IP packet delivery

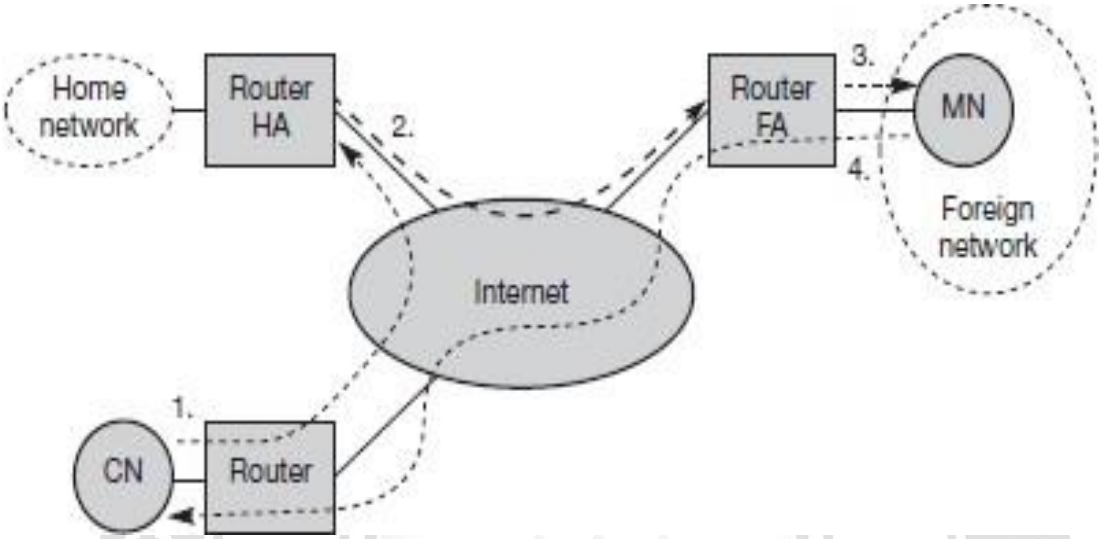

Fig.2. 3 Packet delivery to and from the mobile node

[**Source: Text book**- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The CN wants to send data to the MN. The sends the data packet in which the source address is the address of the CN and the destination address is the IP address of the MN.

The data packet is forwarded to the HA of the Home network.

The HA knows that the MN is not in the home network. It is in the foreign network. The HA encapsulates the data packet with source address of its own and the destination address of the foreign agent and forwards the packet.

The Foreign agent receives, removes the additional header and forwards the data packet to the MN.

The transmission of data packet from the MN to the CN is very simple. If the CNis fixed one, the MN transmits the packet with its own address as source address and the address of the CN as destination address. It the CN is mobile one, the same procedure is to be followed.

Agent discovery

The mobile node is moving from one location to another location. During the movement it has to identify the foreign agent. The mobile IP describes two methods to identify the foreign agent.

1. Agent advertisement
2. Agent solicitation.

Agent advertisement

Mobile nodes use agent advertisements to determine their current point of attachment to the Internet or to an organization's network. An agent advertisement is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension.

A foreign agent can be too busy to serve additional mobile nodes. However, a foreign agent must continue to send agent advertisements. This way, mobile nodes that are already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed.

Also, a foreign agent that supports reverse tunnels must send it's advertisements with the reverse tunnel flag set on.

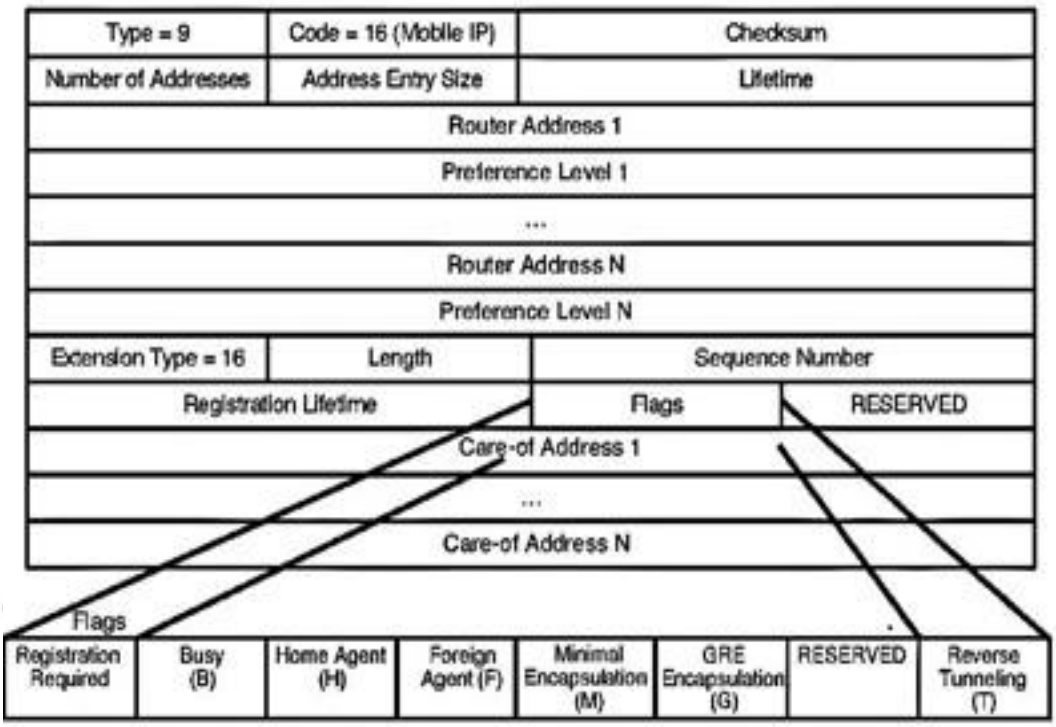

Fig.2.4 The agent advertisement packet format

[**Source: Text book**- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Foreign agents and home agents are periodically advertising their presence using special agent advertisement messages. Routers also advertising their routing services periodically.

The agent advertisement packet format is shown in the figure.

The upper part represents the ICMP packet. The lower part represents the extension needed for the mobility.

For advertisement the TTL field of the IP packet is set to 1.

The IP destination address is either broadcast address 255.255.255.255, or the multicast address 224.0.0.1.

The fields of the agent advertisement packet are:

Type: It is set to 9.

Code: It is set to 0, when the agent routes traffic from both mobile and non- mobile nodes. It is set to 16, when the agent routes traffic from mobile nodes and not from non-mobile nodes.

Number of Addresses: It shows the number of addresses with this packet.

Lifetime: The length of the time over which this advertisement is valid.

Preference: It defines the preference level of each router. It is used to choose the most preferable one.

The fields of the extension of the packet for mobility:

Type: It is set to 16

Length: It defines the number of COAs provided with the message.

Sequence Number: It gives the total number of advertisements from thebeginning.

Registration Lifetime: It specifies the maximum time a MN can request during registration.

Eight bits are used to specify the characteristics of the agent:

R: It specifies that the registration is required with this agent.

B: The agent is busy to accept the new registration.

H: The agent is the Home agent.

F: The agent is the foreign agent.

M: It specifies that the encapsulation method is the Minimal encapsulationmethod.

G: It specifies that the encapsulation method is the Generic routing encapsulation method.

r : Reserved

T: The FA supports the reverse Tunneling.

Agent Solicitation

When a MN enters a new network, It verifies the advertisement messages. If advertisement messages are not there, it will send agent solicitation message. In high dynamic wireless networks, the MN sends three solicitation messages, one per second. Before getting the agent address the MN will loss many data packets.

When the MN receives the address of the agent, it will use it for data transmission. If, it does not receive the answer, it should decrease the rate of solicitations. The solicitation messages will create collision.

After the advertisements and solicitations, the MN receives the COA for an FA. By using it, the MN can make communication.

Tunneling and encapsulation

A tunnel is a virtual path between home agent and current COA. Tunneling is a process of sending data packet through the tunnel.

Encapsulation: It is a process of putting one data packet within another packet. The data packet consists of original data and the header. The entire packet is treated as data and one new header is added. The Diagram shows the operation of the encapsulation process.

Decapsulation: It is a process of extracting the data packet from another packet

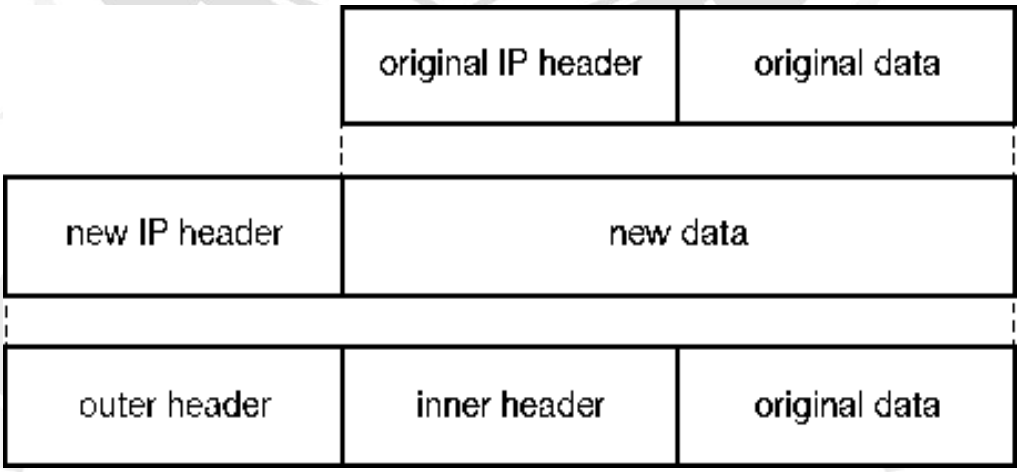

Fig.2.5 IP encapsulation

[**Source: Text book**- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

It consists of two headers . One is inner header which consists of the address of MN and CN.

The second header is the added header which consists of the address of HA and COA.

Three categories of encapsulation process

3. IP-in-IP encapsulation
4. Minimal encapsulation
5. Generic routing encapsulation

2.6.1 IP-in-IP encapsulation

Here one IP packet is kept inside of another IP packet.
The figure shows that the data packet contains two IP headers.

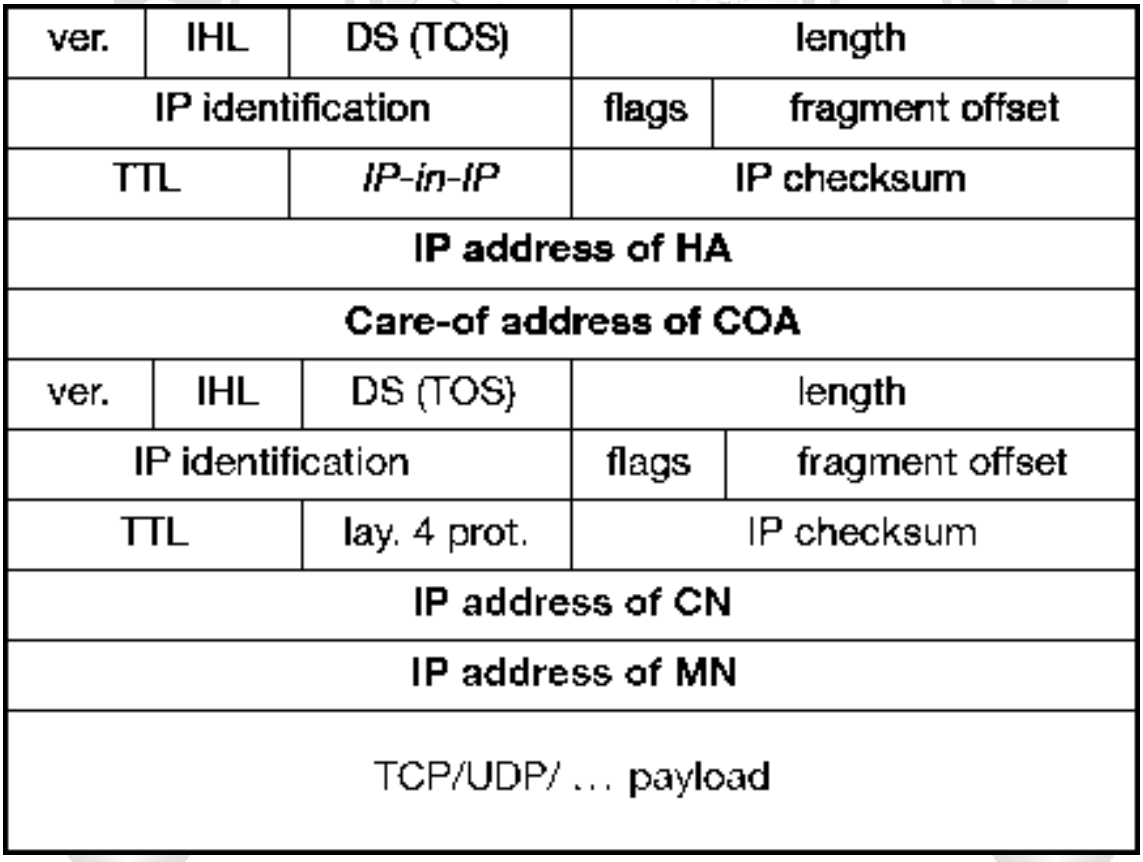

Fig.2.6. IP-in-IP encapsulation

[**Source: Text book**- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The fields of the header are

1. Ver: It specifies the current version of IP packet.
2. IHL (Internet Header Length): It defines the length of the outer header.
3. DS(TOS): It specifies the type of service.
4. Length: It covers the length of the entire packet.
5. TTL: Time To Live It specifies the time over which the data packet can travel through the network. It should be high.
6. Type of Protocol: It specifies the type of the protocol which is used in the packet.
7. IP checksum: The checksum is calculated and added in the packet. At receiverthe checksum is calculated and compared with the value in the data packet. It is used to identify the error.
8. Source address: In outer header it specifies the address of the Home Agent. In inner header it specifies the address of the CN
9. Destination address: In outer header it specifies the address of the COA. In inner header it specifies the address of the MN.

If any options are there , those are added at the end of the outer header. If options are not there, the inner header starts after the outer header with the same fields. The TTL value is decremented by 1. That the whole tunnel is considered as on one hop.

Minimal encapsulation

Some fields are redundant in IP-in-IP encapsulation method. Redundant fields are removed from the inner header. If the S bit is set, the original sender address of the CN is included as omitting the source is quite often not an option. No field for fragmentation offset is left in the inner header and minimal encapsulation does not workwith already fragmented packets.

- It avoids duplication of identical fields and is an optional encapsulation method for mobile IP.
- The inner header is different.
- The tunnel entry point and endpoint are specified.
- The type of the following protocol and the address of the MN are needed.
- If the S bit is 1, the original sender address of the CN is included

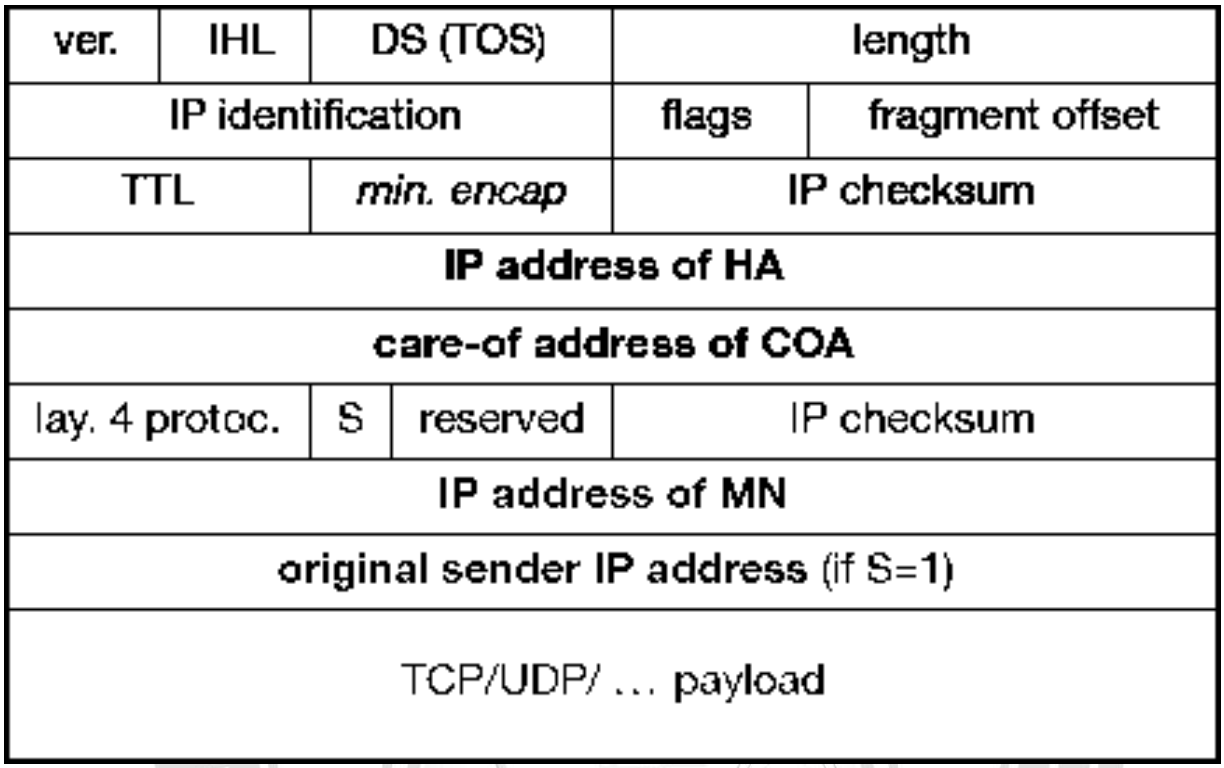

Fig.2.7 Minimal encapsulation

[**Source: Text book**- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Generic routing encapsulation

This encapsulation method is applicable for IP and other network layer protocols. It encapsulates the packet of one protocol into the packet of another protocol.

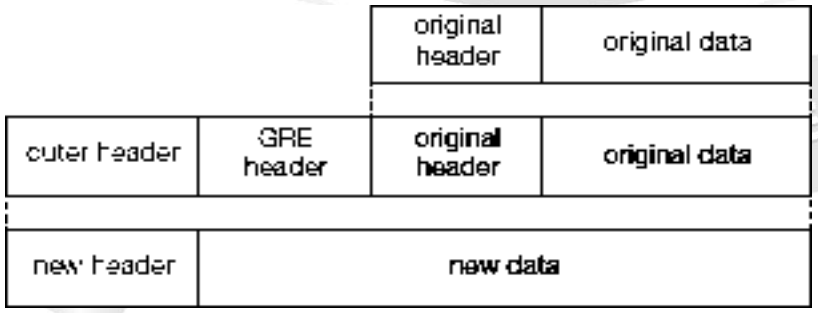

Fig.2.8 Generic routing encapsulation

[**Source: Text book**- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Here one GRE header is added between inner and outer header.

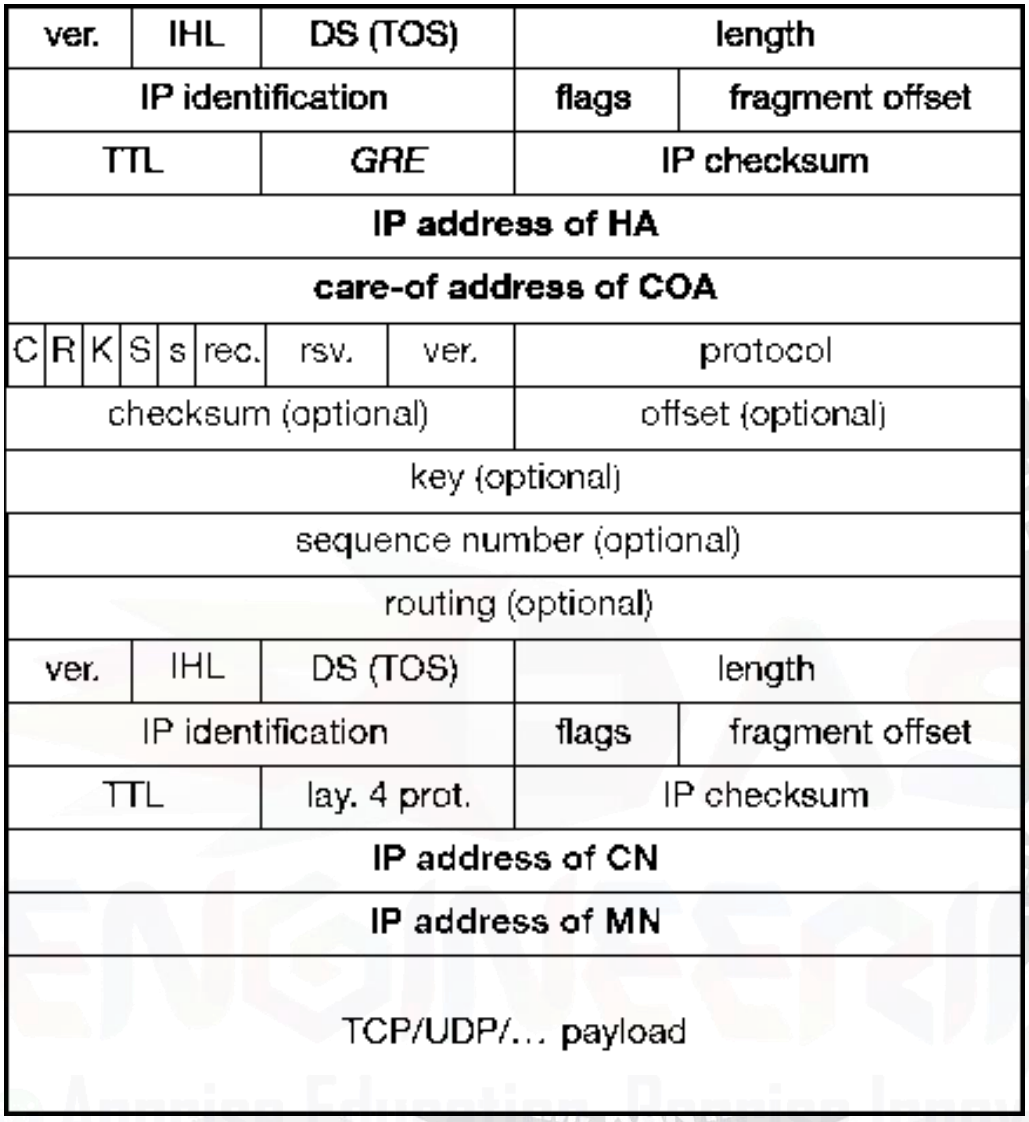

Fig.2.8 Protocol fields for GRE

[**Source: Text book**- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The GRE header is having some flags which are indicating if certain fieldsare present or not. The flags are

C: If C is set, the checksum field contains a valid IP checksum of the GRE header and the payload.

R: If R is set, the routing fields are present and contain valid information.

K: If K is set, a key field is present and is used for authentication. It does not specify authentication algorithm.

S: If S is set, the sequence number field is present.s

: If s is set, strict source routing is used.

Rec: Recursion Control field is used to represent the count of allowed recursive encapsulations. If this field is zero, additional encapsulation is not allowed. If this field is not zero, additional encapsulation is allowed and this is decremented by one.

Reserved: This field must be zero and are ignored on reception.

Version: It is zero for the GRE version.

Protocol: It contains the protocol of the following packet. For Ethernet the field values are 0 x 6558 and for mobile IP tunnel, the fields contains 0 x 800.