Mobile Communications

Chapter 8: Network Protocols/Mobile IP

- Motivation
- Data transfer , Encapsulation
- Security, IPv6, Problems
- Micro mobility support
- DHCP
- Ad-hoc networks, Routing protocols

Prof. Jó Ueyama

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 too long time
  - TCP connections break, security problems

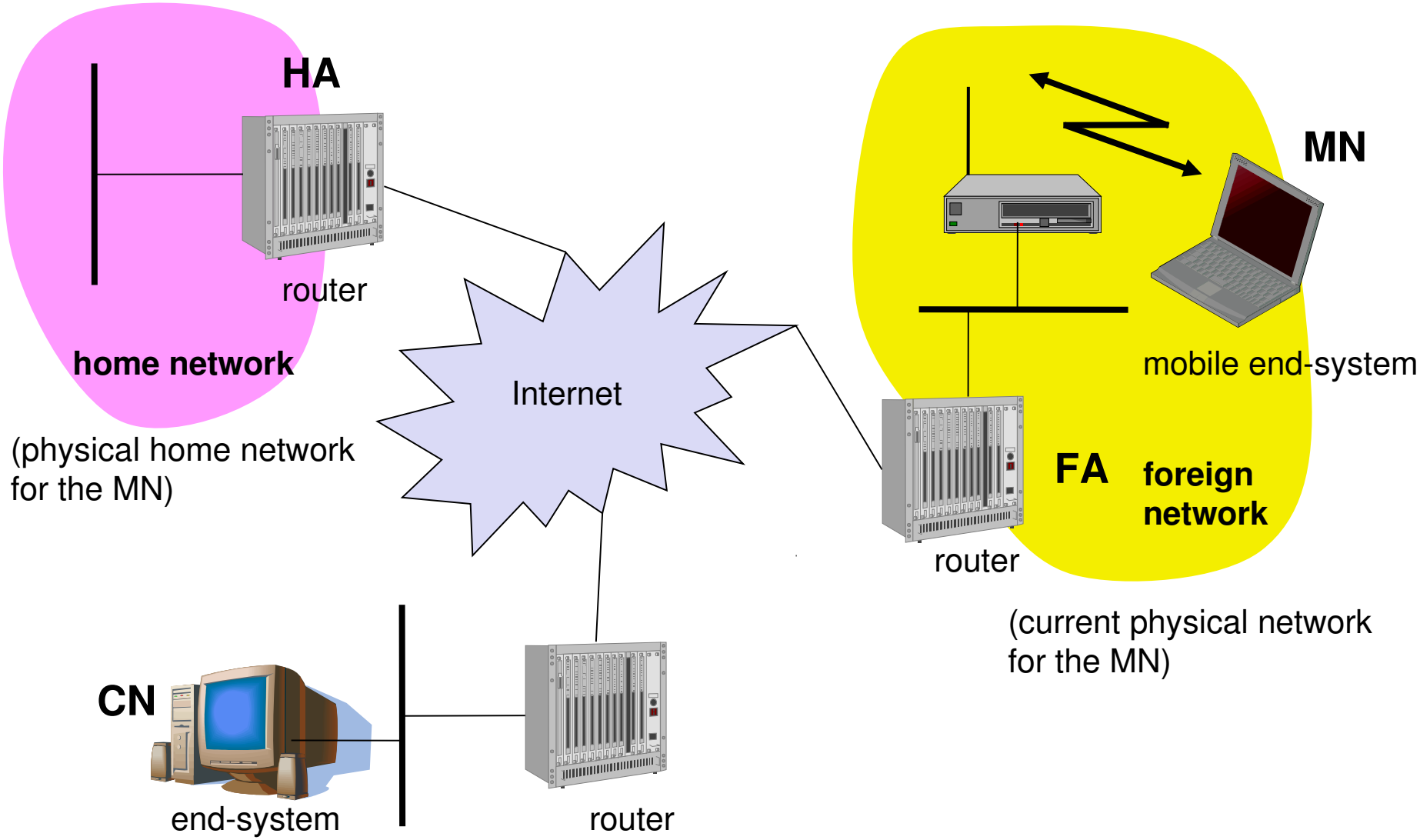
Requirements for Mobile IPv4 (RFC 3344, was: 3220, was: 2002 , updated by: 4721)

- 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

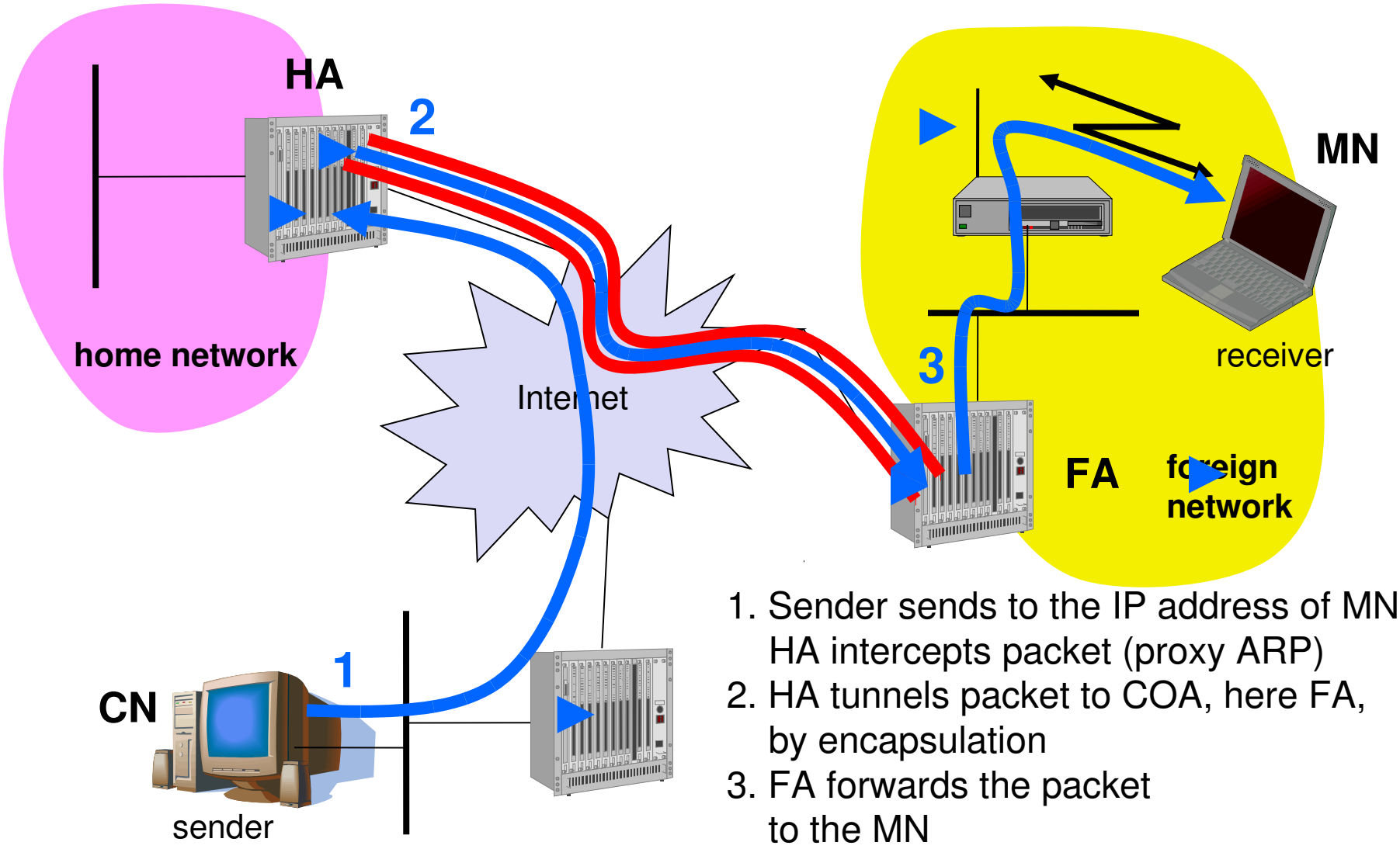
Terminology

- 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)
  - Co-located COA
  - 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

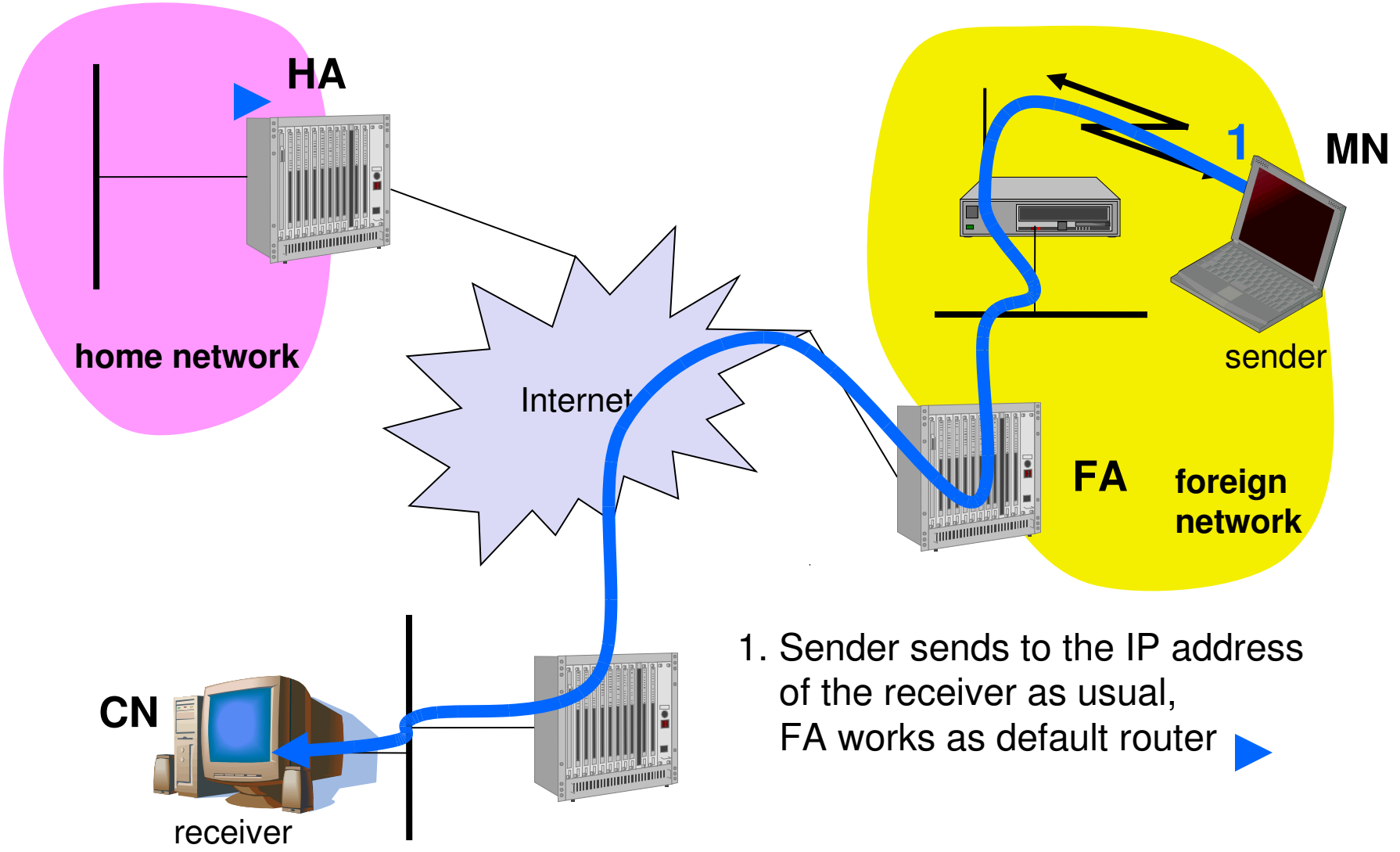


Data transfer to the mobile system

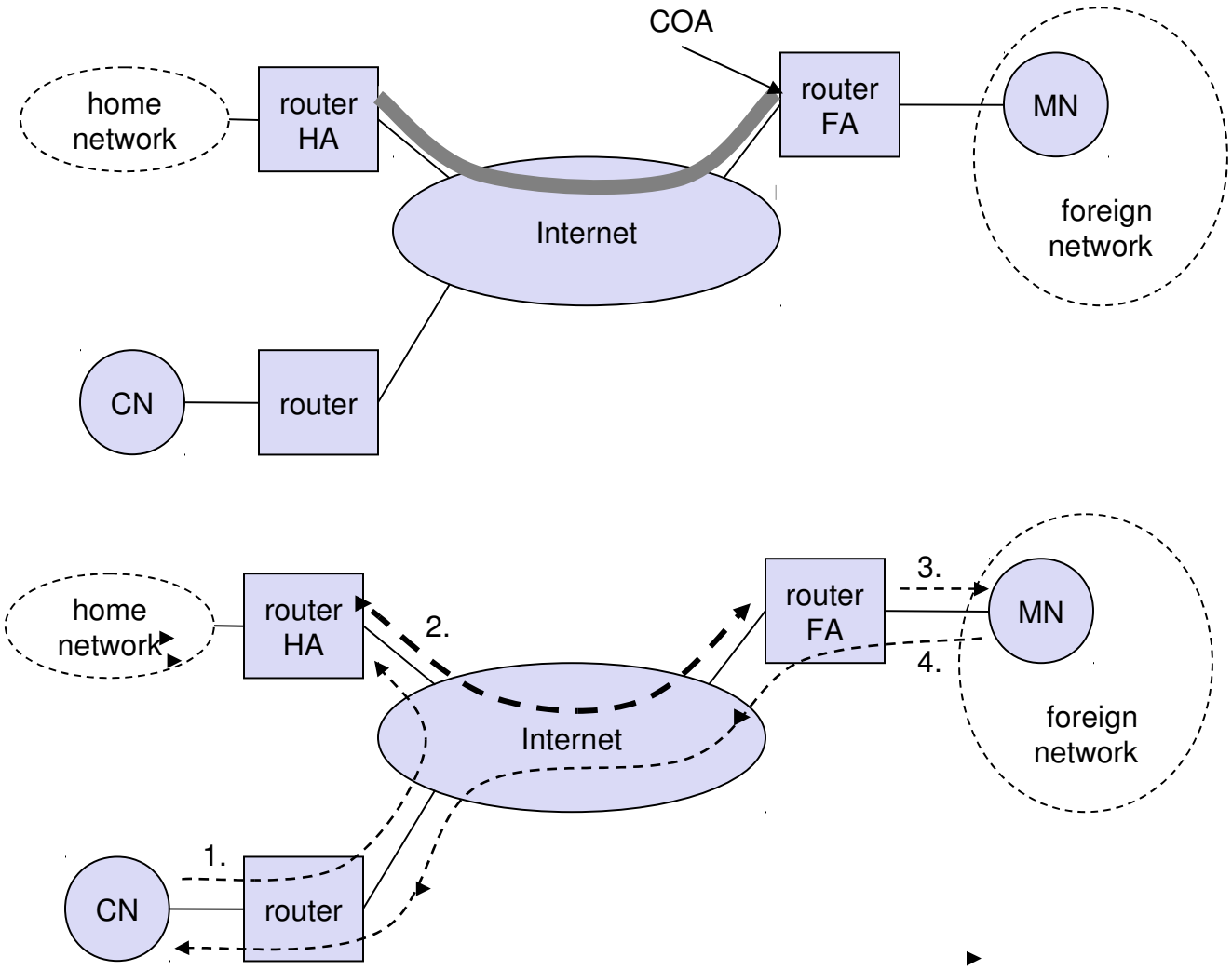


1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



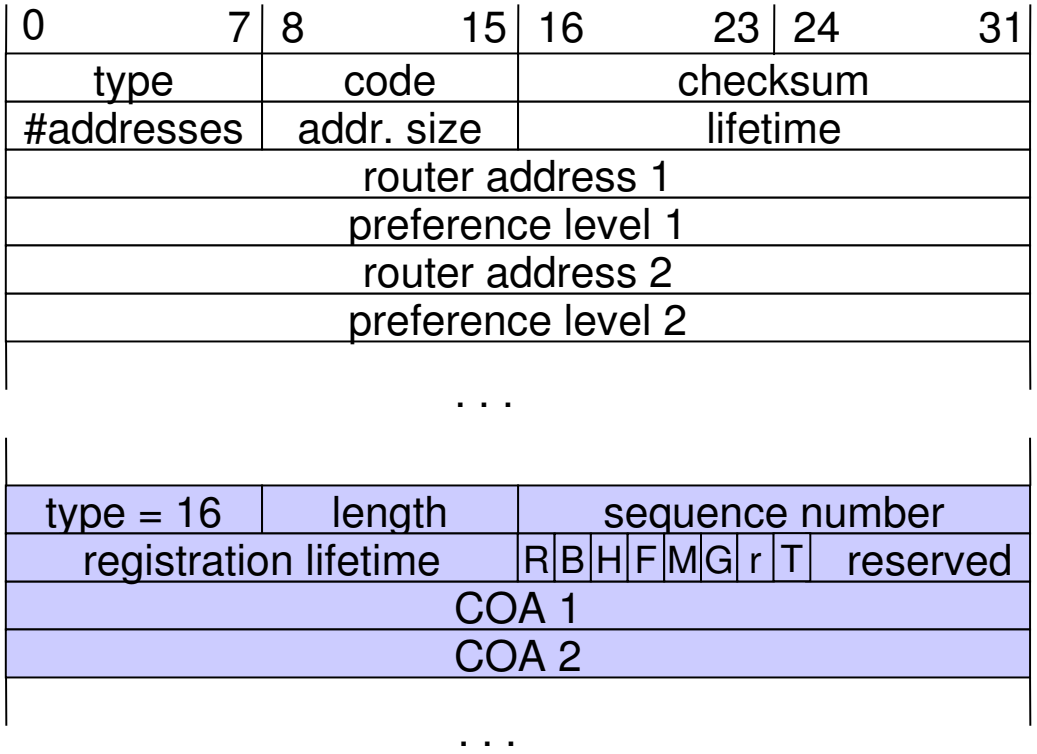
Overview


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

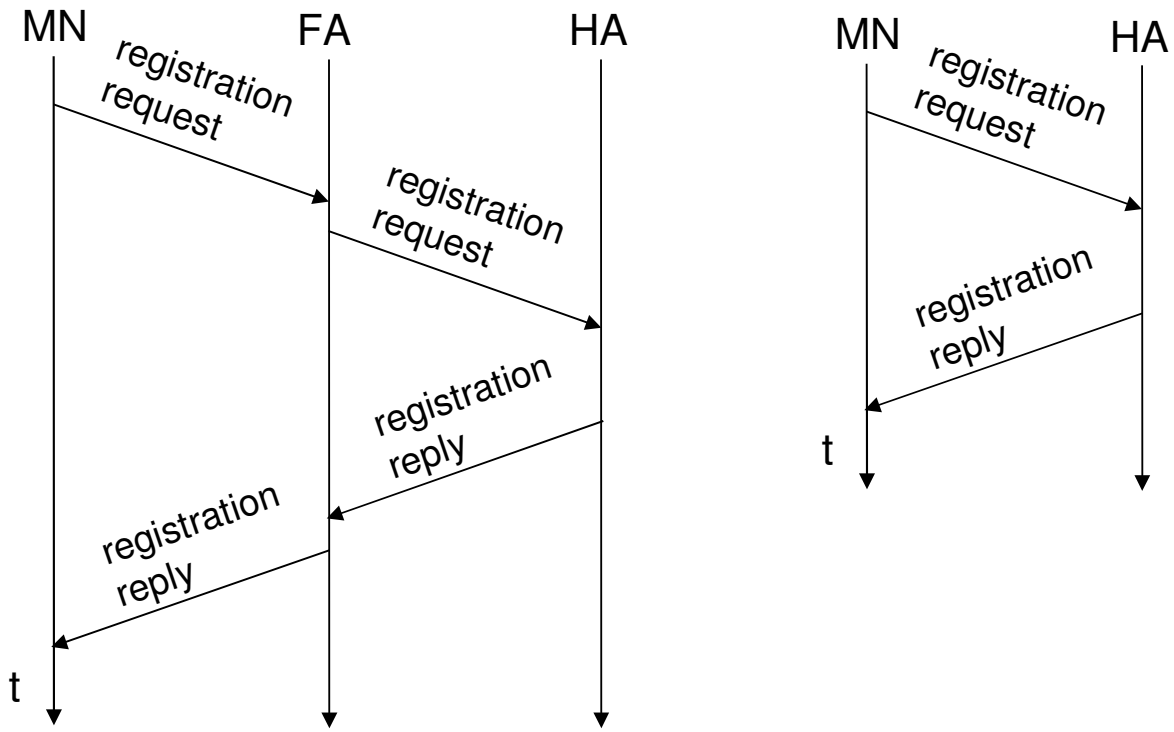
- Agent Advertisement
  - HA and FA periodically send advertisement messages into their physical subnets
  - MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
  - MN reads a COA from the FA advertisement messages
- Registration (always 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
- Advertisement
  - HA advertises the IP address of the MN (as for fixed systems), i.e. standard routing information
  - routers adjust their entries, these are stable for a longer time (HA responsible for a MN over a longer period of time)
  - packets to the MN are sent to the HA,
  - independent of changes in COA/FA

Agent advertisement

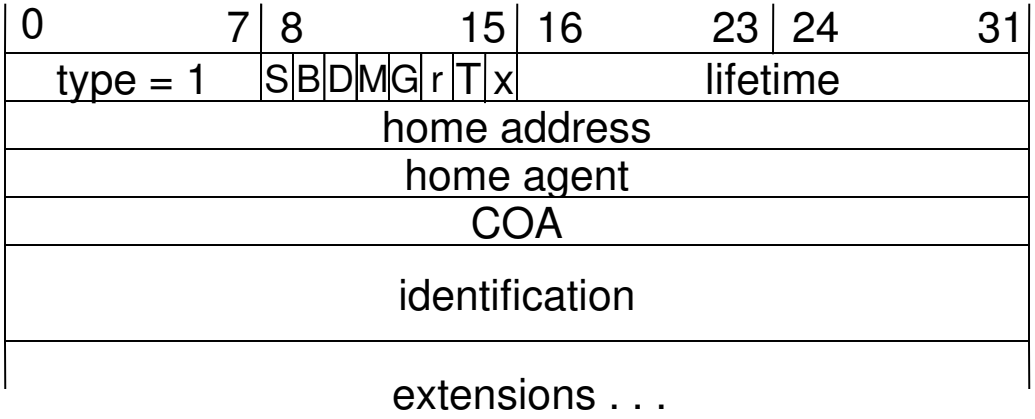


type = 16
length = 6 + 4 * #COAs
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Registration

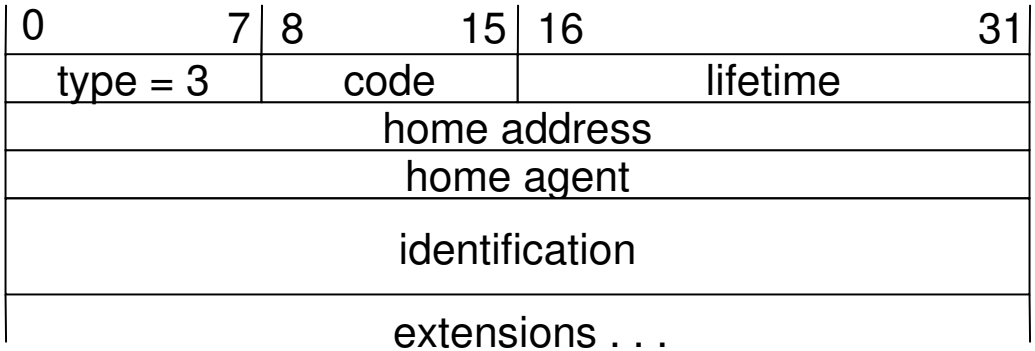


Mobile IP registration request



S: simultaneous bindings
B: broadcast datagrams
D: decapsulation by MN (If Co-located COA is adopted)
M mininal encapsulation
G: GRE encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored

Mobile IP registration reply



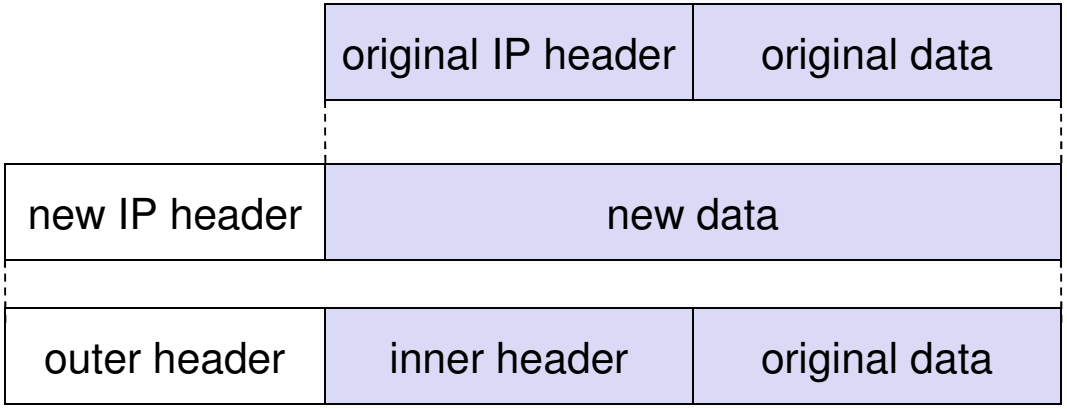
Example codes:

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 Record Encapsulation)
- IP-in-IP-encapsulation (mandatory, RFC 2003)
  - tunnel between HA and COA

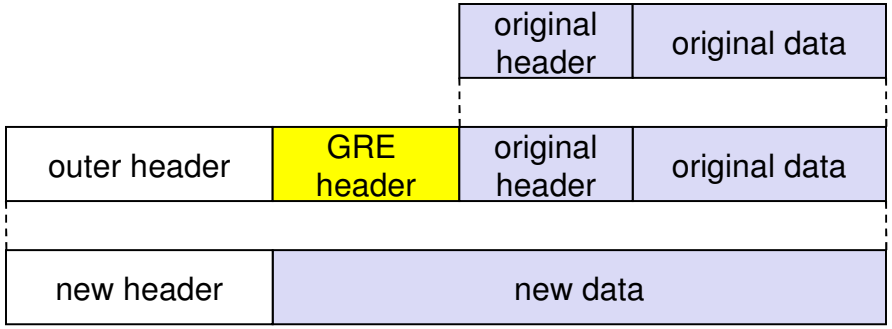
<table>
<tr><td colspan="2">ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td colspan="2">fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">IP-in-IP</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of HA</td></tr>
<tr><td colspan="6">Care-of address COA</td></tr>
<tr><td colspan="2">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 colspan="2">fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of CN</td></tr>
<tr><td colspan="6">IP address of MN</td></tr>
<tr><td colspan="6">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 non fragmented packets, no space left for fragment identification

<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>min. encap.</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>lay. 4 protoc.</td><td>S</td><td colspan="2">reserved</td><td>IP checksum</td></tr>
<tr><td colspan="5">IP address of MN</td></tr>
<tr><td colspan="5">original sender IP address (if S=1)</td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

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															

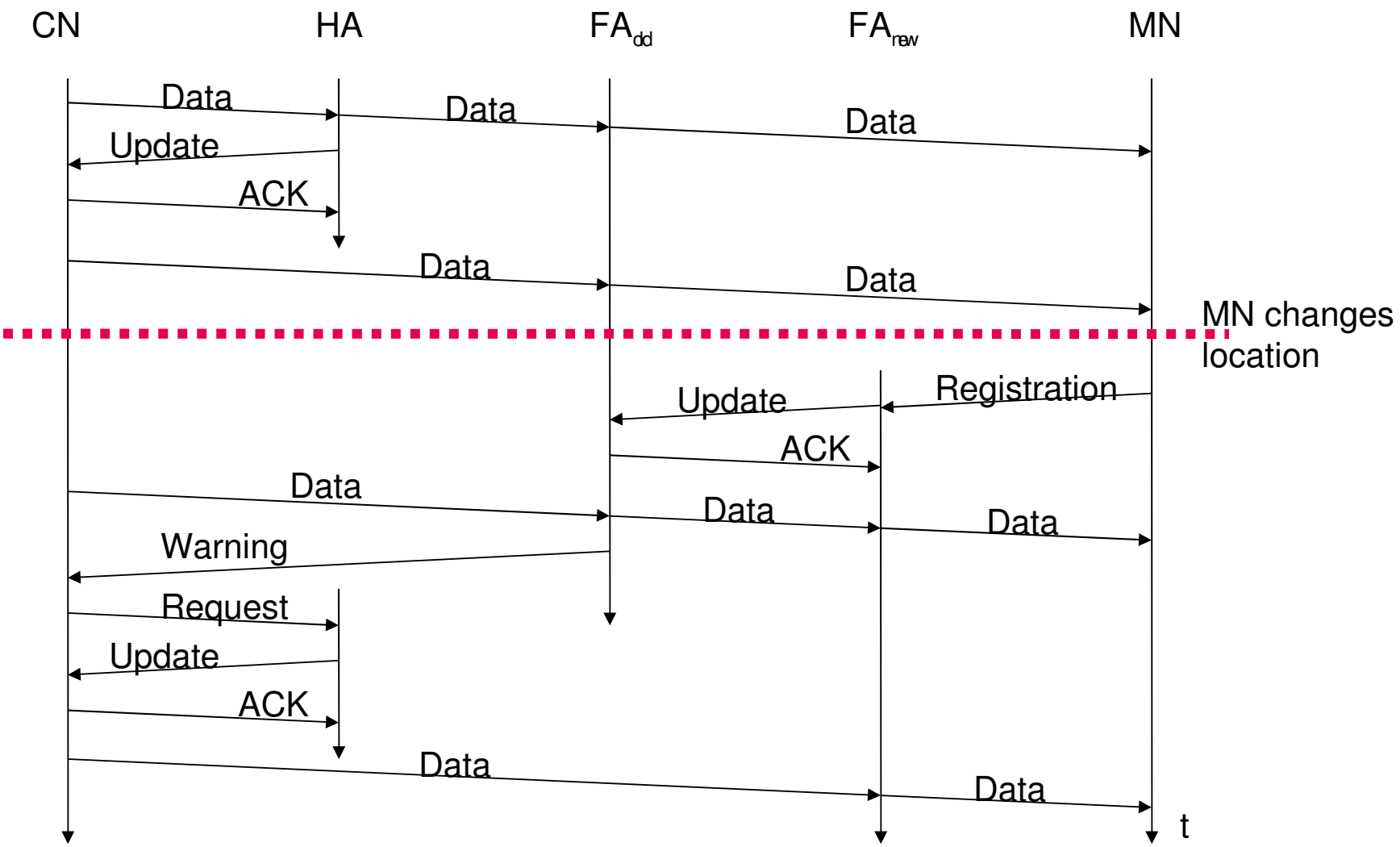
RFC 2784 (updated by 2890)

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

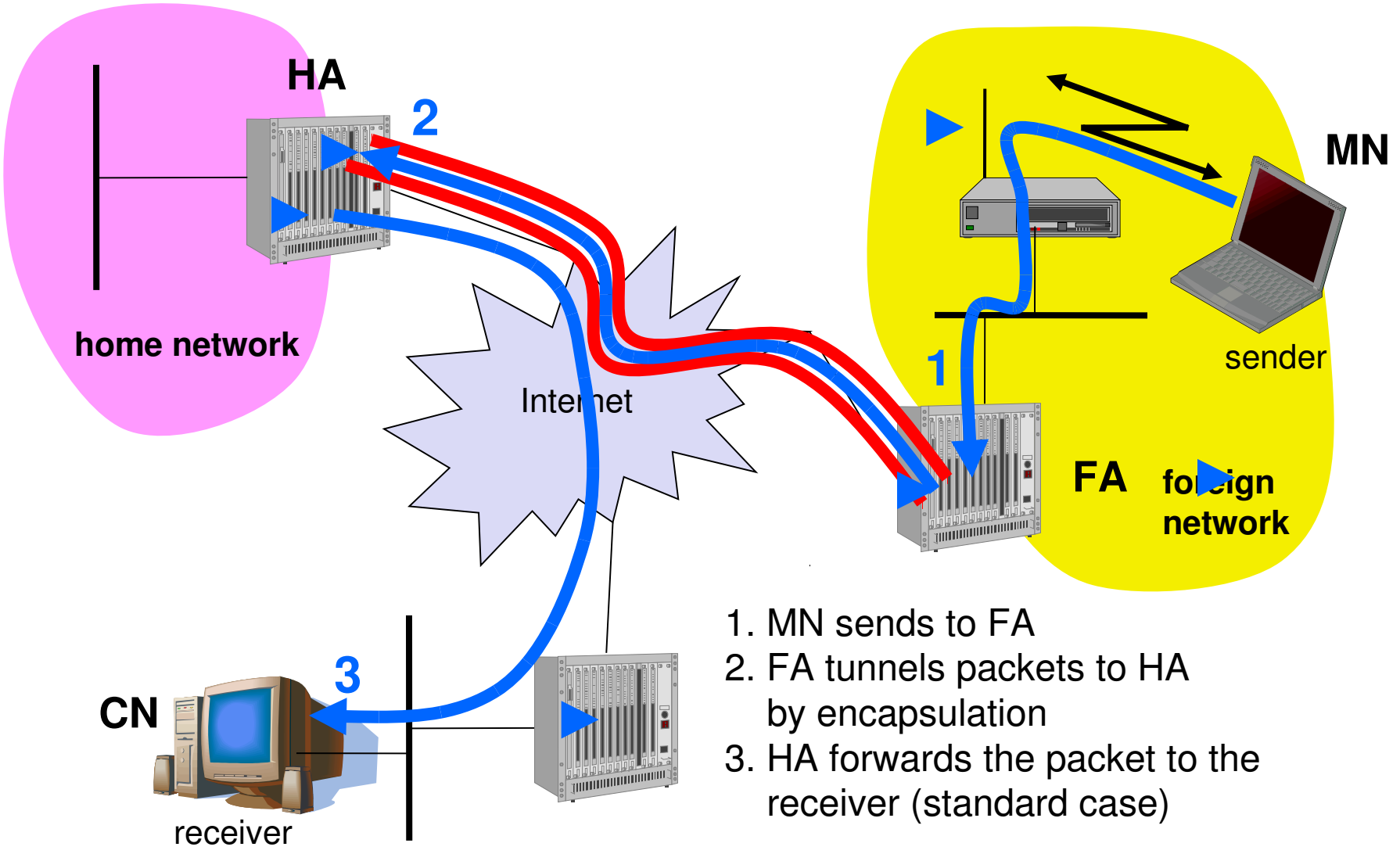
Optimization of packet forwarding

- Problem: 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 accepts 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

Mobile IP and IPv6 (RFC 3775)

- Mobile IP was developed for IPv4, but IPv6 simplifies the protocols
  - security is integrated and not an add-on, authentication of registration is included
  - COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address auto-configuration
  - no need for a separate FA, **all** routers perform router advertisement which can be used instead of the special agent advertisement; addresses are always co-located
  - MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization–COA to MN)
  - „soft“ hand-over, i.e. without packet loss, between two subnets is supported
    - MN sends the new COA to its old router
    - the old router encapsulates all incoming packets for the MN and forwards them to the new COA
    - authentication is always granted

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
- 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 research and discussions

IP Micro-mobility support

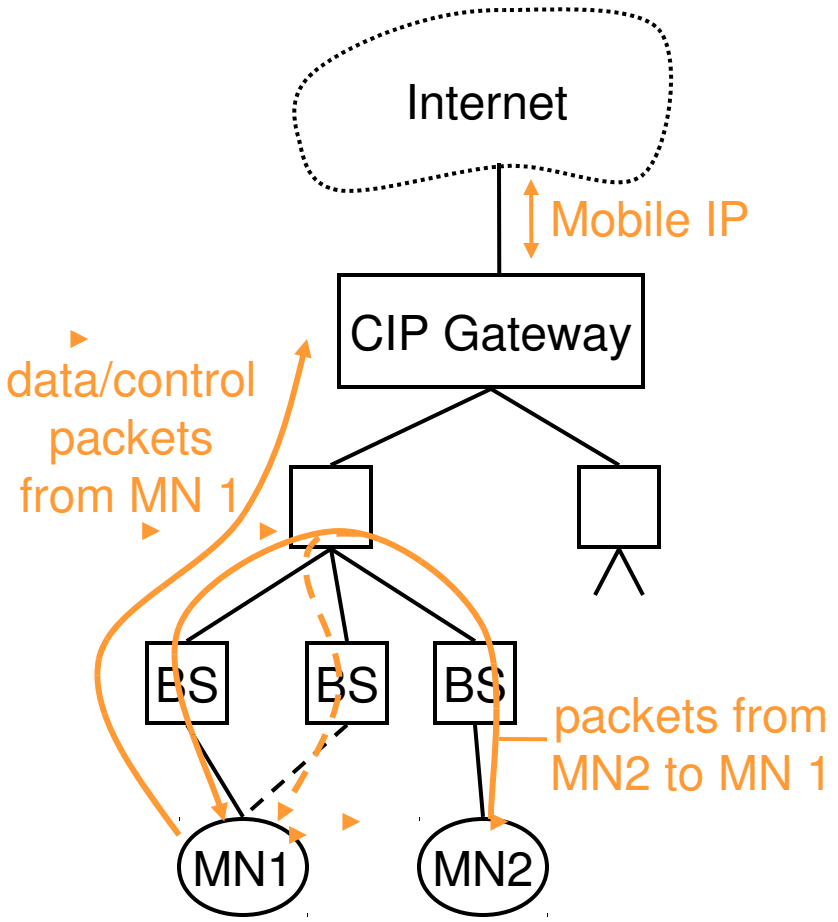
- Micro-mobility support:
  - Efficient local handover inside a foreign domain without involving a home agent
  - Reduces control traffic on backbone
  - Especially needed in case of route optimization

- Example approaches (research, not products):
  - Cellular IP
  - HAWAII
  - Hierarchical Mobile IP (HMIP)

- Important criteria:
  Security Efficiency, Scalability, Transparency, Manageability

Cellular IP

- Operation:
  - “CIP Nodes” maintain routing entries (soft state) for MNs
  - Multiple entries possible
  - Routing entries updated based on packets sent by MN
- CIP Gateway:
  - Mobile IP tunnel endpoint
  - Initial registration processing
- Security provisions:
  - all CIP Nodes share “network key”
  - MN key: MD5(net key, IP addr)
  - MN gets key upon registration



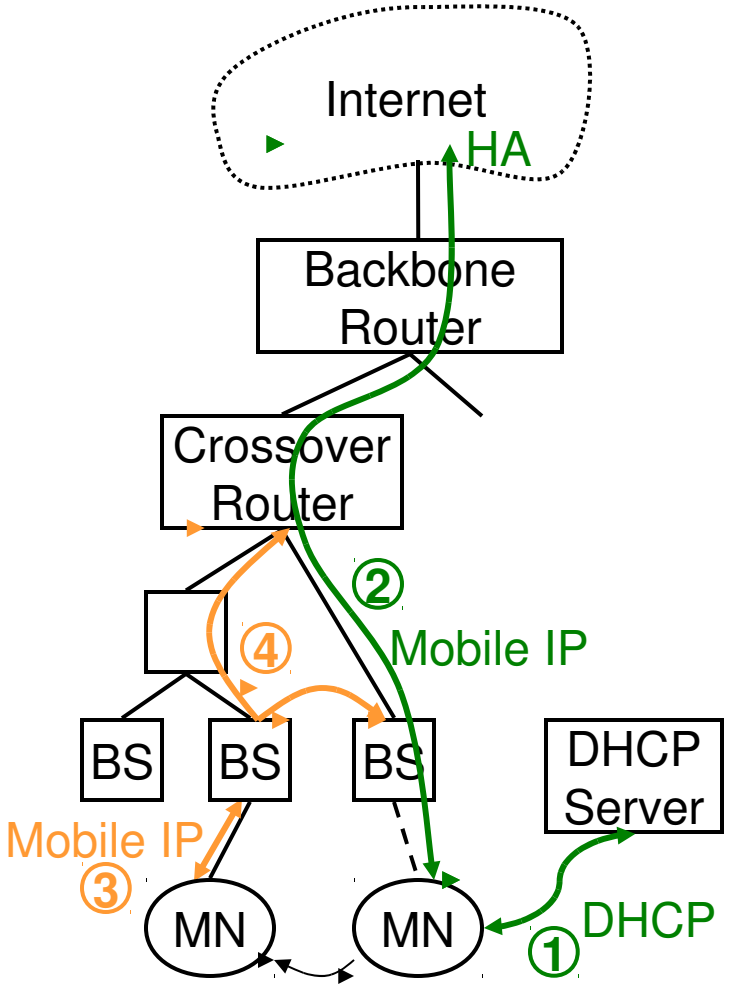
Cellular IP: Other issues

- Advantages:
  - Simple and elegant architecture
  - Mostly self-configuring (little management needed)
  - Integration with firewalls / private address support possible

- Potential problems:
  - Not transparent to MNs (additional control messages)
  - Public-key encryption of MN keys may be a problem for resource-constrained MNs
  - Multiple-path forwarding may cause inefficient use of available bandwidth

HAWAII

- Operation:
  - MN obtains co-located COA and registers with HA ①②
  - Handover: MN keeps COA, new BS answers Reg. Request and updates routers ③④
  - MN views BS as foreign agent
- Security provisions:
  - MN-FA authentication mandatory
  - Challenge/Response Extensions mandatory

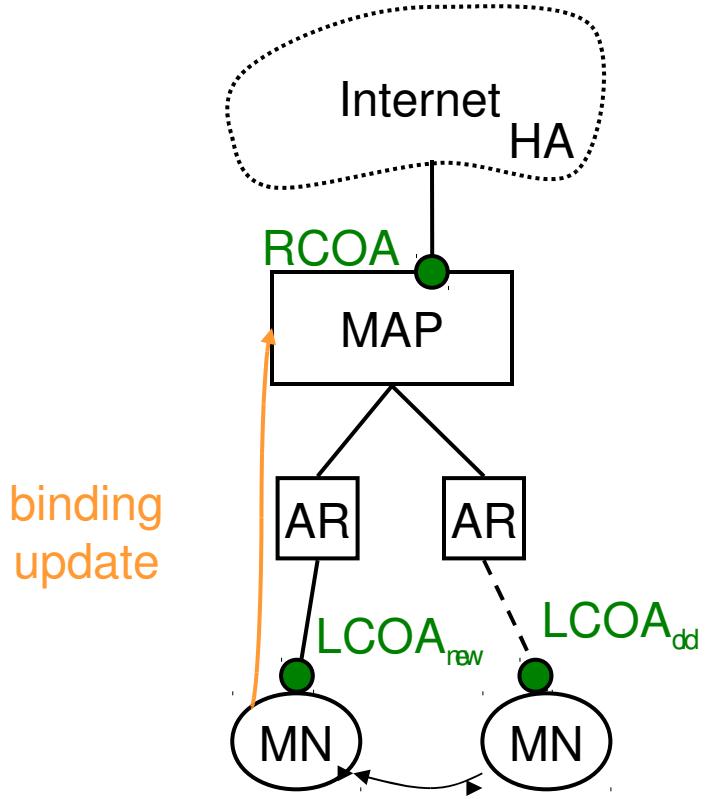


HAWAII: Other issues

- Advantages:
  - Mutual authentication and C/R extensions are mandatory
  - Mostly transparent to MNs
    (MN sends/receives standard Mobile IP messages)
  - Explicit support for dynamically assigned home addresses
- Potential problems:
  - Mixture of co-located COA and FA concepts may not be supported by some MN implementations
  - No private address support possible
    because of co-located COA

Hierarchical Mobile IPv6 (RFC 4140)

- Operation:
  - Network contains mobility anchor point (MAP)
    - mapping of regional COA (RCOA) to link COA (LCOA)
  - Upon handover, MN informs MAP only
    - gets new LCOA, keeps RCOA
  - HA is only contacted if MAP changes
- Security provisions:
  - no HMIP-specific security provisions
  - binding updates should be authenticated



Hierarchical Mobile IP: Security

- Advantages:
  - Local COAs can be hidden,
    which provides at least some location privacy
  - Direct routing between CNs sharing the same link is possible
    (but might be dangerous)
  - The extended mode of HMIPv6 supports both mobile nodes
    and mobile networks

- Potential problems:
  - Decentralized security-critical functionality
    (handover processing) in mobility anchor points
  - MNs can (must!) directly influence routing entries via binding
    updates (authentication necessary)