UNIT-3

Mobile IP:

Mobile IP is an open standard which is defined by Internet Engineering Task Force (IETF) RFC 2002, that allows users to keep the same IP address and stay connected and maintain ongoing applications while roaming between IP networks.

Mobile IP is a protocol developed to allow internetwork mobility for wireless nodes without having them to change their IP addresses.

Requirements for the Evolution of new Mobile IP protocol:

1) Need for Enhancing IP Network Capacity. (Transperency and Compatability)

The use of the existing IP protocol by large numbers of mobile nodes (MNs) will actually lead to a decrease in the network. IP network protocols support 48-bit MAC addresses. But when the number of MNs is large, then other interfaces and lower level protocols are required. So there is a need for upgrading the capacity of Routers and usage of new protocols at the data link layer and physical layers to handle the mobility of mobile node with existing IP protocols.

2) Security Needs:

The mobility of the called MN must be hidden from the calling MN. But when a new IP address allocates at the new hosting subnet of the existing IP based infrastructure, the identity of the mobile node is not hidden from another host. which leads to the exposure of MN and therefore lacks security by using the existing IP protocol.

3) Need for Non-Transparency from higher layers:

The transport layer establishes a connection between a given port at a given IP addres called socket with another port at another IP addres. The connection, once established by the transport layers between the sockets is broken as soon as the new addres is assigned. Any movement of the MN will be transparent to the TCP and to L7 in case the TCP layer re establishes the connection when IP protocol used by the MN. Therefore there is a need for non transparency of the MN to distant ports.

There are some reestablishment problems due to Non-transpe-rency from higher layers.

(a) Reestablishment of the connection takes time which means loss of data during that interval.

(b) Reestablishment proces has to share the same network and the given transmission rate.

(c) Any movement on the part of the MN transparent and thus not secure from the distant hosts on the network of distant routers.

4) Routing Table Problems:

The reconfigeration messages for updating the routing tables have to share the same network and the given transmission rate.

Components of Mobile IP:

* Mobile Node (MN):
  A system or node that can change the point of connection to the network without changing its IP address.

* Home Agent (HA):
  A system in a home network of the MN, typically a router. It registers the location of the MN, tunnels IP datagrams to the COA - Care of address.

* Foreign Agent (FA):
  A system in the current foreign network of the MN, typically a router. It forwards the tunneled datagrams to the MN, typically also the default router for the MN.

* Care of Address (COA):
  It is address of the current tunnel end point for the MN (at FA or MN). It gives the actual location of the MN from an IP point of view.

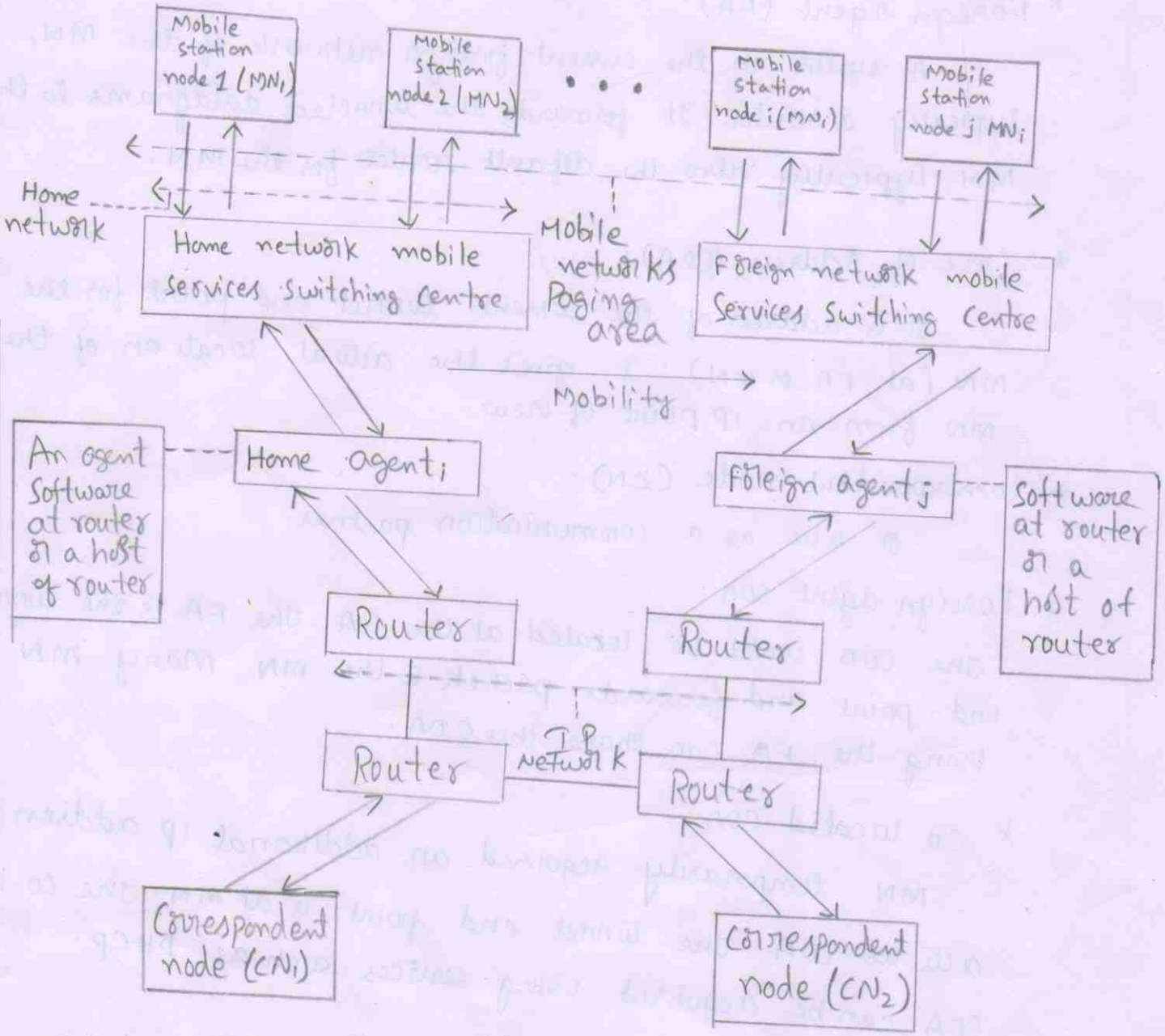
* Correspondent node (CN):
  It acts as a communication partner.

* Foreign agent COA:
  The COA could be located at the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA.

* Co-located COA:
  MN temporarily acquired an additional IP address which acts as COA. The tunnel end point is at MN. The co-located COA can be acquired using services such as DHCP.

Working of Mobile IP:

A router has a home agent (HA) for a set of home networked MNs as well as a foreign agent (FA) for the visiting MNs. An agent is software employed at a router or the host serviced by a router. The same software can function as both the HA and the FA at different instants of time. An MN can also have software which functions as an FA instead of the FA at the router.



Mobile IP Network Employing home and foreign agents

The HA and the FA play a location management role similar to that of the HLR and the VLR in a GSM system. An MN can access Internet services using mobile IP protocol. The MN can change its service router when visiting another location. A home network is a mobile radio subsystems network within an area, called paging area. The area in which the MNs of home as well as foreign networks can be approached through a single MSC or a set of MSCs. Routes of packets through the routes performed when an MN moves within one paging area. Foreign network – another mobile radio subsystem network which the MNs of home network visit within the paging area. A foreign agent is a provider of the IP address and services, including transmitting and receiving packets from the Internet, for MNs on visit to a foreign network. This foreign agent assigns MNs to a router, which supports the MNs of other home networks.

Packet Delivery and Handover Management:

A correspondent node (CN) an MN or a fixed IP host linked to a router, which communicates IP packets to another MN in a home or foreign network.

CASE 1: CN is a fixed node and MN_1 at the home network.

CN message transmits for connection establishment or a packet using the IP protocol. HA_1 (home agent of MN_1) receives the message or packet and, using the information that the destined MN_1 is at the home network itself, it delivers the message or packet to MN_1. It recieves the response message or packet from MN_1. It delivers it to the CN using the IP protocol.

CASE 2: CN and MN_K and MN_1 both at home networks with agents HA_K and HA_1.

MK_K transmits a message from connection establishment or a packet using the IP protocol. The MN_K IP header has the source

and destination IP address. MN_1 sends the message through HA_K. HA_K uses the same IP address of MN_K as in the IP header and forwards the packet on the Internet in the same way as in Case1. The packet is delivered to HA_1 and then to MN_1. Now, MN_1 transmits back to MN_K the HA_K and HA_1 deliver the packets from one end to another and viceversa. Both HA_K and HA_1 delivers by just forwarding the packets to their respective MN using the IP protocol.

CASE 3: CN is a fixed node and MN_1 is at foreign network.

CN transmits a message for connection establishment or a packet using the IP protocol. The CN IP header has source IP address and destination (MN_1) IP address, in the same way as in Case 1. HA_1 recieves the packets and has the information that the destined mobile node MN_1 is not at the home network and is visiting a foreign network with a foreign agent FA_j. It encapsulates the received IP packet using a new header which has a COA (care of addres)

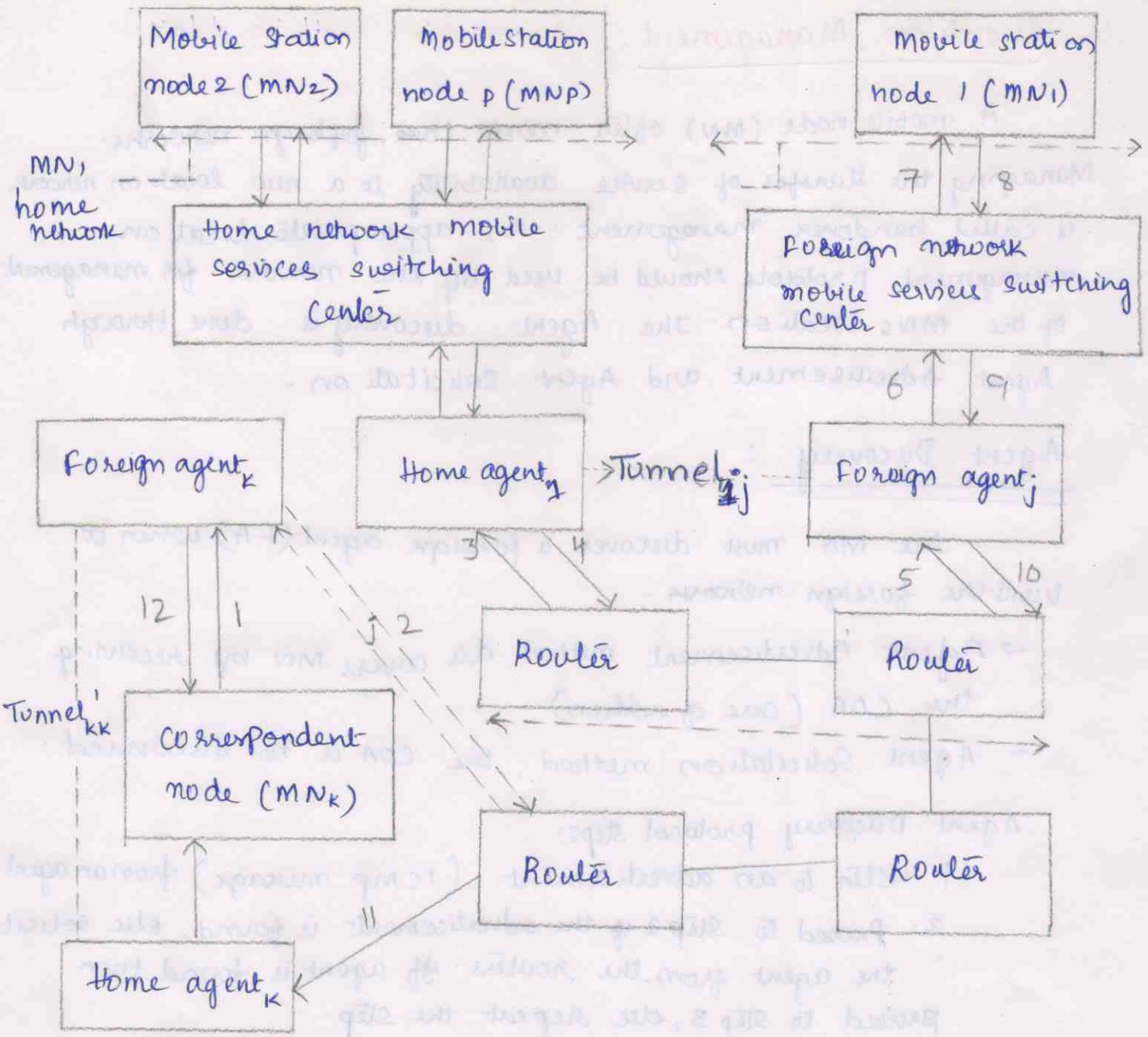
Forward direction: $MN_K \rightarrow FA'_K$, $FA'_K \rightarrow HA_1$, $HA_1 \rightarrow FA_j$, $FA_j \rightarrow MN_1$.

$HA_1 \rightarrow FA_j$ is through a tunnel T_{ij}.

Opposite direction: $MN_1 \rightarrow FA_j$, $FA_j \rightarrow HA_K$, $HA_K \rightarrow FA'_K$, $FA'_K \rightarrow MN_K$

Through another tunnel $HA_K \rightarrow FA'_K$ (T_{KK}).

The packet encapsulated with the new header is transmitted to FA_j by tunnelling. The FA_j reads the COA and decapsulates the IP packet. It then reads the destination IP and transfers the packet to MN_1. When MN_1 sends the response or IP packet with CN as destination address, FA_j transfers the packet to CN as would have been done by HA_1 had MN_1 been at home network. The mobility of MN_1 is secure from the CN as any movement is only known to HA_1 and FA_j



CASE 4 : CN is a mobile node, MN_K, at a foreign network with FA_K and MN_1 is at the home network with agent HA_1.

The packet delivery is similar to that of case 3 when MN_1 transmits to CN. MN_K delivers the packet to FA_K. FA_K is used instead of HA_K as now MN_K is on a visit. FA_K transfers the message to HA_1 like in case 1 where CN transfers the message to HA_j

CASE 5 : CN is a mobile node MN_K at a foreign network with FA_KE and MN_1 is also at another foreign network with agent FA_j.

$$MN_K \rightarrow FA_KE \rightarrow HA_1 \xrightarrow{\text{encap}} FA_j \xrightarrow{\text{decap}} MN_1$$

CASE 6 : CN is mobile node MN_K at the home network with HA_K and MN_1 is at foreign n/w with FA_j. $MN_K \rightarrow CN$. $FA_j \rightarrow MN_1$

tunnelling

Location Management:

A mobile node (MN) often moves, to foreign networks. Managing the transfer of service availability to a new location network is called handover management. So, appropriate location management protocols should be used by the network for management of the MNs location. The Agent discovery is done through Agent Advertisement and Agent Solicitation.

Agent Discovery:

The MN must discover a foreign agent (FA) when it visits the foreign network.

→ Agent Advertisement method discovers MN by receiving the COA (care of address)

- Agent Solicitation method, the COA is not discovered.

Agent Discovery protocol steps:

1. Listen to an advertisement (icmp message) from an agent.
2. Proceed to step 3 if the advertisement is found, else solicit the agent from the routers. If agent is found then proceed to step 3, else repeat the step.
3. If the COA discovered from the message is found to be the same as the previous COA, go back to step 1, else proceed to step 4.
4. If the discovered COA is the same as the home network, de-register at this network and go back to step 1, else if the current COA is new COA, then register with the new COA.

Agent Advertisement:

The MN discovers home and foreign agent while moving from one network area to another. Agent Advertisements are essentially icmp messages, which are sent to number of addresses.

ICMP header & ICMP message format:

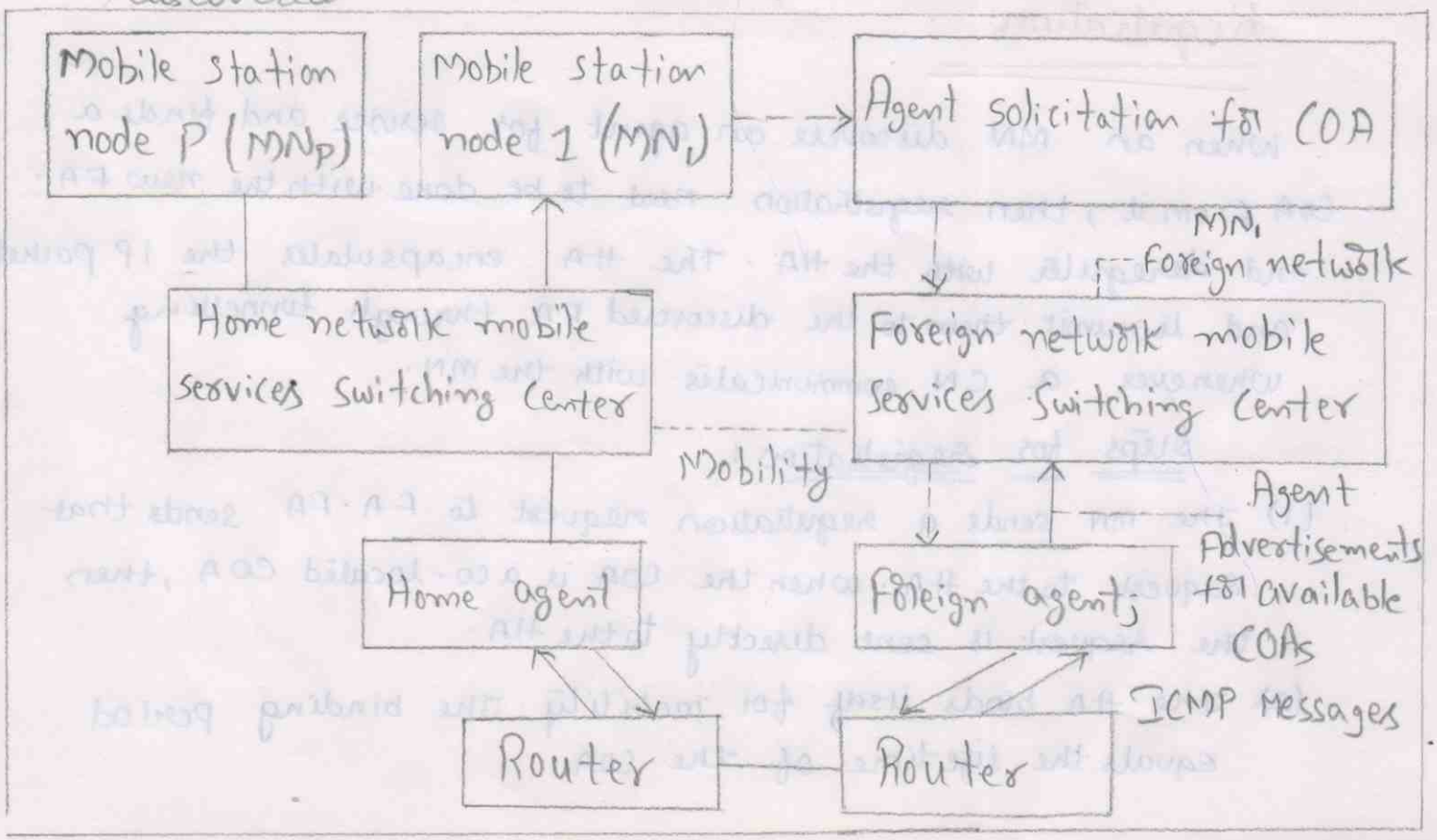
(1) A 32-bit word, with first byte = 00010000 and second byte for length 2 words and two bytes for the 16-bit sequence number. (for ICMP message advertised)

(2) A 32-bit word has a two-byte specification by the agent for registration lifetime during which the MN can register with new COA. It has 8 bits for flags. The remaining byte is not used presently. It is reserved for any future requirements of modifications or specification expansion in ICMP.

(3) A set of 32-bit words for the COA addresses for the MN at that agent.

The second word has eight flag bits. A COA is said to be co-located COA if the MN temporarily acquires an additional IP address while on visit to a new network. else the COA is the same IP address for that MN while on visit and when at home.

fig: Agent discovery by mobile node MN, on receiving COA during agent advertisement or by agent solicitation if COA not discovered.



- The FA uses DHCP and obtains co-located COA. A flag in second word specifies whether the COA is a co-located COA, whether the advertising agent is an FA.
- Another flag bit specifies whether there is reverse tunnelling support by the FA for encapsulation and sending packets by tunnelling to the HA.
- Another flag bit specifies whether the encapsulation method is generic.
- One flag bit specified whether the encapsulation method is mandatory method.
- One flag bit specifies if the agent is busy and cannot register the visiting MN.

Agent solicitation:

When the agent advertisement is not listened to, solication can be done three times at 1 second interval and later this interval can be increased. In this method the MN visiting a network discovers the FA and the COA.

Registration:

When an MN discovers an agent for service and finds a COA from it, then registration need to be done with the new FA. and deregister with the HA. The HA encapsulates the IP packets and transmit them to the discovered FA through tunnelling whenever a CN communicates with the MN.

Steps for registration:

(1) The MN sends a registration request to FA. FA sends that request to the HA. When the COA is a co-located COA, then the request is sent directly to the HA.

(2). The HA binds itself for mobility. The binding period equals the lifetime of the COA.

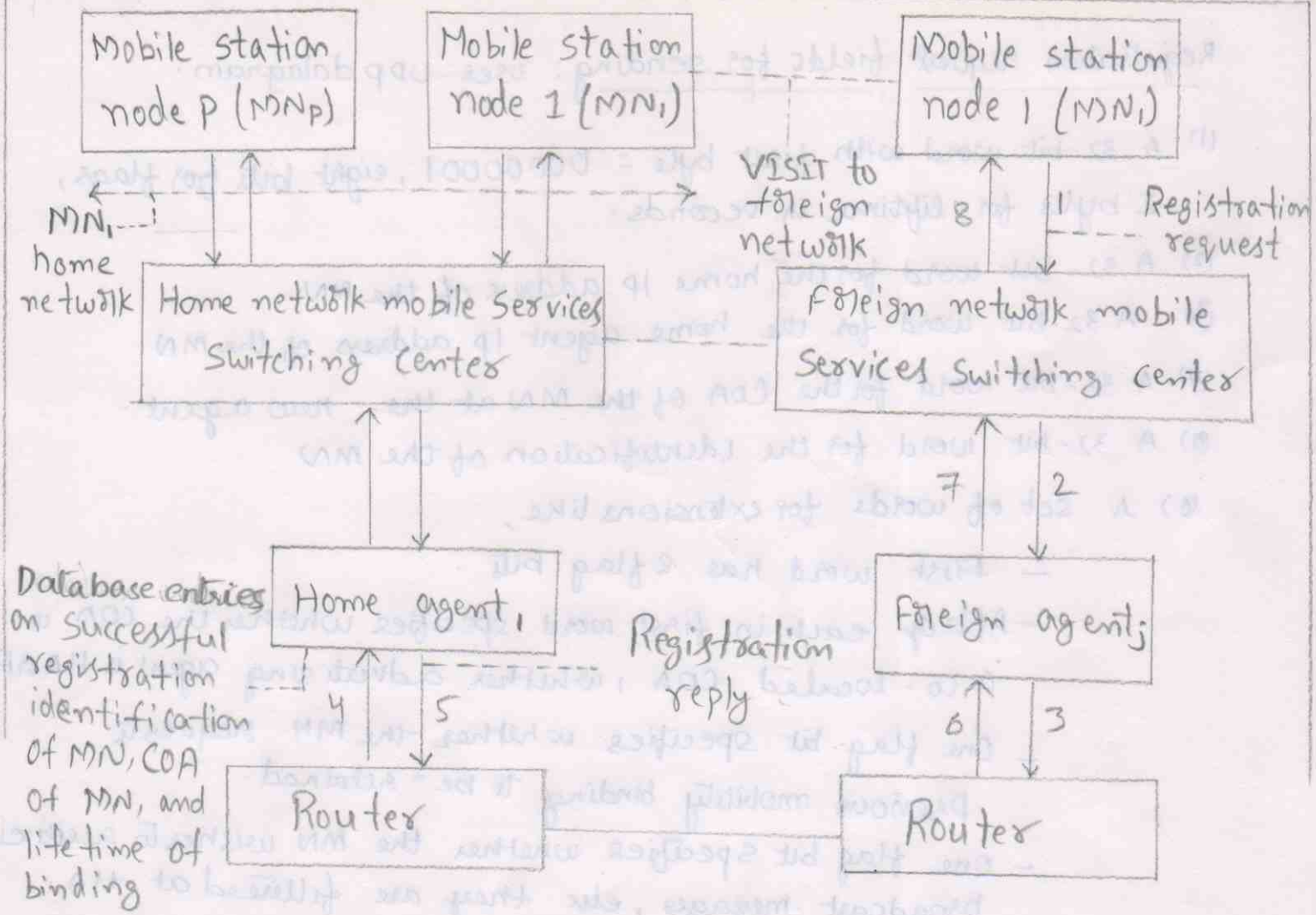


fig: mobile node MN_K at a foreign network after agent discovery of FA_j in a mobile IP network seeking registration for creating tunnel between HA_i and FA_j

(3) The MN registers again before the binding period expires, when it moves to another foreign network, or when it return back to the home network.

(4) The HA sends a registration reply to the FA and the FA to the MN. The MN checks whether the reply shows successful registration when there are too many tunnels created at the HA and the HA does not have the resources to handle new requests or there is an authentication failure or the HA is not reachable to the FA there is a possibility of not successful.

The registration request and reply fields are as follows:

Registration request fields for sending: uses UDP datagram.

(1) A 32-bit word with first byte = 00000001, eight bits for flags, 2 bytes for lifetime in seconds.
(2) A 32-bit word for the home IP address of the MN.
(3) A 32-bit word for the home agent IP address of the MN.
(4) A 32-bit word for the COA of the MN at the new agent.
(5) A 32-bit word for the identification of the MN
(6) A set of words for extensions like,
- First word has 8 flag bits.
- A flag each in first word specifies whether the COA is a co-located COA, whether advertising agent is HA & FA
- One flag bit specifies whether the MN requests previous mobility binding to be retained.
- one flag bit specifies whether the MN wishes to receive broadcast messages, else they are filtered at HA.
- one flag bit to specify if there is reverse tunnelling support from the FA.

Registration reply fields for sending:

(1) A 32-bit word with first byte = 00000011, eight bits for a code specifying the result of registration, and two bytes for lifetime
(2) A 32-bit word for the home IP address of the MN.
(3) A 32-bit word for home agent IP address of the MN.
(4) A 32-bit word for identification of MN
(5) A set of words for extentions like,
(a) On successful registration, whether the previous mobility binding still exists.
(b) FA's rejection with one of the five reasons for it
(c) HA's rejection with one of the six reasons for it.

Tunnelling and Encapsulation:

Tunnelling refers to establishing a pipe. Tonnelling has two primary functions:

1. Encapsulation of the data packet to reach tunnel end point.
2. Decapsulation when packet is delivered at that end point

* Optionally Minimal encapsulation and GRE (Generic Routing Encapsulation) within IP may be used.

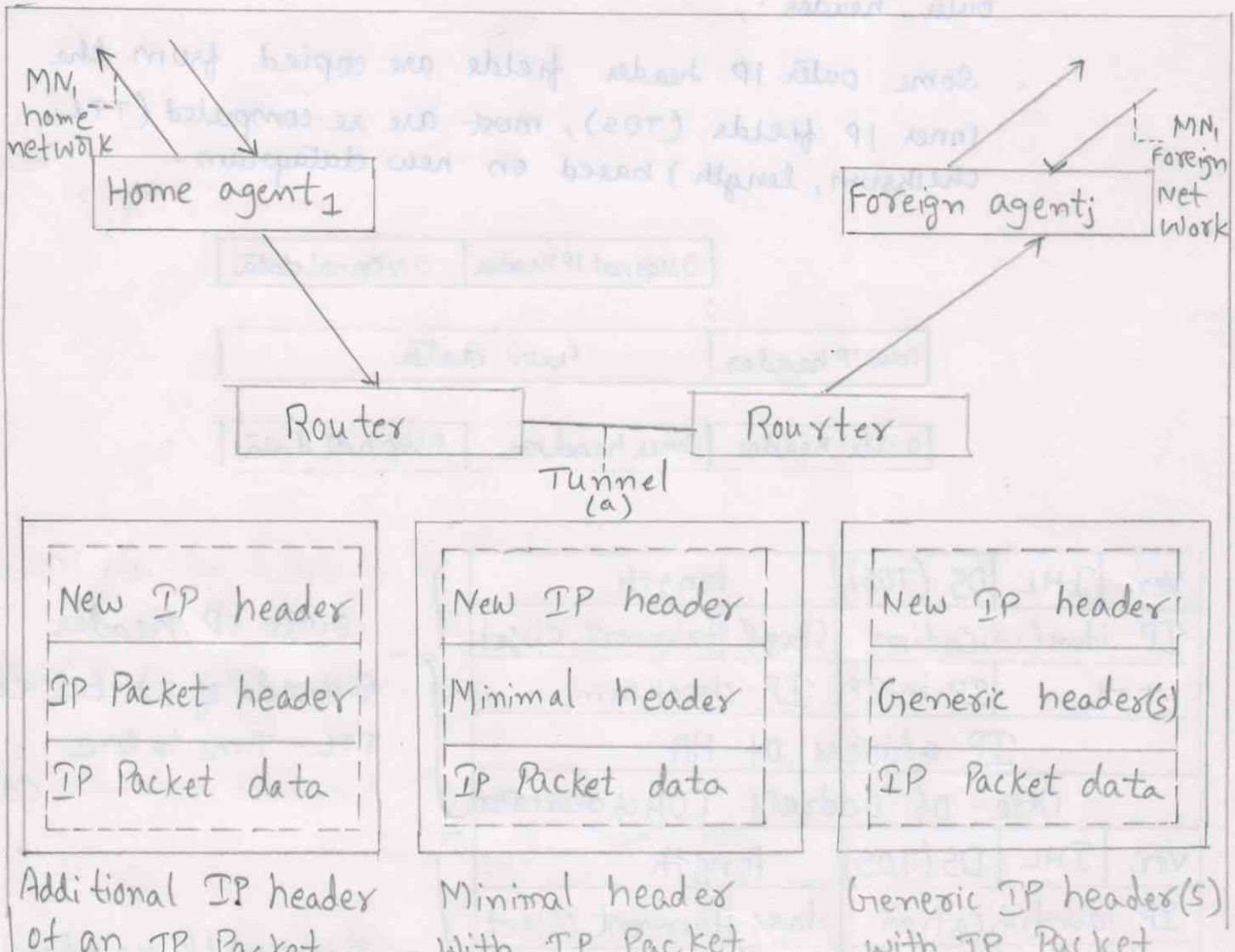
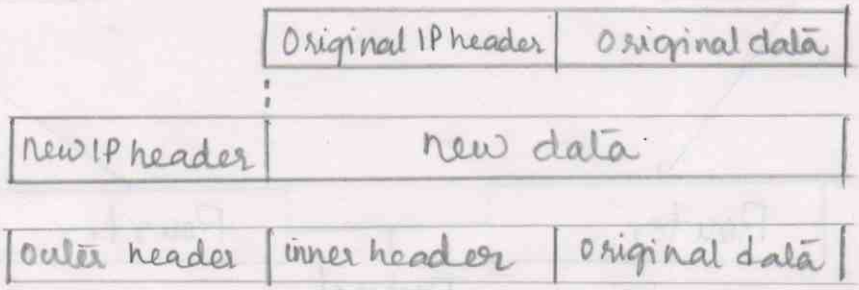


fig: Mobile node MN_K at a foreign network after agent discovery of FAj in a mobile IP network seeking registration for creating a tunnel between HA, and FAj..

Encapsulation is taking a packet consisting of packet header and data and putting it into the data part of new packet.

(1) IP in IP Encapsulation:

- tunnel between HA and COA
- the outer IP header source and destination address identify the tunnel end points.
- outer protocol is '4' i.e) IP datagram Version 4.
- the inner IP header source address and destination address identify the original sender and receiver.
- others headers for authentication might be added to outer header.
- Some outer IP header fields are copied from the inner IP fields (TOS), most are re-computed (TTL, checksum, length) based on new datagram.



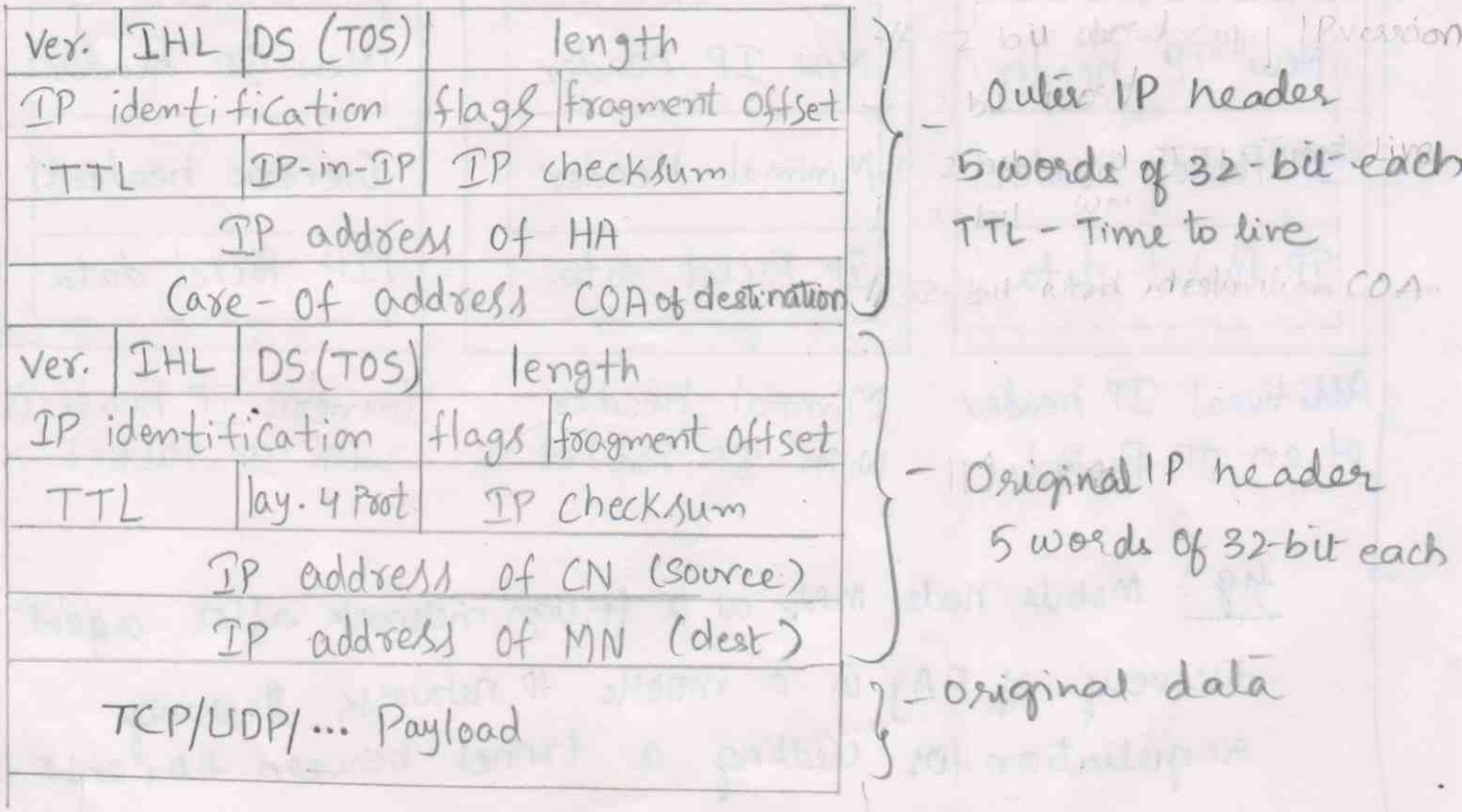


fig: IP in IP Encapsulation

Minimal Encapsulation : (optional)

- It avoids repetition of identical fields.
- Eg: TTL, IHL, Version, DS (RFC 2474, Old: TOS)
- only applicable for unfragmented packets, there is no space left for fragment identification.

Ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	min. encap.	IP Checksum	
IP address of HA			
Care-of address COA			
lay.4 Protoc.	S	reserved	IP Checksum
IP address of MN			
original Sender IP address (if S=1)			
TCP/UDP/... Payload			

} New IP header

} S - 1 bit, Reserved bits - 7
Checksum - 16 bits. rest for protocol.
- minimized header

} - Original data

Generic route Encapsulation :

- IP in IP encapsulation dosent have the routing information for tunnelling; dosent allow recursive encap; no provision for key
- Minimal encapsulation is optional and it dosent have a provision for recursive encapsulations and there is no provision for a key that can be used for authentication or encryption and also no routing info.
- Recursive encap. are needed when the tunnel transmits multiple pieces of information for MN. There can be one or more GRE headers depending on no of recursions required to send multiple pieces of information.

Time To Live = 1;

		original header	original data
outer header	GRE header	original header	original data
new header	new data		

RFC 1701

1	ver.	IHL	DS (TOS)	length				
2	IP identification			flags	fragment offset			
3	TTL = 1		GRE	IP Checksum				
4	IP address of HA							
5	Care-of address COA							
6	C	R	K	S	s	rec.	rsv.	ver.	Protocol
7	checksum (optional)								offset (optional)
8	Key (optional)								
9	Sequence number (optional)								
10	routing (optional)								
11	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								

- Outer header
- GRE header
- Original header
- Original data

fig: GRE encapsulation

RFC 2784

The 6th and 7th words intend to change in the new one (e) RFC 2784. as below.

C	reserved0	Ver.	Protocol
checksum (optional)			reversed 1 (=0)

Route Optimization:

Consider a mobile IP network with home and foreign agents and packet delivery to and from a mobile node MN_K at a foreign network with FA_K and MN_1 at the foreign network with FA_j

(1) Triangular Routing:

A sequence numbered 1,2,3,4,5 to MN_1 is a triangular route without mobility binding. Packets make a triangular trip to reach from CN_K to MN_1. It is also possible that FA_K and FA_j are identical.

Optimization of triangular route can be carried out with Mobility Binding protocol.

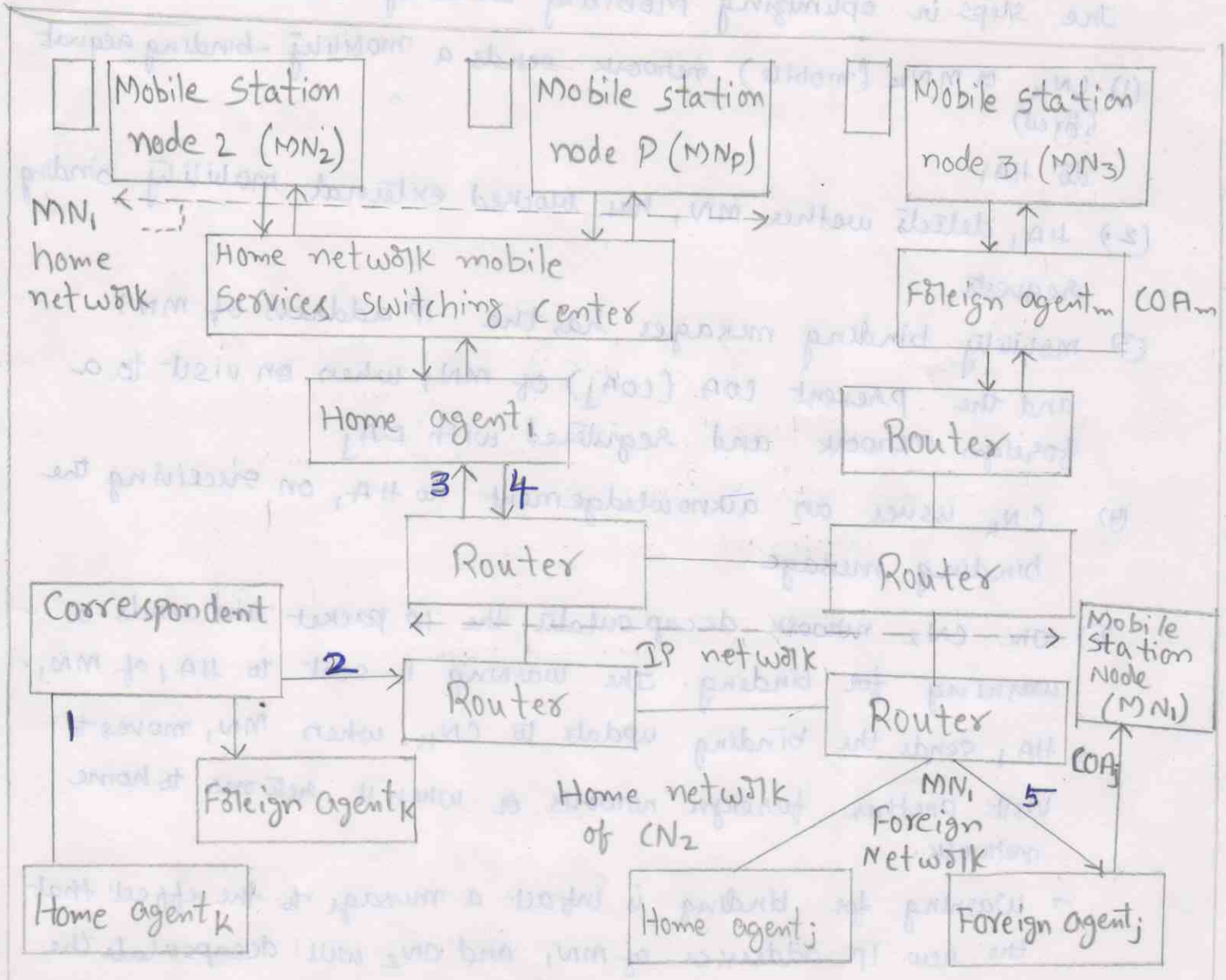


fig: Mobile IP network employing a triangular route without mobility binding between COA_j and CN_K.

Mobility Binding :

Triangular route optimization to a direct route is performed as say, if MN_1 permits the identification of its mobility when it visits a foreign network, then CN can use a mobility binding cache. Mobility-binding cache is a cache that stores the current COA of called MN. CN can directly send the IP packets to MN_1 instead of triangular routing through HA_1 and then to the COA through a tunnel.

The route optimization and path 1,2,3,4,5 after mobility binding of MN_1 at COA_j with CN_K.

The steps in optimizing Mobility Binding Protocol :

(1) CN_K or MN_K (mobile) network sends a mobility-binding request (fixed) to HA_1

(2) HA_1 detects wether MN_1 has blocked external mobility binding requests.

(3) Mobility binding messages has the IP address of MN_1 and the present COA (COA_j) of MN_1 when on visit to a foreign network and registered with FA_j.

(4) CN_K issues an acknowledgement to HA_1 on receiving the binding message.

(5) The CN_2 network decapsulates the IP packet and sends a warning for binding. The warning is sent to HA_1 of MN_1.

→ HA_1 sends the binding update to CN_K when MN_1 moves to visit another foreign network or when it returns to home network.

→ Warning for binding is infact a message to the effect that the new IP addresses of MN_1 and CN_2 will decapsulate the encapsulated IP packets instead of FA_j.

[fig: next page]

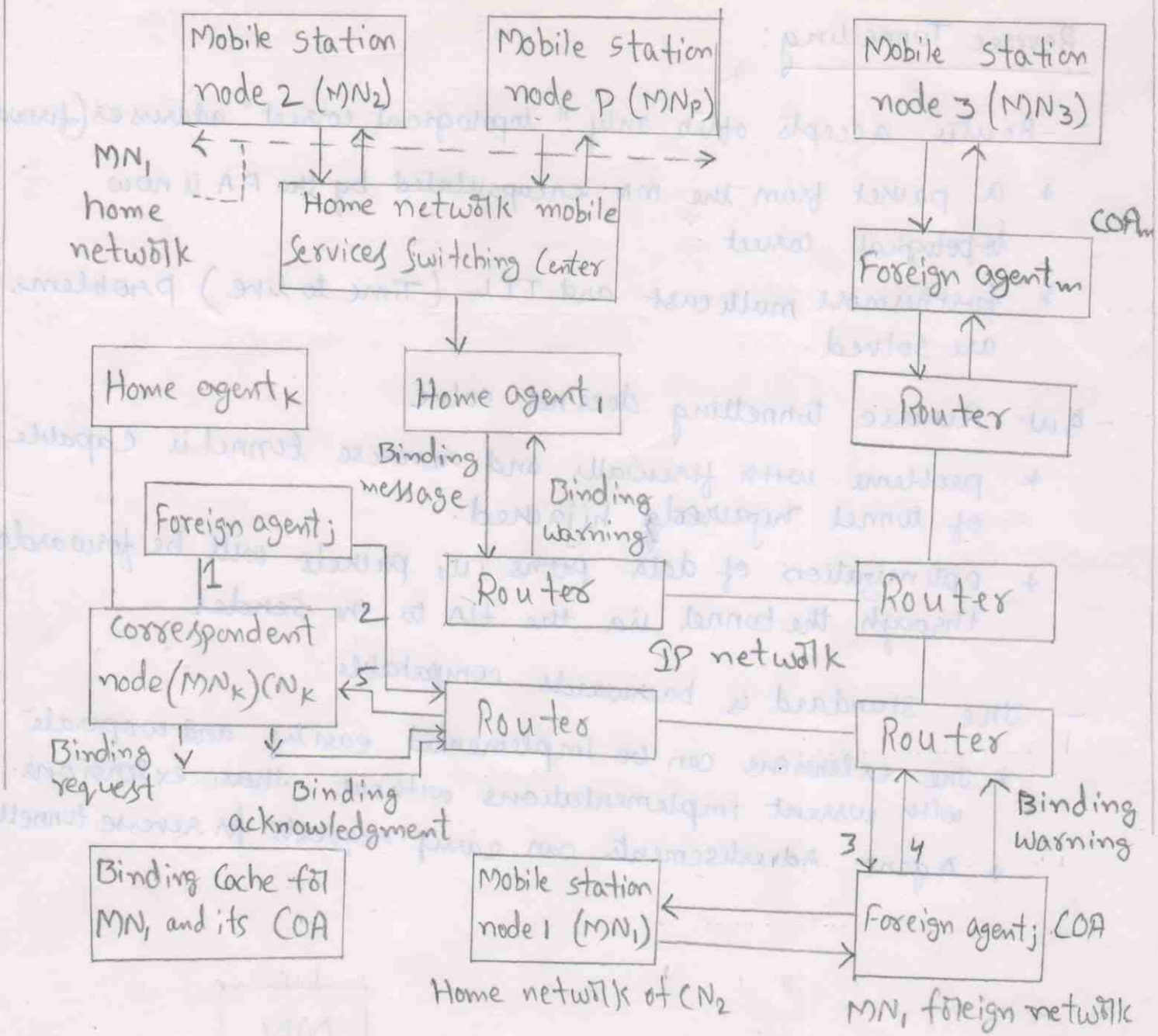


fig: Mobile IP employing route optimization path after mobility binding between COA_j and CN_K - (packet Forwarding)

Optimization for smooth handover:

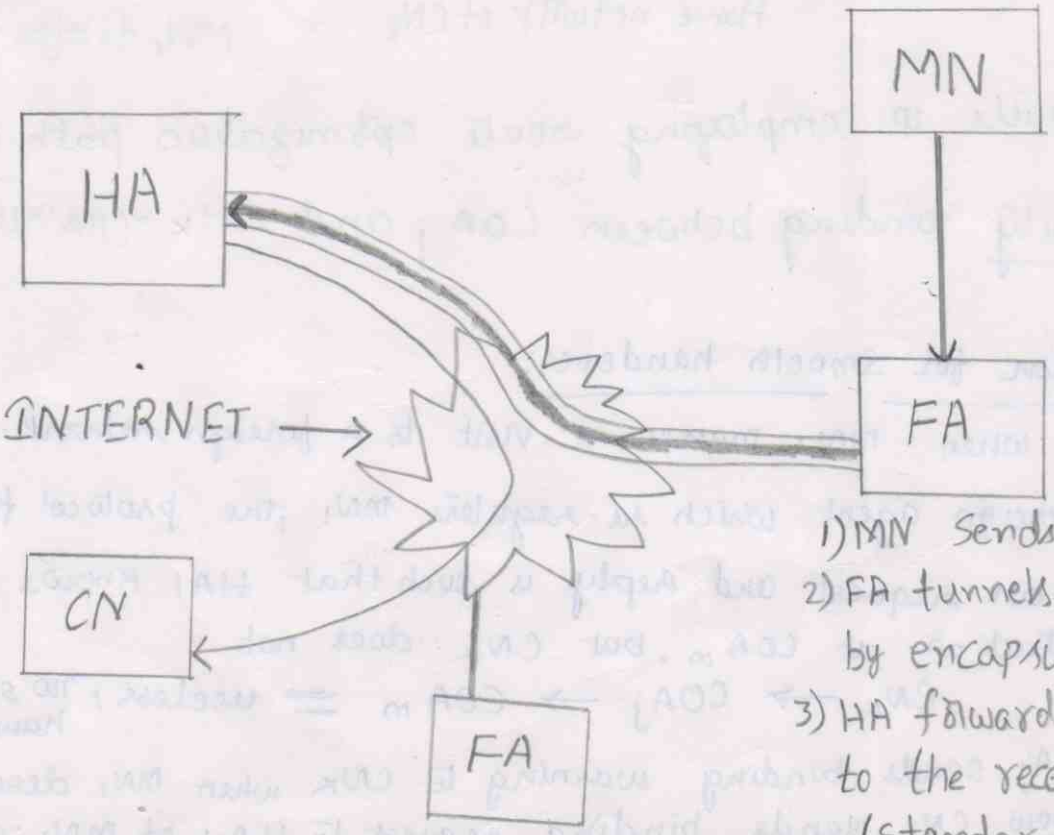
When MN_1 makes a visit to a foreign network and FA_m is a new foreign agent which re-registers MN_1, the protocol for registration request and reply is such that HA1 knows the new registration at COA_m, but CN_K does not.

$CN_K \rightarrow COA_j \rightarrow COA_m \rightleftharpoons$ useless, no smooth handover.

So, now FA_j sends binding warning to CN_K when MN_1 deregisters with it. Now CN_K sends binding request to HA1 of MN_1. CN_K gets the new binding and COA_m address from HA1 in binding cache.

Reverse Tunnelling:

- Router accepts often only "topological correct" addresses (firewall)
  - * a packet from the MN encapsulated by the FA is now topological correct.
  - * furthermore multicast and TTL (Time to live) problems are solved.
- But Reverse tunnelling does not solve
  - * problems with firewalls, and reverse tunnel is capable of tunnel ~~hijacked~~ hijacked.
  - * optimization of data paths, ie, packets will be forwarded through the tunnel via the HA to the sender
- The standard is backwards compatable:
  - * The extensions can be implemented easily and cooperate with current implementations without these extensions.
  - * Agent Advertisements can carry requests for reverse tunnelling



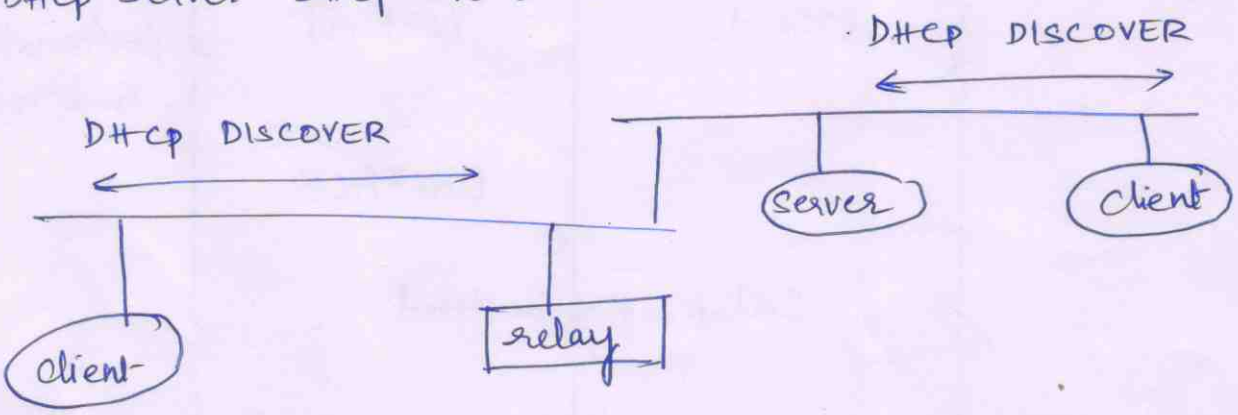
1) MN sends to FA
2) FA tunnels packets to HA by encapsulation
3) HA forwards the packet to the receiver (standard case)

Dynamic Host Configuration Protocol:

If a new computer is connected to a network, DHCP will provide it with all necessary information for full system integration into the network. DHCP supplies systems with all the necessary information such as IP address, DNS server address, domain name, subnet mask, default routes etc. It enables the automatic integration of systems into an Intranet or the internet and can be used to acquire a (COA / Care of address for Mobile IP.

Simple Client Server model:

The client sends via a MAC broadcast request to the DHCP server: DHCP DISCOVER



DHCP Characteristics:

* server: several servers can be configured for DHCP but mostly they are manually configured.
* Renewal of configurations: The IP address have to be requested periodically and is a simplified protocol.
* Options: Available for routers, subnet mask, NTP (network time protocol), timeserver, SLP (service location protocol) directory, DNS (Domain name system).
* Security: No proper authentication is done for the DHCP information specified.

DHCP protocol mechanism: