code - 0 if agent routes traffic from non-mobile nodes as well & else 16.

11/9/19

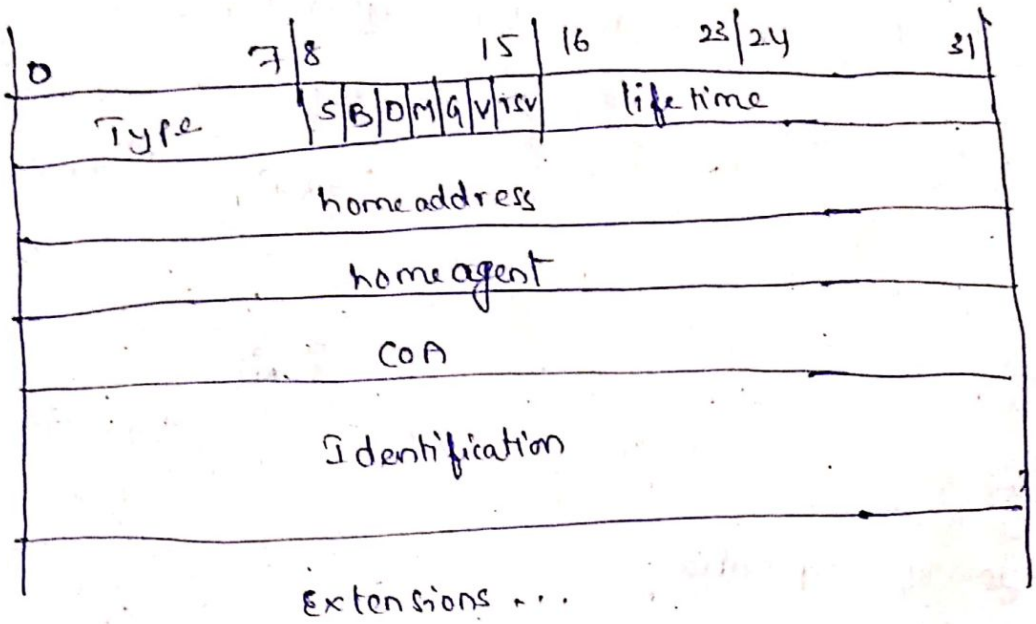
Registration





Scanned by CamScanner

mobile Ip registration request



UDP packet on port 3434

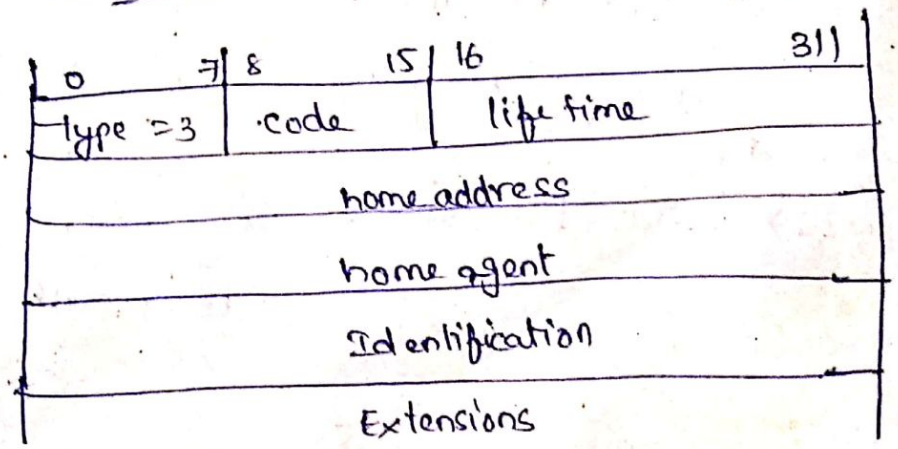
type=1 for regi., request

S = retain prior mobility bindings

B : forward broadcast packets

D : co-located ~~CoA~~ address ⇒ MN decapsulates packets.

mobile Ip registration reply



Registration successful

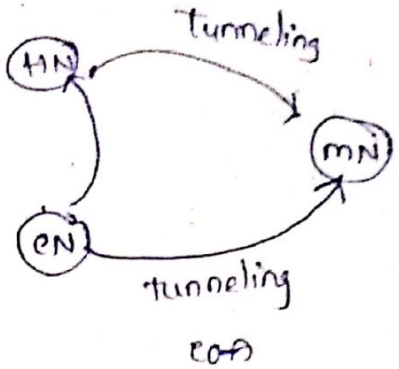
0 - registration accepted

1 -

Scanned by CamScanner

Tunneling & Encapsulation

- where encapsulation starts called tunnel
- through tunnel packet moves from



Types of encapsulation

- IP-in-IP encapsulation
- minimal encapsulation
- Generic Routing Encapsulation (GRP)

- cache invalidation
  - Time based invalidation.
  - command based invalidation
  - Dynacache API and CACHEIVL table invalidation
  - Group based invalidation.

Assignment →

→ <timeout> value </timeout> value may be anything in seconds

< inactivity > value < inactivity>

→ through commands

→

Power aware Computing

- based on the switches & Routers power consumption is measured.
- goal is to conserve the power

- two types of
  - unicast (1 to 1)
  - multicast (1 to many)

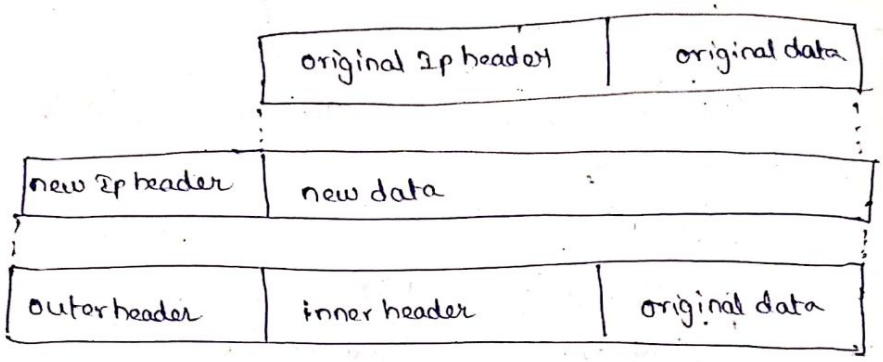
- 5 Routing metrics
  - Energy consumed by one packet
  - Time for n/w partition
  - variance in power level across mobiles
  - cost for one packet
  - maximum mobile cost

- Power aware computing methods
  - Data caching : data is cached at mobile device
  - cache invalidation mechanism : remove old data
  - Normalization of records :

    Before sending data, it should be normalized as Ex puplicate records should be suppressed and not trans

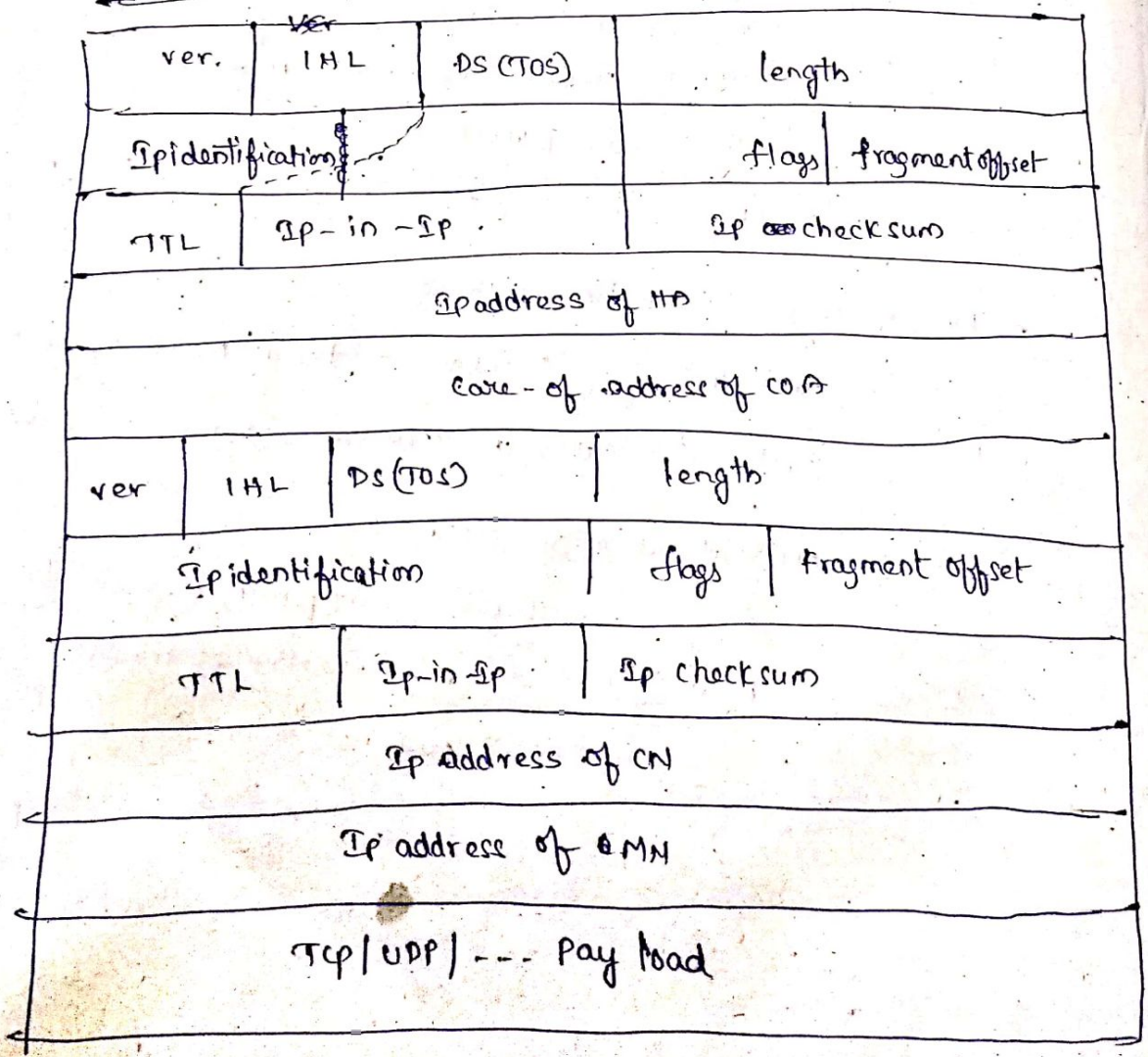
Scanned by CamScanner

Encapsulation



Encapsulation methods

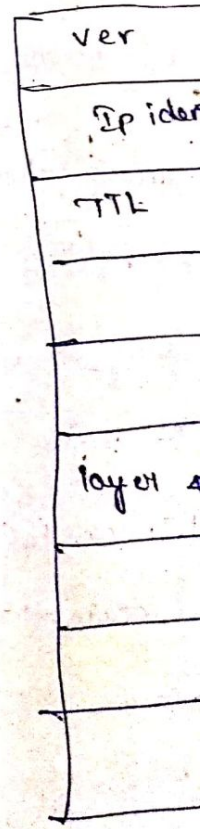
Ip-in-Ip encapsulation packet format



Ip-in-Ip encap

- ver – Ip
- IHL – inter
- TOS – ty
- Length –
- Ip id,
- TTL
- Ip-in

- Minimal

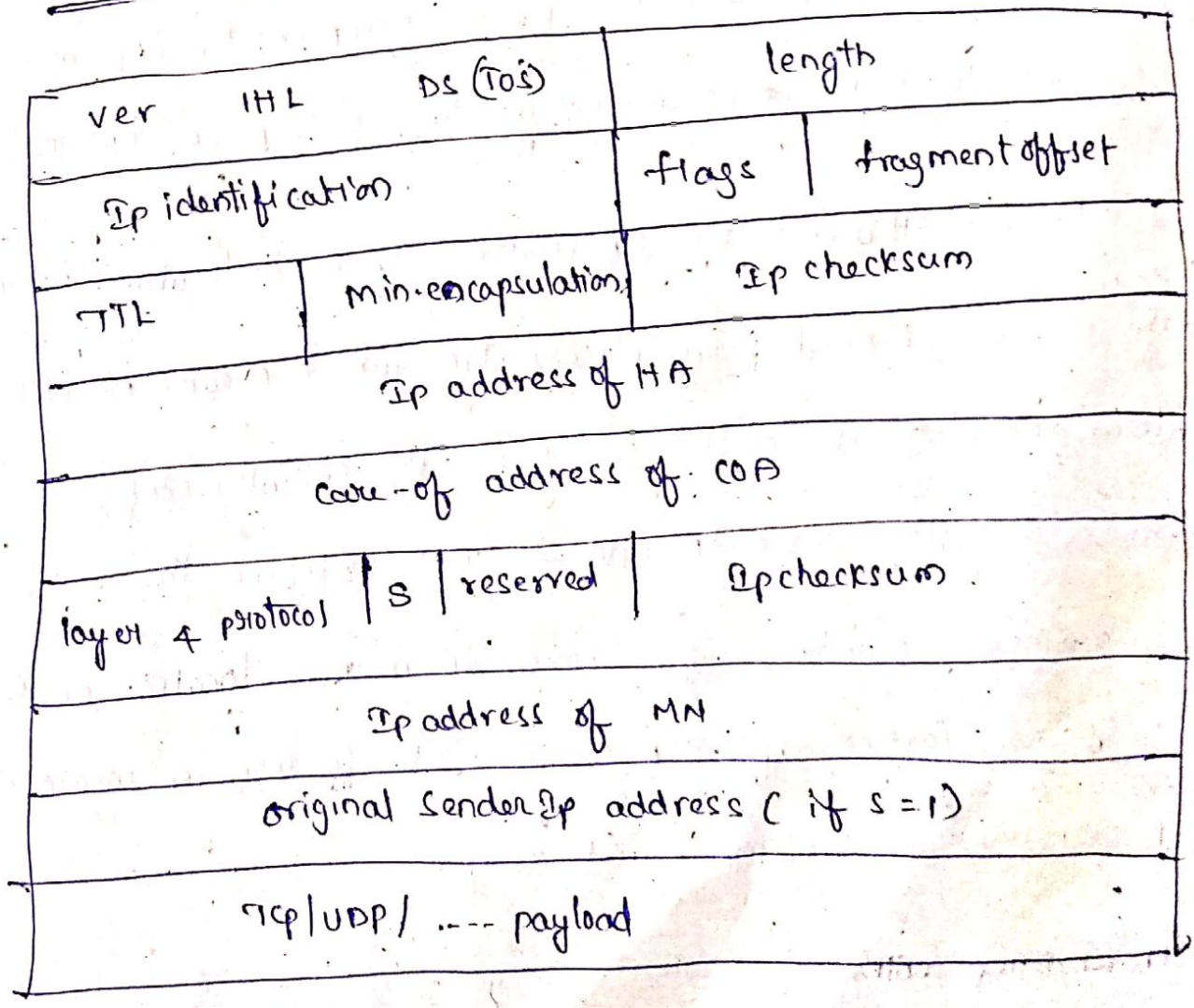


Scanned by CamScanner

Ip-in-Ip encapsulation

- ver - Ip protocol version no.
- IHL - internet header length
- TOS - type of services (copied from inner header)
- Length - complete encapsulated packet length
- Ip id, flags, flag offset - used for fragments
- TTL - time to live
- Ip-in-Ip upper layer protocol

Minimal Routing Encapsulation



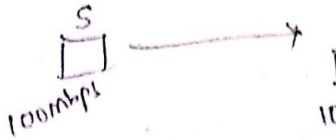
Scanned by CamScanner

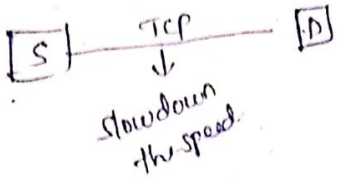
1-1-2013

Traditional TCP

- congestion - due to congestion, the packet may drop

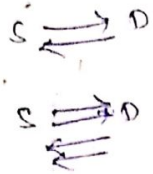
speed of i/p link > speed of o/p link





- If congestion is seen - it will start slow start mechanism
- Udp - is not reliable, may drop packet in b/n the transmission.
- congestion window increases by doubling the previous value
  - the growth is Exponentially.

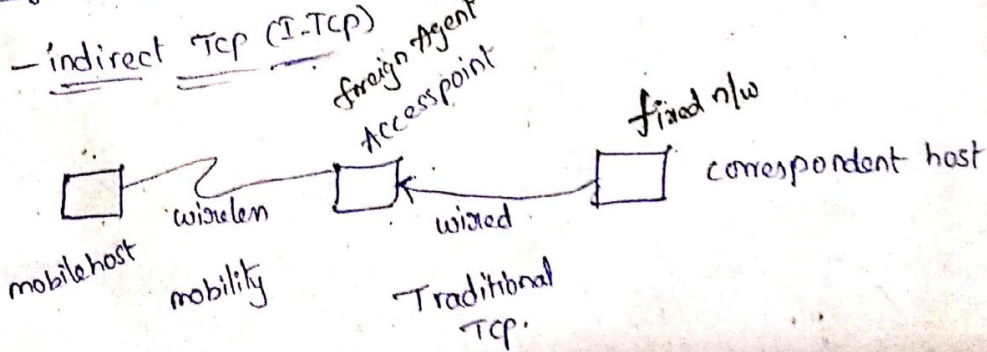
congestion window = 1 2 4 ....



when the value reaches the congestion threshold, then it will show learn relation/linear growth.

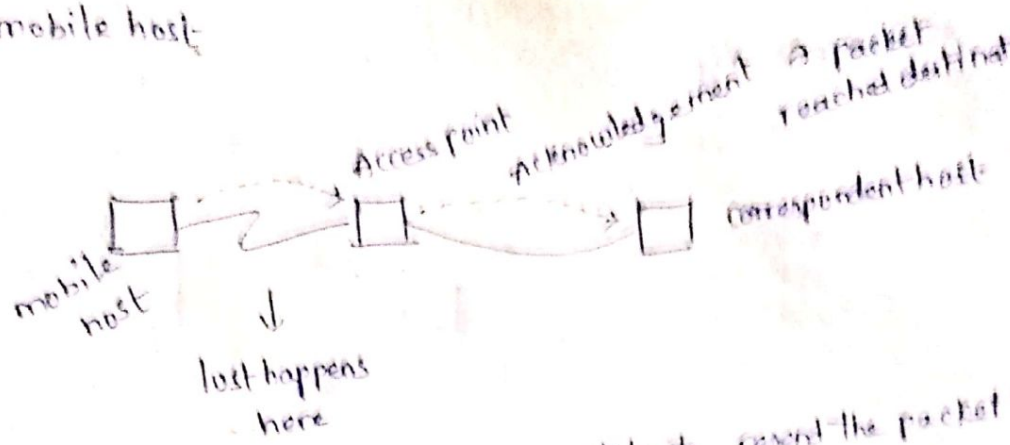
Changes to Traditional TCP / improvements to TCP.

- indirect TCP (I-TCP)



Scanned by CamScanner

the mobile host



- then Access point takes responcibility to resent the packet to the mobile host from buffer.

→ from mobile host to correspondent host, if packet lost, then mobile host takes responsibility to resend

Advantages :-

- Indirect TCP doesn't require any changes in TCP.
- Segmentation & transmission errors will not disturb each other.
- Testings can be preformed in original standard TCP
- shoit Round trip time and easy receiving.

Disadvantage

- Loss of end to end semantics of TCP
- Handovers may create mobe problems if it takes a while to register to the new location
- Foreign agent must be a trusted entity because the TCP connection ends at this point and it has to be integrated into all security mechanisms.

Scanned by CamScanner

- Snoping TCP

Advantages:

- End to End semantics is maintained here
- No improvements & enhancements are needed to the correspon -dent host
- Packet is buffered to new location of another foreign agent, if handover is performed at mobile host
- It doesn't matter if the next foreign agent uses the same enhancement or not

Disadvantages:

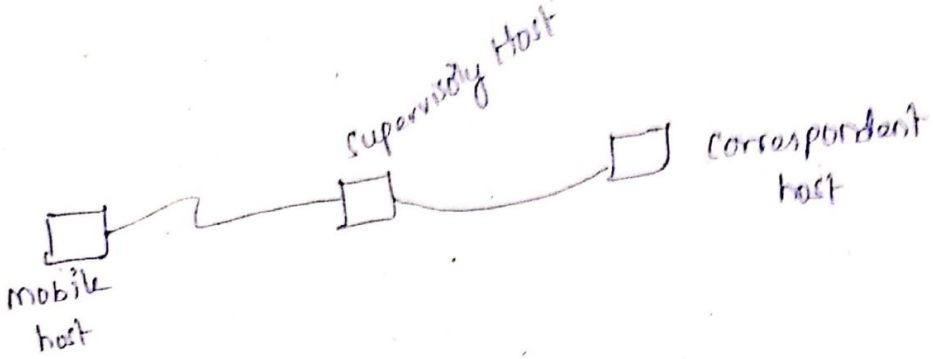
- The problems of the wireless link are now visible for the correspon CH as it is not fully isolated from the original standard TCP.

Scanned by CamScanner

- Using -ve & duplicate acknowledgement between FH & MH requires additional mechanisms on the MH

- Using Ip encapsulation security snooping on the sequence numbers will no longer work because many security schemes prevents replay attack

- Mobile TCP (M-TCP)



SH - request | forces the correspondent node (sender) to set the window size = 0 with help of TCP. It will go to Persistant mode. (when MH doesn't get connected to 'internet)

Advantages:

- It maintains the TCP end-to end semantics
- The SH doesn't send any acknowledge by it self, but forwards the acknowledgement from the MH
- If MH gets disconnected it avoids useless retransmiss -ons & slow start breating the connection.

Scanned by CamScanner

Disadvantages

- SH doesn't acts as proxy as in Indirect TCP so Packet loss on the wireless link is propagated to the sender
- A modified TCP on the wireless link not only requires modifications but also a new n/w element like Bandwidth manager

Scanned by CamScanner