Wireless Networks: Network Protocols/Mobile IP

- Motivation
- Data transfer
- Encapsulation
- Security
- IPv6
- Problems
- DHCP

Adapted from J. Schiller, "Mobile Communications"

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 much time
  - TCP connections break, security problems

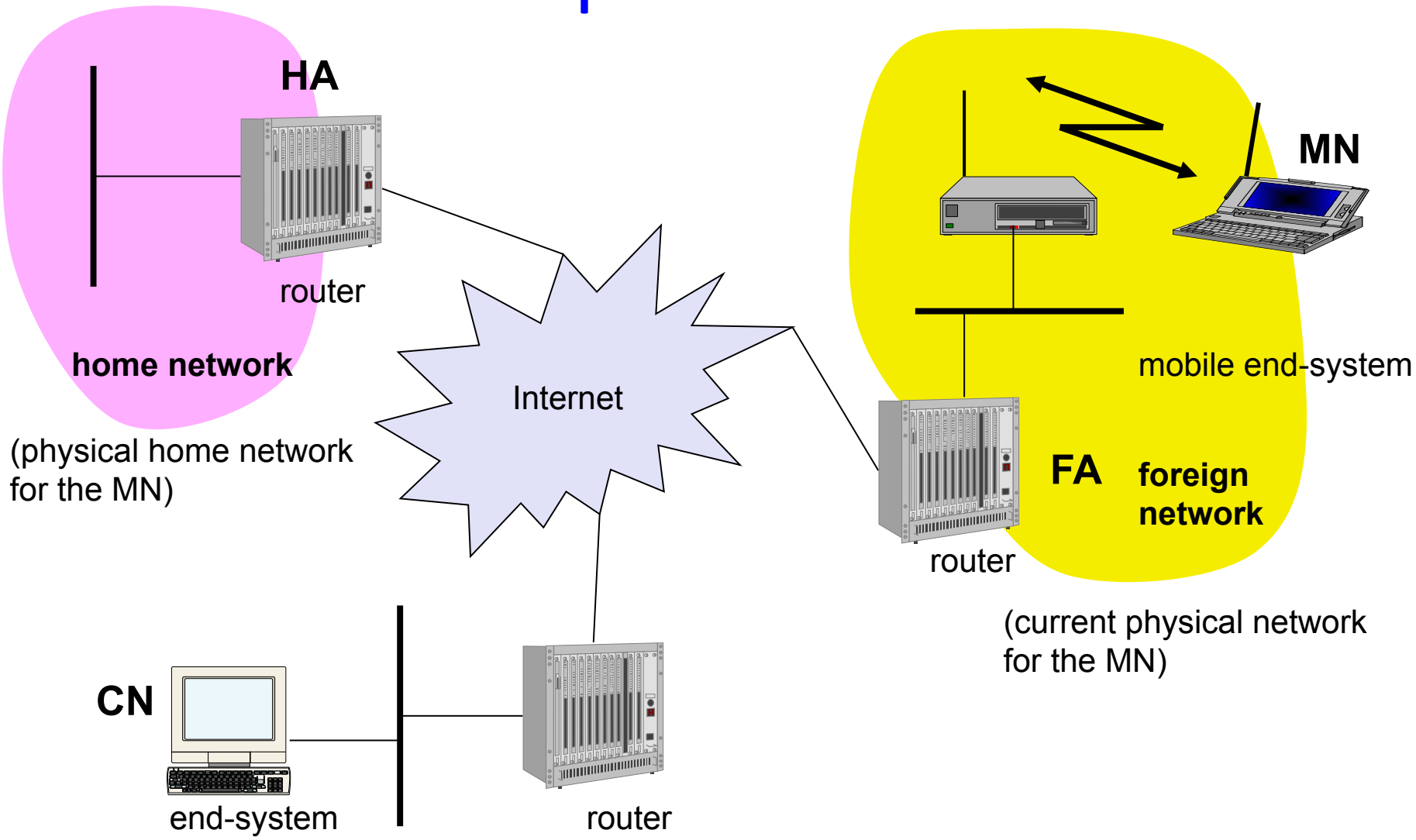
Requirements to Mobile IP (RFC 2002)

- 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

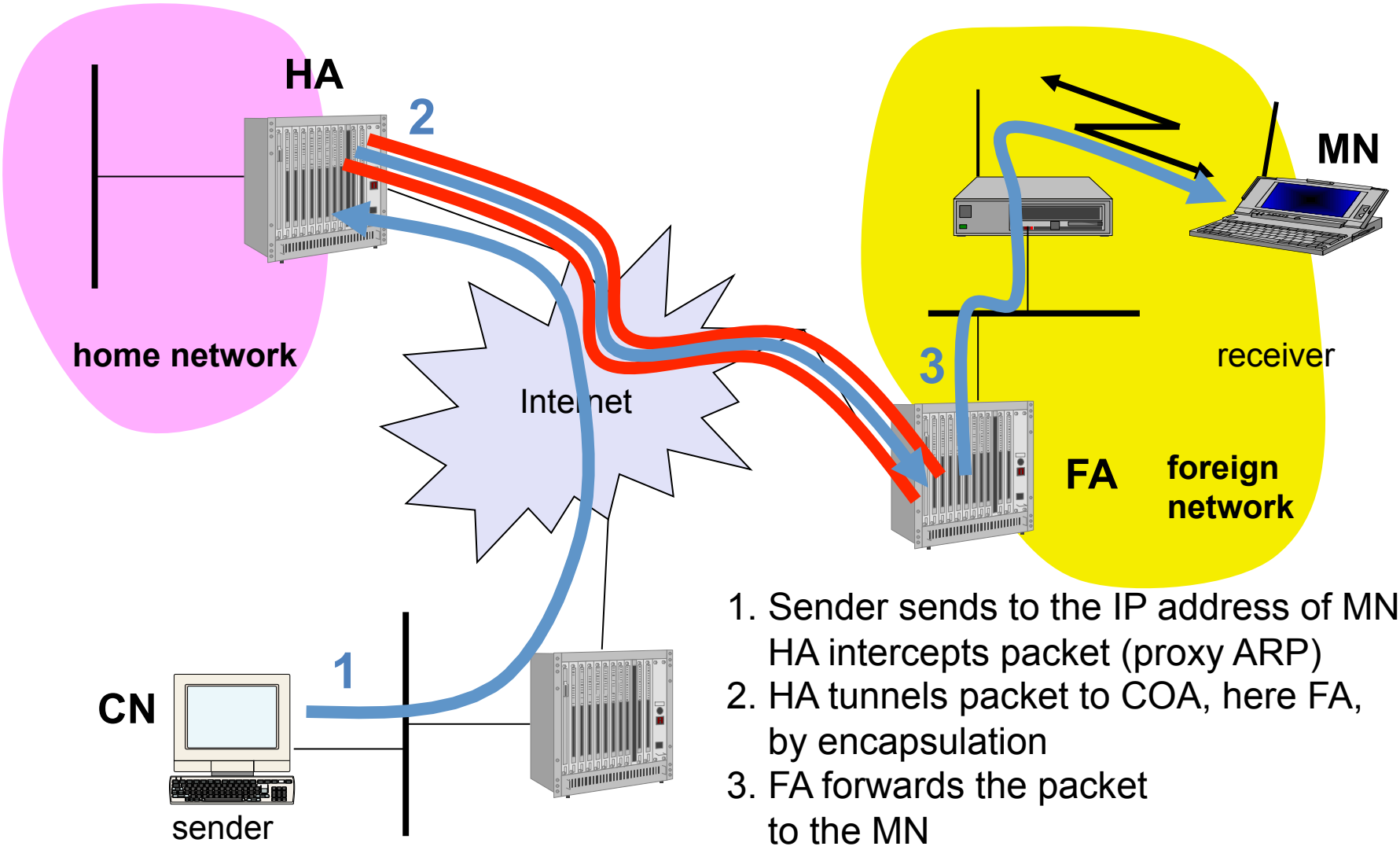
Terminology

- 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)
  - 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

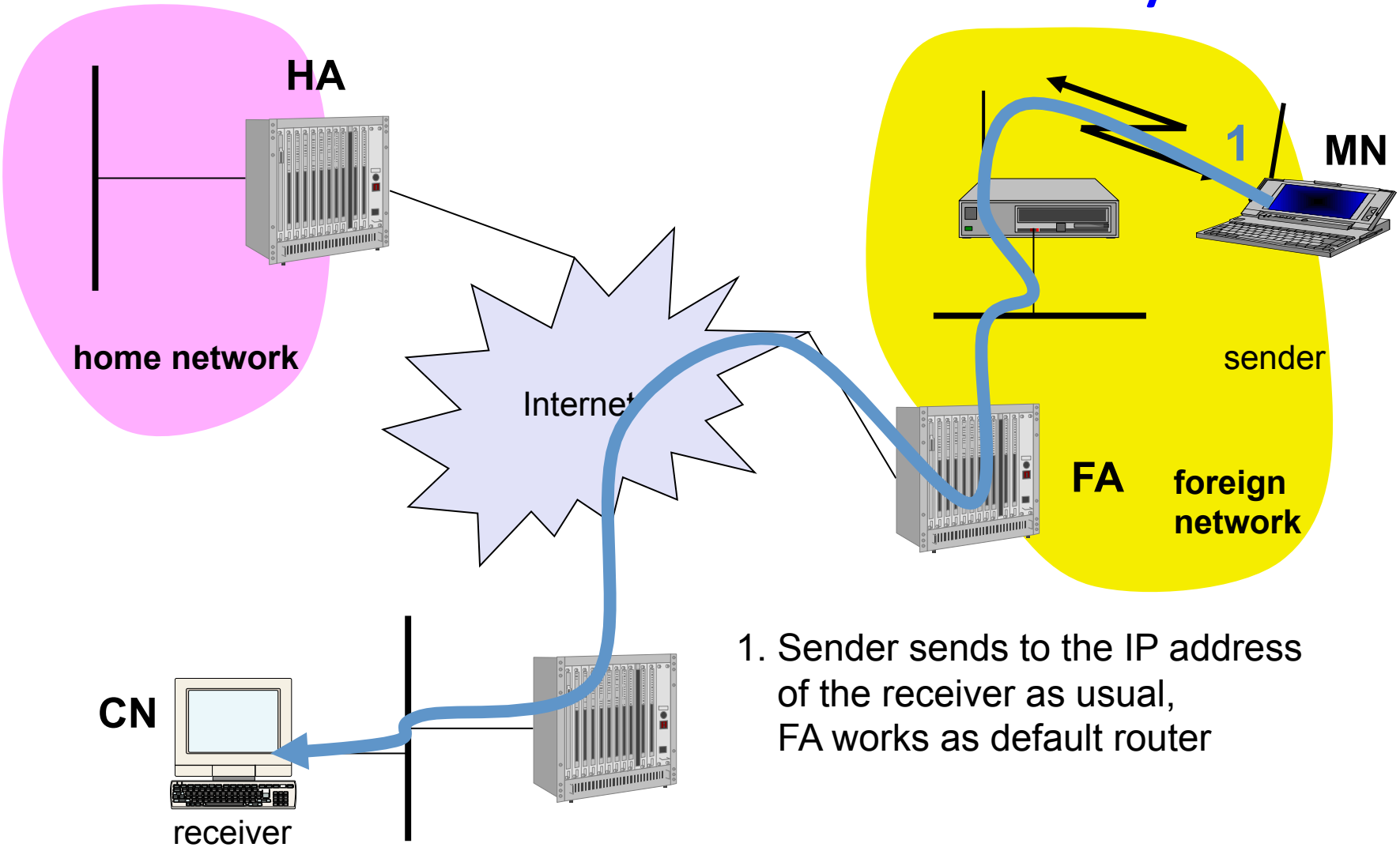


Data transfer to the mobile system



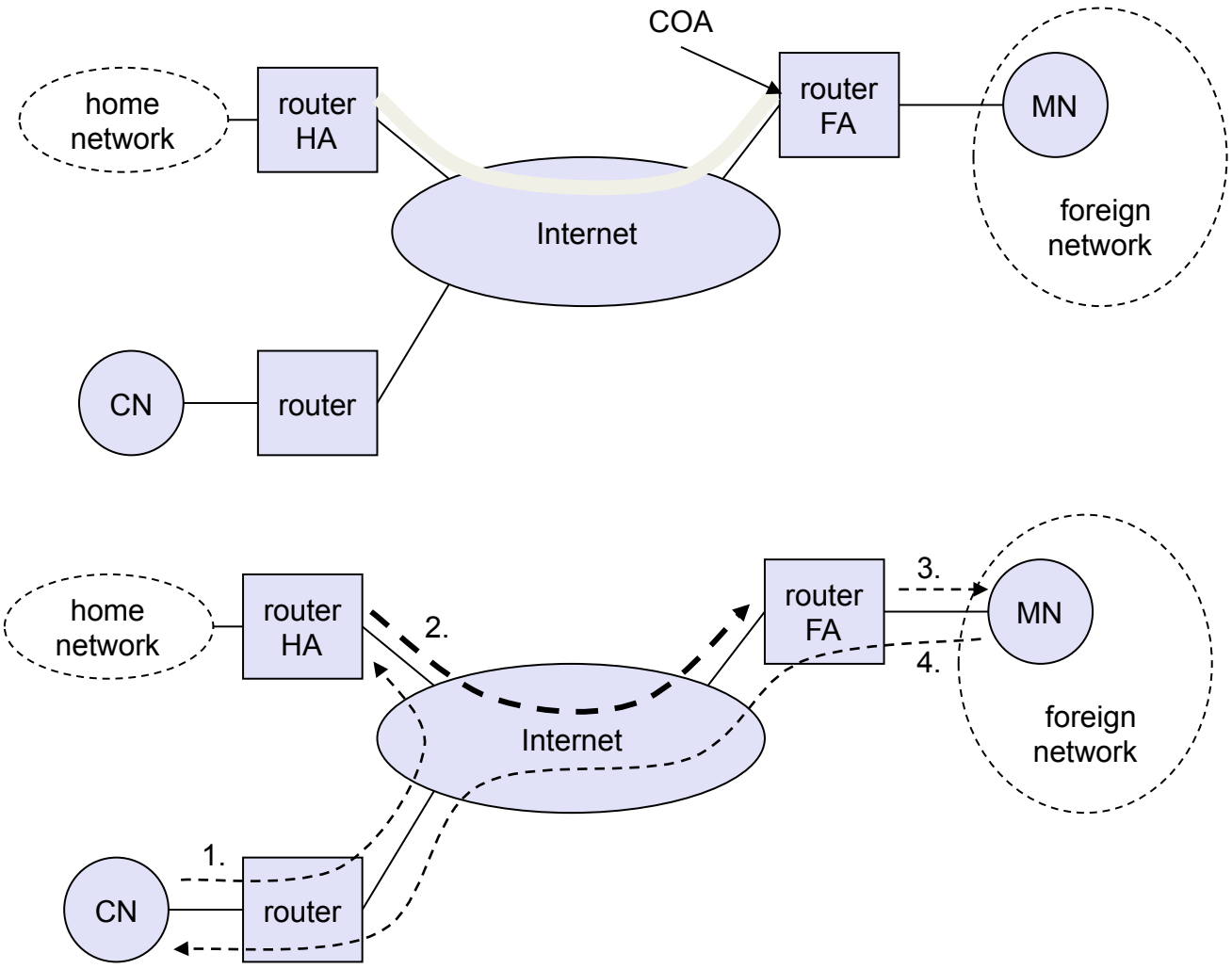
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



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

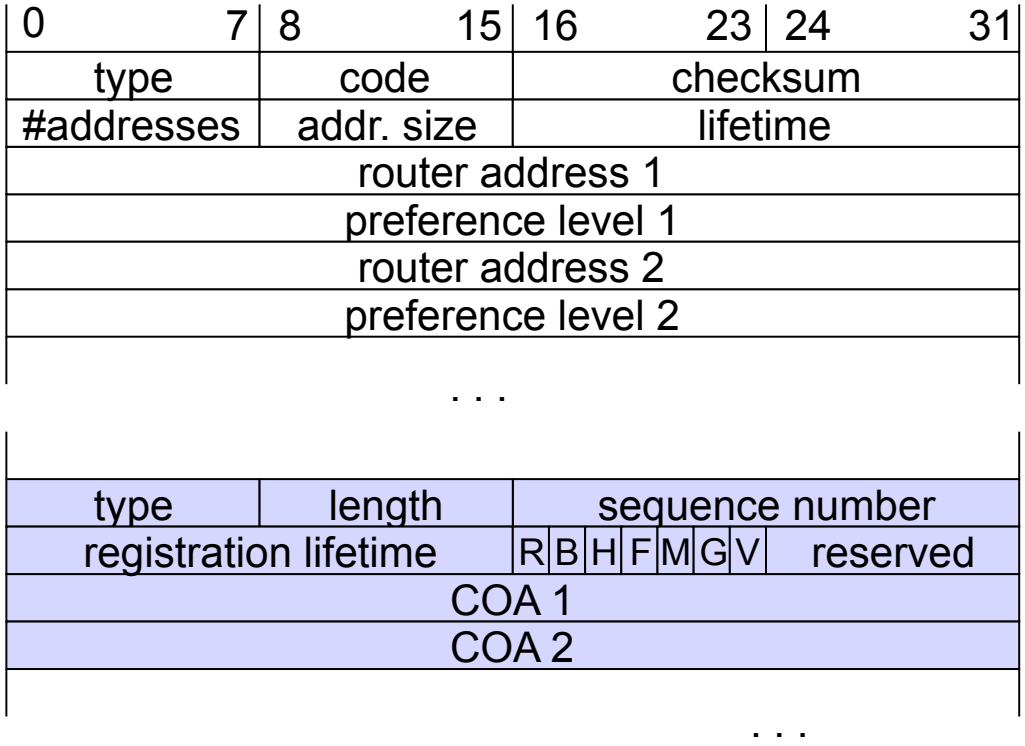
Overview


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 (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

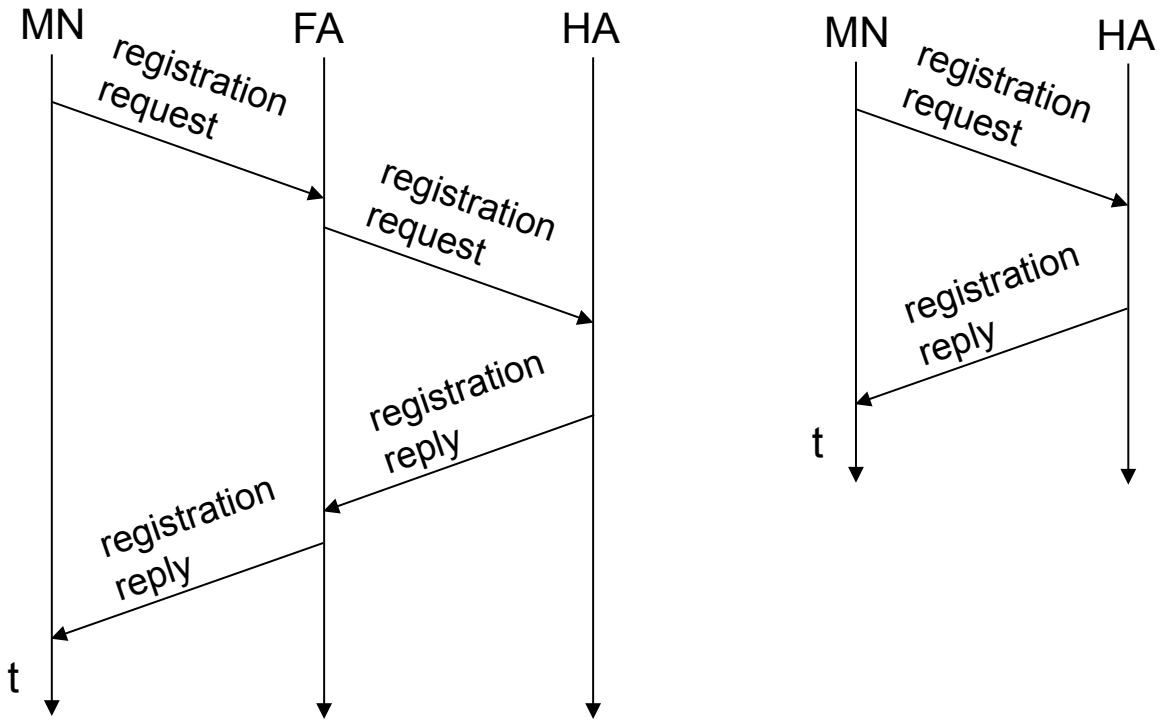


R: registration required
B: busy
H: home agent
F: foreign agent
M: minimal encapsulation
G: generic routing encapsulation
V: header compression

ICMP-Type = 9; Code = 0/16; Extension Type = 16

TTL = 1 Dest-Adr = 224.0.0.1 (multicast on link) or 255.255.255.255 (broadcast)

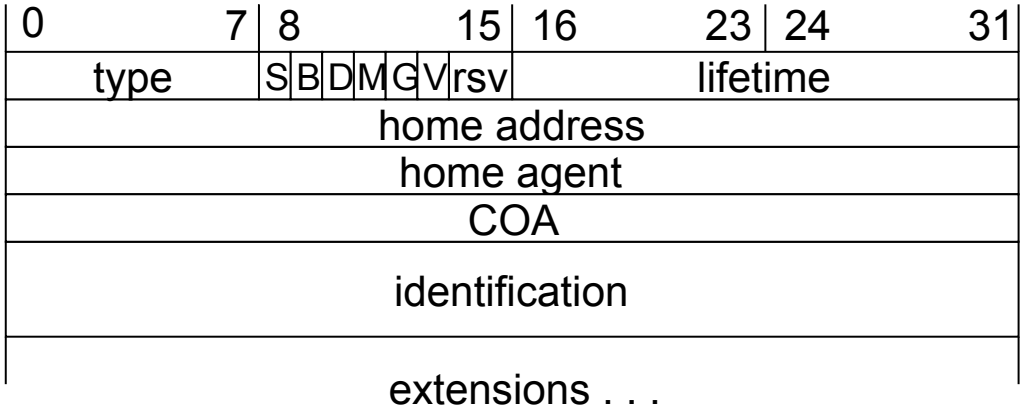
Registration



Goal: inform the home agent of current location of MN (COA-FA or co-located COA)

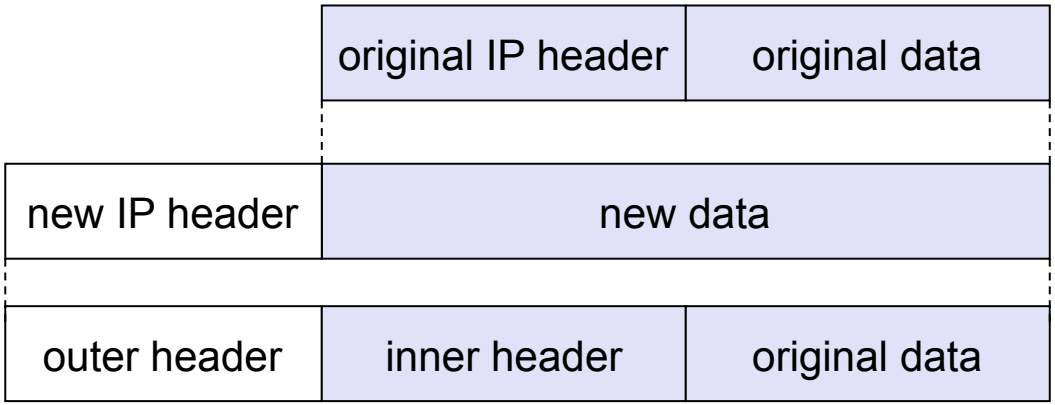
Registration expires automatically (lifetime)
Uses UDP port 434

Mobile IP registration request



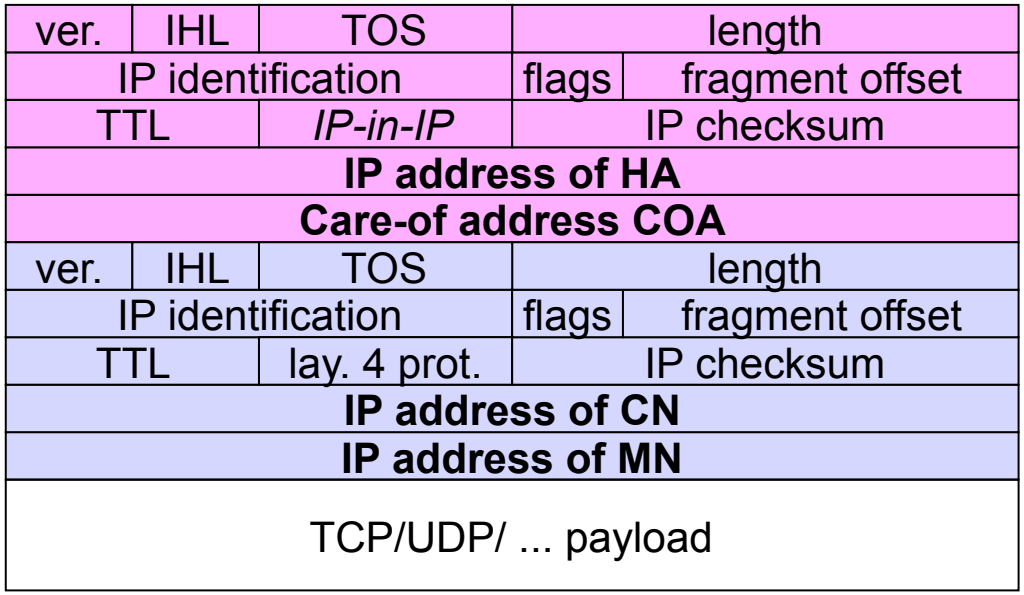
UDP packet on port 343
Type = 1 for registration request
S: retain prior mobility bindings
B: forward broadcast packets
D: co-located address=> MN decapsulates packets

Encapsulation



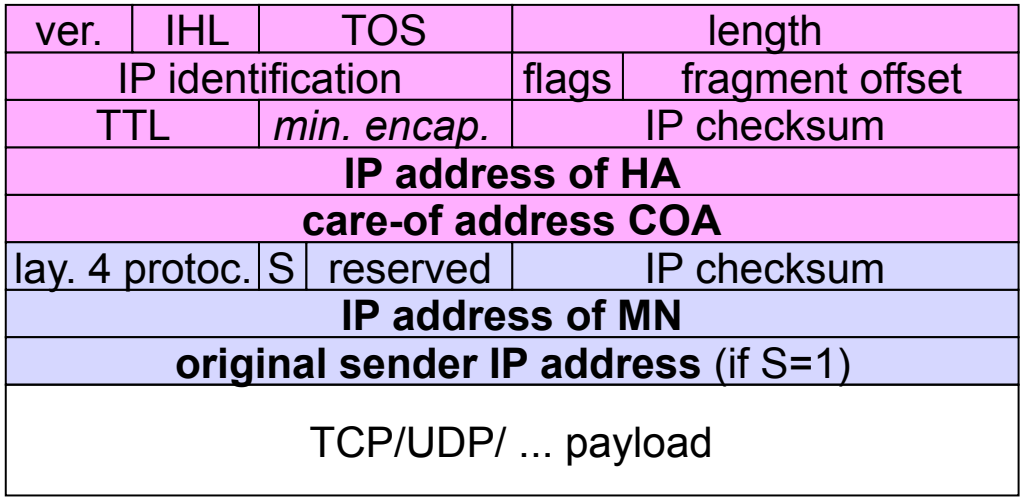
Encapsulation I

- 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 in RFC 2003)
  - tunnel between HA and COA

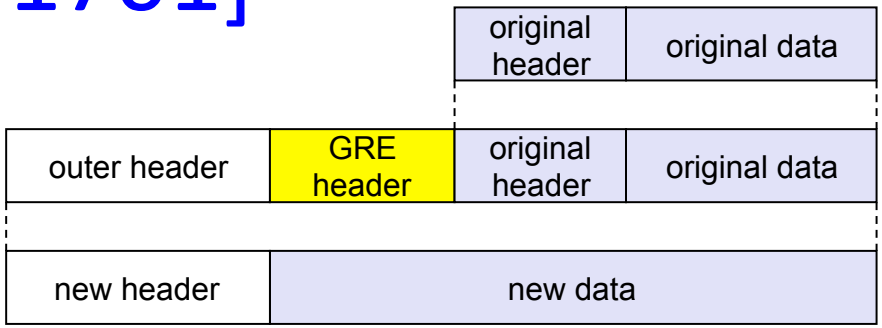


Encapsulation II

- Minimal encapsulation (optional) [RFC2004]
  - avoids repetition of identical fields
  - e.g. TTL, IHL, version, TOS
  - only applicable for unfragmented packets, no space left for fragment identification



Generic Routing Encapsulation [RFC 1701]



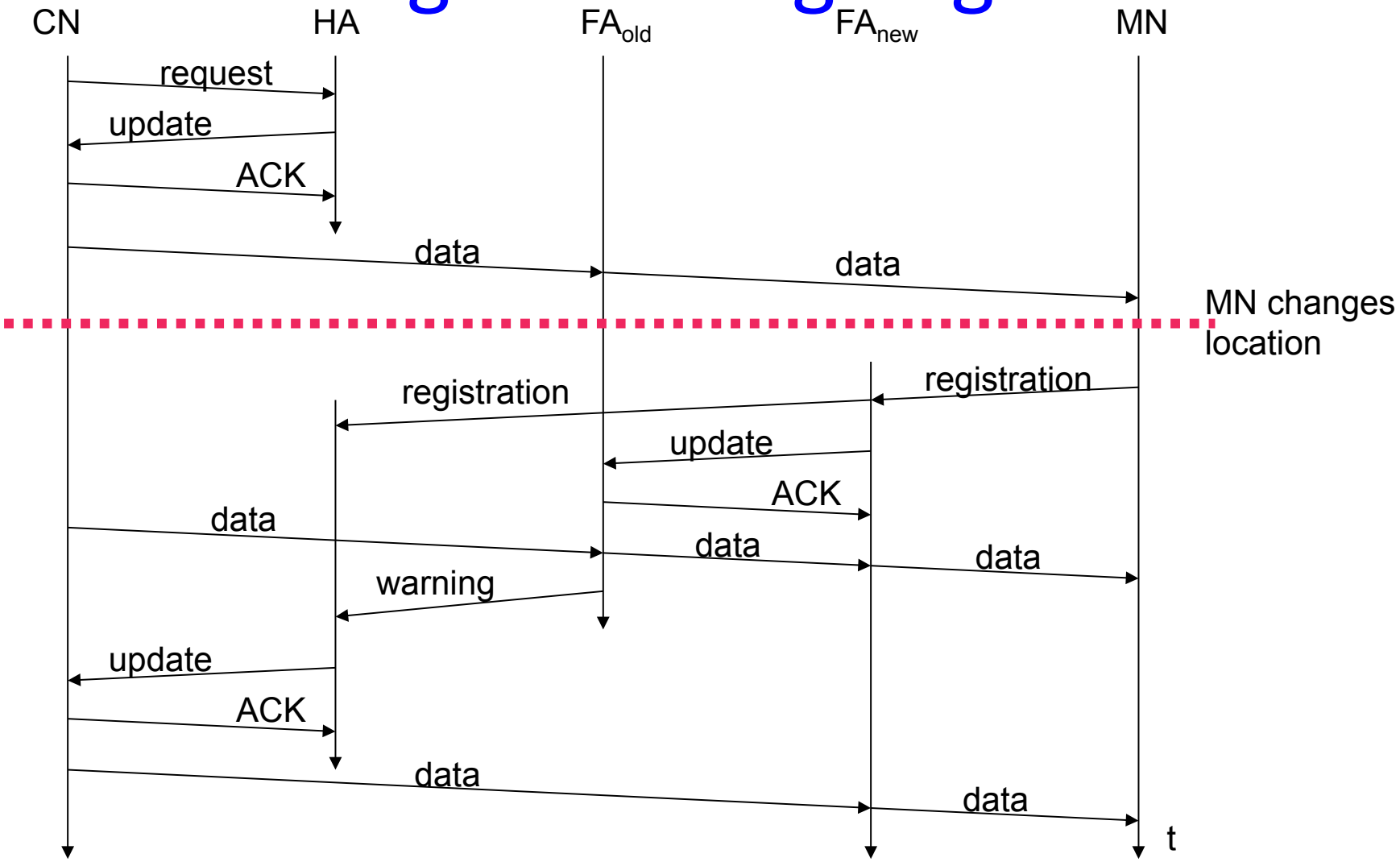
ver.	IHL	TOS	length
IP identification		flags	fragment offset
TTL	*GRE*	IP checksum	
IP address of HA			
Care-of address COA			
C R K S s rec.	rsv.	ver.	protocol
checksum (optional)		offset (optional)	
key (optional)			
sequence number (optional)			
routing (optional)			
ver.	IHL	TOS	length
IP identification		flags	fragment offset
TTL	lay. 4 prot.	IP checksum	
IP address of CN			
IP address of MN			
TCP/UDP/ ... payload			

C: checksum present
R: offset/source routing is present
K: key field for authentication (not implemented)
S:sequence number is present
s: strict source routing is used
rec: Recursion control

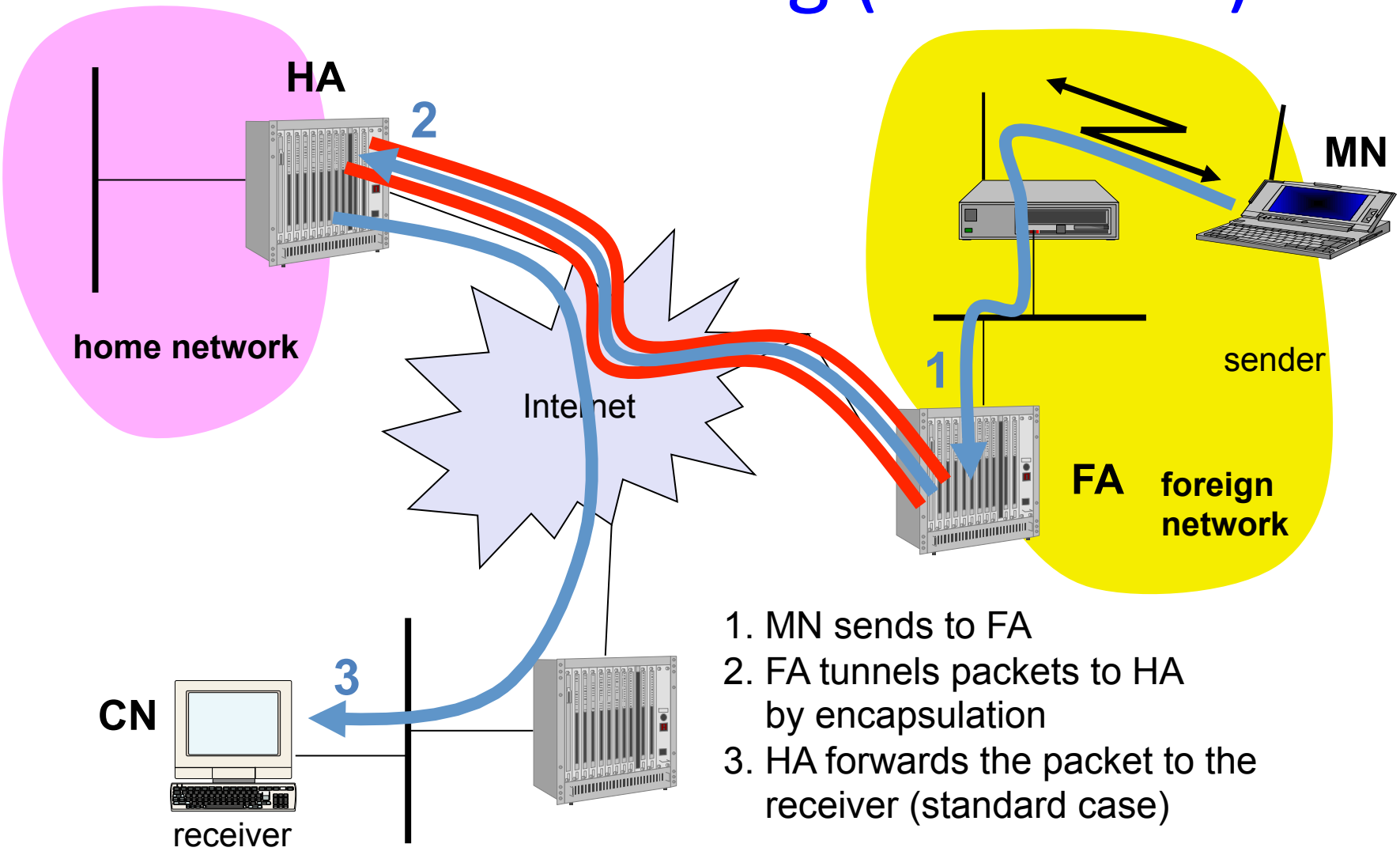
Optimization of packet forwarding

- 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 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 topologically correct
  - furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is too 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 new standard is backwards compatible
  - the extensions can be implemented easily and cooperate with current implementations without these extensions

Mobile IP and IPv6

- 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 autoconfiguration
  - no need for a separate FA, **all** routers perform router advertisement which can be used instead of the special agent advertisement
  - MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
  - „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

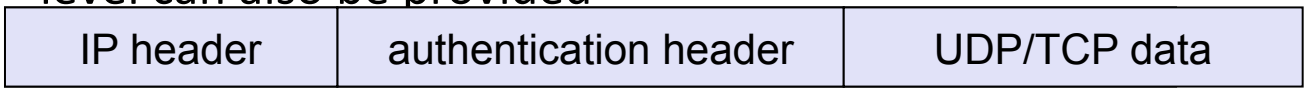
- Security
  - authentication with FA problematic, for the FA typically belongs to another organization
  - no protocol for key management and key distribution has been standardized in the Internet
  - patent and export restrictions
- Firewalls
  - typically mobile IP cannot be used together with firewalls, 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!

Security in Mobile IP

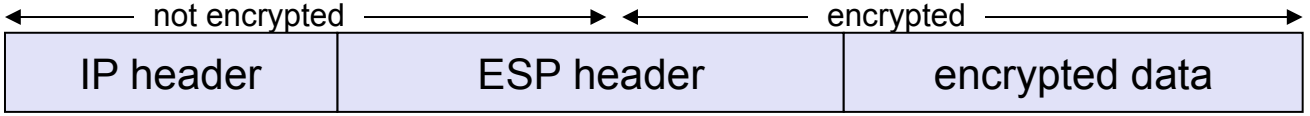
- Security requirements (Security Architecture for the Internet Protocol, RFC 1825, RFC 1826, RFC 1827)
  - Integrity
    any changes to data between sender and receiver can be detected by the receiver
  - Authentication
    sender address is really the address of the sender and all data received is really data sent by this sender
  - Confidentiality
    only sender and receiver can read the data
  - Non-Repudiation
    sender cannot deny sending of data
  - Traffic Analysis
    creation of traffic and user profiles should not be possible
  - Replay Protection
    receivers can detect replay of messages

IP security architecture I

- Two or more partners have to negotiate security mechanisms to setup a security association
  - typically, all partners choose the same parameters and mechanisms
- Two headers have been defined for securing IP packets:
  - Authentication-Header
    - guarantees integrity and authenticity of IP packets
    - if asymmetric encryption schemes are used, some non-repudiation level can also be provided

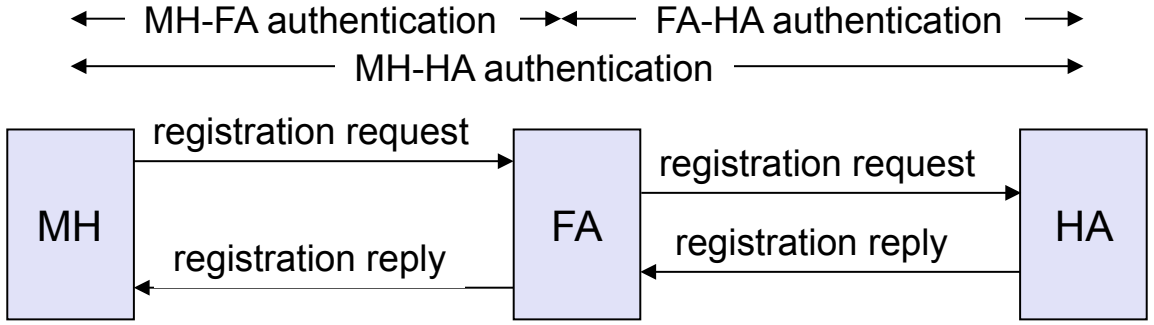


  - Encapsulation Security Payload
    - protects confidentiality between communication partners



IP security architecture II

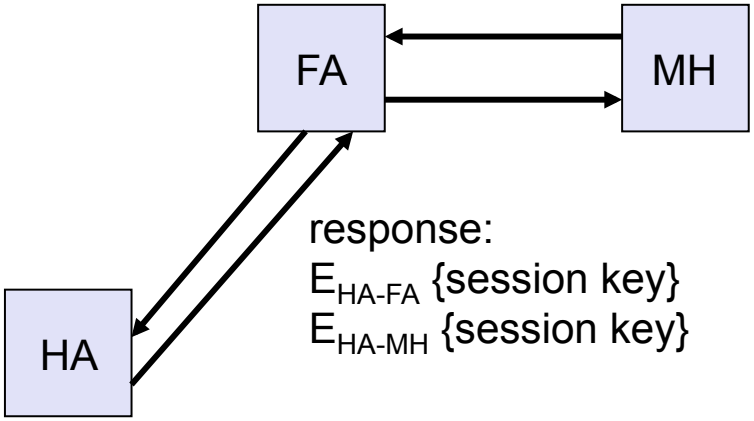
- Mobile Security Association for registrations
  - parameters for the mobile host (MH), home agent (HA), and foreign agent (FA)
- Extensions of the IP security architecture
  - extended authentication of registration



  - prevention of replays of registrations
    - time stamps: 32 bit time stamps + 32 bit random number
    - nonces: 32 bit random number (MH) + 32 bit random number (HA)

Key distribution

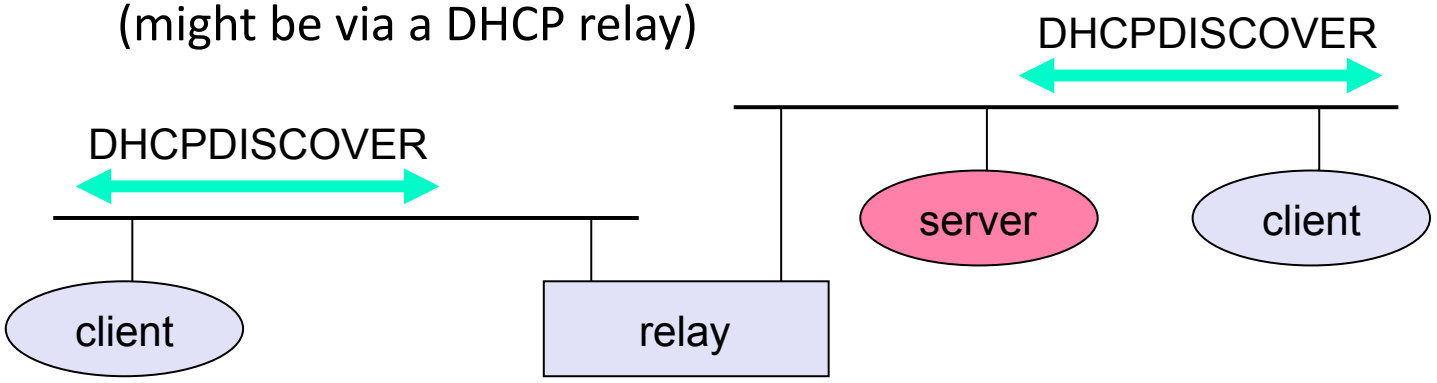
- Home agent distributes session keys



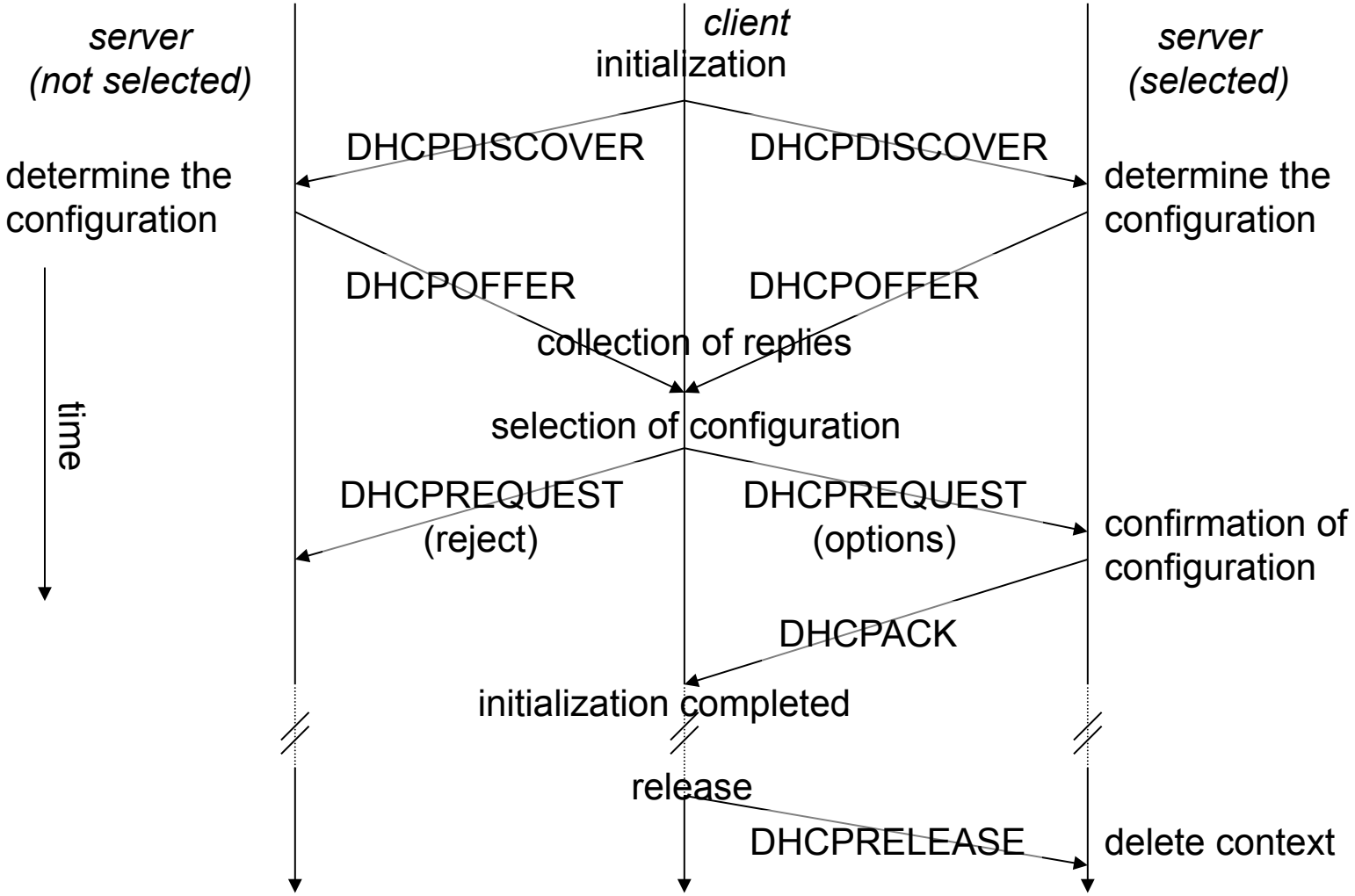
- ❑ foreign agent has a security association with the home agent
- ❑ mobile host registers a new binding at the home agent
- ❑ home agent answers with a new session key for foreign agent and mobile node

DHCP: Dynamic Host Configuration Protocol [RFC 2131]

- 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 - protocol mechanisms



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)
- Security problems!
  - DHCP Authentication IETF-RFC 3118