Assignment-2: Mobile IP

1. Show the delivery of an IP packet (P) to a mobile node (MN) from a corresponding node (CN). Assume mobile node is in foreign network and registered.
Consider IP addresses as:
CN---200.1.1.5/24,
HA---200.2.1.6/24,
FA---200.3.1.7/24,
MN old IP 200.2.1.10/24 and
MN gets care of address 200.3.1.7/24. Hardware address of FA = H-FA, HA = H-HA and of MN = H-MN. You are also required to show table entries done at HA and at FA during the registration process when MN has moved from the home network to the foreign network. If CN is in 200.2.1.0/24 network with an address 200.2.1.100/24, then how packet P will be send to MN from CN.
Ans.

Registration

- FA advertises service
- MN requests registration
- FA relays request to HN and assigns CoA
- HN accepts request and replies acceptance
- FA relays reply to MN
- Table entries
    - HA

DestIP	SubnetMask	NextHop	Interface
200.2.1.10	255.255.255.0	200.3.1.7 (FA)	H-HA

    - FA

DestIP	SubnetMask	NextHop	Interface
200.3.1.7 (CoA)	255.255.255.0	Direct	H-FA

Packet from CN to MN

- CN sends packet with DestIP – 200.2.1.10 (IP-MN) to HN
- HN encapsulates packet with DestIP – 200.3.1.7 (IP-CoA) to FA
- FA unwraps the packet and forwards the internal packet with DestIP – 200.2.1.10 (IP-MN) & DestMAC – H-MN

Packet from CN to MN if CN is in same subnet as HN

- Same routing
- Triangle routing mention

2. If H.A address is 205.50.40.3 and F.A address is 208.80.70.4 show how IP-in-IP encapsulation/de-capsulation will take place for a packet with S.A 196.6.5.3 and D.A as 205.50.40.6.
Ans.
CN (Source) sends packet to HN

- S.A. 196.6.5.3
- D.A 205.50.40.6

HN encapsulates packet in another packet with

- S.A. 205.50.40.3
- D.A. 208.80.70.4 (Assuming F.A = CoA)
    - S.A. 196.6.5.3
    - D.A 205.50.40.6

FN decapsulates packet and forwards packet with

- S.A. 208.80.70.4
- D.A. 205.50.40.6

3. How route is optimized for problem no.1 and show delivery of the packet on this optimized route.

Ans.
Direct Routing

- CN requests CoA of MN from HN
- HN replies with the CoA
- CN directly sends packet to FA
- FA forwards packet to MN

4. How two mobile nodes can use the same COA in mobile IP?
Ans.
In Mobile IP (Internet Protocol), a Care-of Address (CoA) is an IP address temporarily assigned to a mobile node (MN) while it is away from its home network. The CoA allows the MN to continue communicating with other nodes on the internet even when it is not within its home network's reach. It's important to note that the CoA is assigned by the foreign network where the MN is currently located.
When two mobile nodes (MNs) are in the same foreign network and need to use the same CoA, it typically means they are both visiting the same location and are behind the same Network Address Translator (NAT) or firewall in that foreign network. Here's how they can share the same CoA:

1. **Assignment by the Foreign Network:** The CoA is assigned by the foreign network's NAT or firewall. When MNs connect to this network, they receive an IP address from the foreign network's address pool. If two MNs are behind the same NAT or firewall, they can both be assigned the same CoA.
2. **NAT and Port Mapping:** To distinguish traffic from different MNs sharing the same CoA, the NAT or firewall performs Network Address Translation along with port mapping. Each MN can use different source port numbers when communicating with external hosts. The NAT keeps track of which internal MN is associated with which port number and routes incoming packets to the correct MN based on the port number.
3. **UDP and TCP Ports:** In most cases, this port mapping is applied to UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) traffic, which are the two main transport layer protocols. Since the combination of source IP, source port, destination IP, and destination port uniquely identifies a communication session, the NAT can ensure that traffic is correctly directed to the respective MNs.
4. **CoA Remains the Same:** While the two MNs may have different internal IP addresses (private IP addresses within the foreign network), they both share the same CoA (the external IP address). The foreign network's NAT or firewall maintains a mapping table to keep track of which internal MN corresponds to which external CoA.
5. **Bi-Directional Communication:** Both MNs can communicate with external hosts using the same CoA, and the NAT or firewall ensures that incoming packets addressed to the CoA are correctly forwarded to the appropriate MN based on the port mapping.

It's important to note that while multiple MNs can share the same CoA when they are behind the same NAT or firewall in a foreign network, each MN will still have its own unique Home Address (HoA) associated with its home network. The CoA is only used temporarily while the MN is visiting a foreign network, and it allows the MN to maintain connectivity even when it changes its physical location.

5. In what conditions home agent intercepts the ARP packet destined for mobile host. Explain proxy ARP in mobile IP. Explain the usage of gratuitous ARP too.
Ans.
When the Home agent gets ARP request to know the MAC of MN which is already shifted and registered on a Foreign node, to prevent unnecessary broadcasts the home agent acts like a proxy and sends a proxy ARP reply to the CN with the MAC of Home agent itself acting like a proxy.

Proxy ARP in Mobile IP:
Proxy ARP in Mobile IP is the mechanism where the Home Agent responds to ARP requests for the mobile host's IP address with its own MAC address. It acts as a proxy, allowing devices in the foreign network to communicate with the MH even though it's not physically present in that network. This enables seamless mobility for the MH as it moves between networks.

Gratuitous ARP is a technique used in networking where a device sends an ARP request for its own IP address. In the context of Mobile IP, Gratuitous ARP can serve several purposes:

- **Updating ARP Caches:** When a mobile host changes its care-of address (CoA) due to movement to a new foreign network, it can send a Gratuitous ARP with its new CoA. This helps update the ARP caches of devices in its vicinity so that they know the MH's new location without waiting for an ARP request.
- **Address Validation:** Gratuitous ARP can also be used as a form of address validation. When a device sends a Gratuitous ARP, it announces its presence and IP address to the network. If another device responds to that ARP request claiming the same IP address, it can indicate a potential IP address conflict.

In the context of Mobile IP, Gratuitous ARP can help mobile hosts maintain connectivity by proactively updating the network about their new location (CoA) and ensuring that devices in the foreign network are aware of the change.

6. "IP address change required by network layer during mobility creates problem for TCP" Discuss.

Ans.

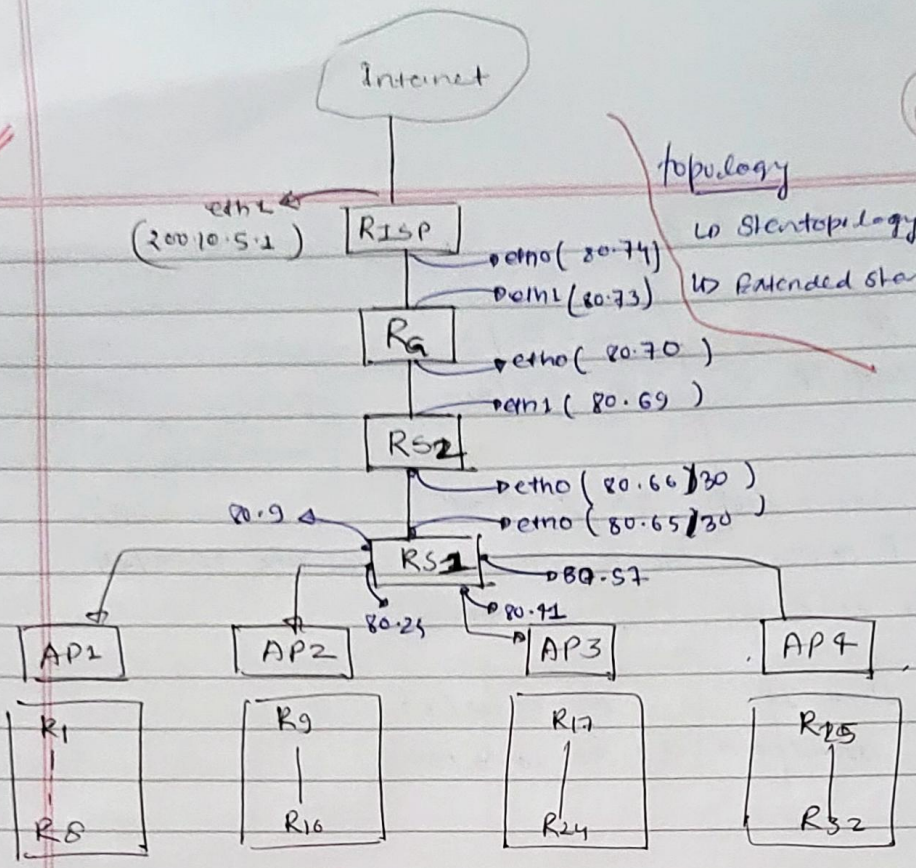
When a mobile device moves from one network to another, such as from its home network to a foreign network, it may be assigned a different IP address due to network layer mobility management protocols like Mobile IP or Dual-Stack Mobile IPv6. This IP address change can introduce challenges for TCP (Transmission Control Protocol) connections, which rely on stable endpoint addresses to maintain their stateful connections. Here are the key issues and challenges that arise when IP addresses change during mobility:

1. **Connection Disruption:** When a mobile device changes its IP address during handover between networks, any existing TCP connections using the previous IP address may be disrupted. This interruption in connectivity can lead to packet loss and temporarily interrupted data transfers.
2. **Session State Invalidation:** TCP connections rely on a set of parameters that include the source and destination IP addresses and port numbers. Changing the IP address of one endpoint invalidates the session state associated with that IP address. As a result, any stateful information related to the connection at the previous IP address must be discarded or updated to reflect the new IP address. This can be particularly problematic for long-lived connections or applications that require low-latency communication.
3. **TCP Timeout and Retransmissions:** When a TCP connection is disrupted due to an IP address change, it can lead to timeout events and retransmissions of unacknowledged packets. These retransmissions can consume network resources and may lead to inefficient use of the network.
4. **Route Optimization:** Some mobility management protocols, like Mobile IP, employ techniques such as route optimization to minimize the impact of IP address changes. However, these techniques can introduce additional complexity and may not be universally supported in all networks.
5. **NAT Traversal:** In some scenarios, network address translation (NAT) may be involved in changing the device's IP address. NAT can complicate the handling of TCP connections, especially if the NAT binding information is not properly updated or if the NAT devices have limited state management capabilities.
6. **Application-Level Adaptations:** To mitigate the impact of IP address changes on TCP, applications may need to be designed to handle such changes gracefully. Techniques like connection pooling, session persistence, and the use of higher-layer protocols like SCTP (Stream Control Transmission Protocol) that are more mobile-friendly can be employed.
7. **Recovery Time:** The time required for a TCP connection to recover from an IP address change can vary based on network conditions, the mobility management protocol in use, and the application's ability to adapt. This recovery time can be a significant factor for real-time or interactive applications.

In summary, the change of IP addresses required by the network layer during mobility can create problems for TCP connections, primarily due to the disruption of established connections and the need to update or recreate session state. To address these challenges, mobility management protocols and application-level adaptations are used to minimize the impact of IP address changes and maintain the continuity of communication during mobile device handovers.

Ques 1

(1)



topology

→ Star topology within wings

→ Extended star for APs.

IP address Block = 202.141.80.0/24

Each AP ~~repe~~ connects to one wing & each wing has 8 rooms which require one wifi connection.

So total 8 connection Required.

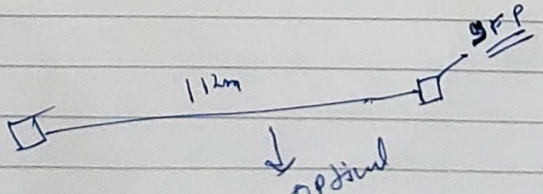
total 10 address necessary.

we allocate 16 address to each wing : /28 mask.

wing 1 (AP1)	202.141.80.0/28	.80.15/28
wing 2 (AP2)	.80.16/28	.80.31/28
wing 3 (AP3)	.80.32/28	.80.47/28
wing 4 (AP4)	.80.48/28	.80.63/28

<100m, UTP Port

>1km SFP.



For link b/w RS2 & RS1
assign 4 addresses — /30 mask.

.80.64/30 — .80.67/30

For link b/w RS2 & RG — /30 mask ⇒ 4 address

.80.68/30 — .80.71/30

for link b/w RG & RISP
~~Let address block 202.142.100.0~~
~~4 address required.~~
4 address Required /30 mask
.80.72/30 — .80.75/30

Channels of APs

→ Non-overlapping channels should be assigned.
wing 1 (AP1) ⇒ channel 1
wing 2 (AP2) ⇒ channel 6
wing 3 (AP3) ⇒ channel 11
wing 4 (AP4) ⇒ channel 2

Cable type

→ each AP will connecting to Nodes via WiFi.
→ we will use. Cat5e or Cat 6 cabling for connecting b/w APs & wing switches
→ b/w wings RS & RS2 ⇒ optical fibre cable.

Switch & Port types

Switch & port types

Wing Switch ⇒ PoE switches with enough ports to connect APs
~~Gigabit Ethernet.~~

Central wing Switch ⇒

IP address of Room.

R_1	·80·1|28	R_9	·80·17|28
R_2	·2	R_{10}	·18
R_3	·3	R_{11}	·19
R_4	·4	R_{12}	·20
R_5	·5	R_{13}	·21
R_6	·6	R_{14}	·22
R_7	·7	R_{15}	·23
R_8	·8	R_{16}	·24

R_{17}	·80.33|28	R_{25}	·80·49|28
R_{18}	·34	R_{26}	·50
R_{19}	·35	R_{27}	·51
R_{20}	·36	R_{28}	·52
R_{21}	·37	R_{29}	·53
R_{22}	·38	R_{30}	·54
R_{23}	·39	R_{31}	·55
R_{24}	·40	R_{32}	·56

Routing table

R51

Network Id	mask	Gateway	Flag
·80·0	·255·240	—	0
·80·16	·255·240	—	0
·80·32	·240	—	0
80·48	·240	—	0
/0	/0·	80·	1

R52

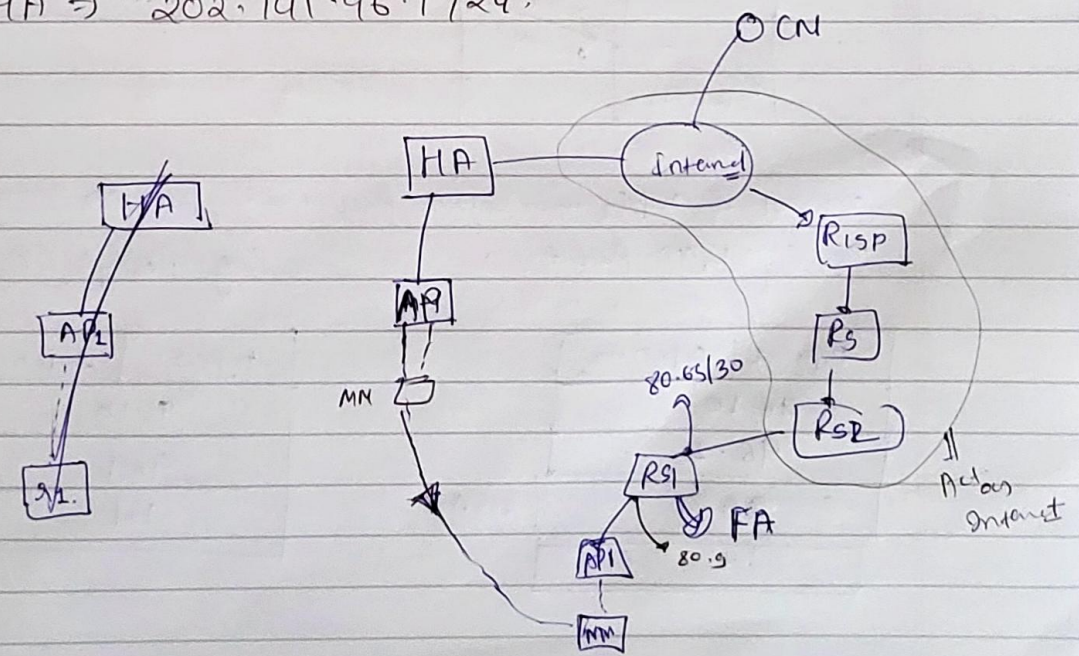
RS2

NW Id	Subnet Mask	Gateway	Flag
.80.0	/28	80.65	1
.80.16	/28	80.65	1
.80.32	/28	80.65	1
.80.48	/28	80.65	1
/0	/0	80.70.1	1

for RISP Router

NW	Subnet Mask	Gateway	Flag
202.141.80.0	/24	80.73	1
0	/0	Internet.	1

(4) CN ⇒ 202.141.64.10/24
MN ⇒ 202.141.96.10/24
HA ⇒ 202.141.96.1/24.

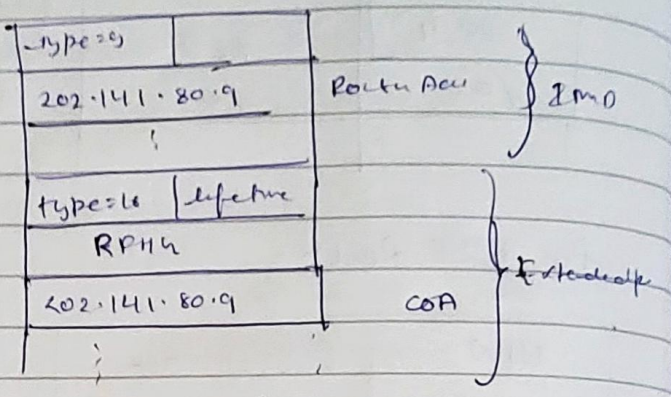


Here RS1 will act as foreign Agent as MN1 moved to AP1.

HA & RS1 will advertise agent advertisement periodically to tell its presence

Advertisement uses ICMP packet.

ICMP packet format



above advertisement received by MN1 & it knows its location and send registration request to FA(RS1) & FA forward it to HA & then HA sends Reg Reply back

Reg Reg & Reply

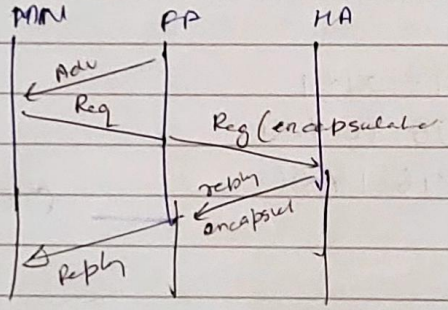
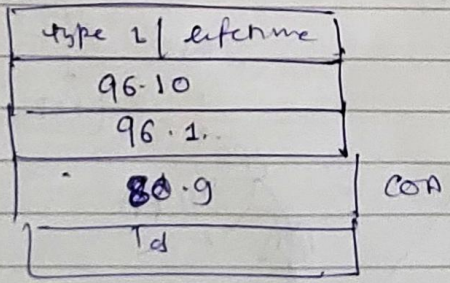


table entry

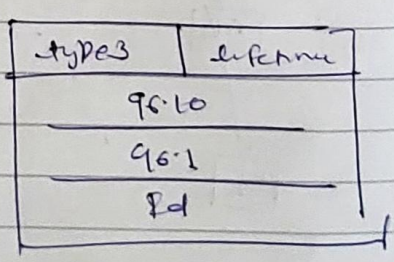
MN-IP	MAC

request & reply uses UDP Packet at port no 434

Reg Req UDP Packet



Reg Reply UDP P



When FA receives above reg req. It makes entry in its table as below.

96.10	—	H-CN

and forward to HA.

HA will bind MN-IP with COA

96.10	—	80.9

and similarly for Registration Reply

Packet Transfer From CN to MN

Packet at CN.

64.10	96.10	Data

using MAC layer. (ARP Rq & Reply will be used to get MAC of next hop Address).

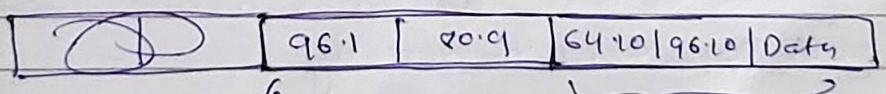
MAC packet

H-CN	—	64.10	96.10	Data

will be transferred to HA via Internet.

When packet arrives at HA, it checks that dst IP is mobile node (by checking COA table entry) so it will create a tunnel b/w HA & FA and encapsulate packet in IP-IN-IP & forwards to FA (RSI).

IP-IN-IP Encapsulation



using MAC Layer

To HA	—	96.1	80.9	Data

Next hop MAC

If will read arrive at RISP.

RISP checks IP routing table. & dstn IP

take and of dst IP & subnet mask of each entry

if AND value matches then check direct or indirect connect.

If indirect connection forward packet to NHA.

at RISP

H-RISP	H-Rg	96.1	80.9	Data

similary packet arrives at Rg from RS2.

and finally at RS1.

when packet reaches at RS1.

as It acts as HA It will check encapsulated packet by checking protocol field

If encapsulate packet decapsulate

decapsulated packet.

S-IP	D-IP	
64.10	98.10	Data

now as It is 802.3 packet & we have to sent at 802.11 n/w

packet will be converted to 802.11 packet by AP.

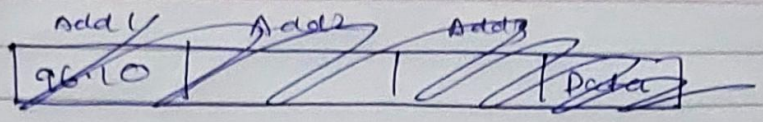
D-IP & subnet mask of each entry in table

If will check table entry, whether mobile node or not, as It is mobile node It will be sent to directly.

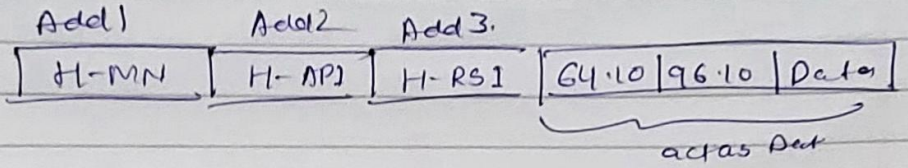
but 802.3 → 802.11

~~802.11~~ is converted by AP in 802.11.

H-RS1 = H-80.9



H-RS1	H-MN	64.10	96.10	Data



Packet recieved by MN

* From MN to CN

Packet at MN (NHA will be RS1(FA))

Add 1	Add 2	Add 3.	S-IP	D-IP	
H-AP1	H-MN	H-RS1.	96.10	64.10	Data

Packet arrived at AP1 & converted to 802.3 pack

S-H	D-H			
H-MN	H-RS1	96.10	64.10	Data

Packet arrived at RS1

at RS2 it check dest IP and accordingly chooses NHA.

forwarded to RS2

H-RS2	H-RS1	96.10	64.10	Data

Similarly packet will reach to CN via Internet.