Mobile IP

IP

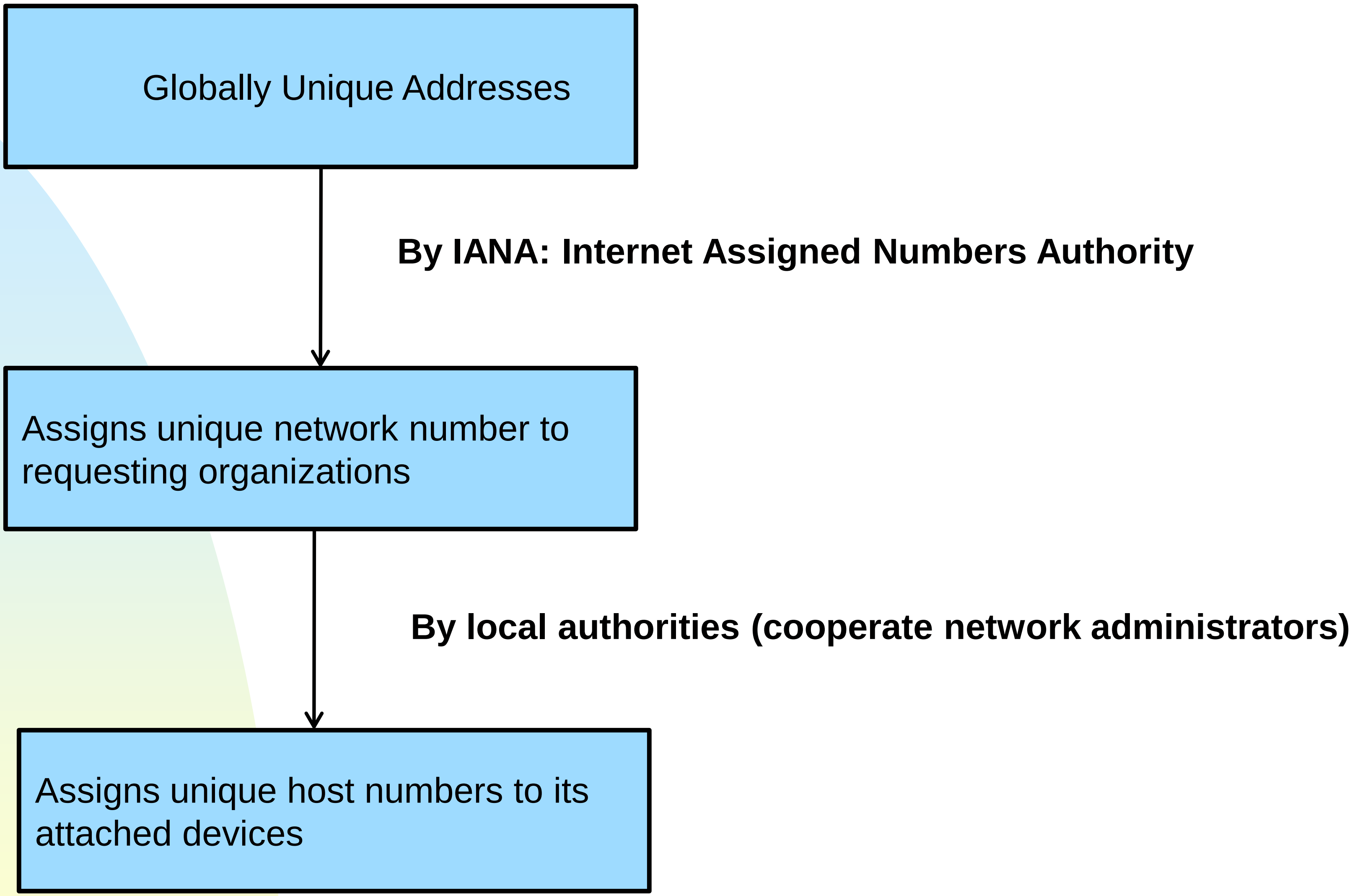
- Defines the addressing schemes for all TCP/IP devices
- Each TCP/IP network interface requires a unique IP addr
- IPv4: 32 bits long (2^32 = over 4B)

Internet → whole world's backbone network
→ IPv4 addressing scheme is gradually running out of gas.

IPv4 → organizes the networked world into a simple two-level hierarchy

- Network numbers
- Host numbers

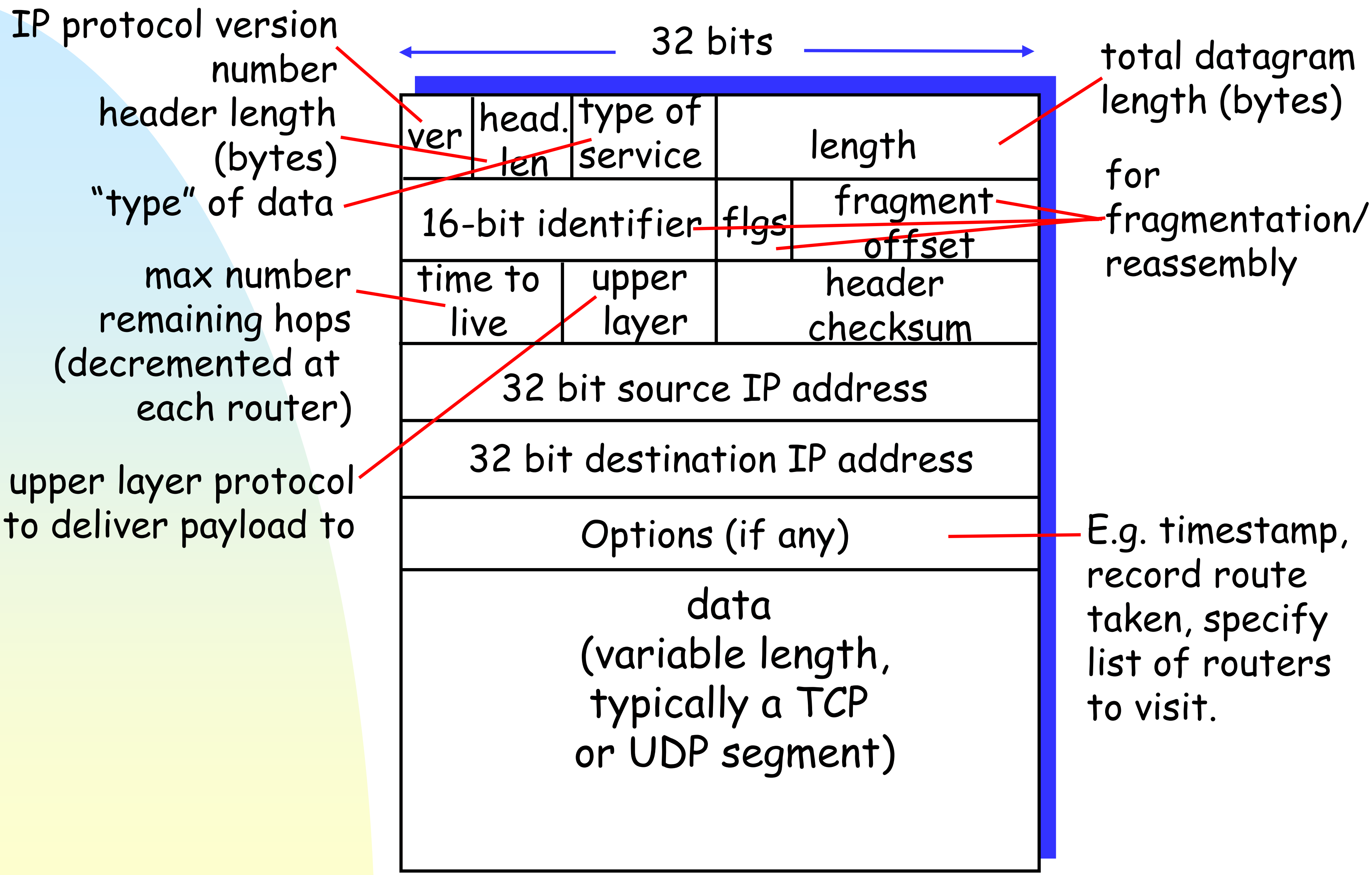
→ **Globally unique address**


Globally Unique Addresses
By IANA: Internet Assigned Numbers Authority
Assigns unique network number to requesting organizations
By local authorities (cooperate network administrators)
Assigns unique host numbers to its attached devices

IPv4 maintains a hierarchical structure

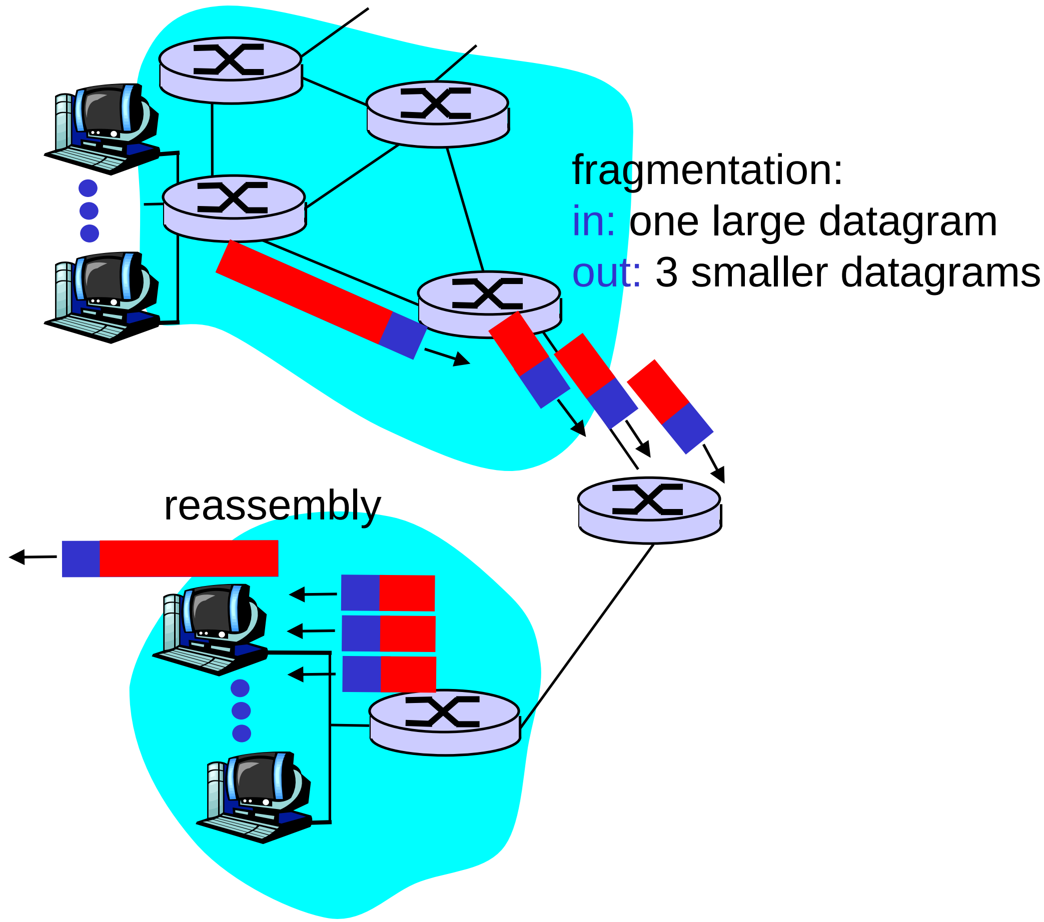
- Class A (0, 7bits) → 0.0.0.0 ~ 127.255.255.255
- Class B (10, 14bits) → 128.0.0.0 ~ 191.255.255.255
- Class C (110, 21bits) → 192.0.0.0 ~ 223.255.255.255
- Class D (1110) → 224.0.0.0 ~ 239.255.255.255
  - · There is no relevance to network and host portions in **multicast** operations
- Class E (1111) → 240.0.0.0 ~ 255.255.255.255
  - · reserved for future use

IP datagram format



IP Fragmentation & Reassembly

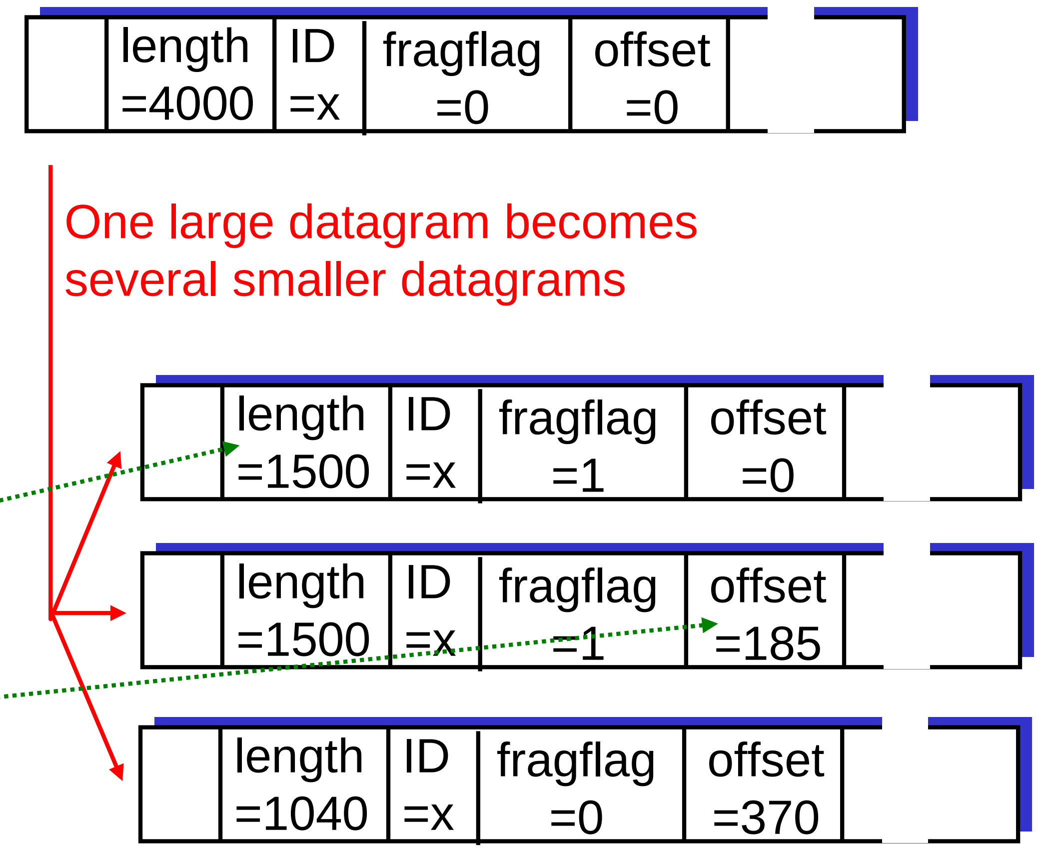
- network links have MTU (max.transfer size) - largest possible link-level frame.
  - different link types, different MTUs
- large IP datagram divided ("fragmented") within net
  - one datagram becomes several datagrams
  - "reassembled" only at final destination
  - IP header bits used to identify, order related fragments



IP Fragmentation and Reassembly

Example

- 4000 byte datagram
- MTU = 1500 bytes



1480 bytes in data field

offset = 1480/8

IP addresses: how to get one?

Q: How does a *host* get IP address?

- hard-coded by system admin in a file
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from a server
  - "plug-and-play"

ICMP: Internet Control Message Protocol

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Motivation for Mobile IP

Routing

- based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
- 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

Specific routes to end-systems?

- 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
- almost impossible to find a mobile system, DNS updates take to long time
- TCP connections break, security problems

Requirements to Mobile IP

Transparency

- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- point of connection to the fixed network can be changed

Compatibility

- support of the same layer 2 protocols as IP
- no changes to current end-systems and routers required
- mobile end-systems can communicate with fixed systems

Security

- authentication of all registration messages

Efficiency and scalability

- only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- world-wide support of a large number of mobile systems in the whole Internet

The Goal of a Mobile IP

Supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols

Terminology

Mobile Node (MN)

- system (node) that can change the point of connection to the network without changing its IP address

Home Agent (HA)

- system in the home network of the MN, typically a router
- registers the location of the MN, tunnels IP datagrams to the COA

Foreign Agent (FA)

- system in the current foreign network of the MN, typically a router
- forwards the tunneled datagrams to the MN, typically also the default router for the MN

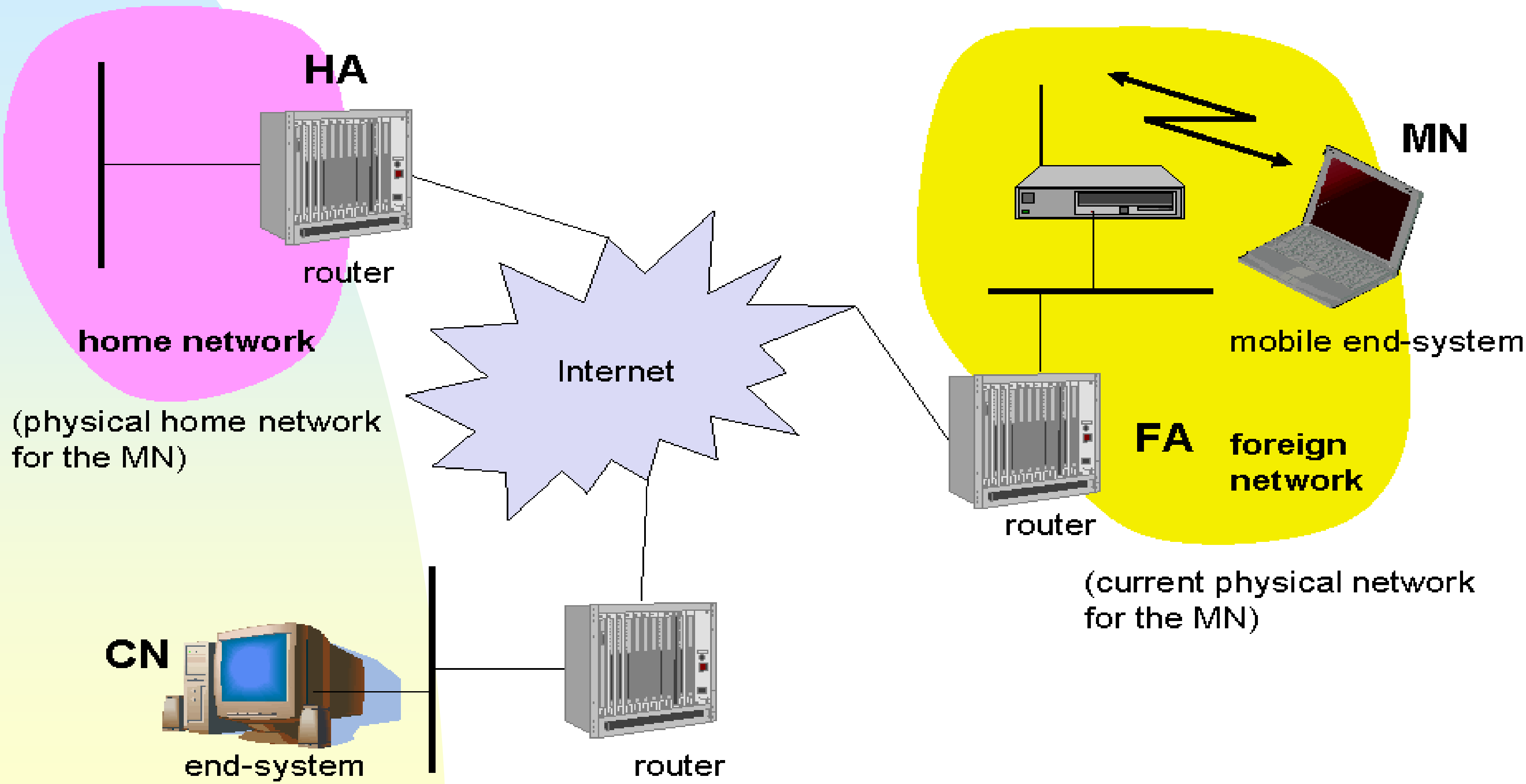
Care-of Address (COA)

- address of the current tunnel end-point for the MN (at FA or MN)
- actual location of the MN from an IP point of view
- can be chosen, e.g., via DHCP

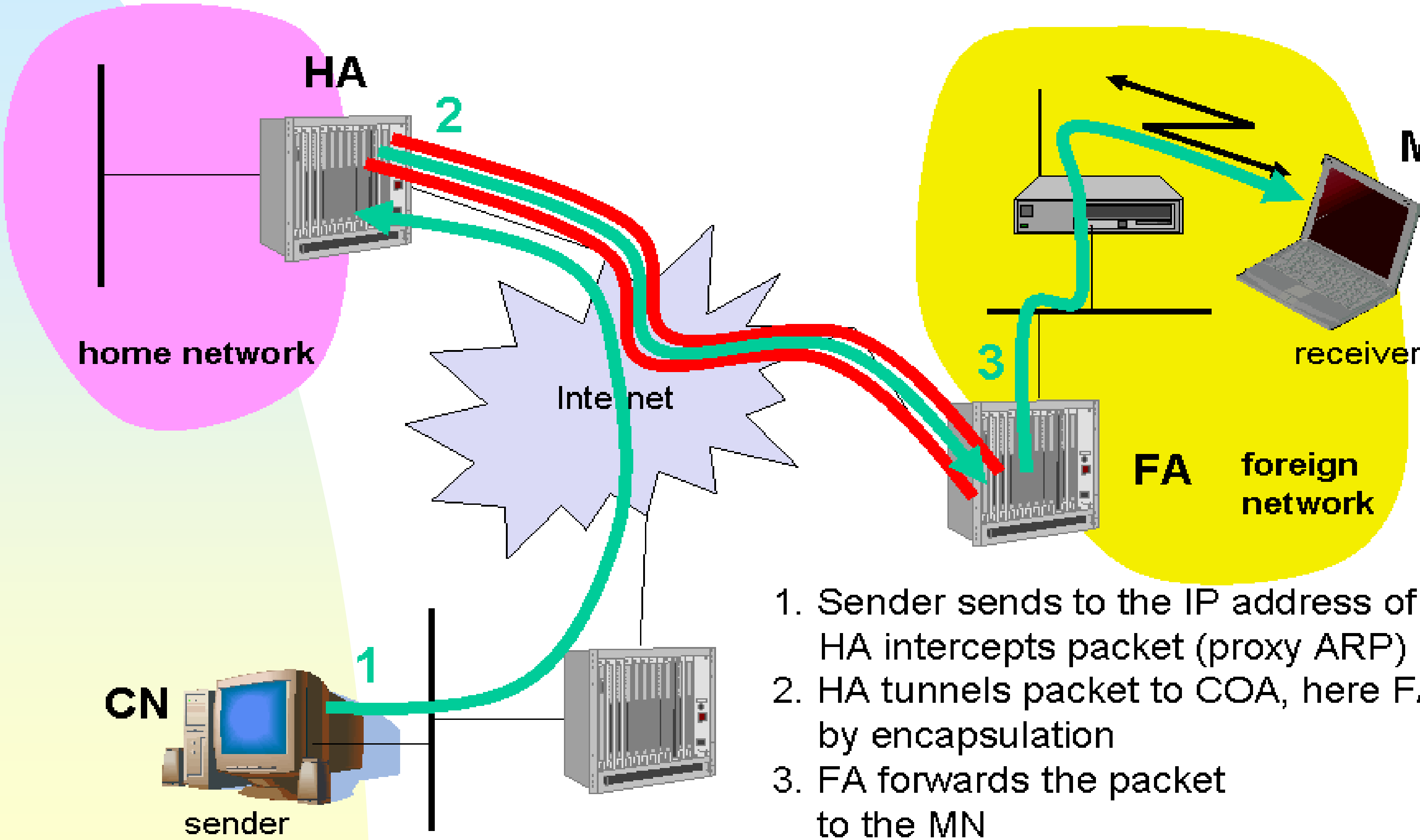
Correspondent Node (CN)

- communication partner

Example network

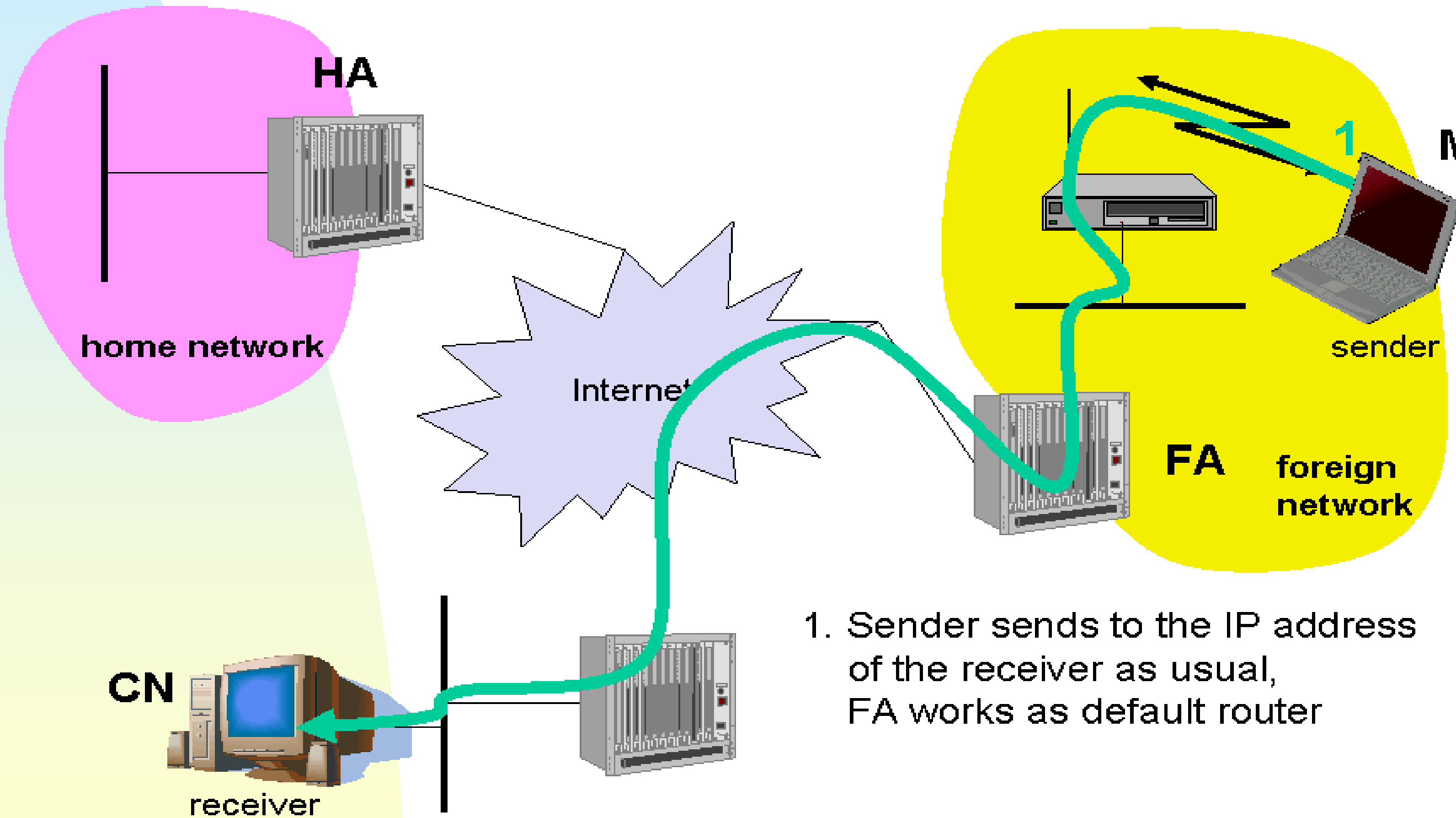


Data transfer to the mobile system



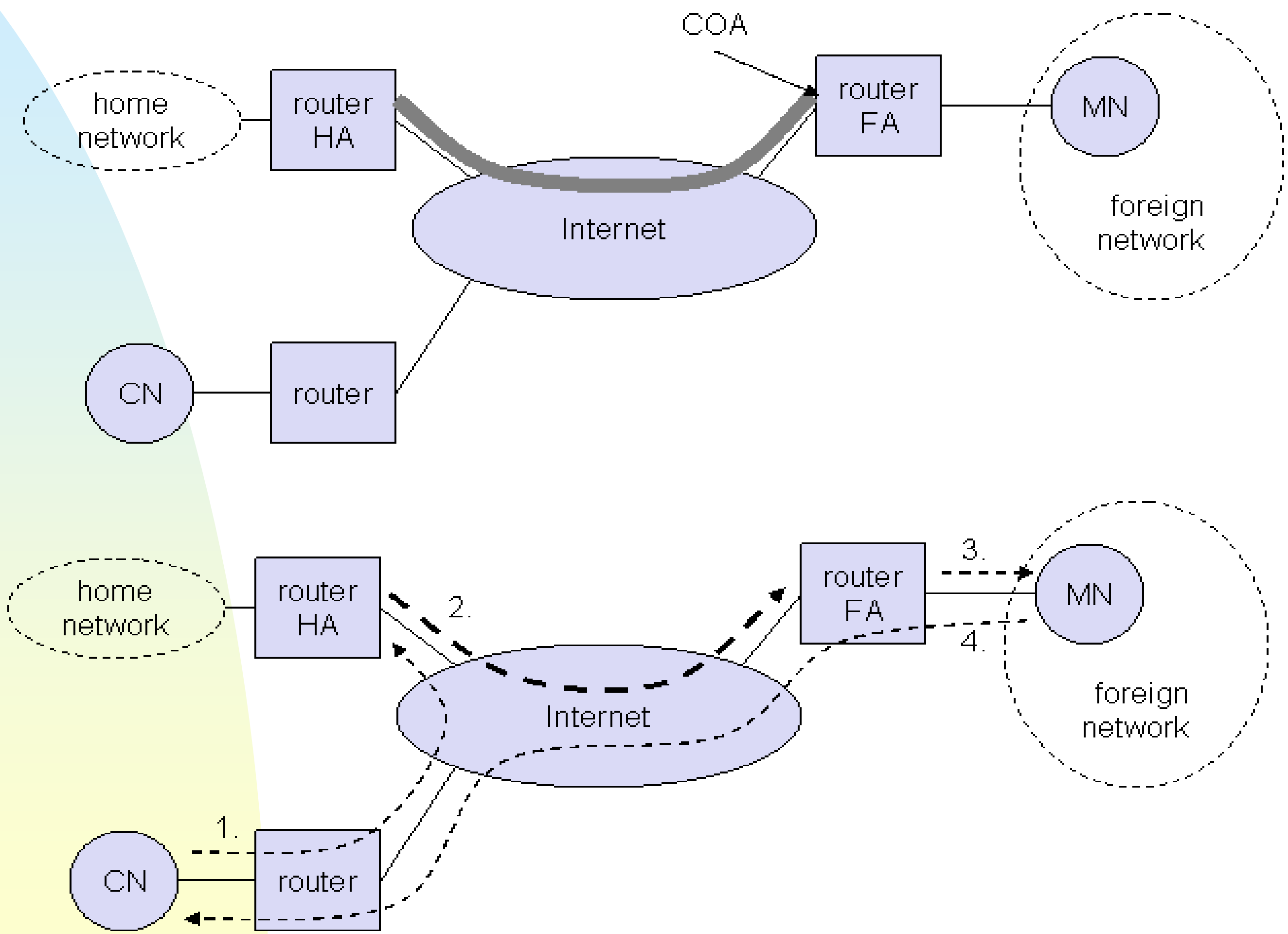
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



1. Sender sends to the IP address of the receiver as usual, FA works as default router

Overview



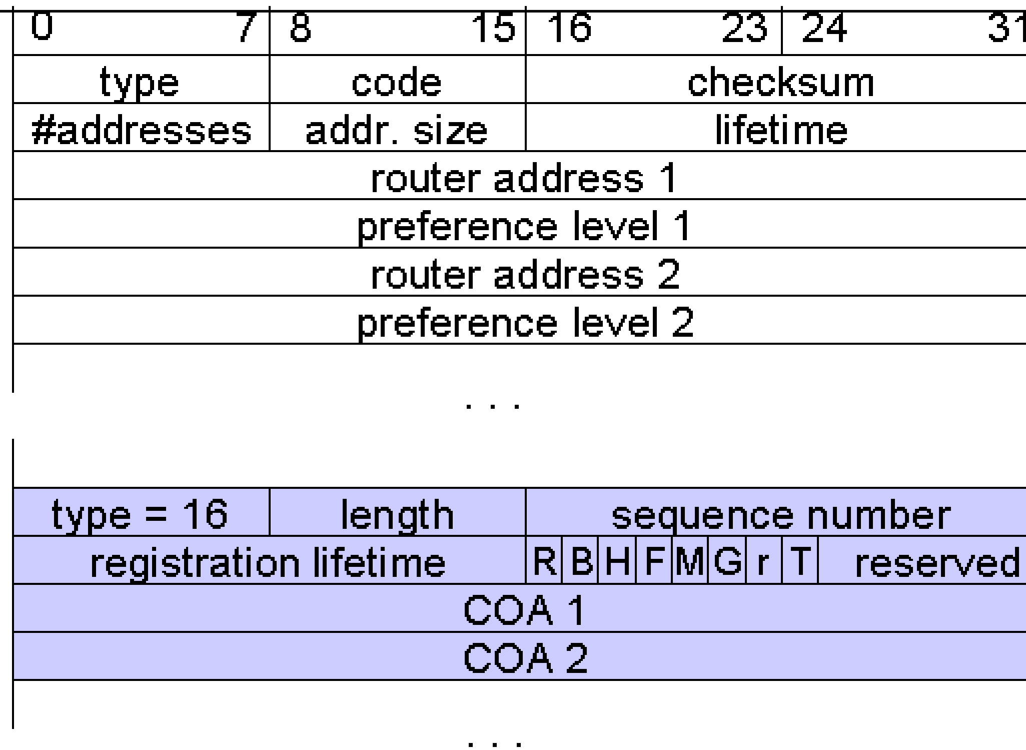
COA
home network
router HA
router FA
MN
Internet
foreign network
CN
router
home network
router HA
2.
router FA
3.
MN
4.
Internet
foreign network
1.
CN
router

Network integration

Agent Advertisement

- HA and FA periodically send advertisement messages into their physical subnets
- MN listens to these messages and detects, if it is in the home or a foreign network
- MN reads a COA from the FA advertisement messages

Agent advertisement



type = 16
length = 6 + 4 * #COAs
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

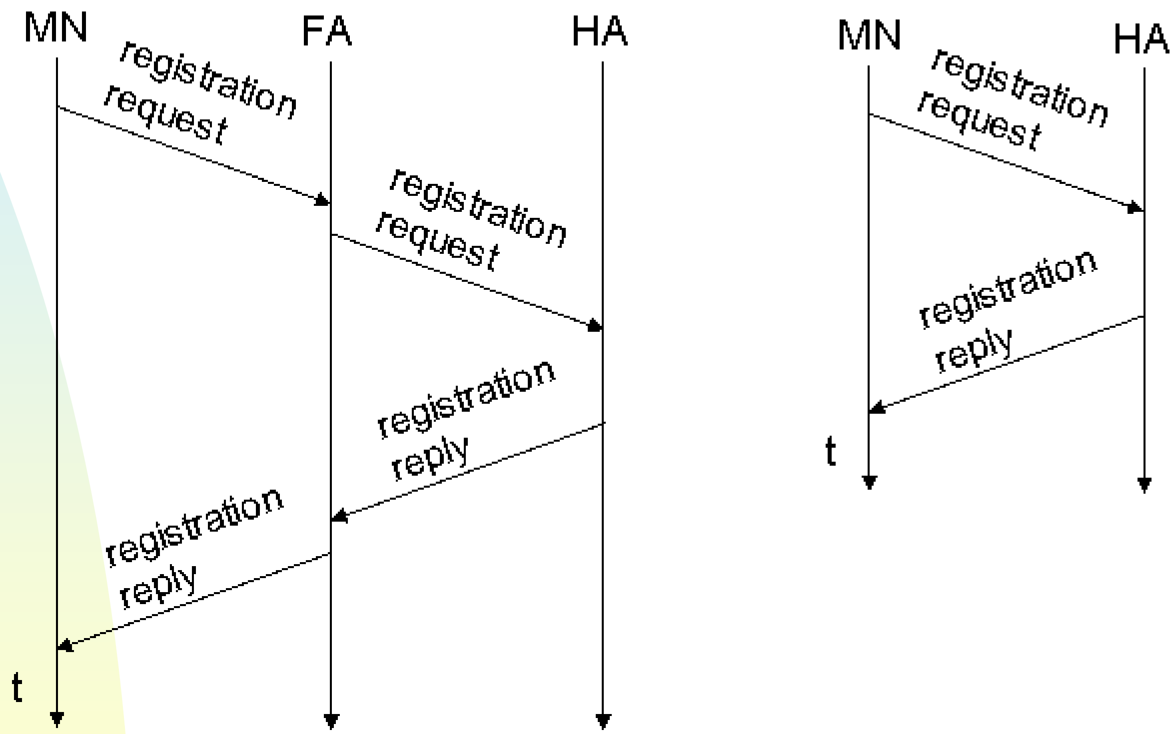
Registration

Registration (always limited lifetime!)

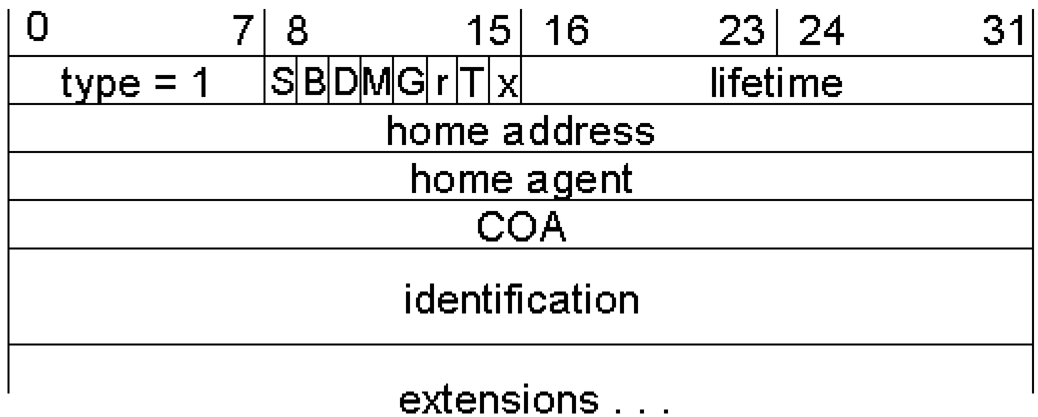
- MN signals COA to the HA via the FA, HA acknowledges via FA to MN

- these actions have to be secured by authentication

Registration



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

Mobile IP registration reply

0 7	8 15	16 31
type = 3	code	lifetime
home address		
home agent		
identification		
extensions . . .		

Example codes:

registration successful

- 0 registration accepted
- 1 registration accepted, but simultaneous mobility bindings unsupported

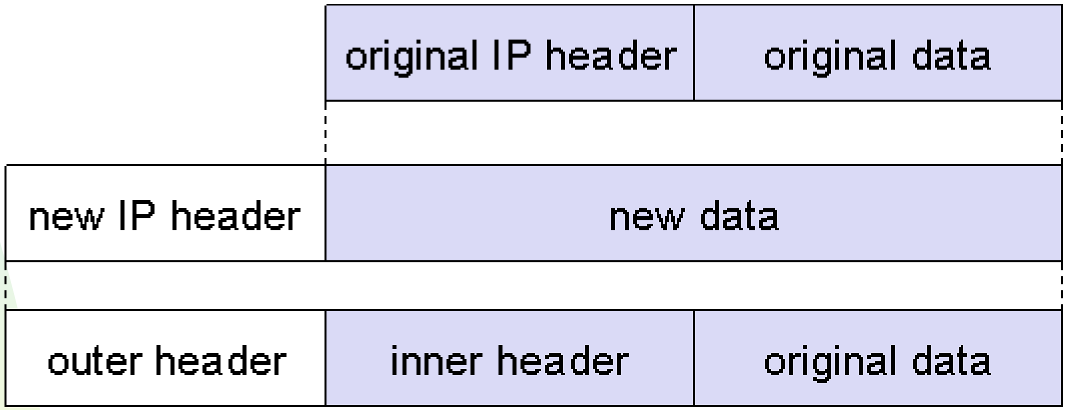
registration denied by FA

- 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

Encapsulation



Encapsulation I

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 Routing Encapsulation)

IP-in-IP-encapsulation (mandatory, RFC 2003)

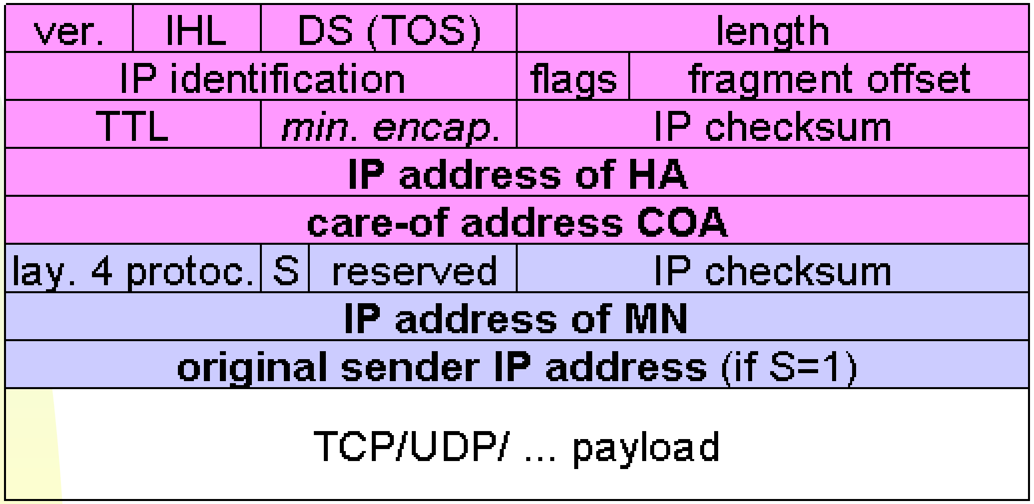
- tunnel between HA and COA

<table>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>IP-in-IP</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of HA</td></tr>
<tr><td colspan="5">Care-of address COA</td></tr>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of CN</td></tr>
<tr><td colspan="5">IP address of MN</td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

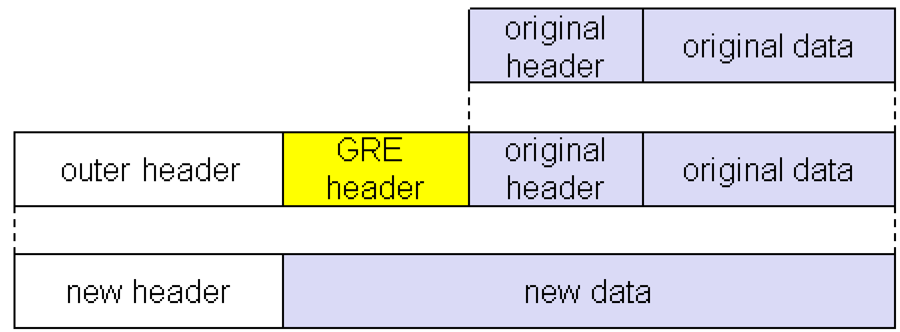
Encapsulation II

Minimal encapsulation (optional)

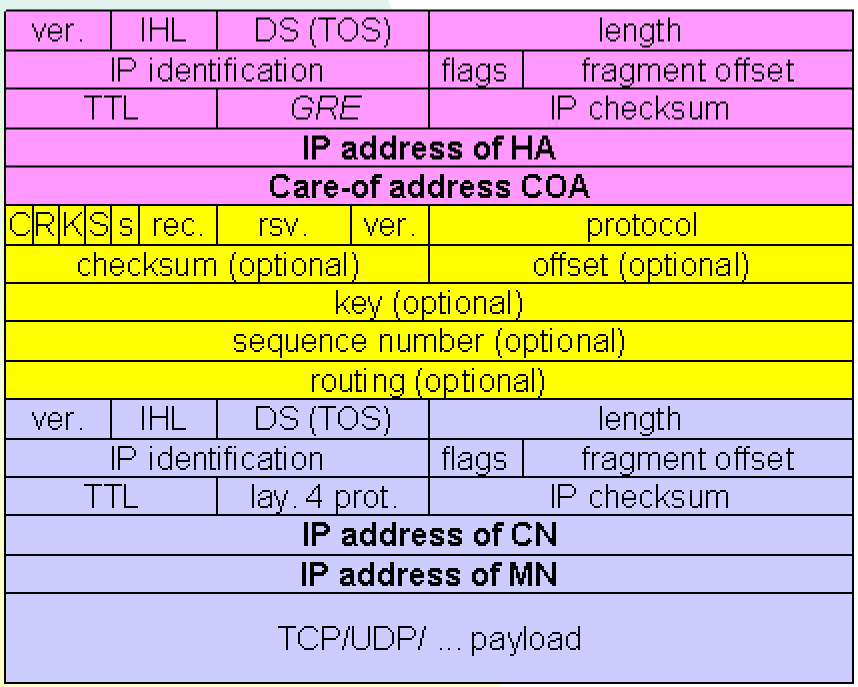
- avoids repetition of identical fields
- e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
- only applicable for unfragmented packets, no space left for fragment identification



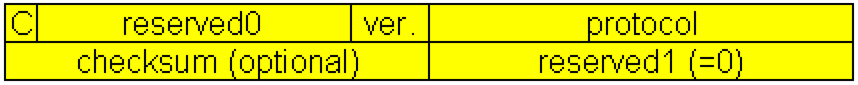
Generic Routing Encapsulation



RFC 1701



RFC 2784



Optimization of packet forwarding

Triangular Routing

- sender sends all packets via HA to MN
- higher latency and network load

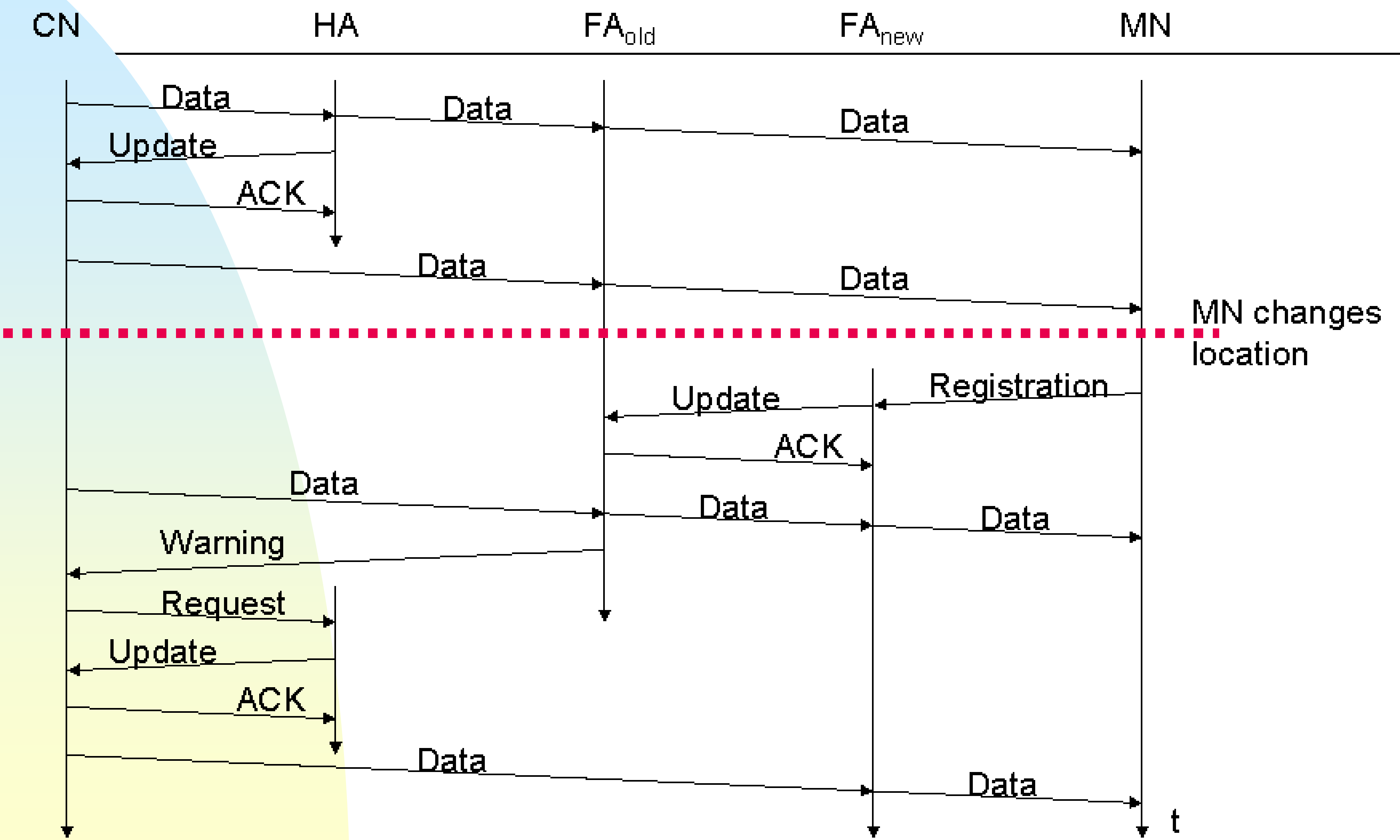
“Solutions”

- sender learns the current location of MN
- direct tunneling to this location
- HA informs a sender about the location of MN
- big security problems!

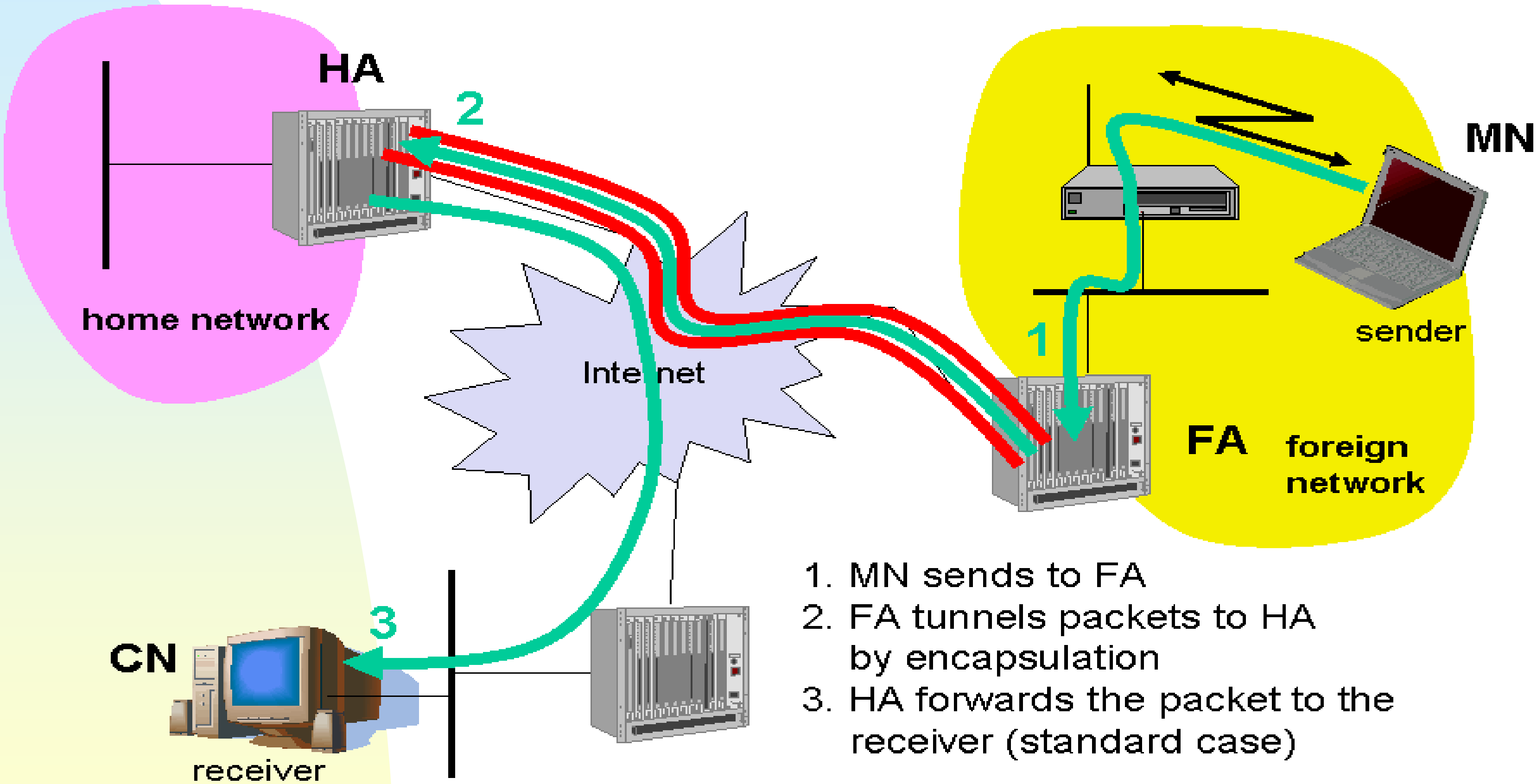
Change of FA

- 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

Change of foreign agent



Reverse tunneling (RFC 3024, was: 2344)



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

Mobile IP with reverse tunneling

Router accept often only “topological correct“ addresses (firewall!)

- a packet from the MN encapsulated by the FA is now topological correct
- furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is to far away from the receiver)

Reverse tunneling does not solve

- problems with *firewalls*, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
- optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)

The standard is backwards compatible

- the extensions can be implemented easily and cooperate with current implementations without these extensions
- Agent Advertisements can carry requests for reverse tunneling

Problems with mobile IP

Security
- authentication with FA problematic, for the FA typically belongs to another organization
- no protocol for key management and key distribution has been standardized in the Internet
- patent and export restrictions

Firewalls
- typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling)

QoS
- many new reservations in case of RSVP
- tunneling makes it hard to give a flow of packets a special treatment needed for the QoS

Security, firewalls, QoS etc. are topics of current research and discussions!