Advanced Networking Concepts
Mobility Mechanisms

Contents - Adv. Networking - Mobility Mechanisms

- Introduction
- Network Layer (Layer 3) Mobility

Introduction

Motivation for Mobility Support in the Internet

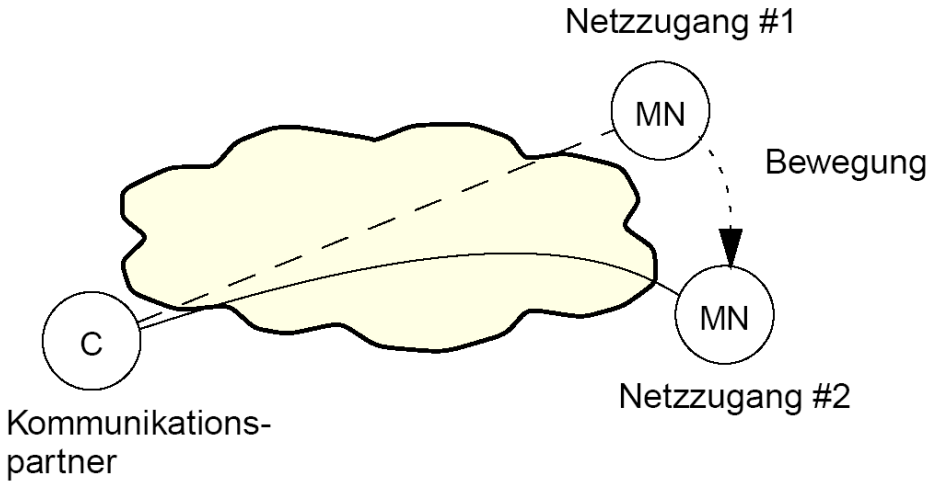
- Many new mobile Internet applications with real-time requirements (e.g. VoIP, audio and video streaming, etc.)
- Users want ubiquitous Internet access, i.e. at any time, any place and via any technology
- Today's mobile networks (GSM, UMTS) provide mobility support, but mainly based on GTP → replace GTP by IP-based mobility mechanism
- In the future, different (heterogeneous) access networks are connected to a common IP-based core network ("All-IP") - this allows an easy integration of other technologies (e.g. WLAN) and heterogeneous services
- Types of mobility support:
  - moving between subnets of the same technology (horizontal handover)
  - moving between subnets of different technology (vertical handover)

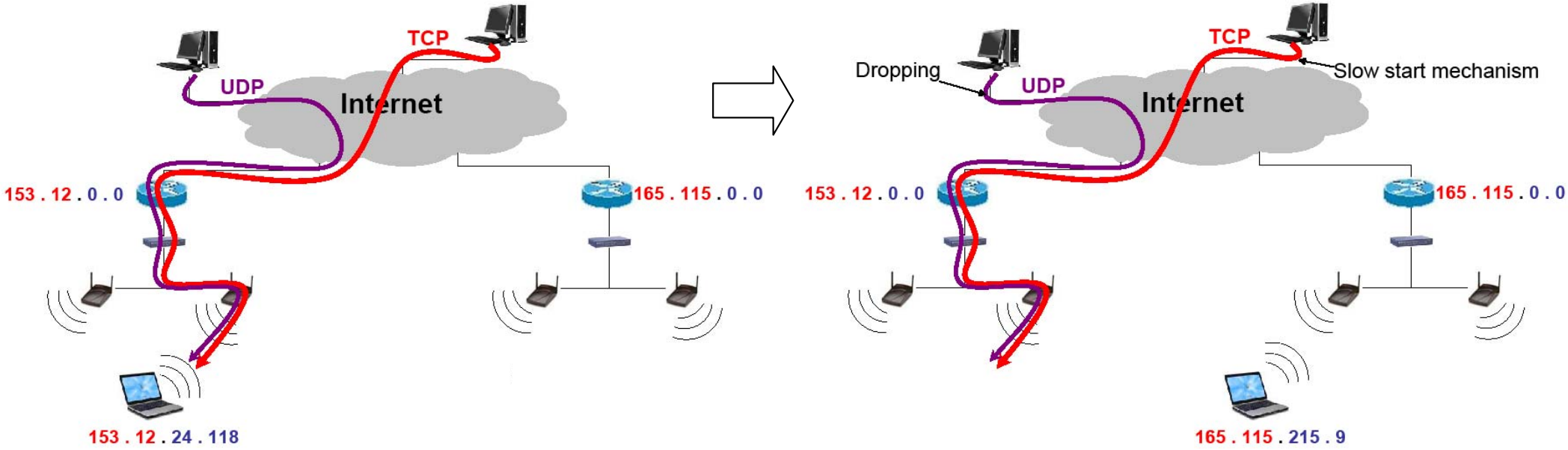
Requirements on Mobility Mechanisms

- Location of a mobile station outside of the home network
- Preservation of active connections despite movement - no impact on running applications
- Good handover performance: fast and seamless handover (low data loss)
- Low mobility signaling overhead
- Well alignment to TCP / IP protocols
- Scalability
- Robustness
- Applicability in different network scenarios
- Security
- Privacy (no unauthorized access to location information)

Mobility in the Internet - Basic Requirement

- The Internet connection (and the ongoing applications) should not be interrupted if the mobile station changes the access point (subnet)
- Example:



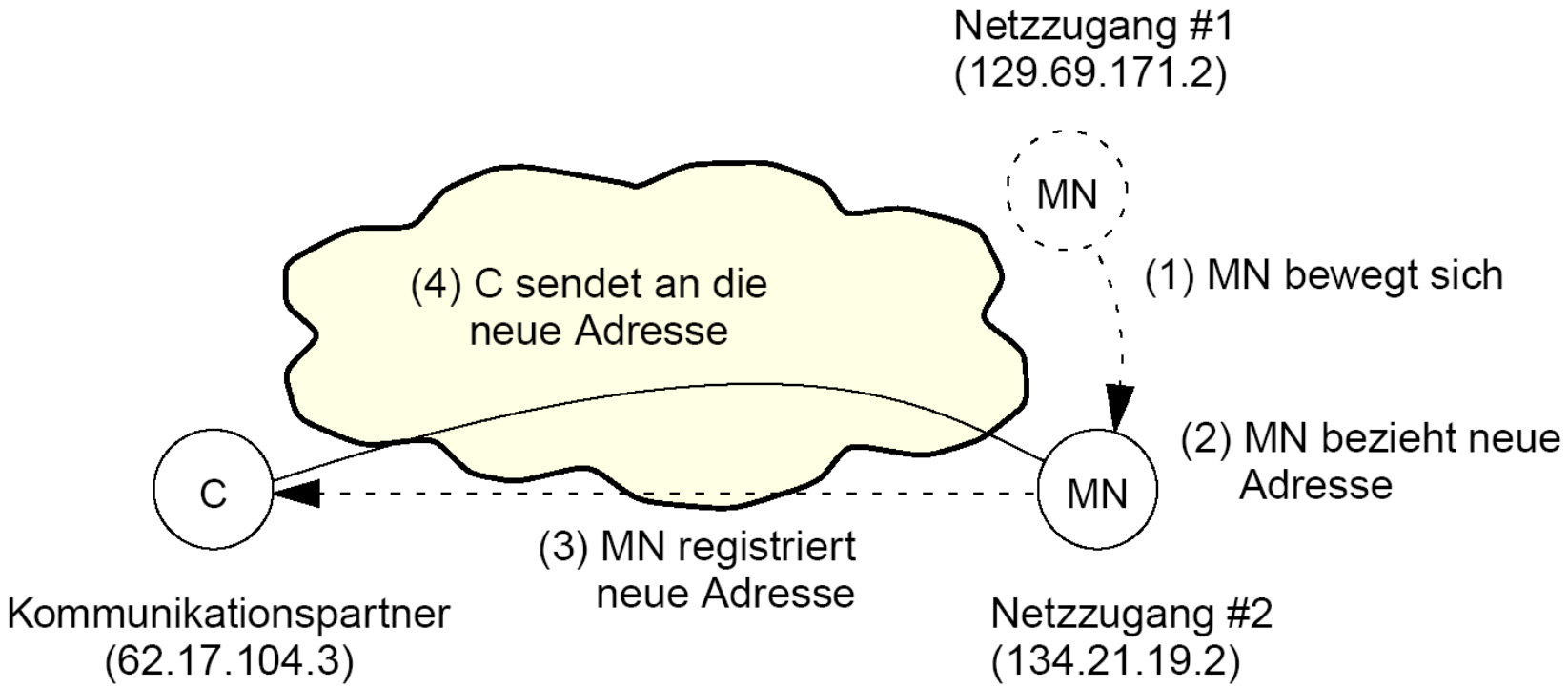


Mobility in the Internet - Problem (1)

- Dual function of IP addresses :
  - the routing of IP packets in the Internet is based on the destination address - the network part of the IP address (prefix) determines the physical subnet in which the recipient is located → **IP Address = Locator**
  - at the same time IP addresses are used by transport protocols and applications to identify stations → **IP Address = Identifier**
- Consequence for mobile stations when moving to a new subnet (if no special mechanism is used for mobility support):
  - a change of the subnet (Location) without changing the routing tables in the network requires a change of the IP address of the station; on the other hand, a change of the IP address leads to a disruption of existing connections (transport protocols and applications) → no transparent mobility
  - a change of the subnet (Location) without changing the station's IP address requires a change of the routing tables (for IP packets with this destination IP address); providing specific routes for each mobile station ("per-host forwarding") prevents an efficient address aggregation in the Internet → poor scalability (very large IP routing tables)

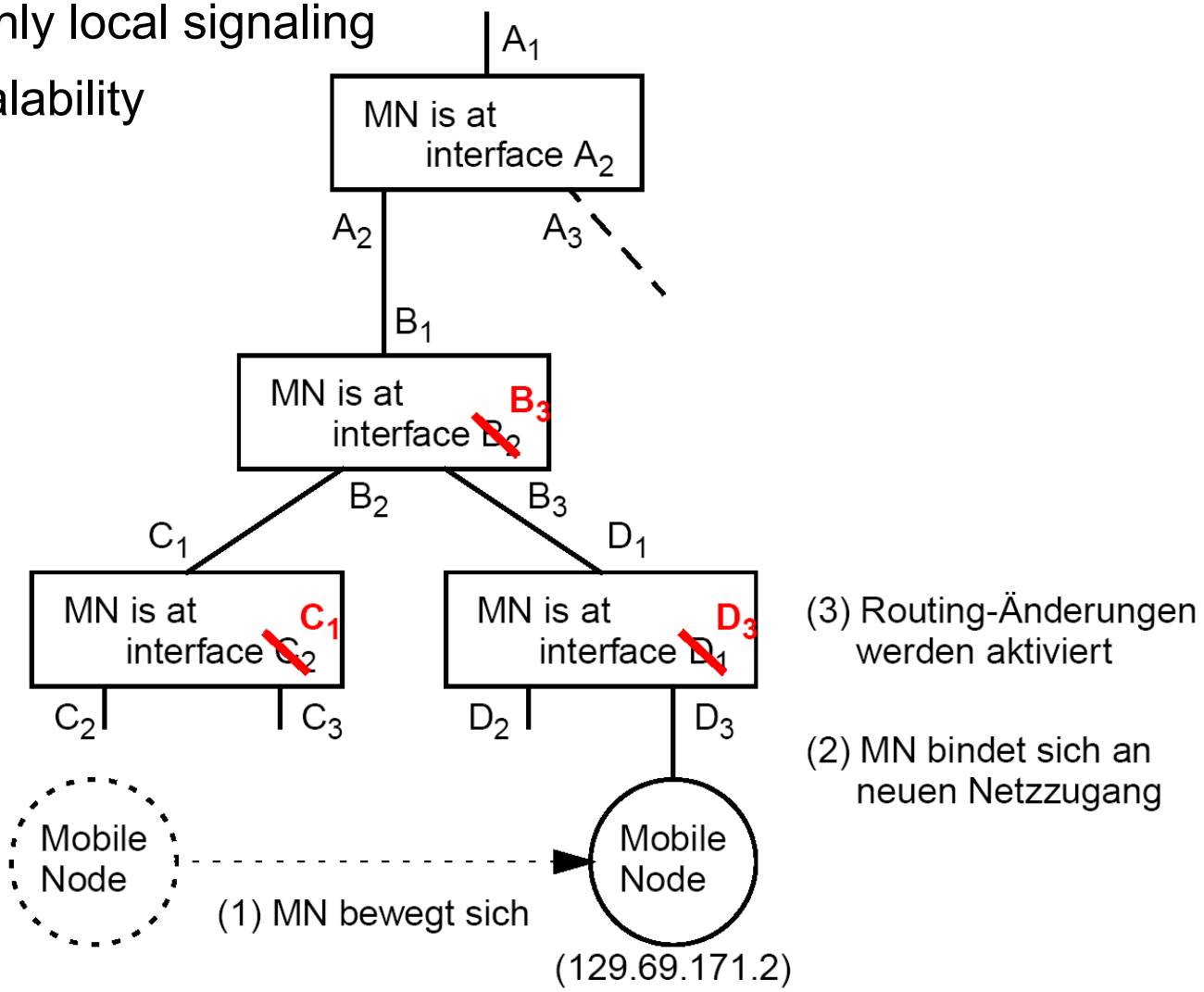
Mobility in the Internet - Problem (2)

- Subnet change with unchanged routing tables and new IP address
  - advantage: good scalability
  - disadvantage: signaling overhead, signaling delay



Mobility in the Internet - Problem (3)

- Subnet change with unchanged IP address and new routing tables
  - advantage: requires only local signaling
  - disadvantage: bad scalability



Mobility in the Internet - Possible Solutions

- Specific routes to mobile stations (per-host forwarding)
  - bad scalability: not suitable for large numbers of mobile stations and frequent subnet changes
  - only applicable to support mobility within smaller networks
- Change of the IP address of the stations according to the current subnet
  - interruption of connections: problem for transport protocols and applications
  - problem of finding stations after address changes; solution via DNS usually is too slow (only suitable for nomadic mobility)
- Multicast (in the transmission range of the mobile stations)
  - very high overhead
- **Tunneling: separate IP addresses for routing and identification**
  - a new IP address which fits to the subnet (location) is assigned to the station to keep the routing stable; additionally the old IP address (identifier) is kept for transport protocols and applications
  - this requires a dynamic address mapping (of new and old address): a solution via DNS is to slow → faster mechanism required, e.g. Mobile IP

Classification of Mobility Mechanisms

- Network and/or mobile station based mobility support:
  - Terminal-based: support from network and stations (stations are involved in mobility procedures)
  - Network-based: support only from the network (no interaction between network and station; the protocol stack in the stations remains unchanged)
- System on which the mobility support is applied:
  - End systems (hosts) → mobility identifier = IP address, host name (DNS)
  - Users → mobility identifier = user name (eg SIP-URL)
  - (Sub-)networks → mobility identifier = address prefix or subnet address
- Types of mobility control:
  - Handover initiation by station or network; the station or the network may assist (e.g. by providing measurements)
  - Handover execution by station or network

Network Layer Mobility

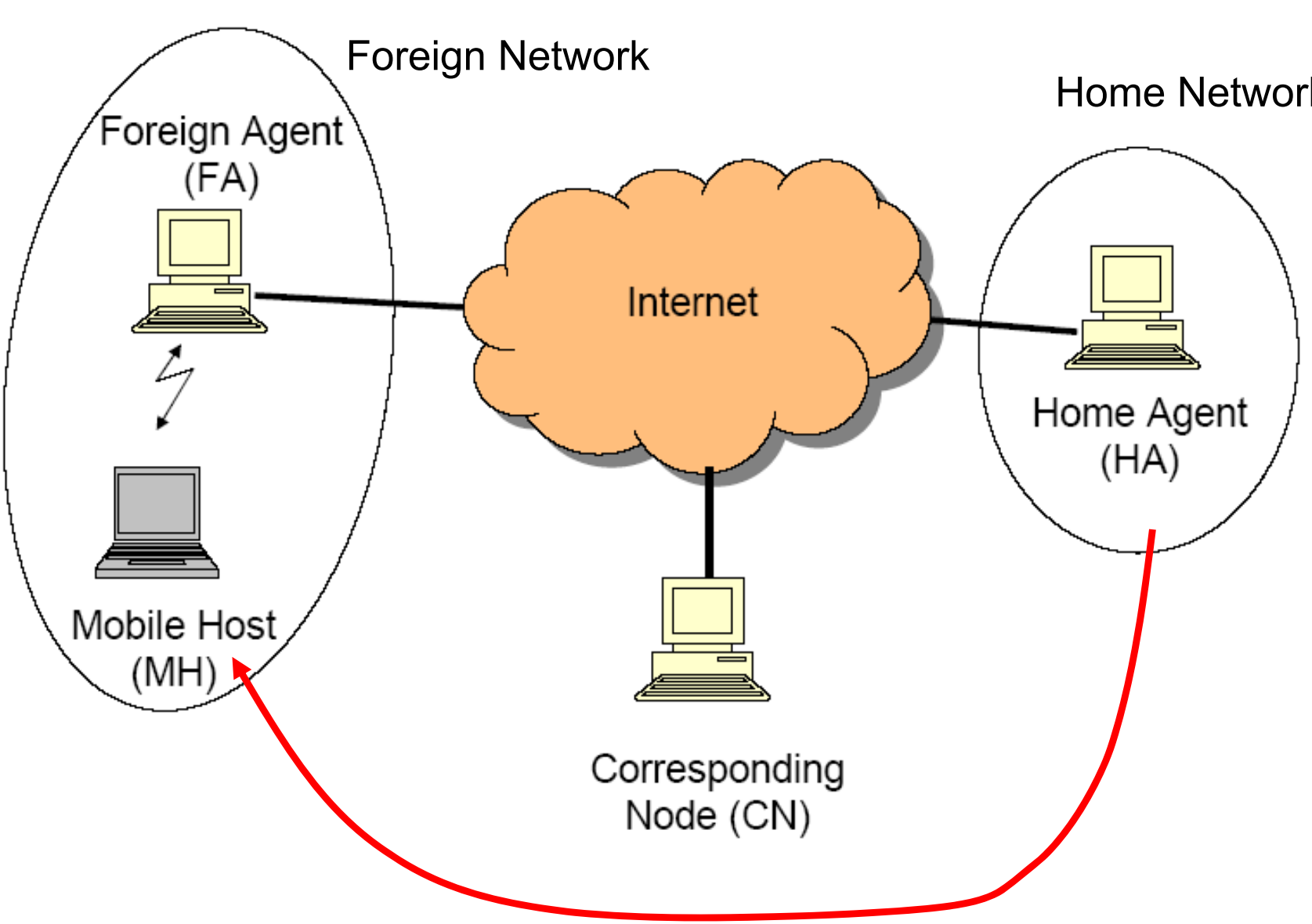
Network Layer Mobility - Overview

- Terminal-based Mobility Management Mechanisms
  - Mobile IPv4 (MIPv4) / Mobile IPv6 (MIPv6)
- Network-based Mobility Management Mechanisms
  - Proxy Mobile IPv6 (Proxy MIPv6)

Network Layer Mobility - Requirements (RFC 3220)

- Transparency
  - mobile stations keep their IP addresses (identifiers) despite of the location change (subnet change)
  - connection continuation after interruptions
- Compatibility
  - no changes in layer-2 protocols required
  - no changes of routers and stations in the fixed network required
  - mobile stations may communicate with stations in the fixed network
- Security
  - authentication of registration message
  - protection of privacy (location information)
- Efficiency and scalability
  - low signaling traffic on the radio interface
  - a large number of mobile stations are supported

Mobile IPv4 (RFC 3344) - Scenario



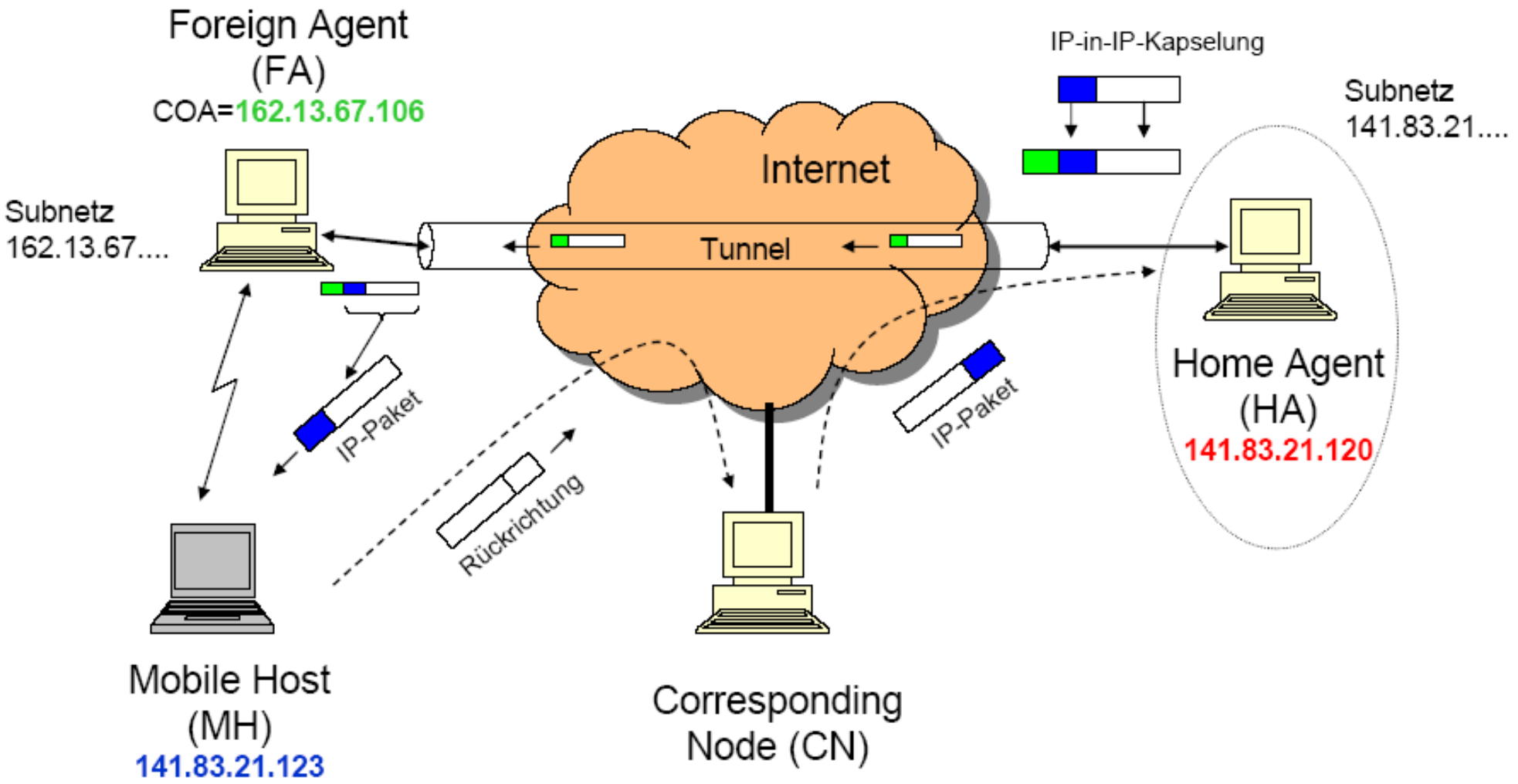
Mobile IPv4 - Terminology (1)

- **Mobile Station (Mobile Host, MH)**
  - the MH moves between different subnets but has a fixed IP address
- **Communication Partner (Corresponding Node, CN)**
  - the CN is the end system, which wants to exchange data with the MH (the CN might be a fixed or mobile system)
- **Home Agent (HA)**
  - the HA is the representative of the MH in the home network (HN) in case the MH is located in a foreign network; the HA has a similar role than the HLR in GSM - it is permanently informed about the location of the MH
  - the HA is the endpoint of a tunnel to the foreign network; it tunnels the data units obtained from the CN to the foreign network or forwards the tunneled data units from the foreign network to the CN (in case of reverse tunneling)
- **Foreign Agent (FA)**
  - the FA takes care of the MHs in the foreign network
  - the FA is the endpoint of a tunnel to the HA; it tunnels data units obtained from the MH to the HA (in case of reverse tunneling) or forwards the data units tunneled from the HA to the MH
  - remark: a separate implementation of FA is not necessary - e.g. in MIPv6 the FA function is integrated in the MH (co-located COA)

Mobile IPv4 - Terminology (2)

- **Home Address:**
  - the home address is the IP address with which the MH is permanently reachable
  - the home address is a topologically correct address in the home network - it has the same address prefix (or is in the same subnet) as the home agent
- **Delivery Address (Care-of Address (COA)):**
  - the COA is the IP address that the MH uses in the foreign network
  - there are two types of COA:
    - **Foreign-Agent COA:**
      - the COA belongs to the FA, the FA is the tunnel endpoint towards the HA
      - the MH registers to the HA via the FA
      - advantage: several MHs can have the same FA and thus use the same COA → saving of IP addresses
    - **Co-located COA:**
      - the COA belongs to the MH (it is assigned to the MH in the foreign network e.g. via DHCP); the MH is the tunnel endpoint towards the HA
      - the MH registers directly at the HA
      - advantage: no FA required
      - disadvantage: Co-located COA must be different for each MH in the foreign network

Mobile IPv4 - Data Transfer (1)



Mobile IPv4 - Data Transfer (2)

- The Correspondent Node (CN) sends an IP packet to the Mobile Host (which has e.g. the address 141.83.21.123)
- The IP network routes the packet to the subnet with the corresponding prefix (e.g. 141.83.21....)
- In the subnet the packet is intercepted by the Home Agent
- The packet is encapsulated (tunneled) in a packet with a destination address that corresponds to the COA of the Foreign Agent (e.g. 162.13.67.106)
- At the Foreign Agent the packet is unpacked and the original packet is passed to the Mobile Host (MH)
- For the reverse direction the MH can use the normal address of the CN and the normal routing mechanisms of the Internet (but this usually does not work because of some security mechanisms)

Mobile IPv4 - Network Integration - Overview

The integration of Mobile IPv4 in a network is performed according to the following steps:

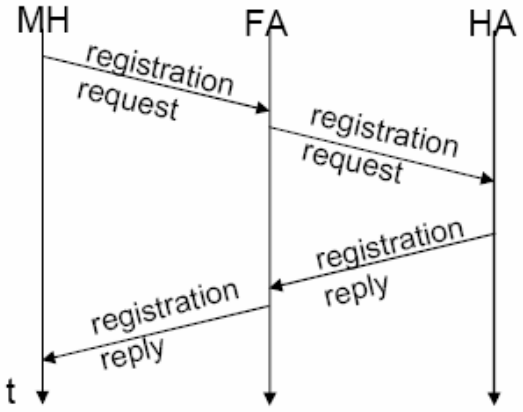
- Discovery of the agents (Agent Discovery)
  - Agent Advertisement
  - Agent Solicitation
- Registration
  - Registration Request
  - Registration Replay
- Advertisement of the address of the MH in the home network
  - by the HA using the IP routing protocol
- Tunneling (tunneled data transfer between HA and FA)
  - Forward tunneling
  - Reverse tunneling (optional, but frequently required due to security mechanisms)

Mobile IPv4 - Network Integration - Agent Discovery

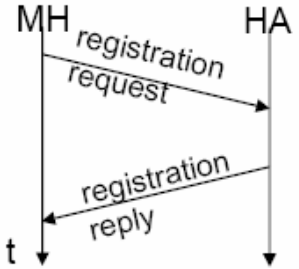
- Agent Advertisement
  - HA and FA periodically send special (ICMP) messages (RFC 3344) to announce their presence in the respective physical subnets
  - the MH hears these messages and recognizes whether it is located in the home network or in the foreign network
  - the MH can indentify a COA from the messages of the FA
- Agent Solicitation (optional)
  - the MH itself sends a request to the foreign network to perform an agent advertising
  - Agent Solicitation is used in case the foreign network does not announce on its own or the MH does not want to wait for the periodic transmission of ICMP messages
  - by that, the MH enforces that the agents immediately announce themselfes
- Remark:
  - if the MH does not receive agent advertisements, it assumes that it is in the home network and tries to contact known routers; if that is unsuccessful it tries to get a (co-located) COA via DHCP

Mobile IPv4 - Network Integration - Registration

- Registration of the MH at the HA via FA (for Foreign Agent COA):
  - the MH reports the COA to its HA via FA (Registration Request), the HA confirms the registration via FA to the MH (Registration Reply)
- Registration of the MH directly with the HA (for co-located COA):
  - the MH reports the COA (Registration Request) directly to his HA, the HA confirms the registration directly to the MH (Registration Reply)
- Remarks:
  - the registration has only a finite life time (soft state)
  - the registration should be protected by authentication mechanism



Registrierung via Foreign Agent



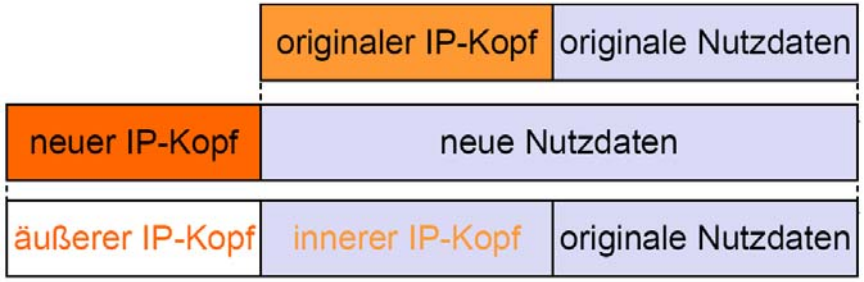
Registrierung bei Co-located-COA

Mobile IPv4 - Network Integration - Advertisement

- The HA announces the IP address of the MH, i.e. it notifies other routers that the MH is accessible via itself; the announcement is done via the IP routing protocol
- The routers set their routing table entries accordingly; the routing table remain quite stable since the HA is now responsible for the MH for usually a long time period
- Now, IP packets to the MH are first sent to the HA; the HA forwards these packets in a tunnel to the destination subnet

Mobile IPv4 - Encapsulation (Tunneling)

- Why is encapsulation (tunneling) necessary?
  - the communication partner sends data units to the home address; the home agent intercepts the data units and forwards them to the foreign agent
  - but: IP address of the foreign agent (COA) ≠ home address
- Basic idea:
  - the original data unit (including header and payload) becomes the payload of a new data unit where the IP address of the foreign agent (COA) is the destination address in the new IP header



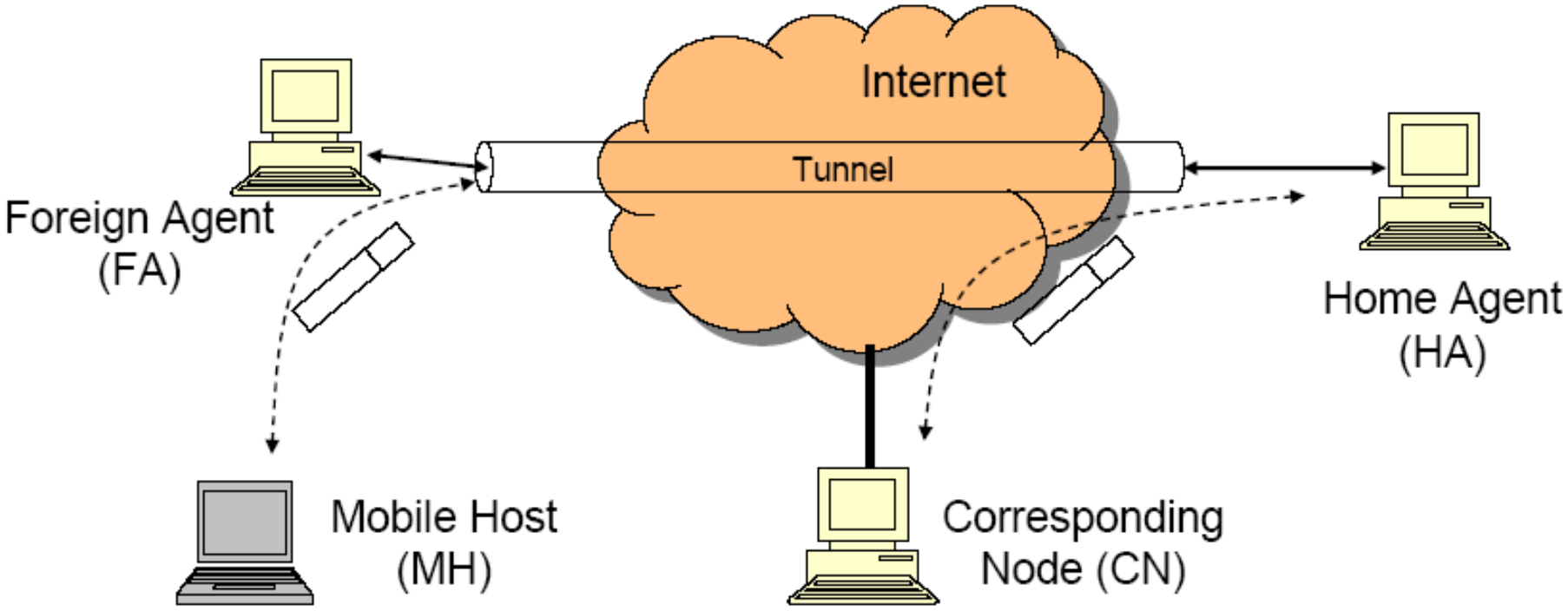
- Encapsulation methods in MIPv4:
  - IP-in-IP Encapsulation (mandatory in the MIP standard, RFC 2003)
  - Minimal Encapsulation (optional)
  - Generic Routing Encapsulation (GRE) (optional)

Mobile IPv4 - Reverse Tunneling (RFC 2344)

- Packets from MH to CN might be sent directly (i.e. without FA-HA tunneling) since for their forwarding only the destination adress (address of the CN) is important
- However, many routers - especially in the foreign network - due to security reasons do not forward these packets, because the source address (home address of the MH) is not topologically correct i.e. does not fit to the address range of the foreign network
- A tunnel in the reverse direction (reverse tunneling) i.e. from FA to HA solves the problem, but increases the inefficiency of the routing e.g. if FA and CN are geographically close together (double triangular routing problem with reverse tunneling)
- Remark: MIP with Reverse tunneling is backward compatible to MIP implementations without reverse tunneling; in the Agent Advertisement the request for reverse tunneling can be specified

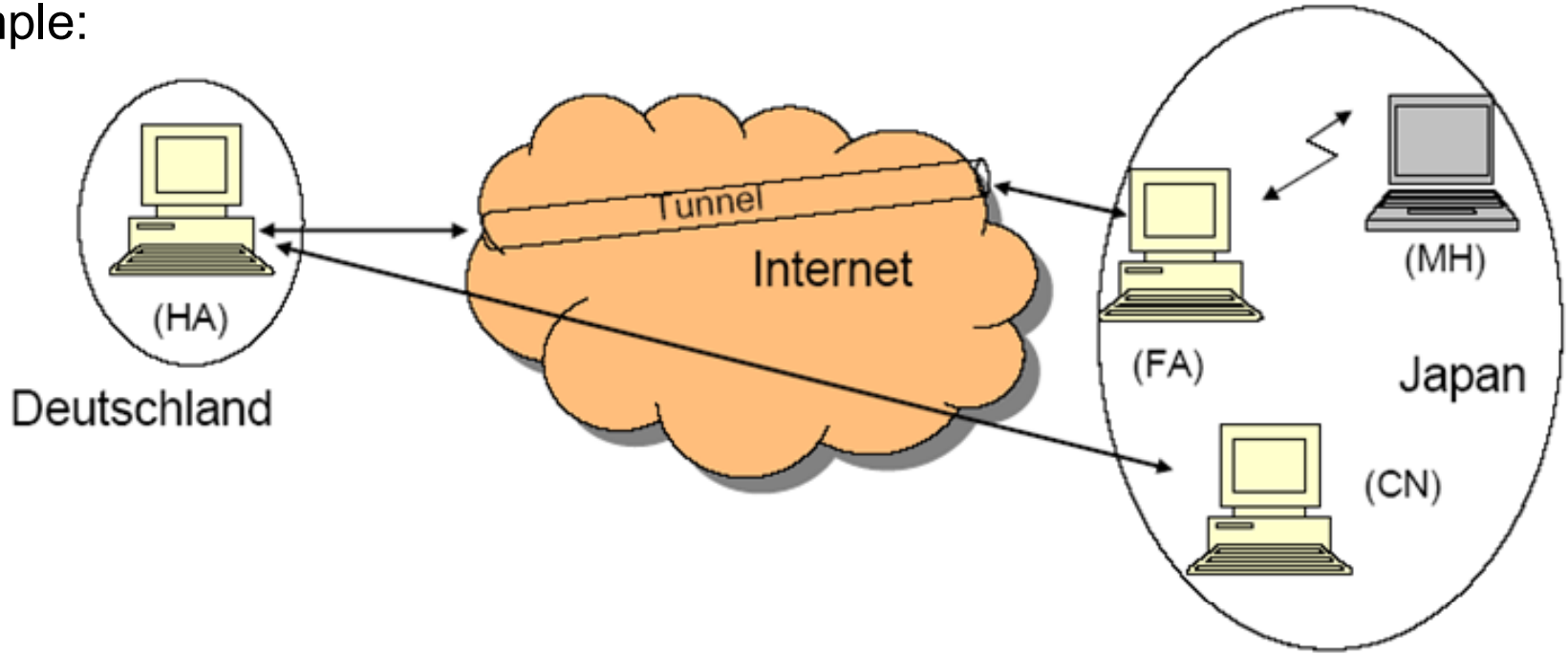
Mobile IPv4 - Reverse Tunneling (RFC 2344)

- Reverse Tunneling:



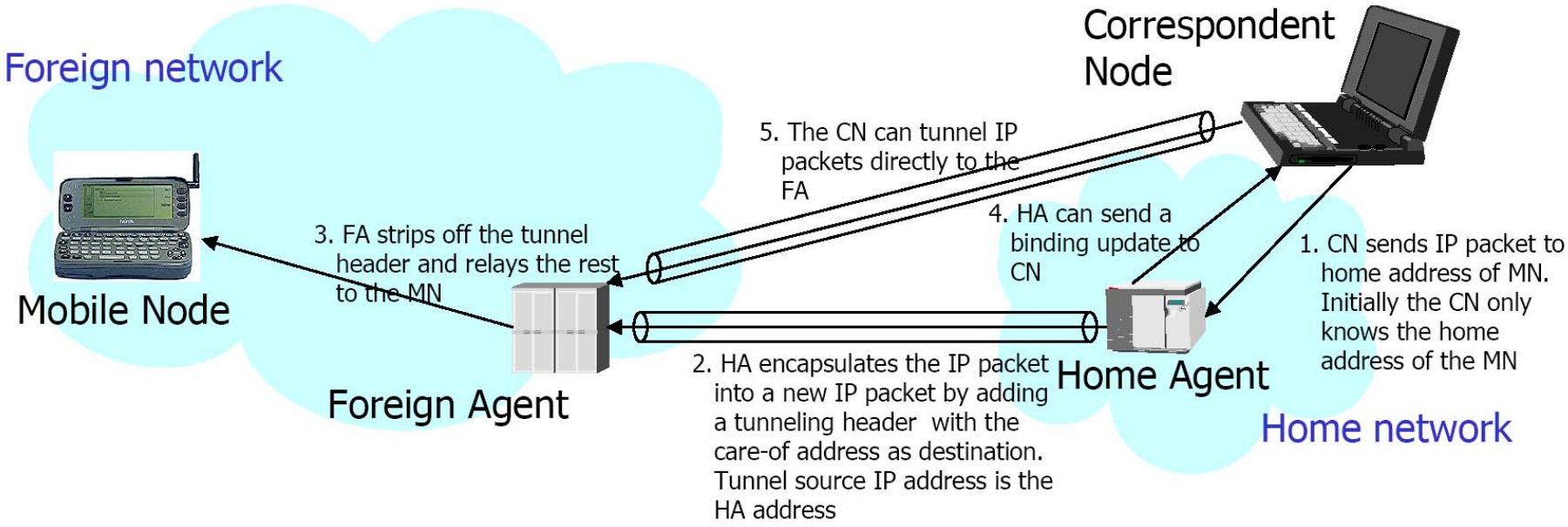
Mobile IPv4 - Route Optimization (Avoiding Triang. Routing)

- Triangular Routing (TR) Problem:
  - the sender (CN) sends all packets via HA (tunneled) to MH; in case of reverse tunneling this also happens in reverse direction
  - this causes unnecessary delays and network load, especially if CN and MH are geographically close to each other; there is also the possibility of overloading the HA
  - example:



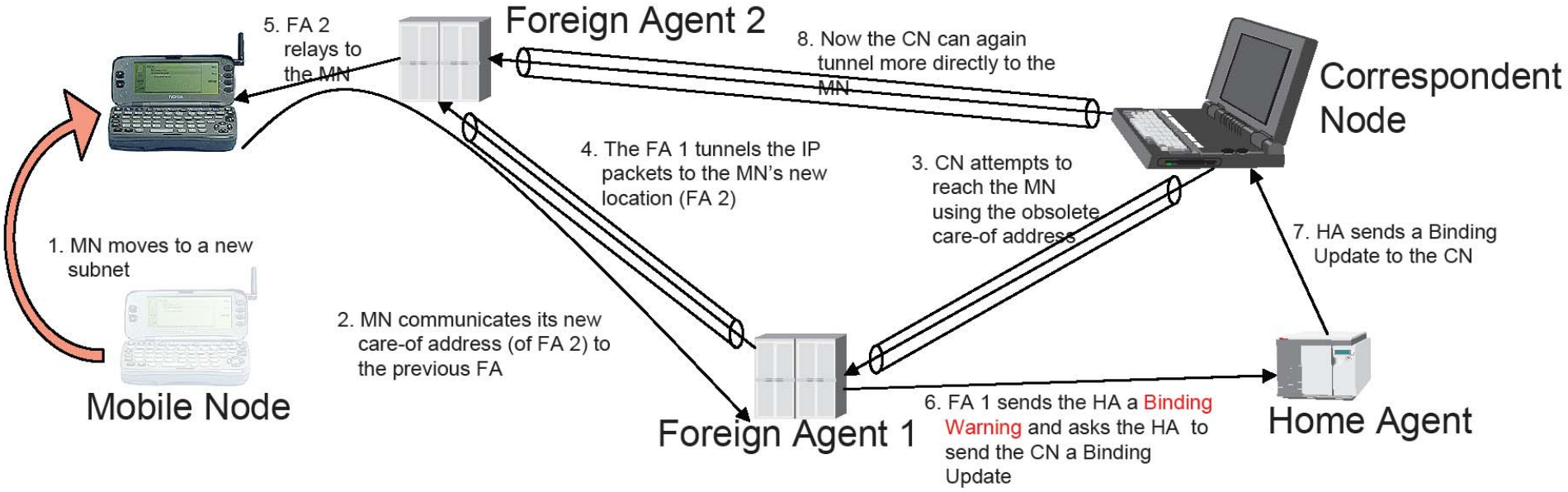
Mobile IPv4 - Route Optimization (Avoiding Triang. Routing)

- Solution of the triangular routing problem:
  - the sender (CN) learns the current location of the FA (for FA-COA) or MH (for co-located COA); e.g. the HA informs the sender (CN) about the FA or MH location (Binding Update)
  - then a direct tunnel between CN and FA or MH is established and the MH registers via FA or directly at the CN
  - problem: security (can be solved by encryption)
  - example:



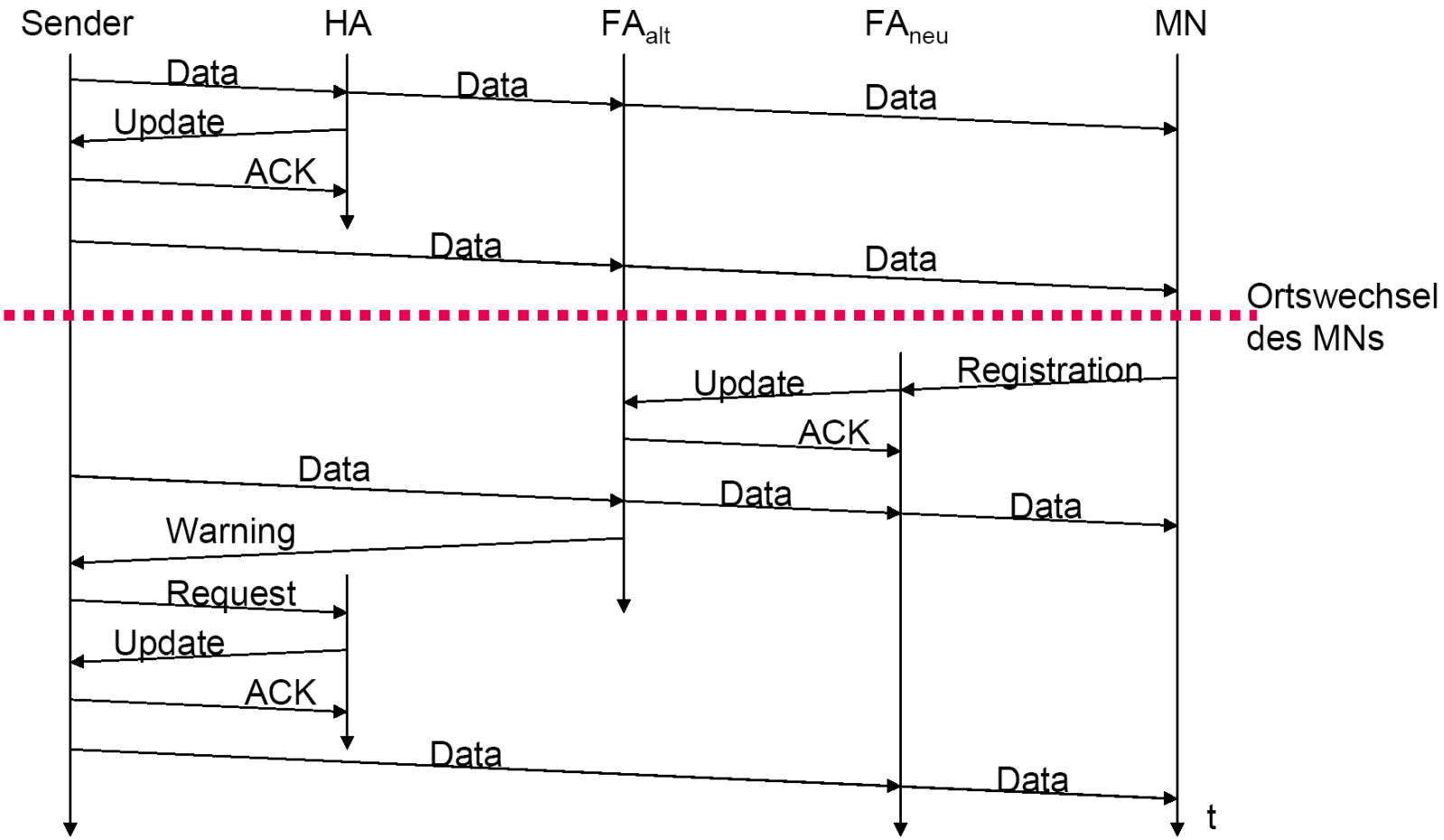
Mobile IPv4 - Change of Location (Change of FA)

- A change of the location (subnet) of the MH also requires a change of the FA
- Problem: during the change of the FA packets (belonging to an ongoing connection) may be lost
- Solution: the new FA informs the old FA about the change - the old FA can now forward incoming packets to the new FA; as long as the old FA does not know the new FA (i.e. the new COA), it must send the packets back to the HA again; the HA then forwards the packets over the new tunnel to the new FA
- Route optimization example:



Mobile IPv4 - Change of Location (Change of FA)

- Signaling procedure in case of changing the foreign agent (FA):



Mobile IPv6 (RFC 3775) - Properties of MIPv6 (1)

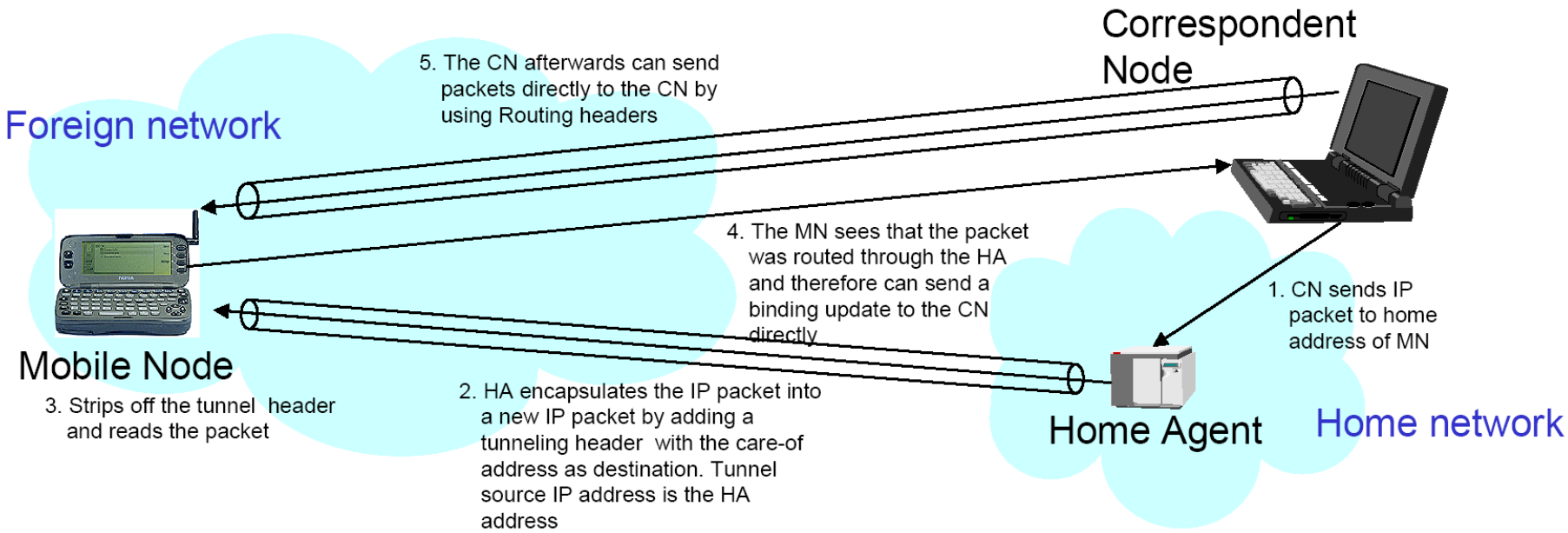
- Only co-located COA - no Foreign Agents (FAs)
  - Co-located COA are feasible in IPv6 due to high number of IPv6 addresses
  - COA are assigned to the MH via address auto configuration:
    - stateful assignment: COA via DHCPv6
    - stateless assignment: COA as combination of layer 2 address (e.g. MAC address) of the MH and the subnet prefix; the prefix of the subnet is learned via the IPv6 neighbor discovery mechanism
  - recognition of duplicate addresses via Duplicate Address Detection
  - all IPv6 router can perform router advertisements - these are used instead of the special agent advertisements
- Bidirectional tunnel (forward und reverse tunneling)
  - more efficient encapsulation by using a IPv6 routing extension header instead of IPv6-in-IPv6 tunneling
- Route optimization (solution of the TR problem)
  - the MH can notify the sender (CN) directly (without going through the HA); the CN will then replace the MH home address with the COA during sending

Mobile IPv6 (RFC 3775) - Properties of MIPv6 (2)

- Built-in security mechanisms
  - e.g. authentication at registration; IPsec for tunneling
- Support for "seamless handover" (fast handover without packet loss) between different subnets
  - the MH sends the new COA to the router (in the old subnet) it is connected to
  - the router in the old subnet then automatically encapsulates all later incoming packets for the MH and forwards them to the new COA
- Changed terminology compared to IPv4
  - **Binding Update = Registration Request in Mobile IPv4**
  - **Binding Acknowledgement = Registration Reply in Mobile IPv4**
- Further special features of Mobile IPv6
  - Dynamic HA Discovery: query of the HA's address, in case it is unknown
  - Mobile Prefix Discovery: adaptation of the home address of the MH, in case a new prefix has been assigned to the home network

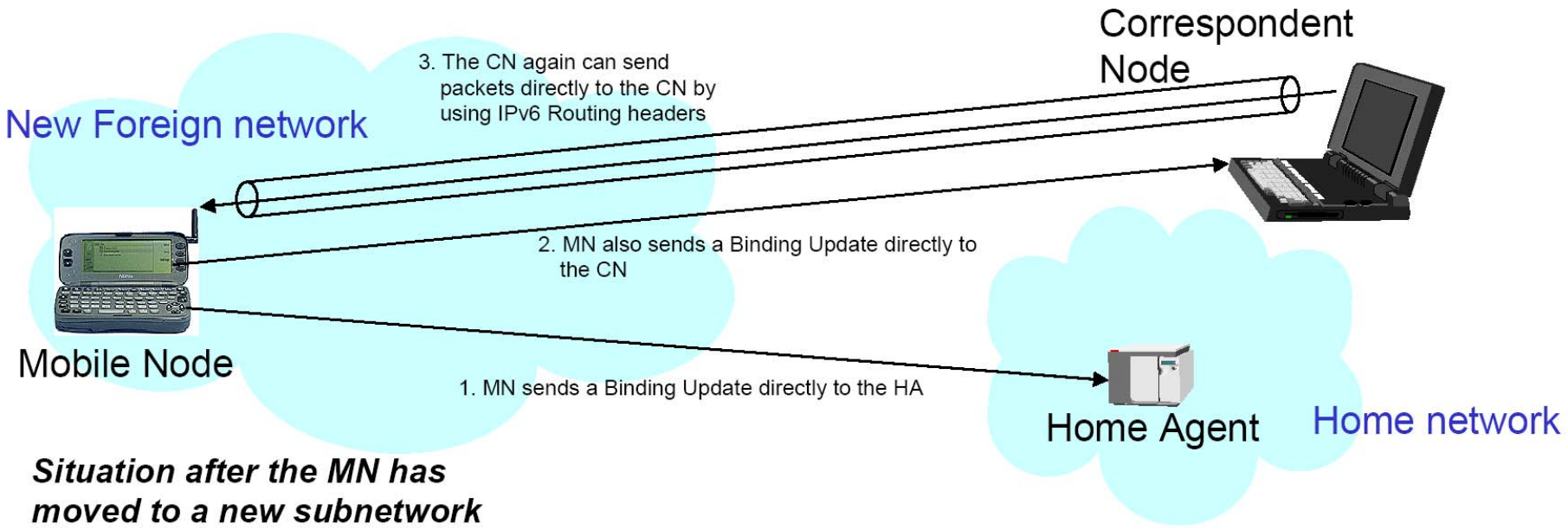
Mobile IPv6 - Route Optimization (Avoiding TR)

- The sender (CN) learns the current location of the MH directly via a binding update from the MH (remark: binding updates are carried in the IPv6 Destination Options Extension Header of normal IPv6 packets)
- Then a direct tunnel between CN and MH is set up (remark: IPv6 Routing Extension Headers are used instead of IPv6-in-IPv6 tunneling)
- Example:



Mobile IPv6 - Change of Location

- In case of a location change (subnet change) a binding update is sent directly from the MH to the CN or HA (remark: binding updates are carried in the IPv6 Destination Options Extension Header of normal IPv6 packets)
- After the route optimization the CNs are notified by the MH of the location change and then can send packets directly to the MH without loss
- Example (with completed route optimization):



Mobile IPv6 - Advantages and Disadvantages

- Advantages
  - IPv6 has a built-in mobility support - contrary to that, many IPv4 systems do not support MIPv4
  - enables real end-to-end mobility
  - good interworking with TCP/IP (Internet Protocol Stack)
  - transparent to higher layer protocols
- Disadvantages
  - overhead due to encapsulation (tunneling)
  - delays during handover (change of location) because the MH has to notify HA and CN every time (via binding updates); even short interruptions may occur
  - high signaling load in case of fast-moving MHs (due to frequent binding updates)
  - suboptimal routing and unnecessary delays due to triangular routing - triangular routing cannot be avoided, if the CN does not support Mobile IP (no route optimization possible)

Mobile IPv4 vs. Mobile IPv6

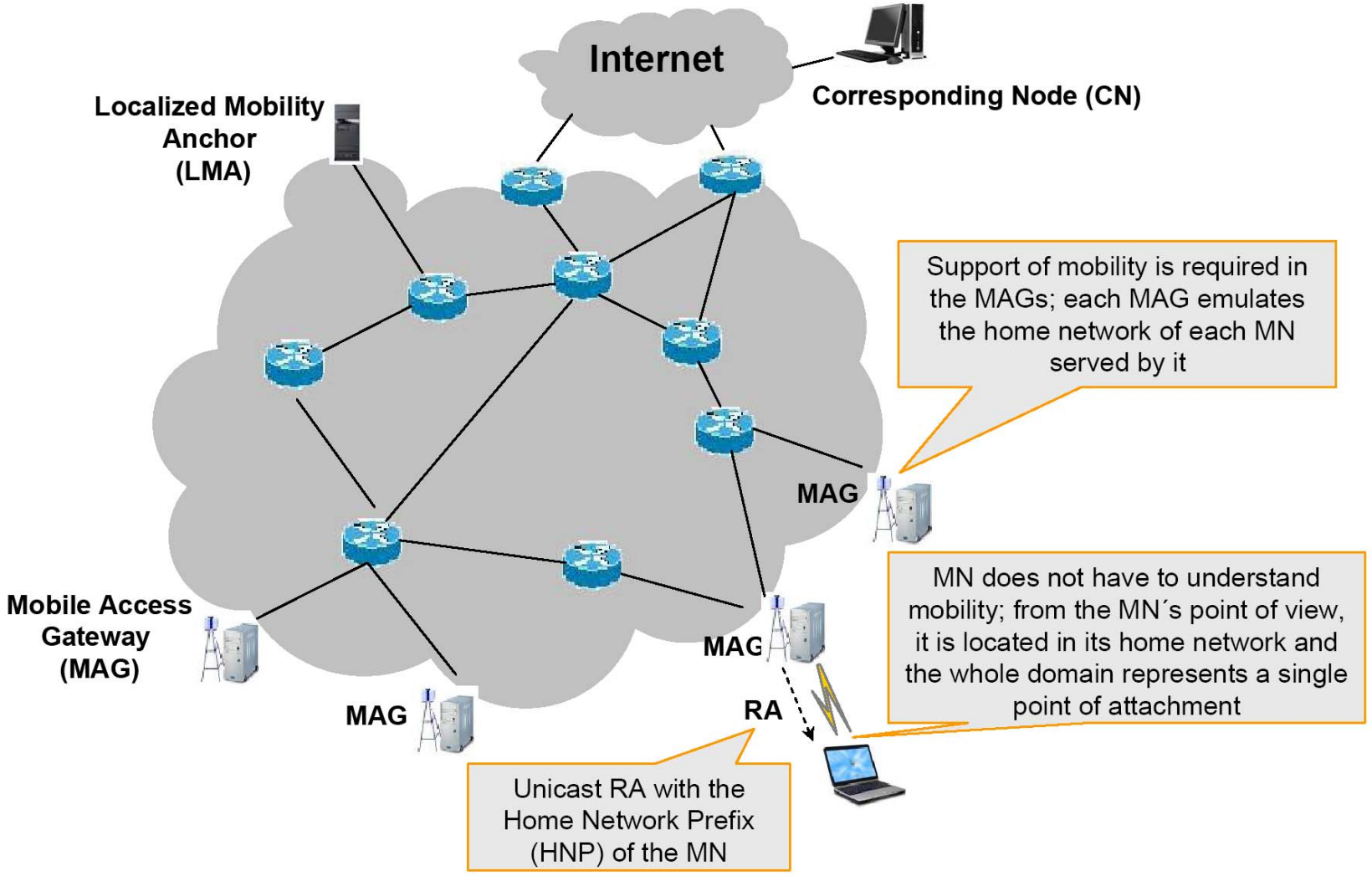
	Mobile IPv4	Mobile IPv6
Routing	Optimal Routing only if MN in the *Home Network*. (Otherwise non-efficient „Triangle“-Routing)	Optimal Routing is generally possible if CN knows the Care-of Address
Bottlenecks	HA is a possible bottleneck, because all traffic to the MN is processed by it	HA load is essentially reduced, because CNs can just directly communicate with MNs
Security	Authentication is mandatory only for registration and then only between HA and MN	Authentication and encryption are possible anywhere, because they are supported by IPv6
Robustness	Used FAs / HAs must not be off-line	Short-time failure/re-configuration of HA is masked thanks to Automatic Home Agent Discovery. IPv6 is essentially simpler to upgrade, therefore also Mobile IPv6
Performance	No good performance due to IPv4-limitations and non-optimal Routing	Essentially better due to characteristics of IPv6 (uniform Headers, less over-heads) and optimal Routing

Proxy Mobile IPv6 (RFC 5213)

- Full network-based mobility support
  - MHs are not involved in the mobility management
  - from the perspective of the MHs, they are always located in the home network
- Network infrastructure components required to support mobility:
  - Mobile Access Gateway (MAG): access router which emulates the respective home network for each MH in its subnet (proxy function)
  - Localized Mobility Anchor (LMA): mobility anchor point (HA) in the home network of the MH; tunnelled data transfer between LMA and MAG
- Operation:
  - similar to Mobile IPv6, but bindings and tunneled data transfer are not performed between MH and HA but rather between MAG and LMA

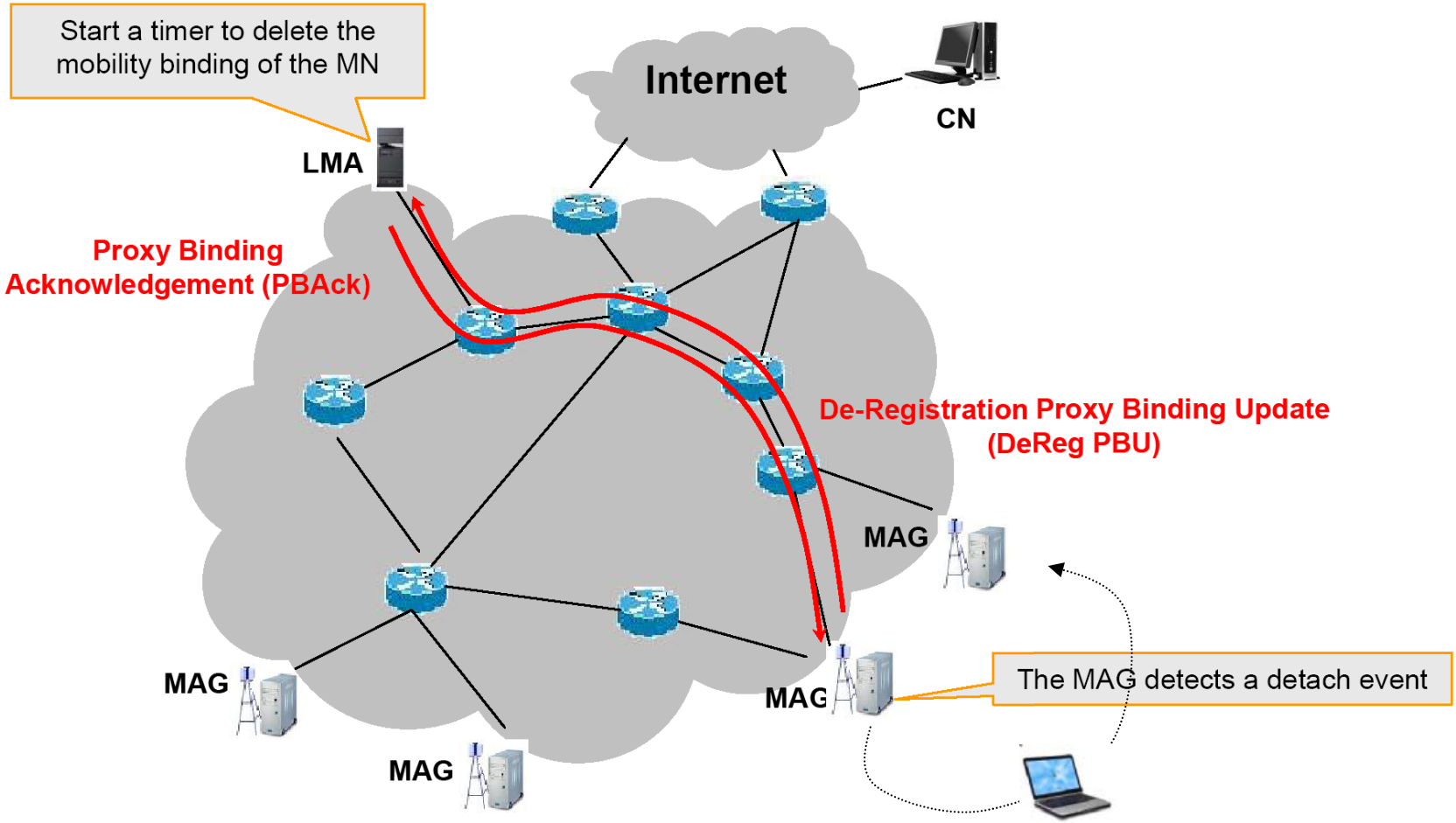
Proxy Mobile IPv6 - Operation (Details)

- Proxy Mobile IPv6 Scenario:



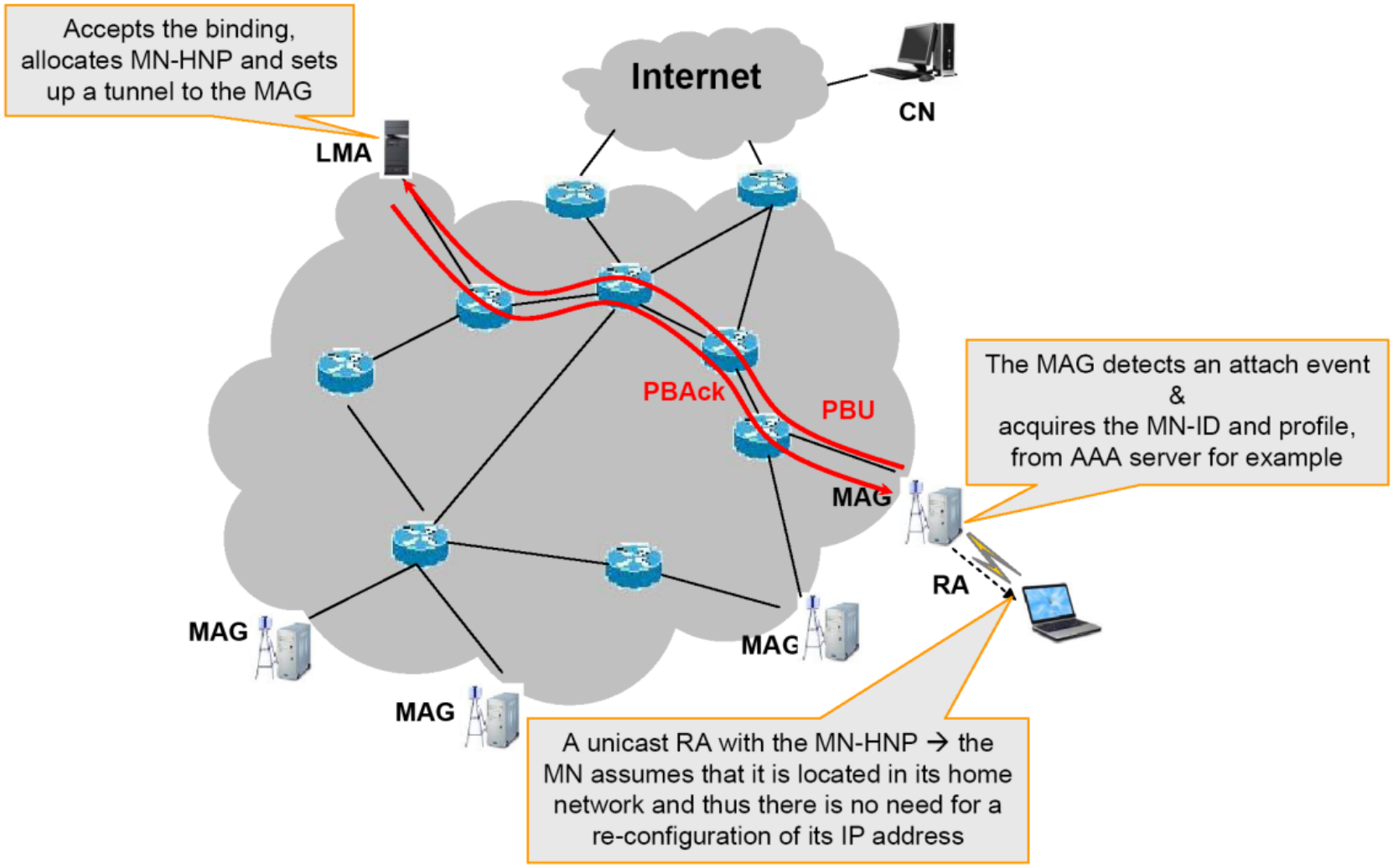
Proxy Mobile IPv6 - Operation (Details)

- Proxy Mobile IPv6 Handover (1):



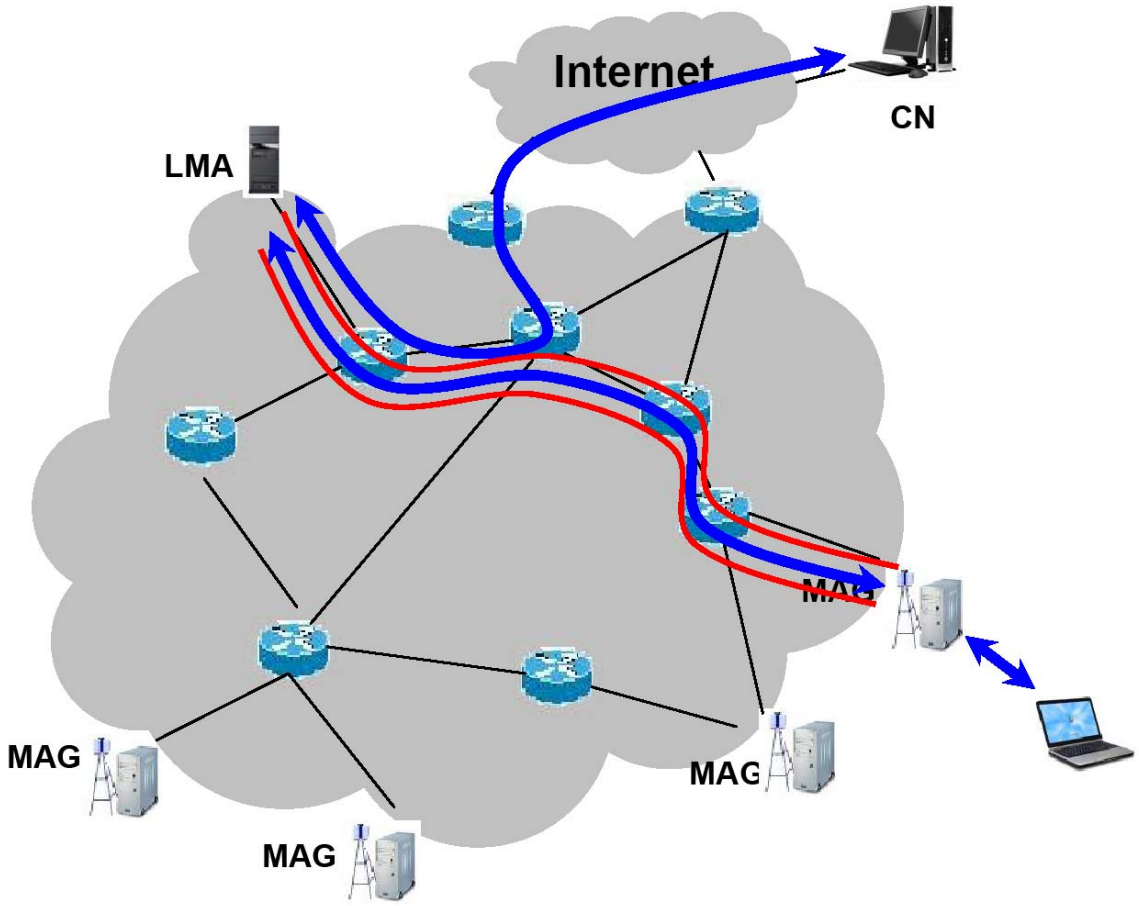
Proxy Mobile IPv6 - Operation (Details)

- Proxy Mobile IPv6 Handover (2):



Proxy Mobile IPv6 - Operation (Details)

- Proxy Mobile IPv6 Data Transfer:



Proxy Mobile IPv6 - Advantages and Disadvantages

- Advantages:
  - completely transparent for MHs
  - no mobility signaling between network and MH
    → no loss of signaling messages on the access link + no signaling overhead on the access link (important for wireless access)
  - low overhead on the access link, as the tunnel already ends in the MAG (important important for wireless access)
- Disadvantages:
  - triangular routing problem - no route optimization possible
  - overhead due to tunneling
  - delays during handover, since the MAG has to inform the LMA about each subnet change of the MH → a short interruption of the connection during the handover might occur

Further Mobile IP based Mobility Mechanisms

- Dual Stack Mobile IPv6 (DSMIPv6, RFC 5555)
  - extension of MIPv6 wrt. the following scenarios:
    - the foreign network, in which the MH is located, is only IPv4 capable
    - the CN is located in an IPv4 network (and generates IPv4 traffic)
    - an application which runs on the MH is only IPv4 capable (produces IPv4 traffic)
  - extension of DSMIPv6: Flow specific Mobility / Flow Binding (RFC 5648):
    - different (flow-specific) COAs are mapped to a home address
      → flow-specific multi-homing via multiple access technologies possible
- Fast handovers for Mobile IPv6 (FMIPv6, RFC 4068)
  - extension of MIPv6 to realize seamless handover:
    - Neighborhood Discovery
    - Fast Binding Update
    - Fast Neighbor Advertisement
    - (temporary) tunneling between the MH and the old access router during handover
    - Predictive Fast Handover
    - Reactive Fast Handover
- NEtwork MObility (NEMOv4, RFC 5177 or NEMOv6, RFC 3963)
  - mobility support for networks as a whole (not only for mobile hosts)

New Mobility Approaches - Locator-Identifier Split Principle

- Locator ID Split (LISP)
  - described in draft RFCs (Farinacci)
  - available in IPv4 and IPv6 environments
- Host Identity Protocol (HIP, RFC 4423)
  - many HIP extensions exist
- Identifier Locator Network Protocol (ILNP)
  - described in draft RFCs (Atkinson)
  - specified for IPv4 and IPv6