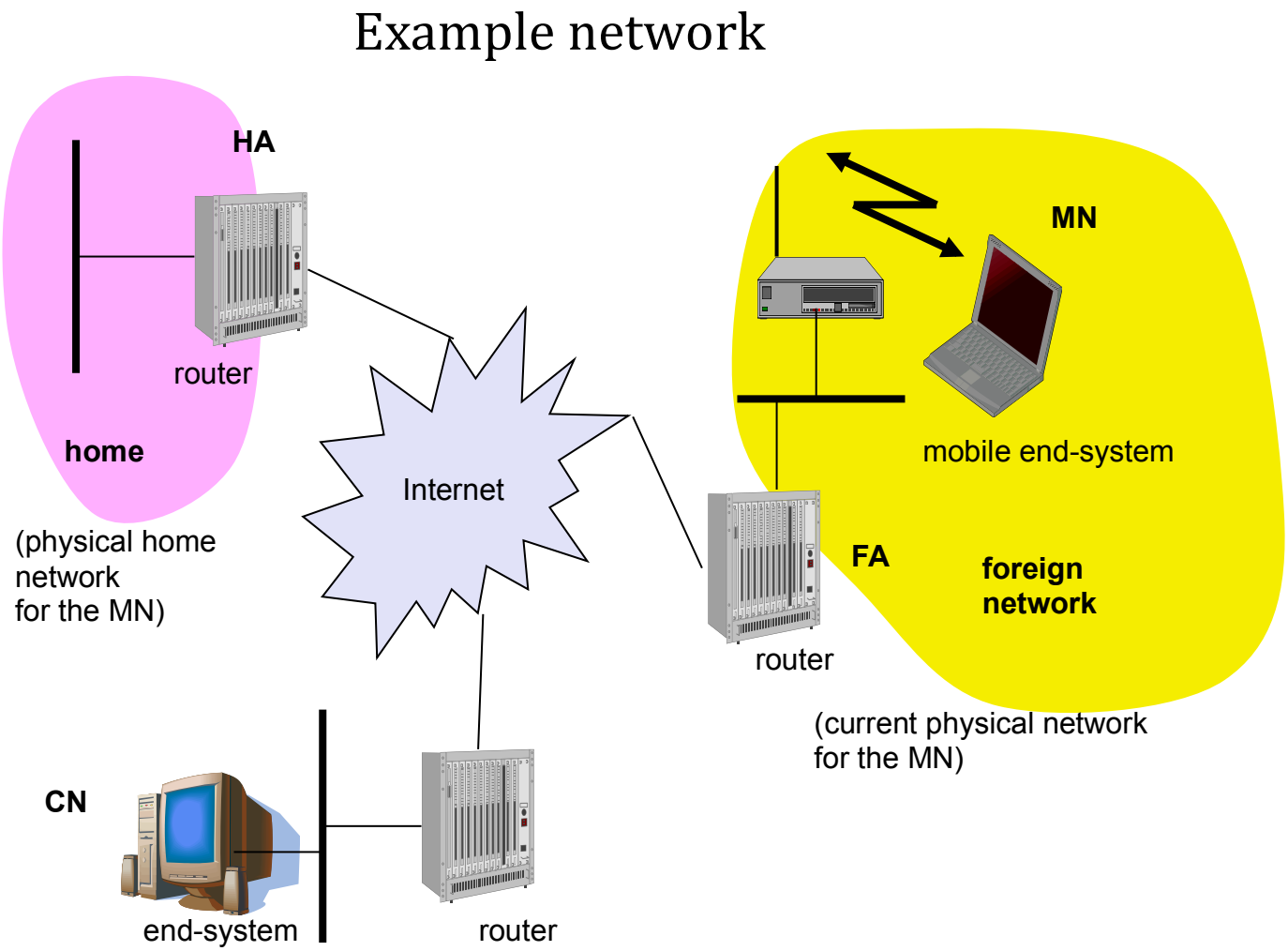
Mobile Computing

Unit-II

Mobil IP

- was proposed by IETF – Internet Engineering Task Force
- allows mobile computers to stay connected to the Internet regardless of their location and without having to continually change their IP address
- standard protocol that extends the IP by making mobility transparent to applications and to higher level protocols likeTCP
- traditional IP does not supports user mobility
- to enable users to keep the same IP address while travelling to different networks



Terminology

- **Mobile Node (MN)**
  - End-system (node/ handheld equipment with roaming capabilities) or router that change its point of attachment to the internet using mobile IP without changing its IP address
- **Correspondent Node (CN)**
  - communication partner for the MN & can be a fixed or mobile node
- **Home network**
  - Network within which the device receives its identifying IP address
  - subnet the MN belongs to with respect to its IP address.
  - No mobile IP support is needed within the home network.
- **Home agent (HA)**
  - provides several services for the MN and is located in the home network.
  - the tunnel for packets toward the MN starts at the HA.
  - The HA maintains a location registry, i.e., it is informed of the MN's location by the current COA.

  Three alternatives for the implementation of an HA exist.

  a) **The HA can be implemented on a router that is responsible for the home network.**

  This is obviously the best position, because without optimizations to mobile IP, all packets for the MN have to go through the router anyway.

  b) **If changing the router's software is not possible, the HA could also be implemented on an arbitrary node in the subnet.**

  disadvantage of this solution: the double crossing of the router by the packet if the MN is in a foreign network. A packet for the MN comes in via the router; the HA sends it through the tunnel which again crosses the router.

  c) **A home network is not necessary at all.**

  The HA could be again on the 'router' but this time only acting as a manager for MNs belonging to a virtual home network. All MNs are always in a foreign network with this solution.
- **Foreign network**
  - current subnet the MN visits and which is not the home network.
- **Foreign Agent (FA)**
  - Router in a foreign network that functions as the point of attachment for a mobile node (MN) when it roams to the foreign network
  - can provide several services to the MN during its visit to the foreign network.

- can have the COA, acting as tunnel endpoint and forwarding packets to the MN.
- can be the default router for the MN.
- can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.
- are not necessarily needed for mobile IP functioning.
- implemented on a router for the subnet the MN attaches to.

- **Care-of address (COA):**
  - defines the current location of the MN from an IP point of view.
  - All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN.
  - Packet delivery toward the MN is done using a tunnel.
  - COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel.
  - typically associated with the mobile node's foreign agent (FA)

There are two different possibilities for the location of the COA:

Foreign agent COA

- ❑ The COA could be located at the FA, i.e., the COA is an IP address of the FA.
- ❑ The FA is the tunnel end-point and forwards packets to the MN.
- ❑ Many MN using the FA can share this COA as common COA.

Co-located COA:

- ❑ The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. → This address is now topologically correct, and the tunnel endpoint is at the MN.
- ❑ Co-located addresses can be acquired using services such as DHCP.
- ❑ **One problem associated with this approach:** The need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

Tunnel – path taken by the encapsulated packets

Tunneling - Packet is forwarded by home agent to foreign agent. When packet comes to the foreign agent (COA) it delivers packet to mobile node.

Tunnelling involves 2 primary functions:

Encapsulation of the data packet to reach the tunnel endpoint and

Decapsulation when the packet is delivered at that end point

IP packet delivery

Eg. packet delivery to and from the MN

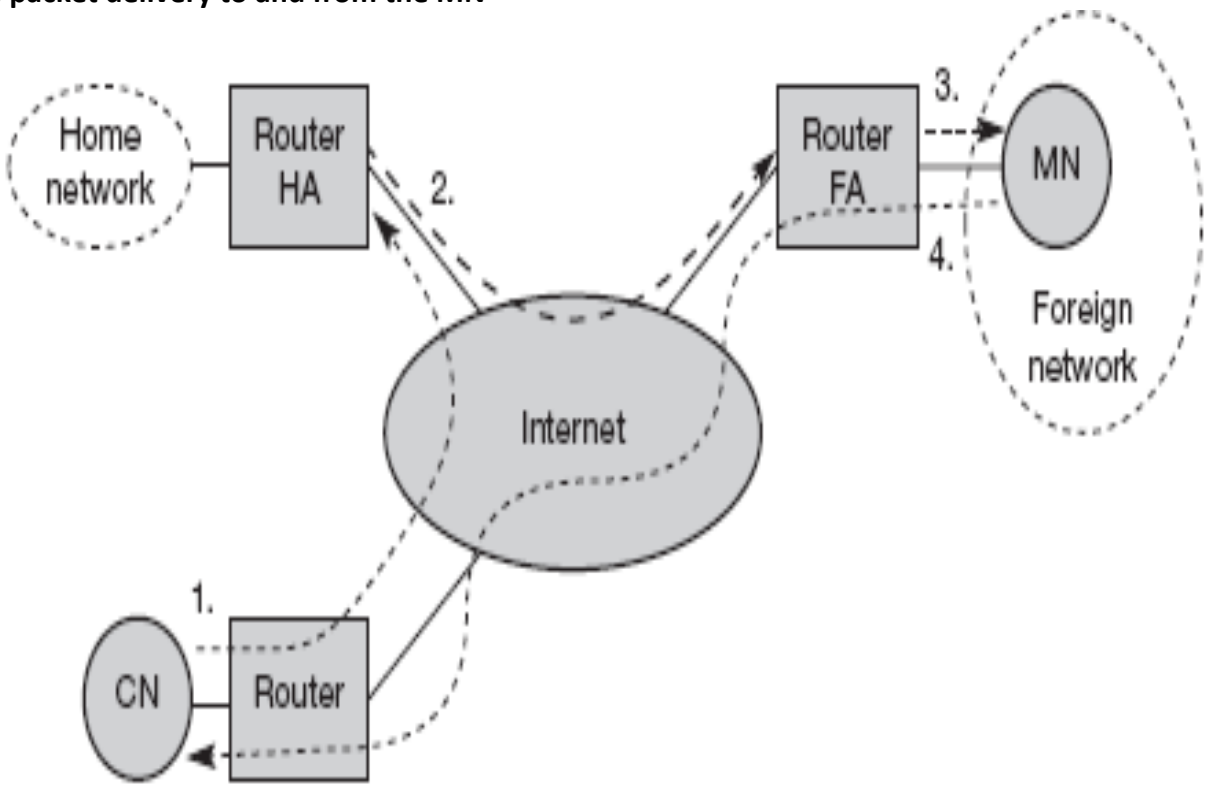


Figure: Packet delivery to and from the mobile node

CN wants to send an IP packet to the MN.

One of the requirements of mobile IP was to support hiding the mobility of the MN.

Step 1:

CN does not need to know anything about the MN's current location and **sends an IP packet** with MN as a destination address and CN as a source address

The internet, not having information on the current location of MN, **routes the packet to the router responsible for the home network of MN.** This is done using the standard routing mechanisms of the internet.

Step 2:

- HA now intercepts the packet, knowing that MN is currently not in its home network.

- The packet is not forwarded into the subnet as usual, but **encapsulated and tunnelled to the COA.**

- A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet

Step 3:

- foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN

Again, for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network.

Sending packets from the MN to the CN

Step 4:

- **MN sends the packet** as usual with its own fixed IP address as source and CN's address as destination

- **router with the FA acts as default router and forwards the packet** in the same way as it would do for any other node in the foreign network.

- **If CN is a fixed node** the remainder is in the fixed internet as usual.

- **If CN were also a mobile node** residing in a foreign network, the same mechanisms as described in steps 1 through 3 would apply now in the other direction.

Agent discovery

Problem of an MN after moving :

how to find a foreign agent?

How does the MN discover that it has moved?

For this purpose mobile IP describes two methods:

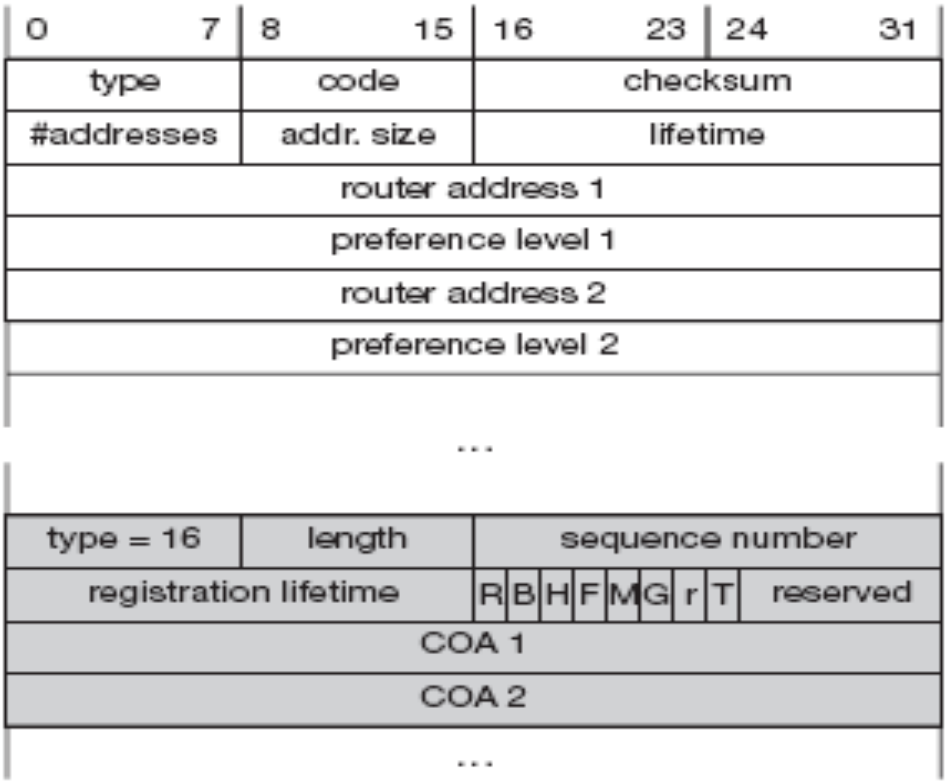
1. Agent advertisement and
2. Agent solicitation

1. Agent Advertisement

- HA and FA periodically send advertisement messages into their physical subnets
- Advertisement messages can be seen as a beacon broadcast into the subnet.
- Advt msg lists one or more COAs and a flag indicating whether it is a home agent or a foreign agent
- For these advertisements Internet control message protocol (ICMP) messages according to RFC 1256 are used with some mobility extensions.
- Routers in the fixed network implementing this standard also advertise their routing service periodically to the attached links.
- MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
- MN reads a COA from the FA advertisement messages

Agent advertisement packet (RFC 1256 + mobility extension)

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



Fields in the ICMP part :

Type - is set to 9,

Code - can be 0, if the agent also routes traffic from non-mobile nodes, or 16, if it does not route anything other than mobile traffic.

Foreign agents are at least required to forward packets from the mobile node.

#addresses - the number of addresses advertised with this packet

Lifetime - denotes the length of time this advertisement is valid.

Preference levels for each address - help a node to choose the router that is the most eager one to get a new node.

Extension for mobility has the following fields:

Type - is set to 16,

length - depends on the number of COAs provided with the message and equals 6 + 4*(number of addresses). An agent shows the total number of advertisements sent since initialization in the sequence number.

Registration lifetime: the agent can specify the maximum lifetime in seconds a node can request during registration

The following bits specify the characteristics of an agent in detail.

R bit (registration) - shows, if a registration with this agent is required even when using a colocated COA at the MN.

B bit – is set if the agent is currently too busy to accept new registrations

H and F bit - denote if the agent offers services as a home agent (H) or foreign agent (F) on the link where the advertisement has been sent.

Bits M and G - specify the method of encapsulation used for the tunnel.

M - can specify minimal encapsulation and

G - generic routing encapsulation while IP-in-IP encapsulation is the mandatory standard

r - is set to zero and must be ignored.

Field **T - indicates that reverse tunneling is** supported by the FA.

The following fields contain the **COAs advertised.**

A foreign agent setting the F bit must advertise at least one COA.

A mobile node in a subnet can now receive agent advertisements from either its home agent or a foreign agent.

This is one way for the MN to discover its location.

Agent solicitation

- MN must send **agent solicitations i**f no agent advertisements are present or the inter-arrival time is too high, and an MN has not received a COA by other means
- Ensure that these solicitation messages do not flood the network, but basically an MN can search for an FA endlessly sending out solicitation messages.
- A mobile node can send out three solicitations, one per second, as soon as it enters a new network.
- In highly dynamic wireless networks with moving MNs and probably with applications requiring continuous packet streams even one second intervals between solicitation messages might be too long.
- Before an MN even gets a new address many packets will be lost without additional mechanisms.

- A node must decrease the rate of solicitations exponentially to avoid flooding the network until it reaches a maximum interval between solicitations (one minute), if a node does not receive an answer to its solicitations
- Discovering a new agent can be done anytime, not just if the MN is not connected to one.
- MN is looking for a better connection while still sending via the old path.
- After these steps of advertisements or solicitations the MN can now receive a COA, either one for an FA or a co-located COA.
- The MN knows its location (home network or foreign network) and the capabilities of the agent
- The next step for the MN is the registration with the HA if the MN is in a foreign network.

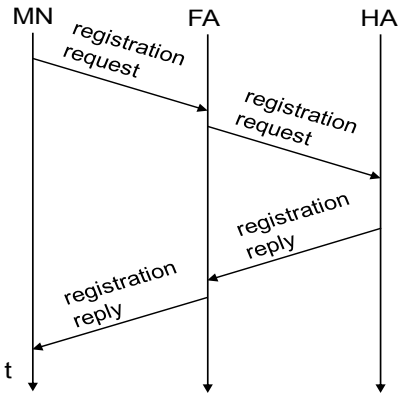
Registration

- MN has to register with the HA after having received a COA.
- Main purpose of the registration - To inform the HA of the current location for correct forwarding of packets.
- Registration can be done in two different ways depending on the location of the COA.

1) COA is at FA:

- MN sends its registration request containing the COA to the FA which is forwarding the request to the HA.
- HA now sets up a **mobility binding containing the mobile node's home IP address and the current** COA.
- Mobility binding contains - the lifetime of the registration which is negotiated during the registration process.
- Registration expires automatically after the lifetime and is deleted; so, an MN should reregister before expiration.
- This mechanism is necessary to avoid mobility bindings which are no longer used. After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN.

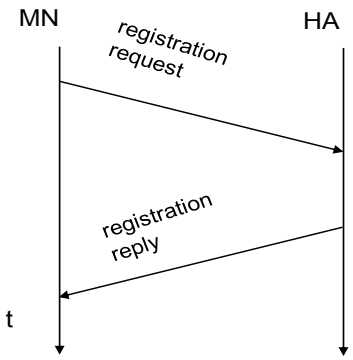
Registration



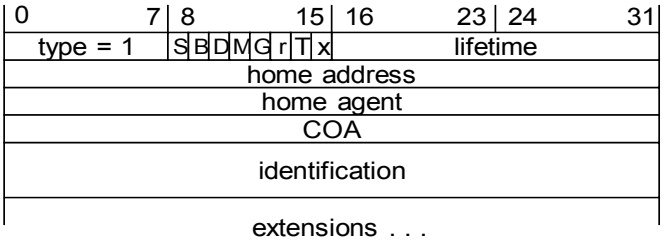
COA is at FA

2) COA is co-located:

- MN may send the request directly to the HA and vice versa.
- also the registration procedure for MNs returning to their home network.
- if the MN received an agent advertisement from the FA it should register via this FA if the R bit is set in the advertisement.



Mobile IP registration request



S: simultaneous bindings
B: broadcast datagrams
D: decapsulation by MN
M mininal encapsulation
G: GRE encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored

UDP packets are used for registration requests.

IP source address of the packet - interface address of the MN,
IP destination address - FA or HA (depending on the location of the COA).

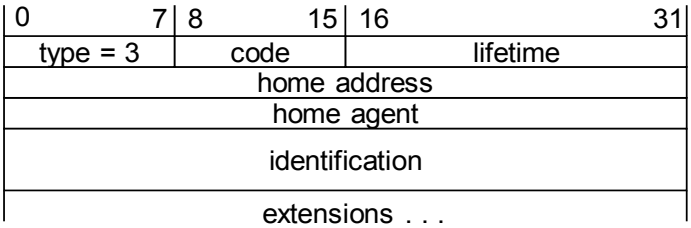
The UDP destination port is set to 434.

UDP is used because of low overheads and better performance compared to TCP in wireless environments.

The fields are defined as follows:
type - is set to 1 for a registration request.
S bit - an MN can specify if it wants the HA to retain prior mobility bindings. This allows for simultaneous bindings.

The following bits denote the requested behavior for packet forwarding.
B bit - indicates that an MN also wants to receive the broadcast packets which have been received by the HA in the home network.
D bit - if an MN uses a co-located COA, it takes care of the decapsulation at the tunnel endpoint.
M and G - denote the use of minimal encapsulation or generic routing encapsulation, respectively.
T - indicates reverse tunneling,
r and x are set to zero.

Mobile IP registration reply



Registration reply - is conveyed in a UDP packet, contains:

type field - set to 3 and

code - indicating the result of the registration request.

lifetime field - indicates how many seconds the registration is valid if it was successful.

Home address and home agent - addresses of the MN and the HA, respectively.

64-bit identification - used to match registration requests with replies. (value is based on the identification field from the registration and the authentication method)

extensions - must at least contain parameters for authentication.

Lifetime - denotes the validity of the registration in seconds.
A value of zero - indicates deregistration;
all bits set - indicates infinity.

Home address - fixed IP address of the MN,

home agent - IP address of the HA, and

COA - represents the tunnel endpoint.

64 bit **identification -** generated by the MN to identify a request and match it with registration replies. - used for protection against replay attacks of registrations.

extensions - must at least contain parameters for authentication.

Example codes:

registration successful

0 registration accepted

1 registration accepted, but simultaneous mobility bindings unsupported

registration denied by FA

65 administratively prohibited

66 insufficient resources

67 mobile node failed authentication

68 home agent failed authentication

69 requested Lifetime too long

registration denied by HA

129 administratively prohibited

131 mobile node failed authentication

133 registration Identification mismatch

135 too many simultaneous mobility bindings

Tunneling and encapsulation

Tunnel - establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.

Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.

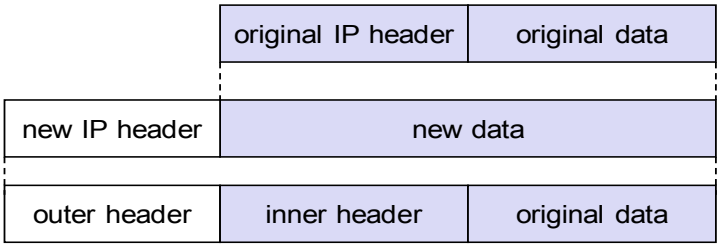
Tunneling - sending a packet through a tunnel, is achieved by using encapsulation.

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

The reverse operation, taking a packet out of the data part of another packet, is called **decapsulation.**

Encapsulation and decapsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively.

IP Encapsulation



HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sets the new IP header in such a way that the packet is routed to the COA.

The new header is also called the **outer header** for obvious reasons.

inner header - can be identical to the original header as this is the case for IP-in-IP encapsulation, or the inner header can be computed during encapsulation.

IP-in-IP Encapsulation

- Mandatory for mobile IP
- tunnel between HA and COA
- Encapsulation of one packet into another as payload
  - e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
  - here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*IP-in-IP*		IP checksum
IP address of HA			
Care-of address COA			
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			

The fields of the outer header are set as follows:

ver is 4 - for IP version 4,

Internet header length (IHL) - denotes the length of the outer header in 32 bit words.

DS(TOS) - copied from the inner header,

Length - covers the complete encapsulated packet.

TTL - must be high enough so the packet can reach the tunnel endpoint.

IP-in-IP - type of the protocol used in the IP payload (this field is set to 4, the protocol type for IPv4 because again an IPv4 packet follows after this outer header).

IP checksum - calculated as usual.

tunnel entry - source address - the IP address of the HA and
tunnel exit point - destination address (COA).

Inner header remains almost unchanged during encapsulation, thus showing the original sender CN and the receiver MN of the packet.

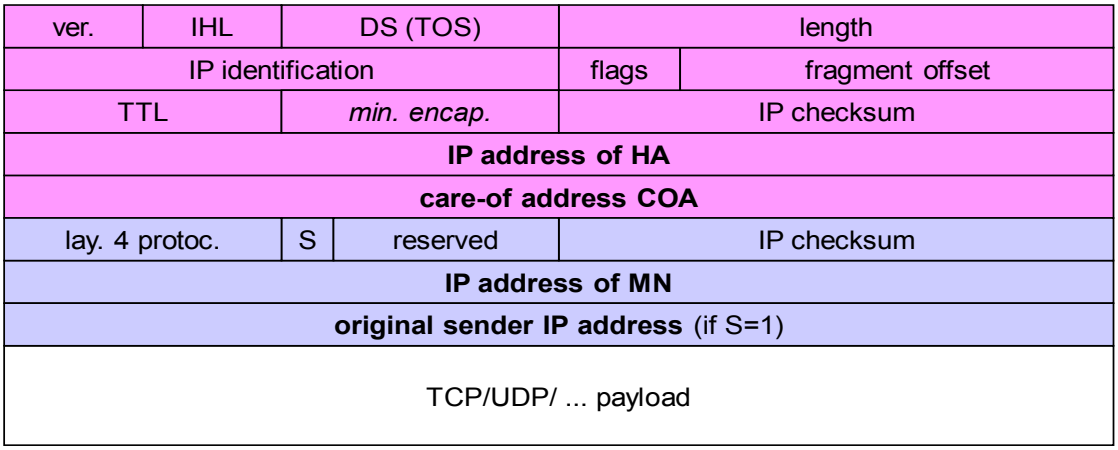
The only change is TTL which is decremented by 1.

- This means that the whole tunnel is considered a single hop from the original packet's point of view.
- MN to behave as if it were attached to the home network. No matter how many real hops the packet has to take in the tunnel, it is just one (logical) hop away for the MN.

Payload follows the two headers.

Minimal Encapsulation

- avoids repetition of identical fields
- optional encapsulation method for mobile IP
- e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
- only applicable for unfragmented packets, no space left for fragment identification



Inner header remains almost unchanged during encapsulation, thus showing the original sender CN and the receiver MN of the packet.

The only change is TTL which is decremented by 1.

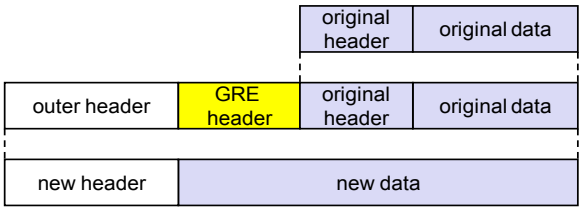
- This means that the whole tunnel is considered a single hop from the original packet's point of view.
- MN to behave as if it were attached to the home network. No matter how many real hops the packet has to take in the tunnel, it is just one (logical) hop away for the MN.

Payload follows the two headers.

Generic Routing Encapsulation (GRE)

- supports other network layer protocols in addition to IP.
- allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.
  - The packet of one protocol suite with the original packet header and data is taken and a new GRE header is prepended.
  - Together this forms the new data part of the new packet.
  - Finally, the header of the second protocol suite is put in front.

Generic Routing Encapsulation



RFC 1701

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*GRE*	IP checksum	
IP address of HA			
Care-of address COA			
C R K S s rec.	rsv.	ver.	protocol
checksum (optional)		offset (optional)	
key (optional)			
sequence number (optional)			
routing (optional)			
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			

RFC 2784

C	reserved0	ver.	protocol
checksum (optional)			reserved1 (=0)

Optimization of packet forwarding

- Triangular Routing
  - sender sends all packets via HA to MN
  - higher latency and network load
- "Solutions"
  - sender learns the current location of MN
  - direct tunneling to this location
  - HA informs a sender about the location of MN
  - big security problems!
- Change of FA
  - packets on-the-fly during the change can be lost
  - new FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
  - this information also enables the old FA to release resources for the MN

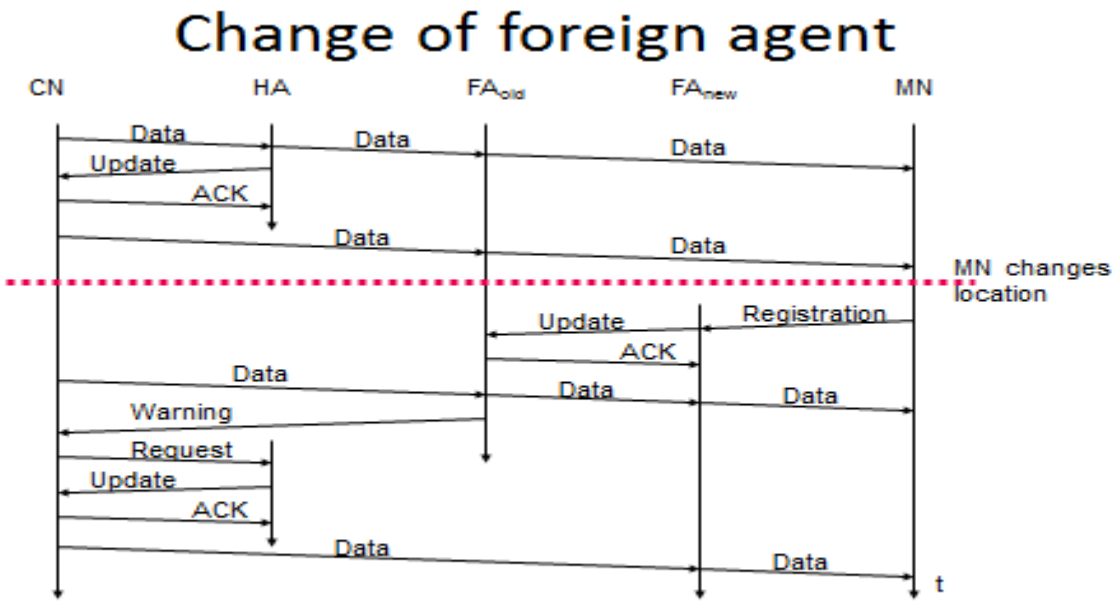
The optimized mobile IP protocol needs four additional messages.

- **Binding request:** Any node that wants to know the current location of an MN can send a binding request to the HA. The HA can check if the MN has allowed dissemination of its current location. If the HA is allowed to reveal the location it sends back a binding update.

- **Binding update:** This message sent by the HA to CNs reveals the current location of an MN. The message contains the fixed IP address of the MN and the COA. The binding update can request an acknowledgement.

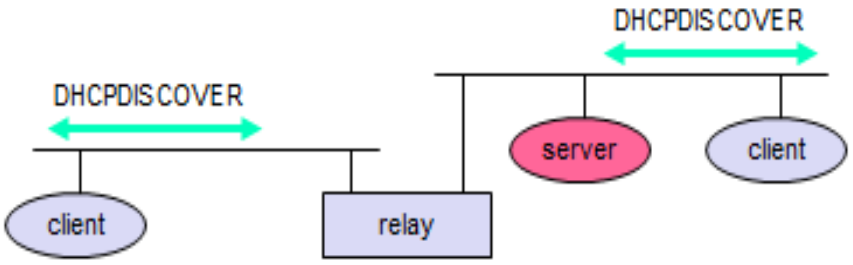
- **Binding acknowledgement**: If requested, a node returns this acknowledgement after receiving a binding update message.

- **Binding warning:**
  - If a node decapsulates a packet for an MN, but it is not the current FA for this MN, this node sends a binding warning.
  - The warning contains MN's home address and a target node address, i.e., the address of the node that has tried to send the packet to this MN.
  - The recipient of the warning then knows that the target node could benefit from obtaining a fresh binding for the MN.
  - The recipient can be the HA, so the HA should now send a binding update to the node that obviously has a wrong COA for the MN.



DHCP: Dynamic Host Configuration Protocol

- Application
  - simplification of installation and maintenance of networked computers
  - supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
  - enables automatic integration of systems into an Intranet or the Internet, can be used to acquire a COA for Mobile IP
- Client/Server-Model
  - the client sends via a MAC broadcast a request to the DHCP server (might be via a DHCP relay)



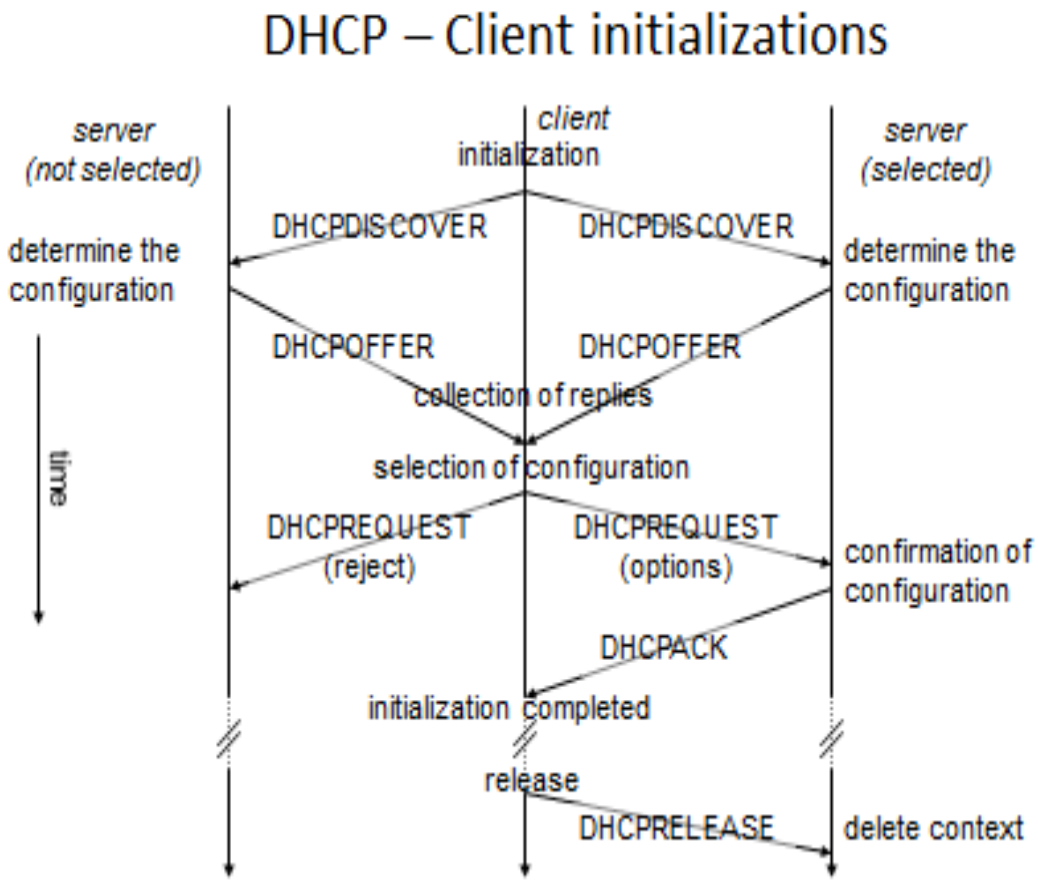
DHCP is an extension of BOOTP and compatible with it. For eg., if a host is running BOOTP, it can also request configuration from a DHCP server node. The importance of DHCP in a mobile computing environment is that it provides temporary IP addresses whenever a node moves from one network to another network

DHCP supports the following three important mechanisms for IP address allocation.

Automatic Allocation – DHCP assigns a permanent IP address to a particular client

Dynamic Allocation – DHCP assigns IP address to a client for a specific period of time

Manual Allocation – a Client's IP address is assigned by the network administrator, where the DHCP is used to inform the address assigned to clients



DHCP characteristics

- Server
  - several servers can be configured for DHCP, coordination not yet standardized (i.e., manual configuration)
- Renewal of configurations
  - IP addresses have to be requested periodically, simplified protocol
- Options
  - available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system)

- Big security problems!
  - no authentication of DHCP information specified