Mobile network layer

Overview

- IP packet delivery
- Agent discovery
- Tunneling and encapsulation

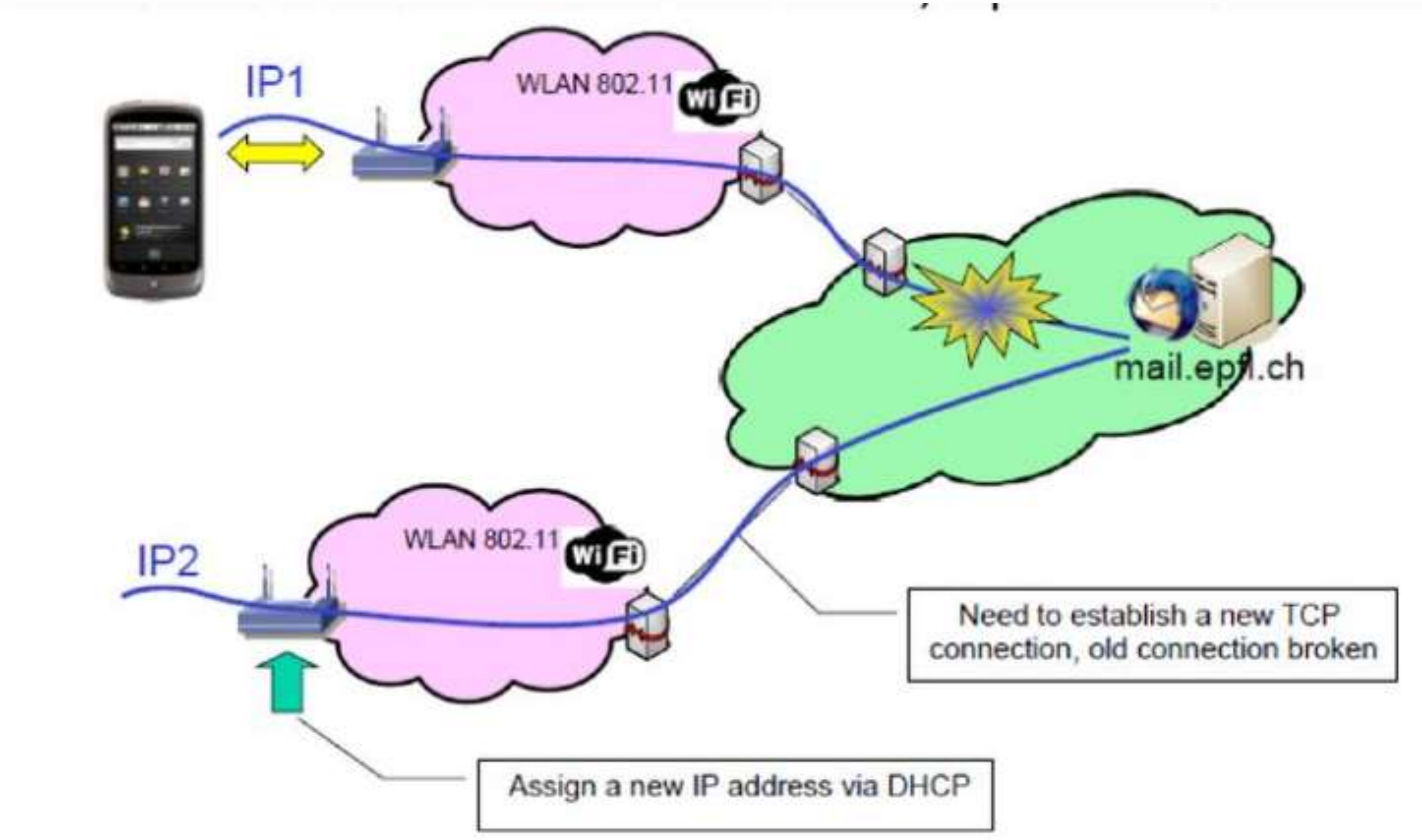
Introduction

- We will discuss about network layer to support mobility
- The most prominent example is Mobile IP, which adds mobility support to the internet network layer protocol IP
- While systems like GSM have been designed with mobility in mind, the internet started at a tie when no one had thought about mobile computers
- Today's internet lacks any mechanism to support users travelling around the world

Introduction

- A host sends an IP packet with the header containing a destination address with other fields
- The destination address not only determines the receiver of the packet but also the physical subnet of the receiver
- For example, the destination address : 129.13.42.99
- Routers in the internet now look at the destination address of incoming packets and forward them according to internal look-up tables

Introduction



Introduction

What is an IP ?

- A computer’s return address
- Each computer on the network has a unique set of numbers (0-255) in the form of

  XXX.XXX.XXX.XXX

- It can be static or dynamic

Introduction

Domain Name System (DNS)

- it is used to translate a host name to an IP address.
- A host sends a query to a server to obtain the IP address of a destination of which it only has the host name.

Motivation for Mobile IP

- Routing
  - based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
  - To avoid an explosion of routing tables, only prefixes are stored and further optimizations are applied.
  - change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables

Motivation for Mobile IP

- Specific routes to end-system ?
  - change of all routing table entries to forward packets to the right destination
  - does not scale with the number of mobile hosts and frequent changes in the location, security problems
- Changing the IP-address?
  - adjust the host IP address depending on the current location
  - Problem: nobody knows about this new address.
  - Almost impossible to find a mobile system, DNS updates take to long time
  - TCP connections break, security problems
    - TCP connection = {source IP, source port, destination IP, destination port}
    - TCP connection cannot survive any address change.

Evolution of Mobile IP

In standard IP, end host are in fixed physical location. So, if a host moves to another physical location, it has to change its IP address

Mobile IP allows hosts to stay connected to the internet regardless of their location

Mobile IP

- Mobile IP was created to allow users to KEEP THE SAME IP ADDRESS while travelling to a different network

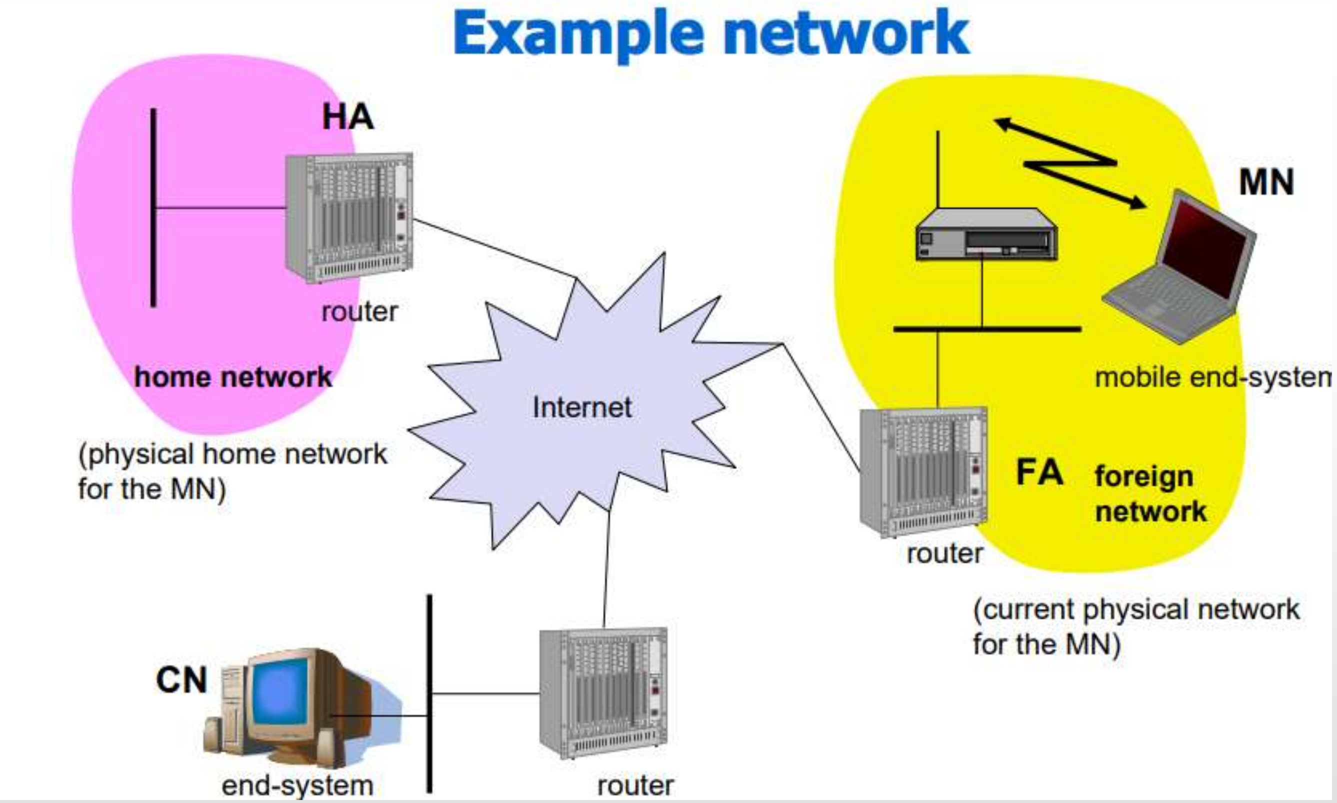
Requirements to Mobile IP

- Transparency
- Compatibility
- Security
- Efficiency and scalability

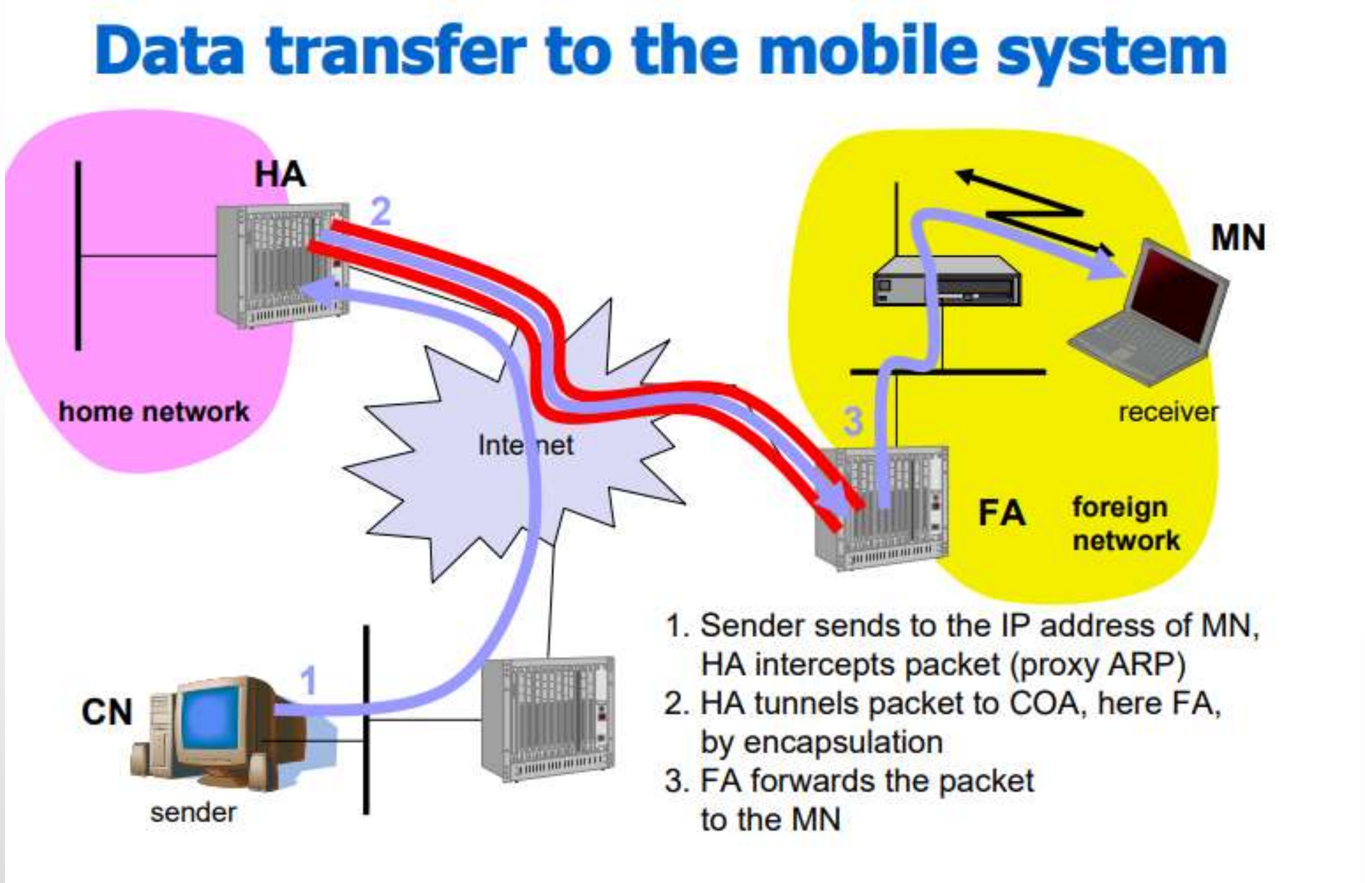
Terminology

- Mobile Node (MN)
- Correspondent Node (CN)
- Home network
- Foreign network
- Home Agent (HA
- Foreign Agent (FA)
- Care-of Address (COA)

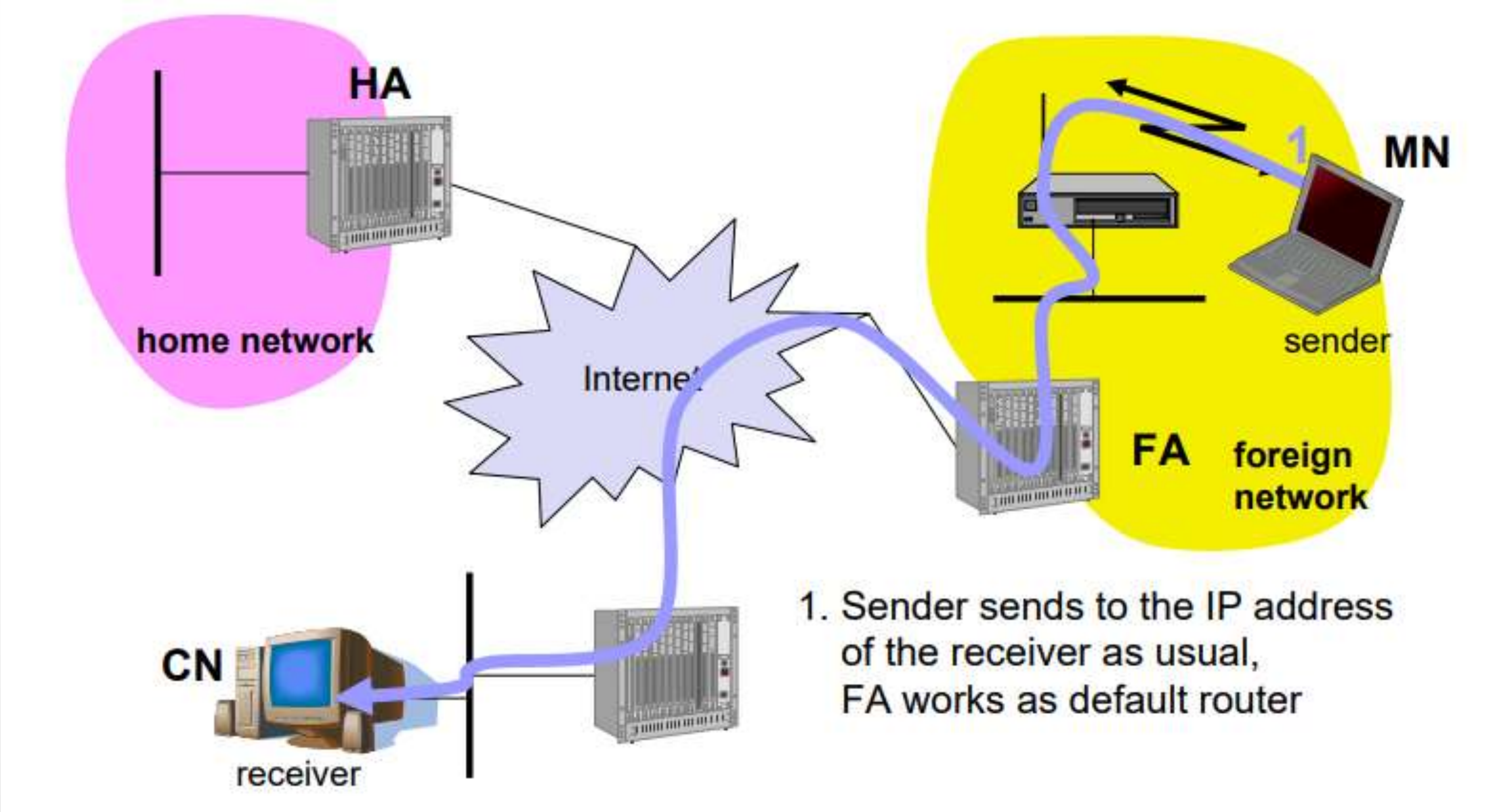
Terminology



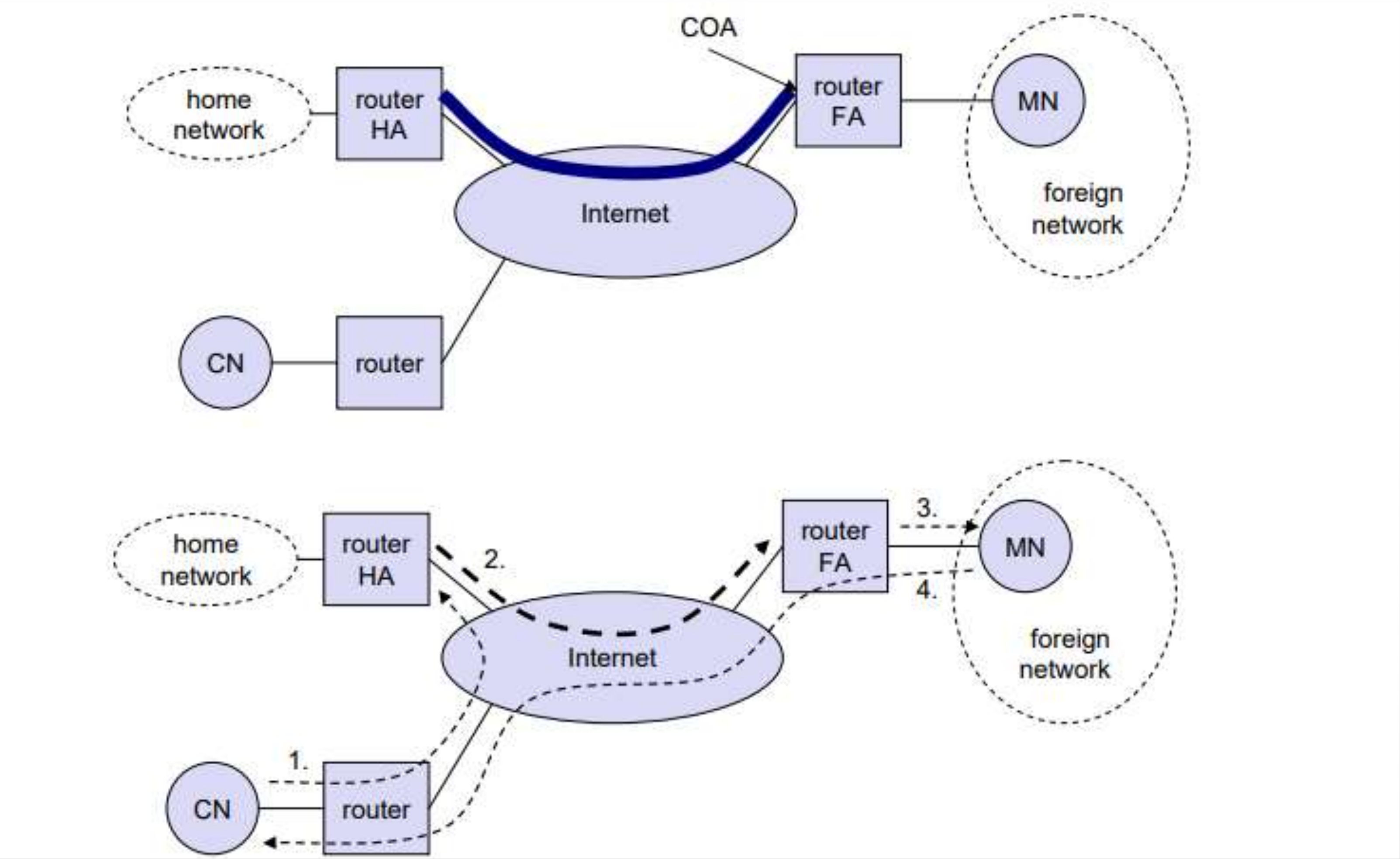
Terminology



Terminology



Terminology



Mobile IP Design Goals

- A mobile node must be able to communicate with other nodes after changing it's link-layer attachment, yet without changing its IP address
- A mobile node must be able to communicate with other nodes that do not implement mobile IP
- Mobile IP must use authentication to offer security against redirectment attacks
- The number of administrative messages should be small to save bandwidth & power
- Mobile IP must impose no additional constraints on the assignment of IP addresses

1. Agent Discovery

One initial problem of an MN after moving is how to find a foreign agent ?

- Two types of methods:
  - – Agent advertisement – in this HA and FA advertise their presence.
  - – Agent solicitation – the mobile node send agent solicitations messages.

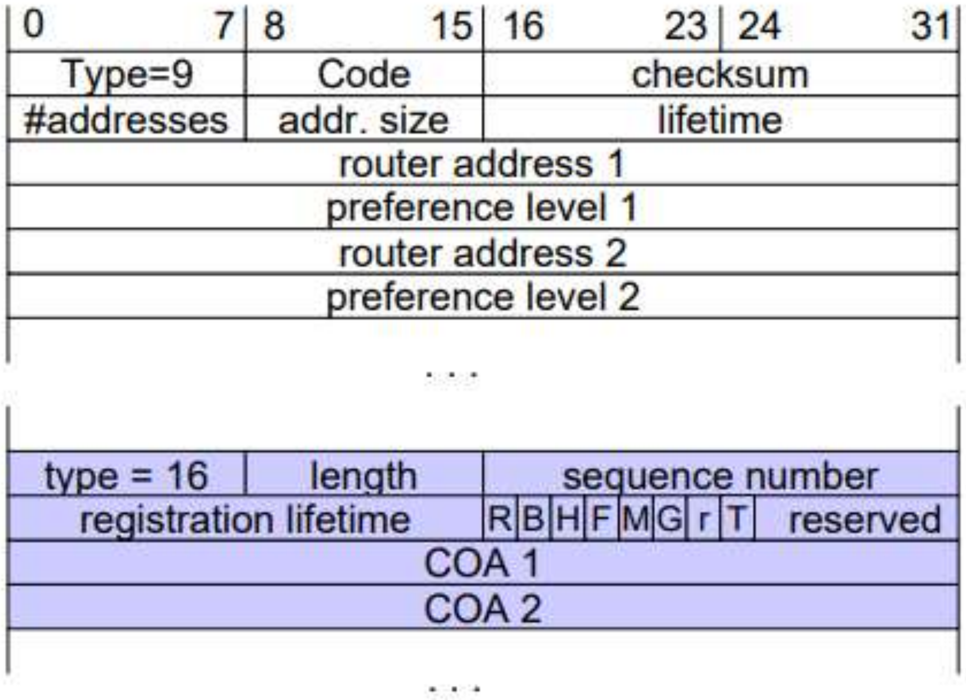
Agent advertisement

FA and HA advertise their presence periodically using special agent advertisement message.

● ICMP messages are used with some mobility extensions.

● Upper part represent ICMP while lower part represent extention needed for mobility.

Agent advertisement packet

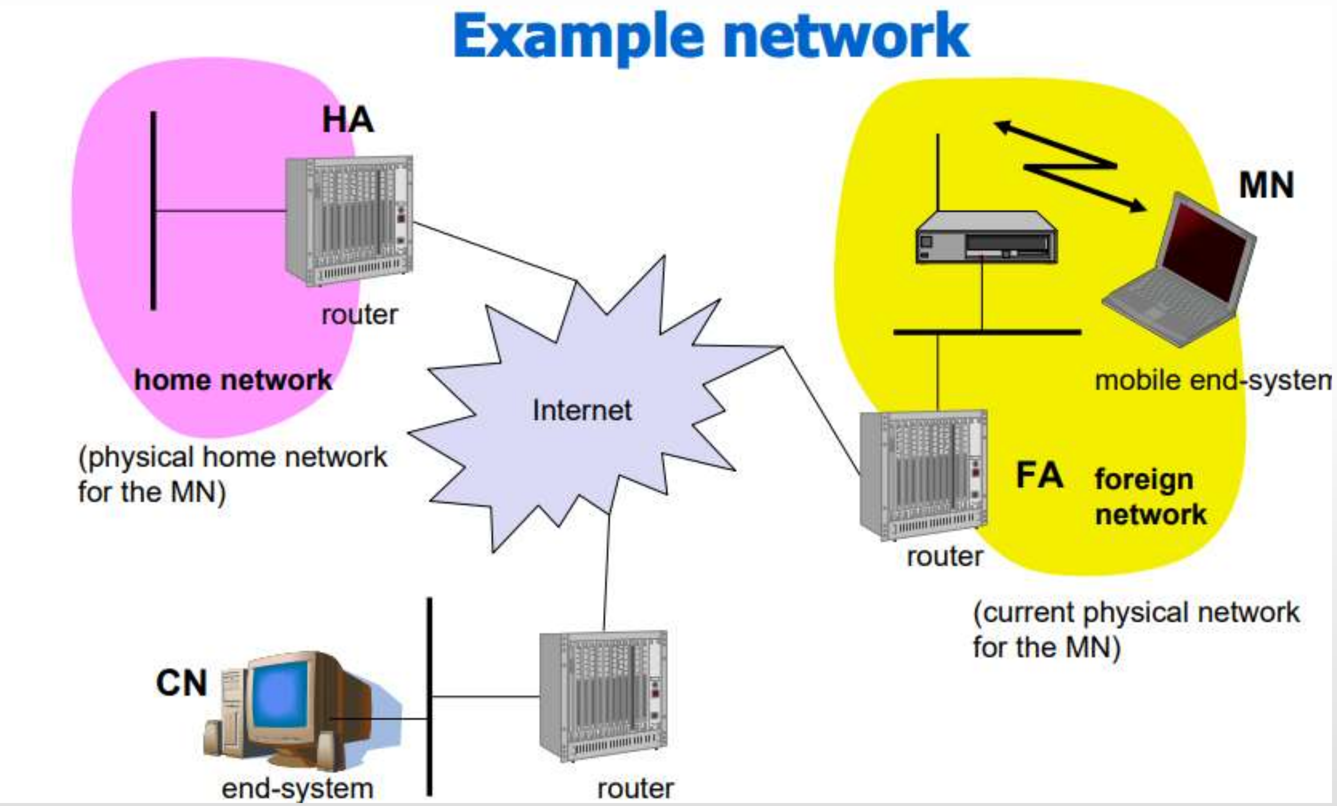


type = 16
length = 6 + 4 * #COAs
Lifetime: max lifetime in seconds
a node can request
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Agent Solicitation

- No agent advertisement
- Mobile node must send agent solicitations.
- Should not flood the network
- MN can send three solicitations messages. , one per sec. , as soon as enter in new network.
- Discovery of new agent can be done anytime.

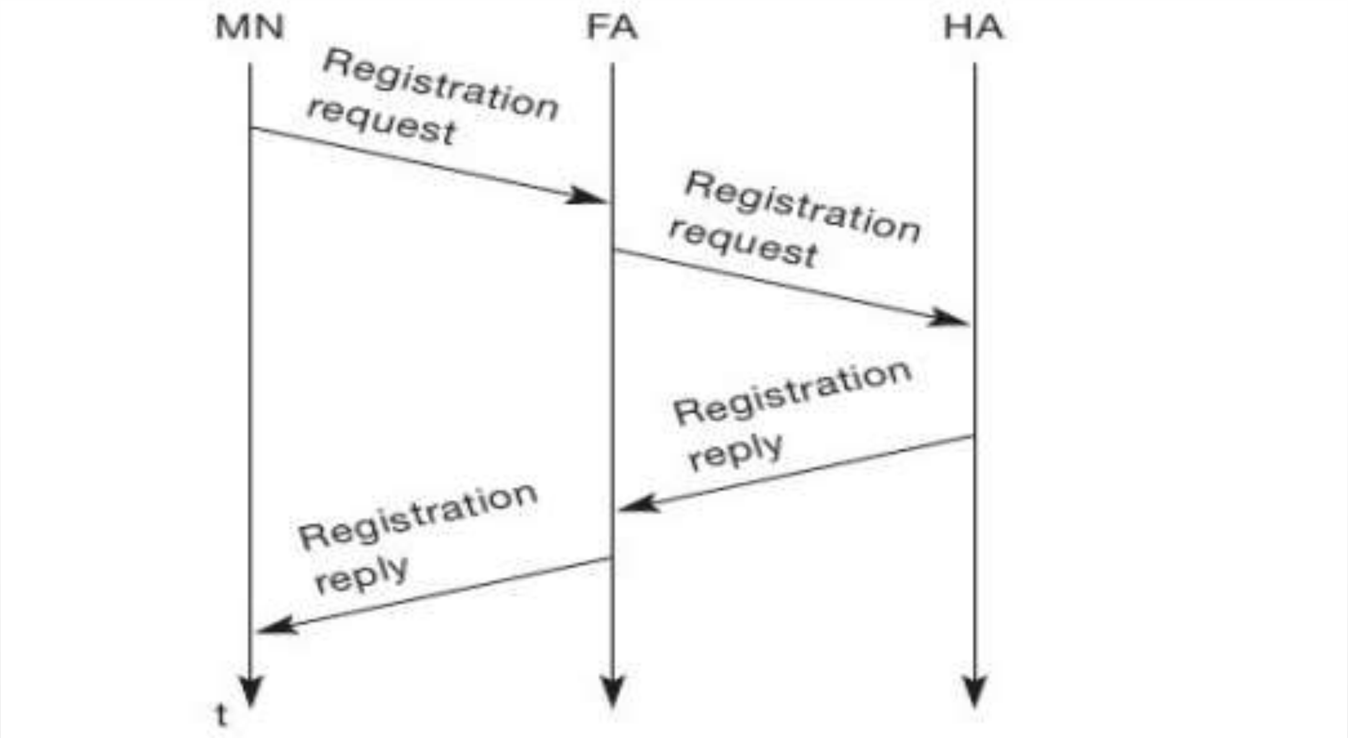
Recall Agent discovery



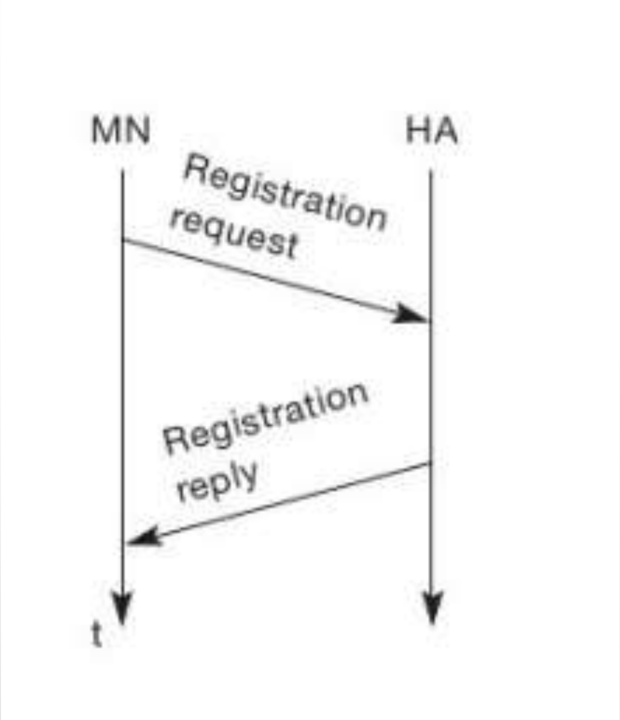
2. Registration

- Objective – is to inform the HA of the current location for correct forwarding of packets
- After receiving COA address the MN has to register with the HA.
- Registration can be done in two ways:-
  - Registration of mobile node via the FA
  - Or , directly with the HA

Registration (COA is the FA)



Registration (COA is co located)



Registration request

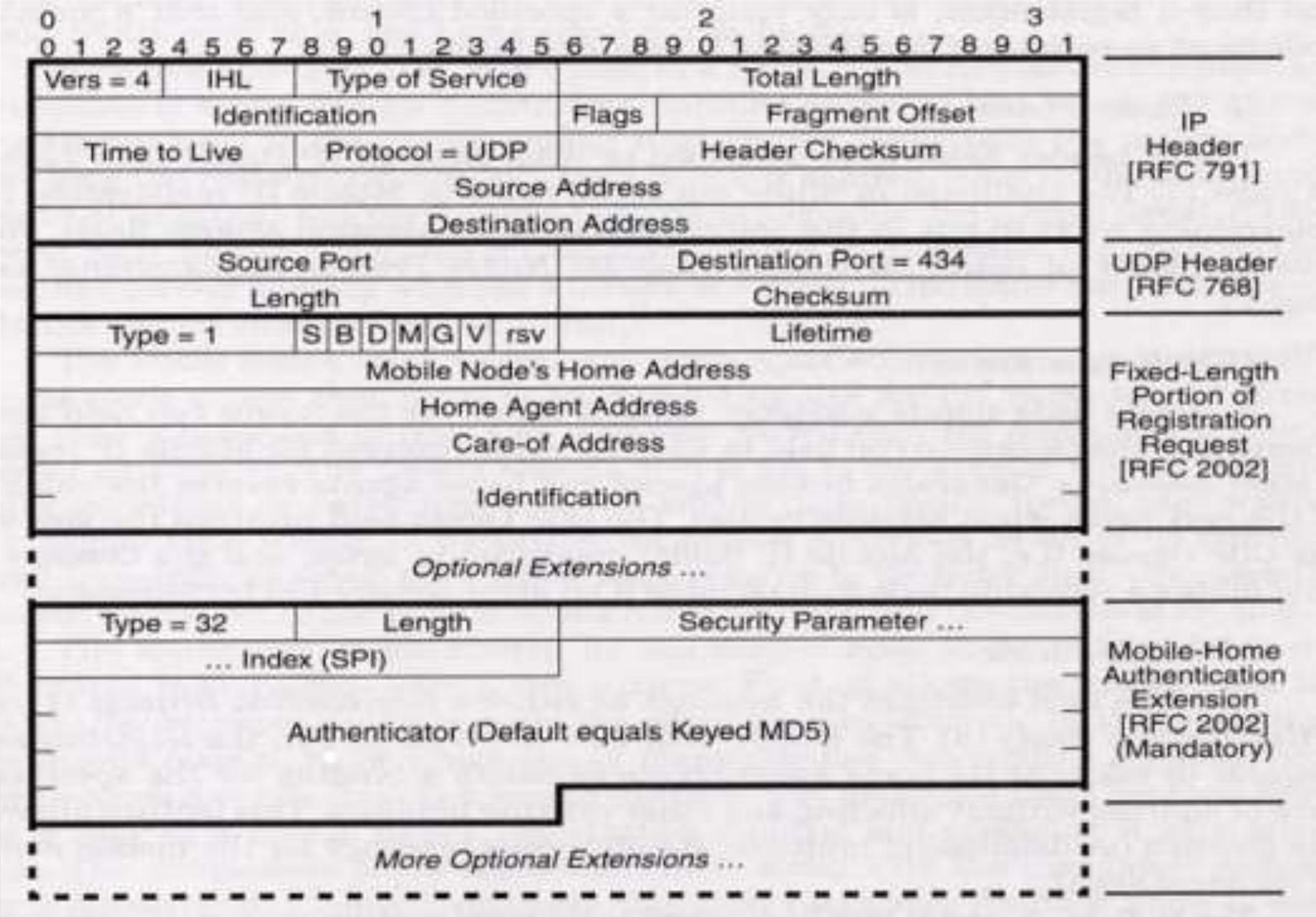


Figure 5-4 Registration Request Message

Registration Reply

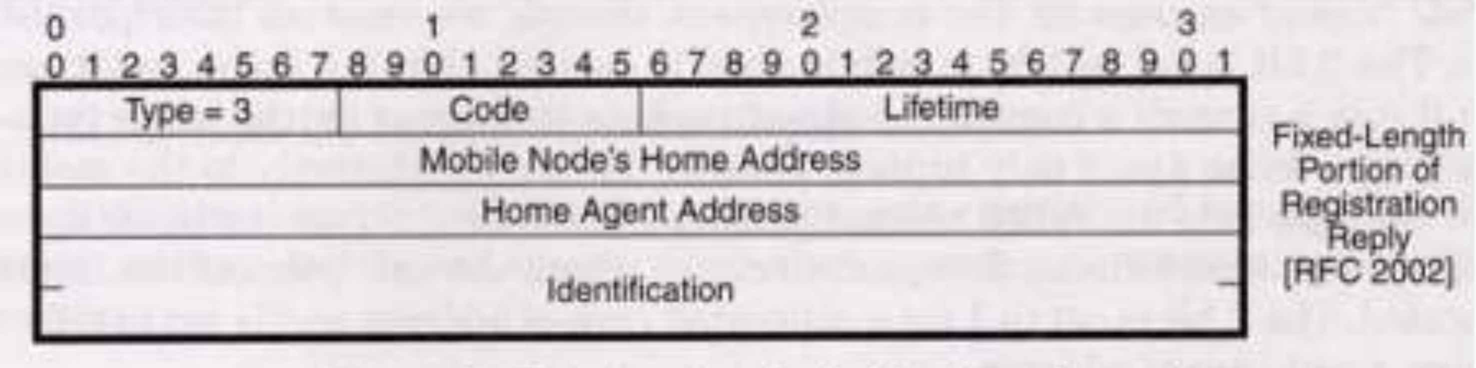
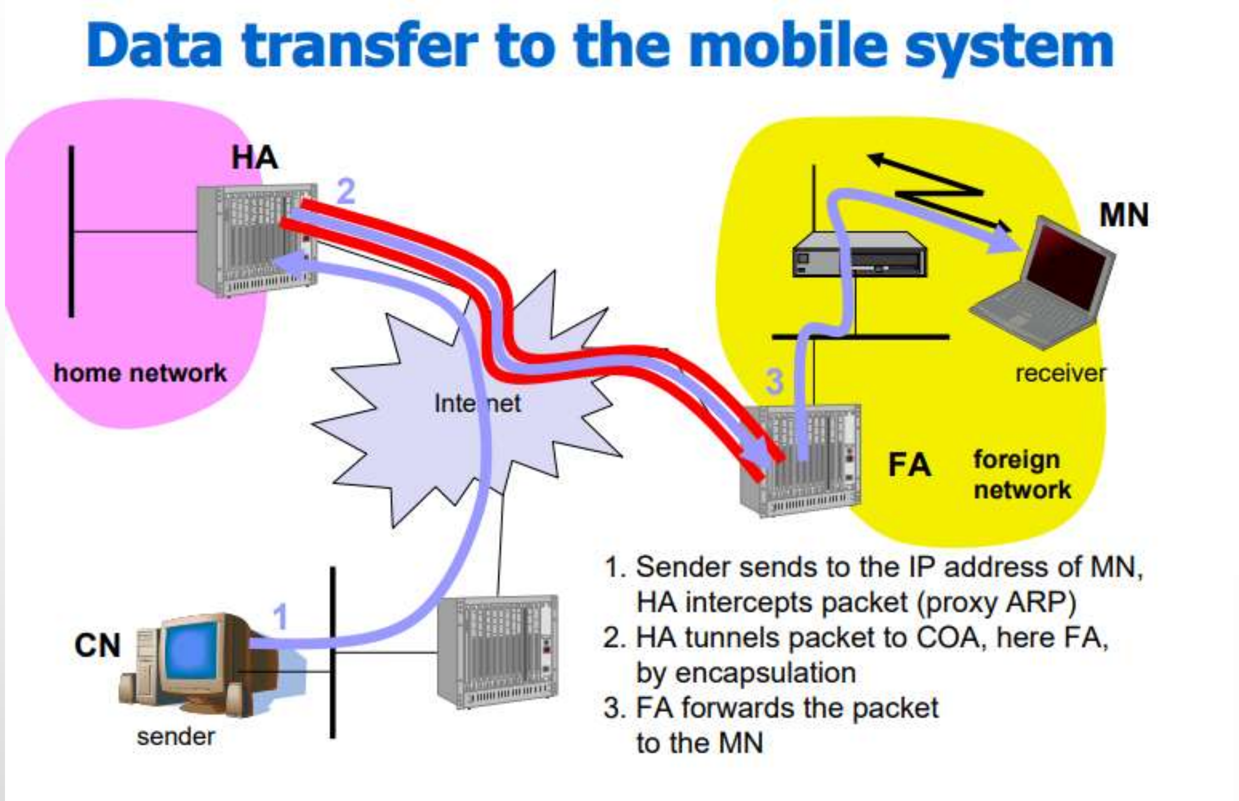


Figure 5-5 Registration Reply (fixed portion only)

Registration Reply

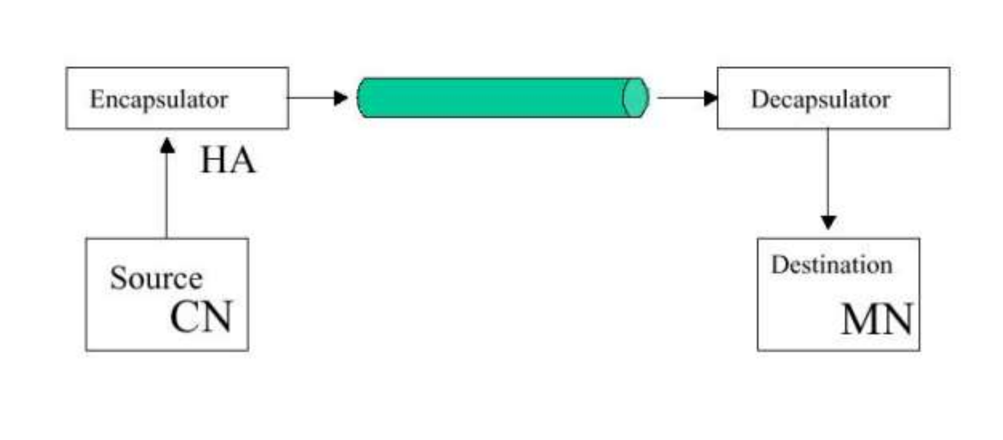
Registration	Code	Explanation
successful	0	registration accepted
	1	registration accepted, but simultaneous mobility bindings unsupported
denied by FA	65	administratively prohibited
	66	insufficient resources
	67	mobile node failed authentication
	68	home agent failed authentication
	69	requested lifetime too long
denied by HA	129	administratively prohibited
	130	insufficient resources
	131	mobile node failed authentication
	132	foreign agent failed authentication
	133	registration identification mismatch
	135	too many simultaneous mobility bindings

3. Tunneling


Data transfer to the mobile system
HA
2
home network
Inte net
MN
receiver
3
FA
foreign network
CN
1
sender
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

3. Tunneling

- Tunnel
  - Establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.
  - Tunneling is achieved by using encapsulation

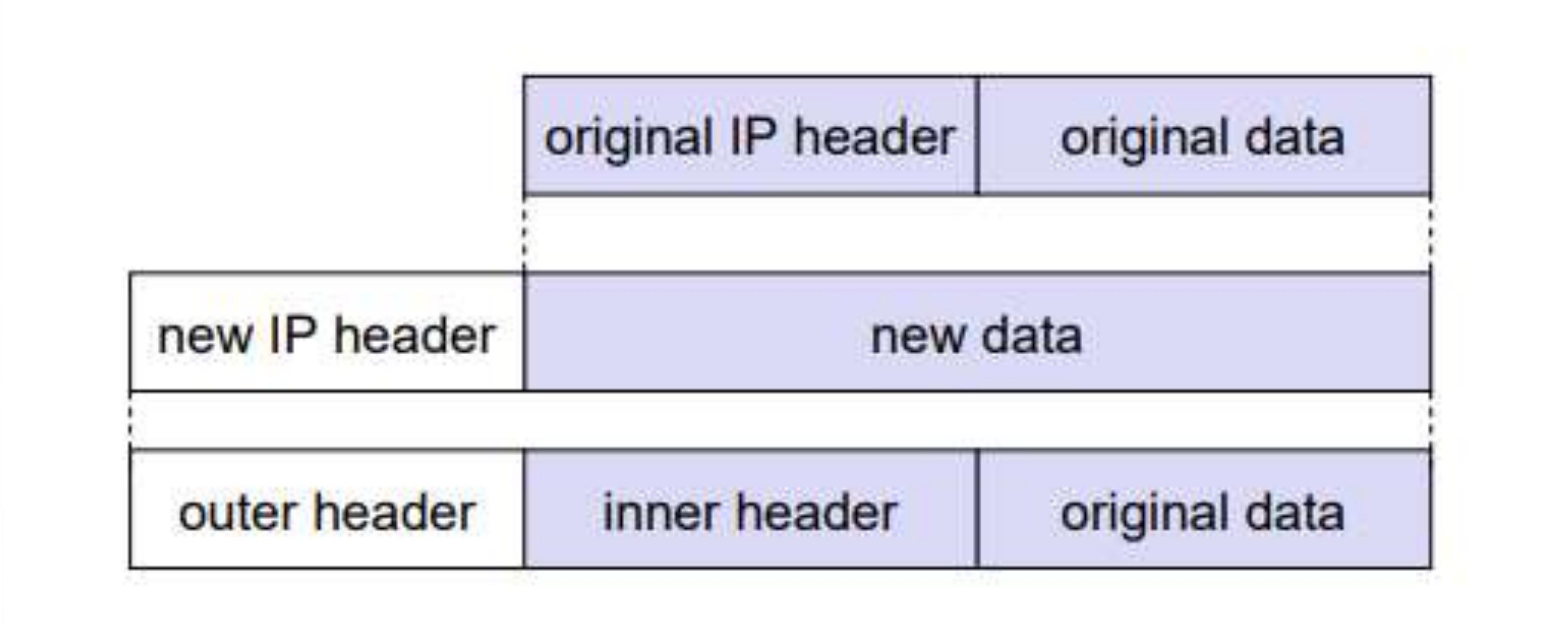


3. Tunneling

Encapsulation

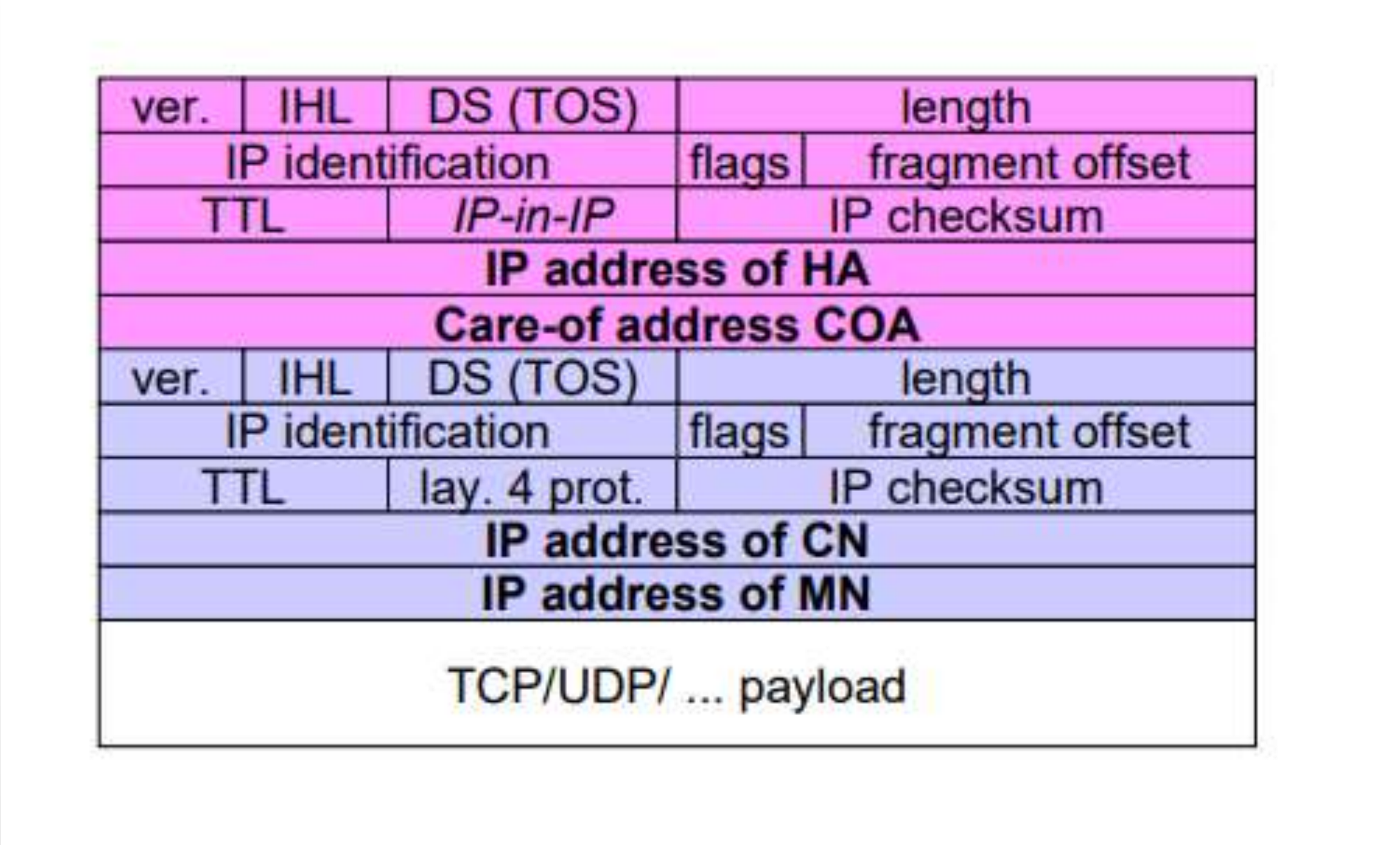
- Mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.
- Decapsulation: reverse operation
- Outer header: the new header
- IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)

3. Tunneling


original IP header
original data
new IP header
new data
outer header
inner header
original data

3. Tunneling

Encapsulation (IP – in – IP)



3. Tunneling

Encapsulation (IP – in – IP)

- The outer IP header source & destination address identify the tunnel endpoints (e.g., HA & FA).
- Outer protocol is ‘4’ (IP protocol)
- The inner IP header source address and destination address identify the original sender & recipient
- Other 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

3. Tunneling

Encapsulation (Minimal)

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