

Chapter 6

Mobile Network Layer

Mobile IP

- Routing
 - based on IP destination address, 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 for Mobile IP

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

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

-Scalability and Efficiency

- 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

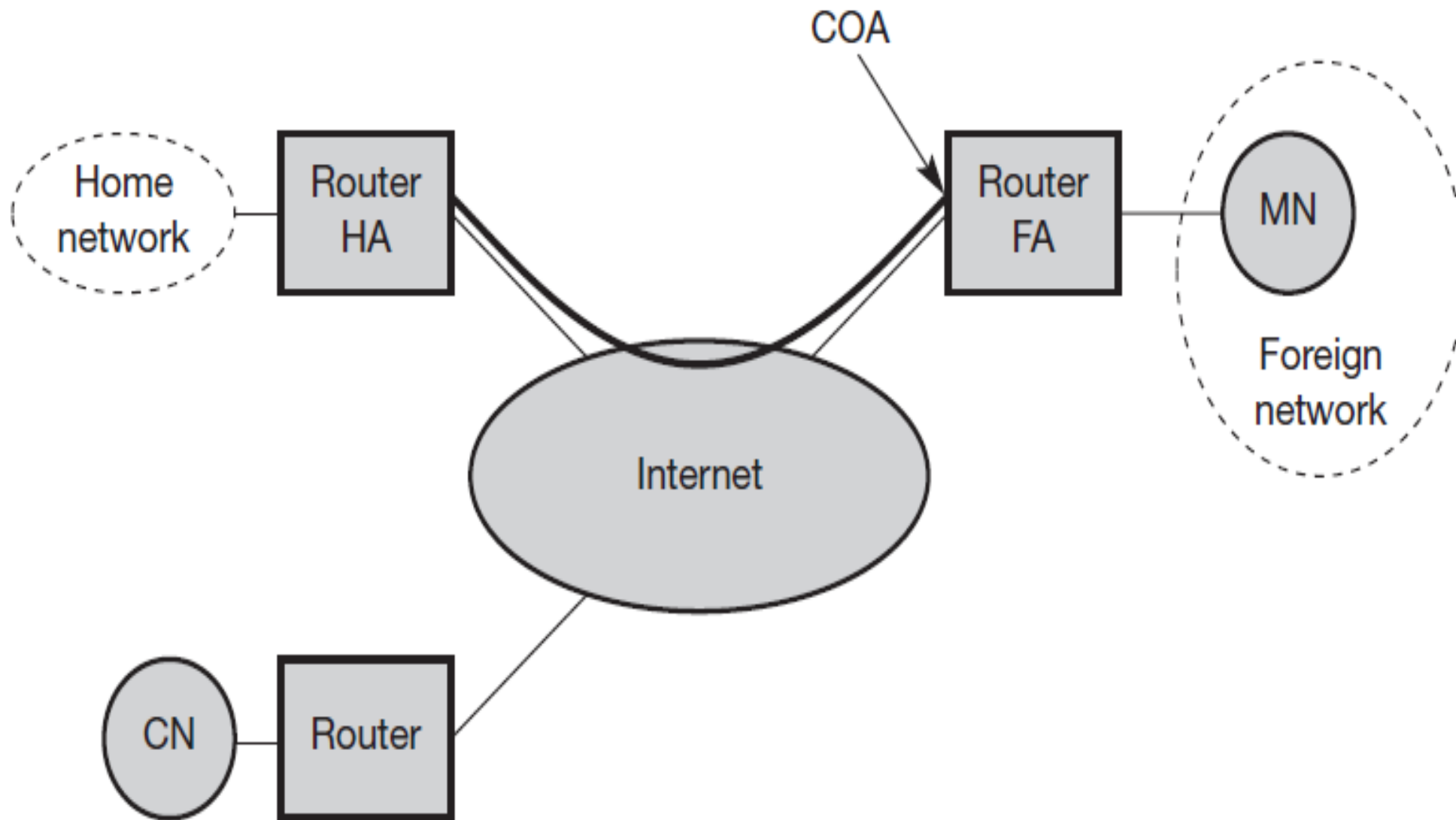
Security

- authentication of all registration messages

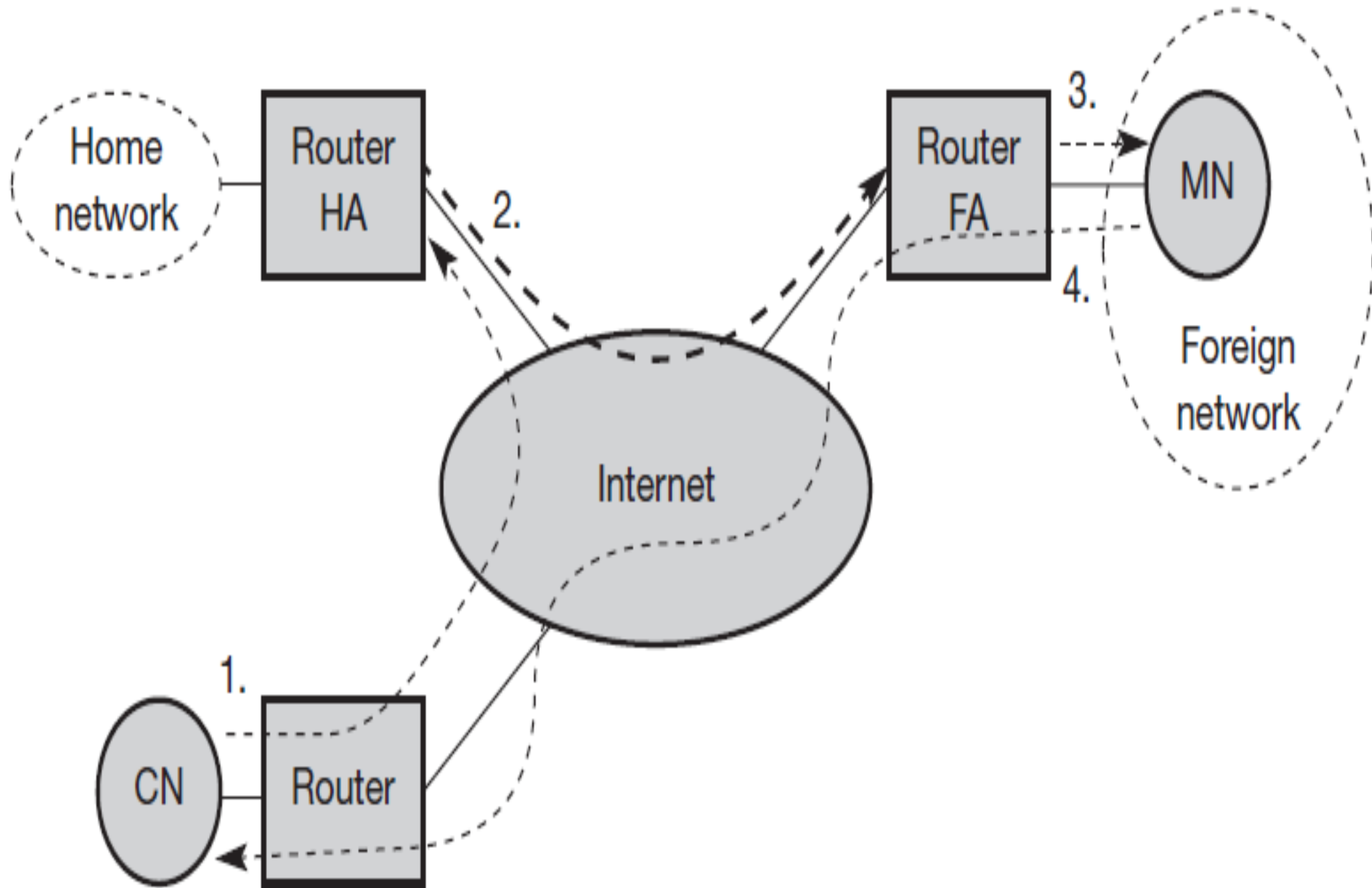
Terminology

- Mobile Node (MN)
 - system (**node**) that can **change point of connection** to network **without changing** its **IP** address
- Home Agent (HA)
 - system in **home network** of the **MN**, typically a **router**
 - **registers location** of **MN**, **tunnels IP datagrams** to **COA**
- Foreign Agent (FA)
 - system in **current foreign network** of **MN**, typically a **router**
 - **forwards tunneled datagrams** to **MN**, typically also **default router** for **MN**
- Care-of Address (COA)
 - **address** of **current tunnel end-point** for **MN** (at **FA** or **MN**)
 - **actual location** of **MN** from an **IP** point of view
 - can be **chosen**, e.g., via **DHCP**
- Correspondent Node (CN)
 - **communication partner**, device that communicates with **MN**

Mobile IP example network



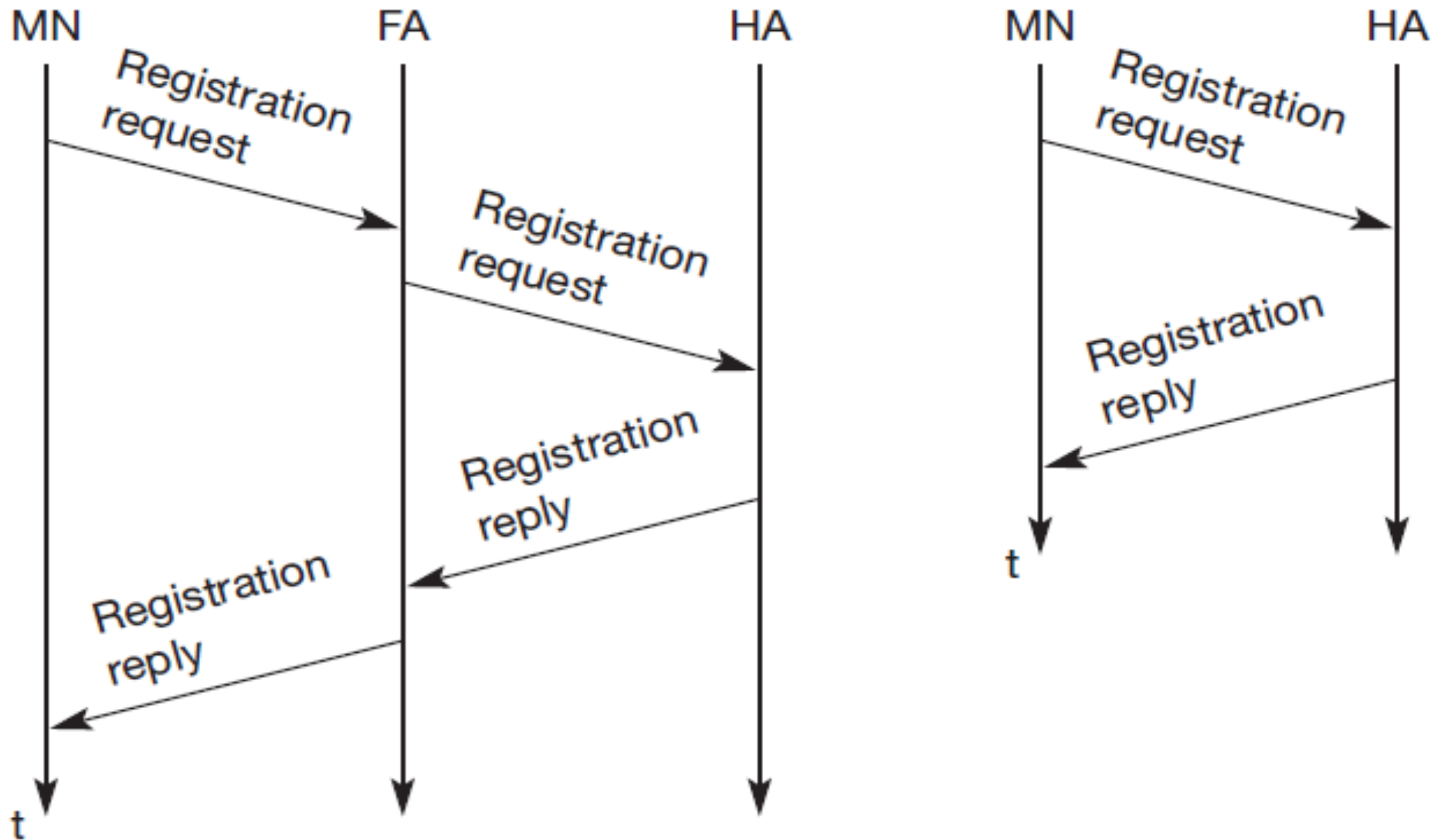
IP Packet Delivery



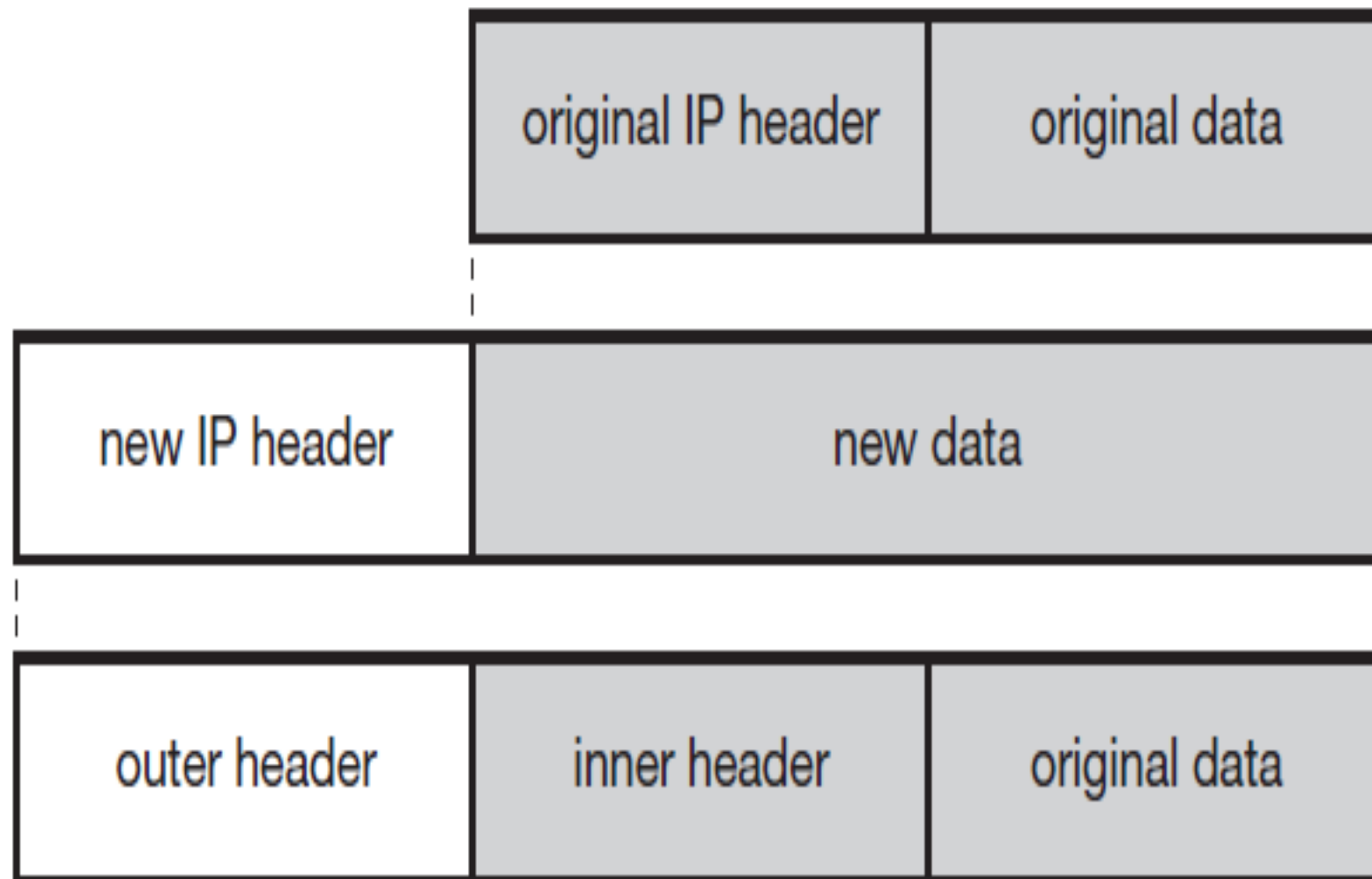
Network Integration

- 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 FA, HA acknowledges via FA to MN
 - these actions have to be secured by authentication
- Advertisement
 - HA advertises IP address of 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 MN are sent to HA,
 - independent of changes in COA/FA

Registration



Tunneling and Encapsulation



IP-in-IP encapsulation

Encapsulation of one packet into another as payload

e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)

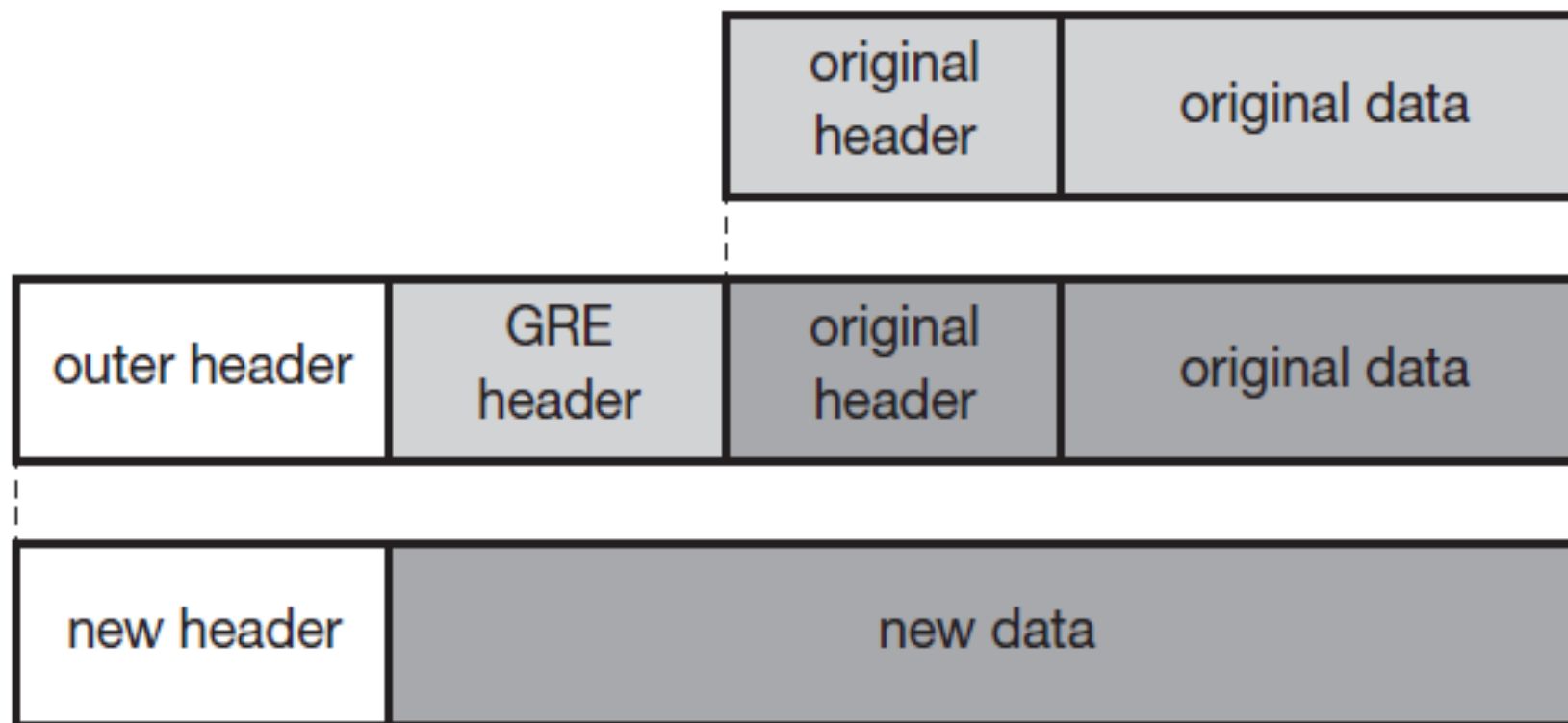
here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)

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

tunnel between HA and COA

ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		<i>IP-in-IP</i>	IP checksum	
IP address of HA				
Care-of address of 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				

Generic Routing Encapsulation (GRE)



Protocol fields for GRE according to RFC 1701

ver.		IHL		DS (TOS)		length			
IP identification						flags		fragment offset	
TTL				GRE		IP checksum			
IP address of HA									
care-of address of 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									

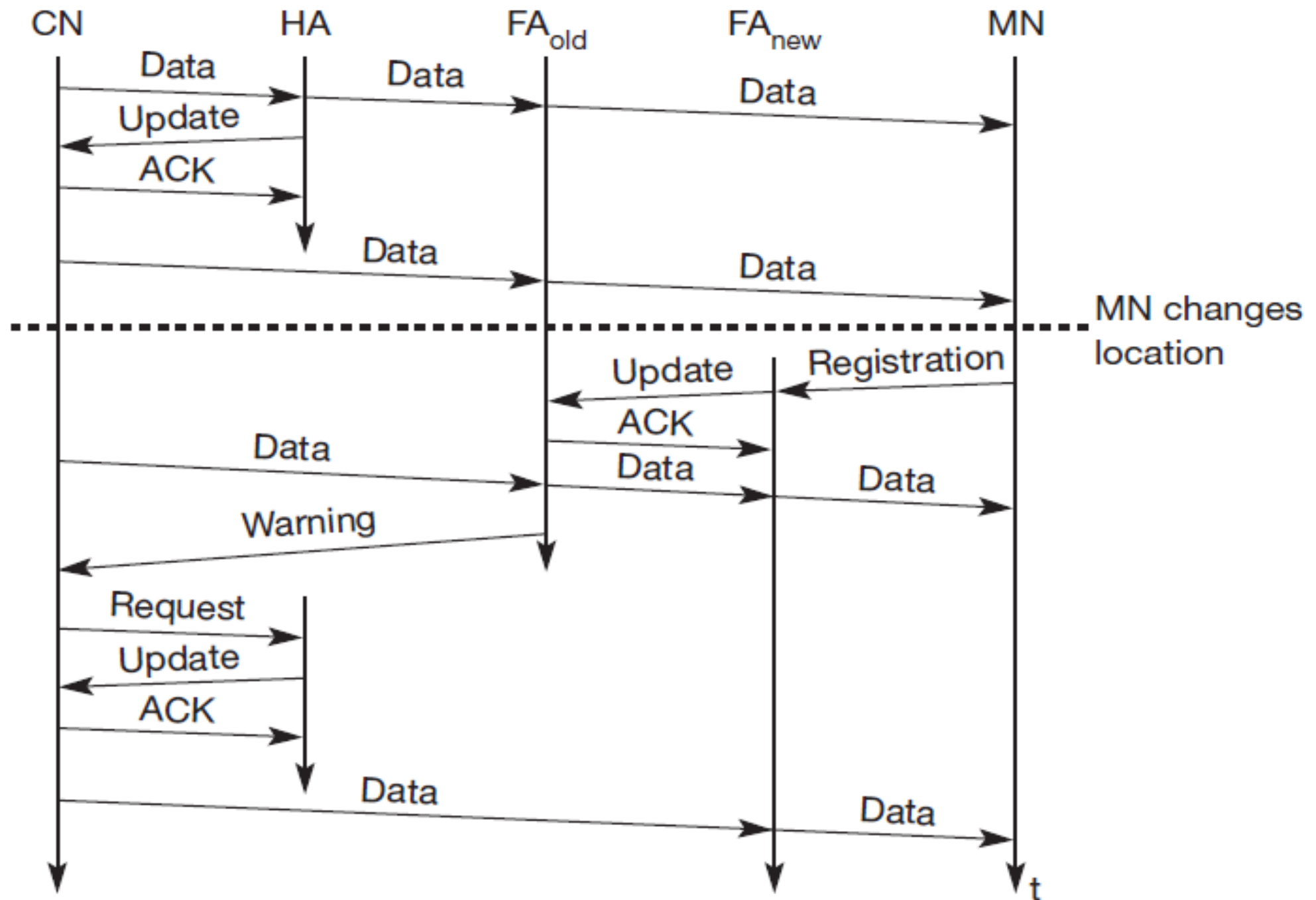
Protocol fields for GRE according to RFC 2784

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

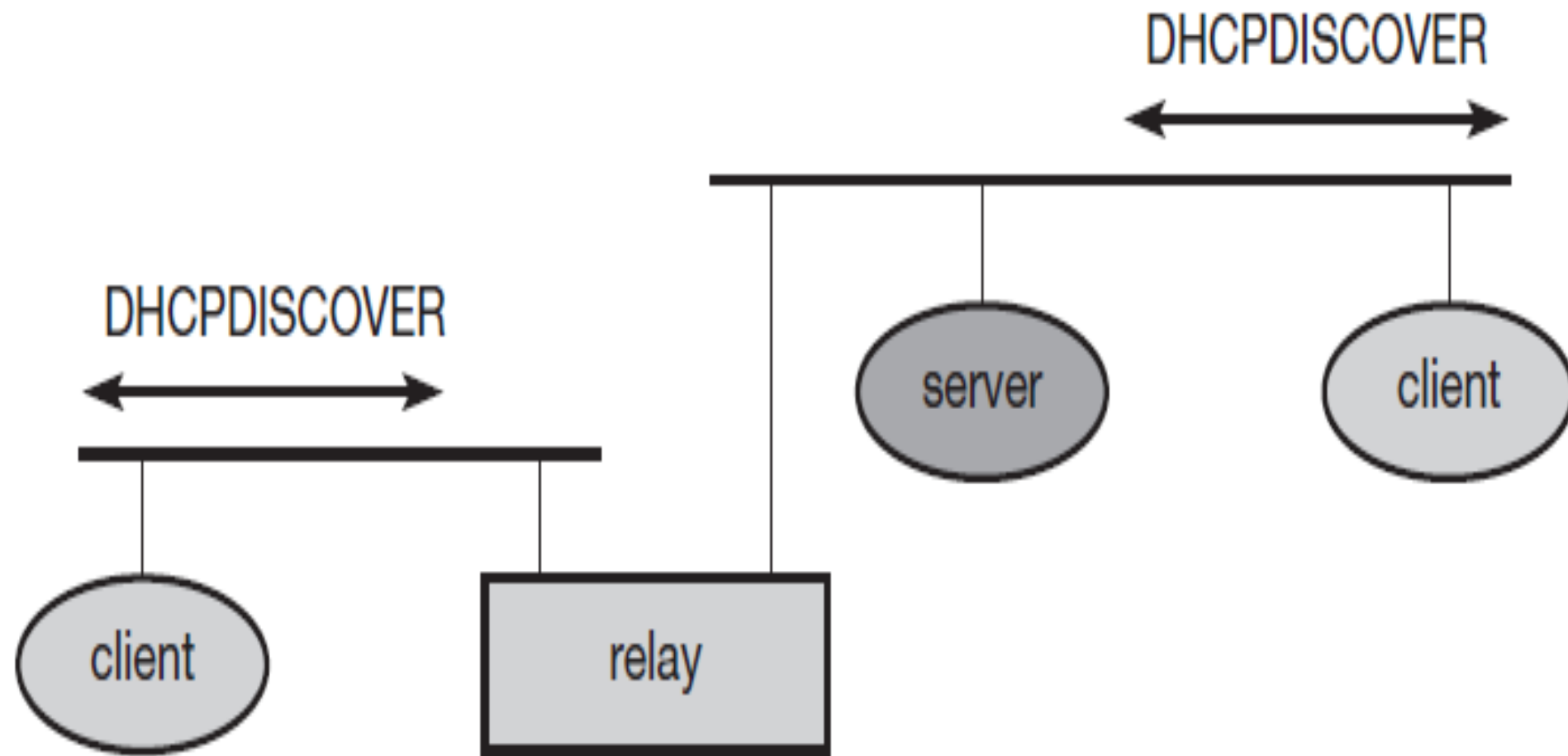
Change of the foreign agent with an optimized mobile IP



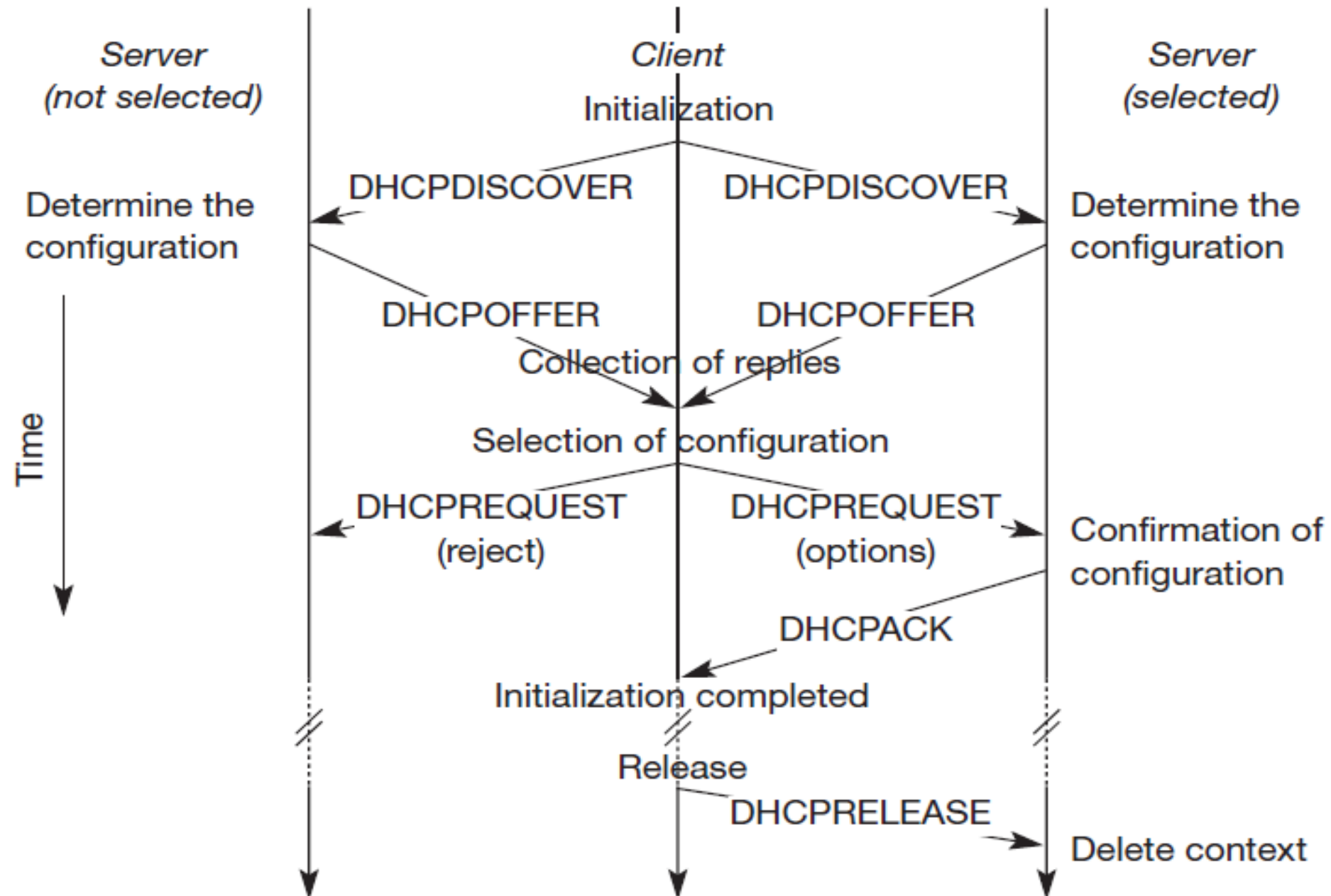
DHCP: Dynamic Host Configuration Protocol

- 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)

Basic DHCP Configuration



Client initialization via DHCP



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)

Mobile Ad hoc Networks

- Standard Mobile IP needs an infrastructure
 - Home Agent/Foreign Agent in the fixed network
 - DNS, routing etc. are not designed for mobility
- Sometimes there is no infrastructure!
 - remote areas, ad-hoc meetings, disaster areas
 - cost can also be an argument against an infrastructure!
- Main topic: Routing
 - no default router available
 - every node should be able to forward

Mobile Ad hoc Networks

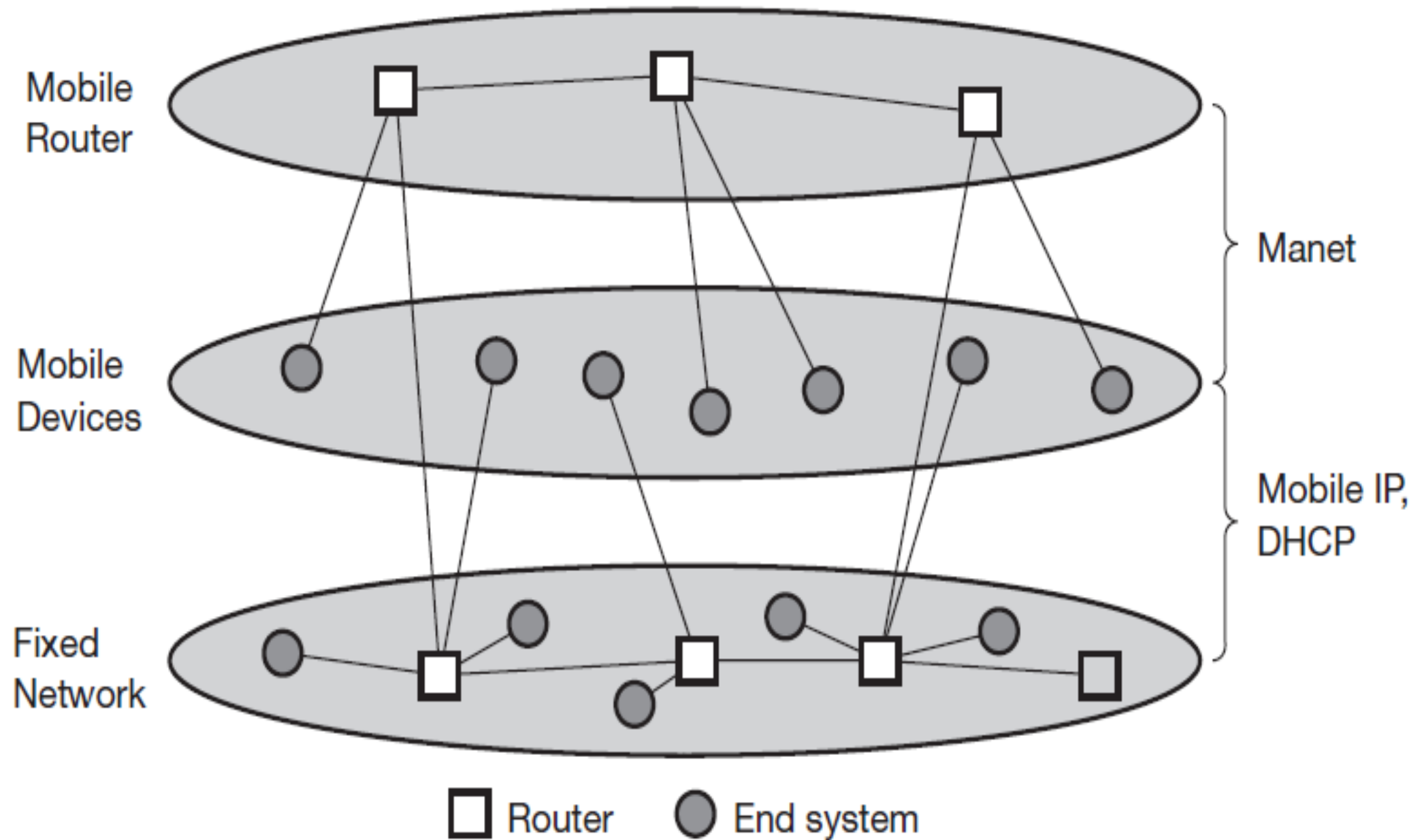
Single Hop

- nodes do not act as routers and communication between nodes is within each other's Radio Frequency (RF) range.

Multihop

- nodes act as routers and route or forward the traffic of other nodes.

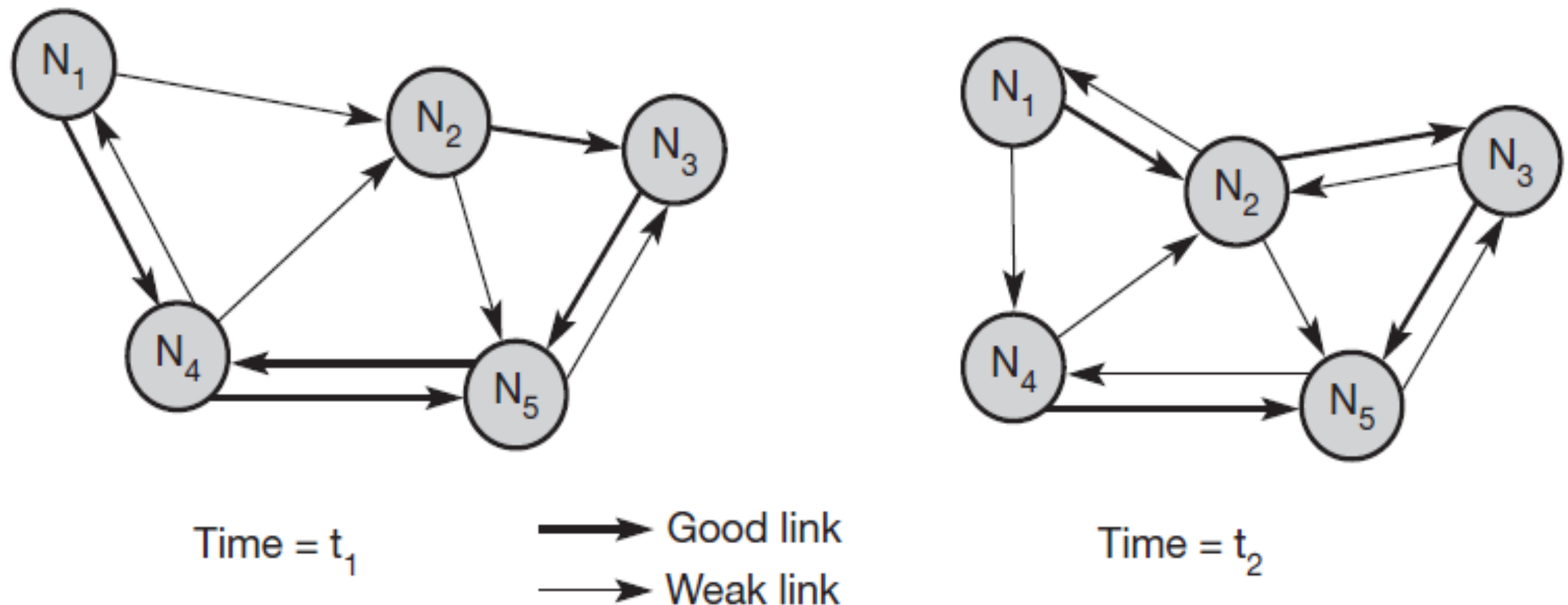
MANETs and Mobile IP



Example Ad-hoc Network

► Highly dynamic network topology

- ☐ Device mobility plus varying channel quality
- ☐ Separation and merging of networks possible
- ☐ Asymmetric connections possible



MANET Routing

Wired networks and Ad-hoc Wireless networks

☐ Asymmetric links

☐ Redundant links

☐ Interference

☐ Dynamic topology

Traditional Routing Algorithms

- Distance Vector
 - periodic exchange of messages with all physical neighbors that contain information about who can be reached at what distance
 - selection of the shortest path if several paths available
- Link State
 - periodic notification of all routers about current state of all physical links
 - router get a complete picture of the network
- Example
 - ARPA packet radio network (1973), DV-Routing
 - every 7.5s exchange of routing tables including link quality
 - updating of tables also by reception of packets
 - routing problems solved with limited flooding

Routing in Ad-hoc Networks

- THE big topic in many research projects
 - Far more than 50 different proposals exist
 - The most simplest one: Flooding!
- Reasons
 - Classical approaches from fixed networks fail
 - Very slow convergence, large overhead
 - High dynamicity, low bandwidth, low computing power
- Metrics for routing
 - Minimal
 - Number of nodes, loss rate, delay, congestion, interference ...
 - Maximal
 - Stability of the logical network, battery run-time, time of connectivity

Problems of Traditional Routing Algorithms

- Dynamic nature of the topology
 - frequent changes of connections, connection quality, participants
- Limited performance of mobile systems
 - periodic updates of routing tables need energy without contributing to the transmission of user data, sleep modes difficult to realize
 - limited bandwidth of the system is reduced even more due to the exchange of routing information
 - links can be asymmetric, i.e., they can have a direction dependent transmission quality

DSDV (Destination Sequenced Distance Vector)

- Early work: AODV
 - AODV - on demand version: AODV = Ad-hoc On Demand Distance Vector
 - AODV - establishes routes to destinations on demand (routes are requested by the source node)
 - AODV - used in ZigBee – a low power, low data rate wireless ad hoc network
- DSDV: Expansion of distance vector routing
 - solve the routing loop problem
 - Each entry in routing table contains a **sequence number**,
 - sequence numbers = **even** if a **link is present**; else, an **odd** number is **used**
- **Sequence numbers for all routing updates**
 - assures **in-order execution** of all updates
 - avoids loops and inconsistencies
- **Decrease of Update Frequency**
 - store time between first and best announcement of a path
 - inhibit update if it seems to be unstable (based on the stored time values)

Dynamic Source Routing (DSR)

- Split routing into two parts:
 - discovering a path and
 - maintaining a path
- Route Discovery = source routes to destination (Route Request/Reply)
 - only if a path for sending packets to a certain destination is needed and no path is currently available
- Route Maintenance = maintain broken links (Route Error)
 - only while the path is in use one has to make sure that it can be used continuously
- No periodic updates needed!

Dynamic Source Routing (DSR)

- Path Discovery
 - broadcast a packet with destination address and unique ID
 - if a station receives a broadcast packet
 - if the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet)
 - if the packet has already been received earlier (identified via ID) then discard the packet
 - otherwise, append own address and broadcast packet
 - sender receives packet with the current path (address list)
- Optimizations - use the cached information for path discovery
 - limit broadcasting if maximum diameter of the network is known
 - caching of address lists (i.e. paths) with help of passing packets
 - stations can use the cached information for path discovery (own paths or paths for other hosts)

Thank you!

Questions?