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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

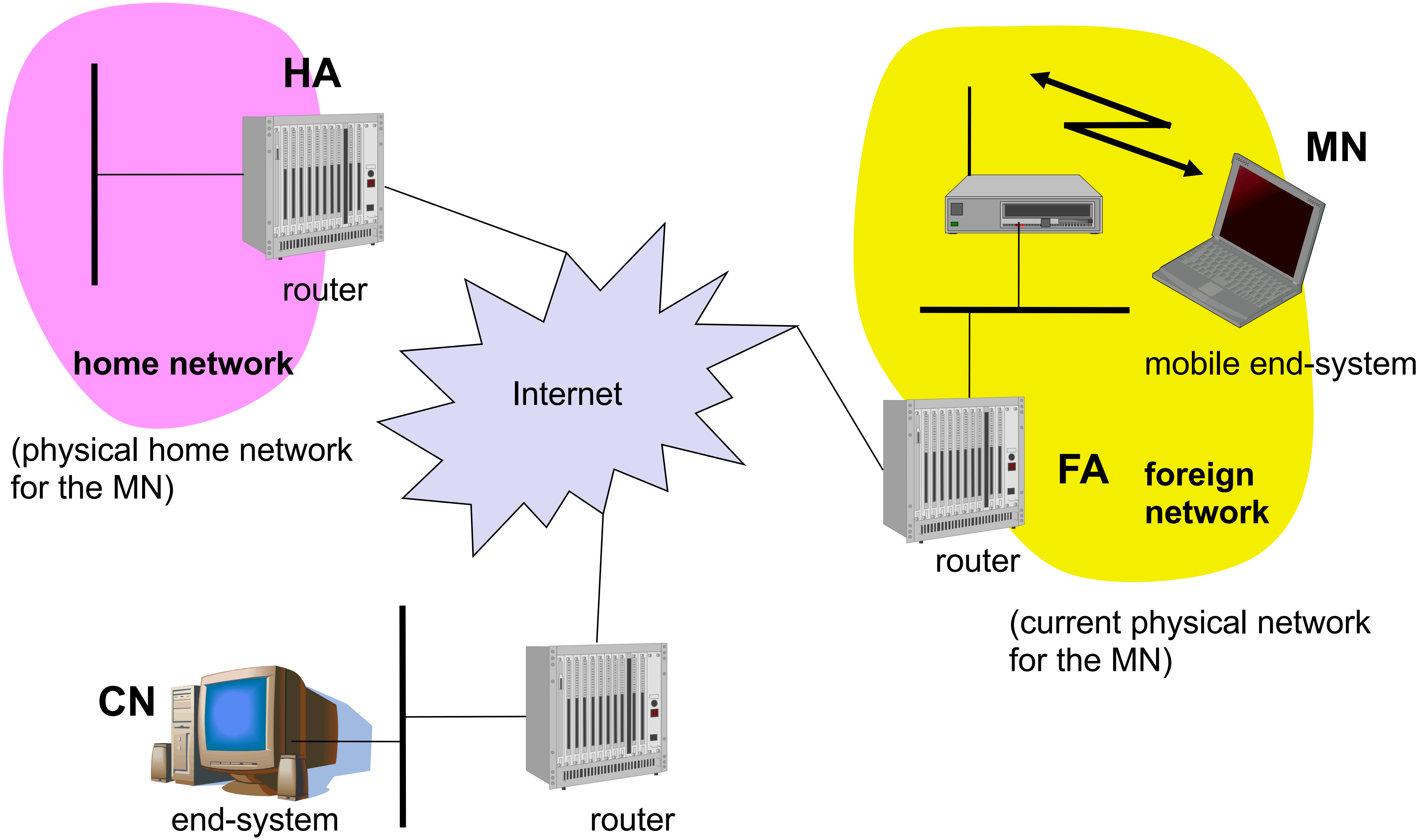
Terminology

- 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

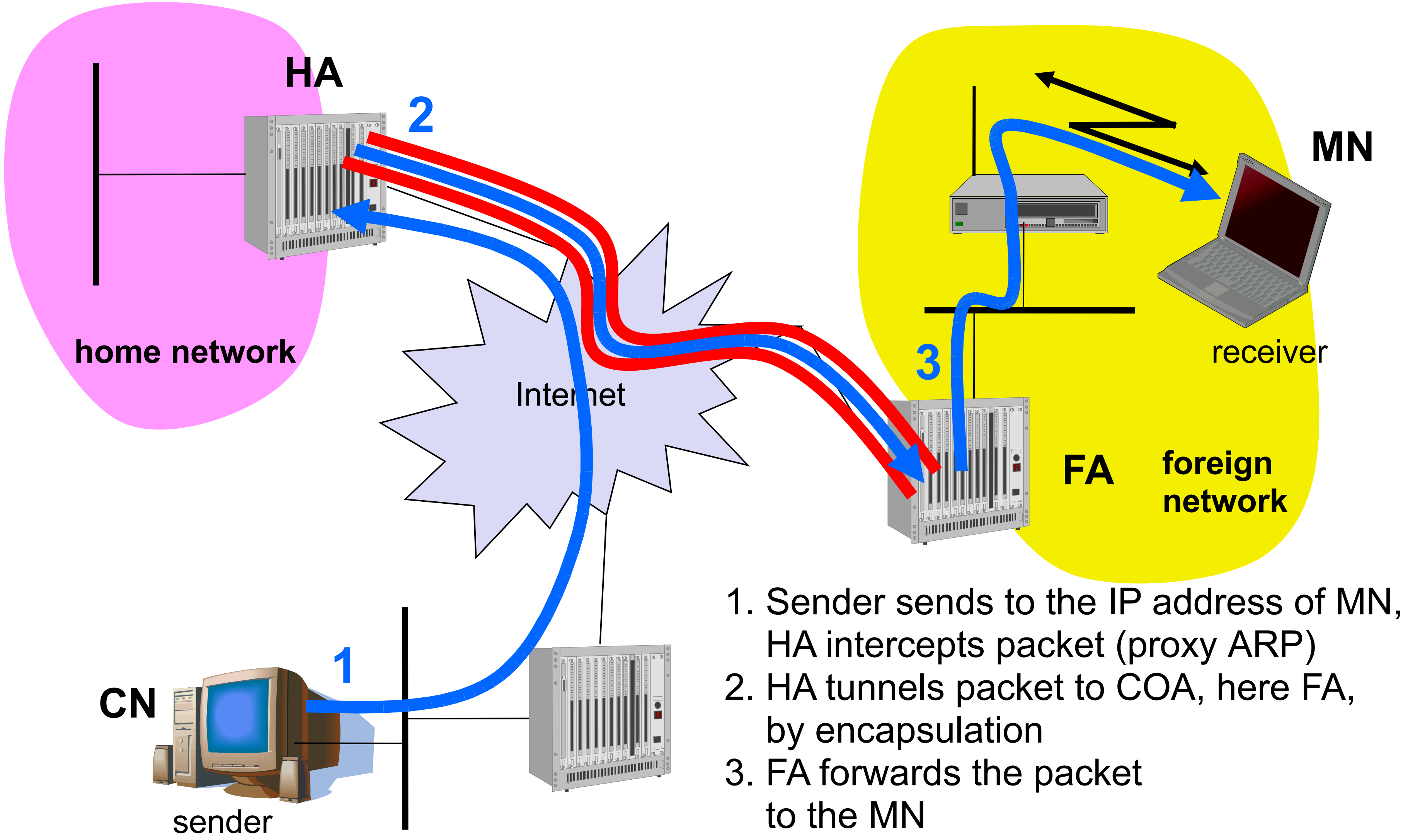
courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Example network



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

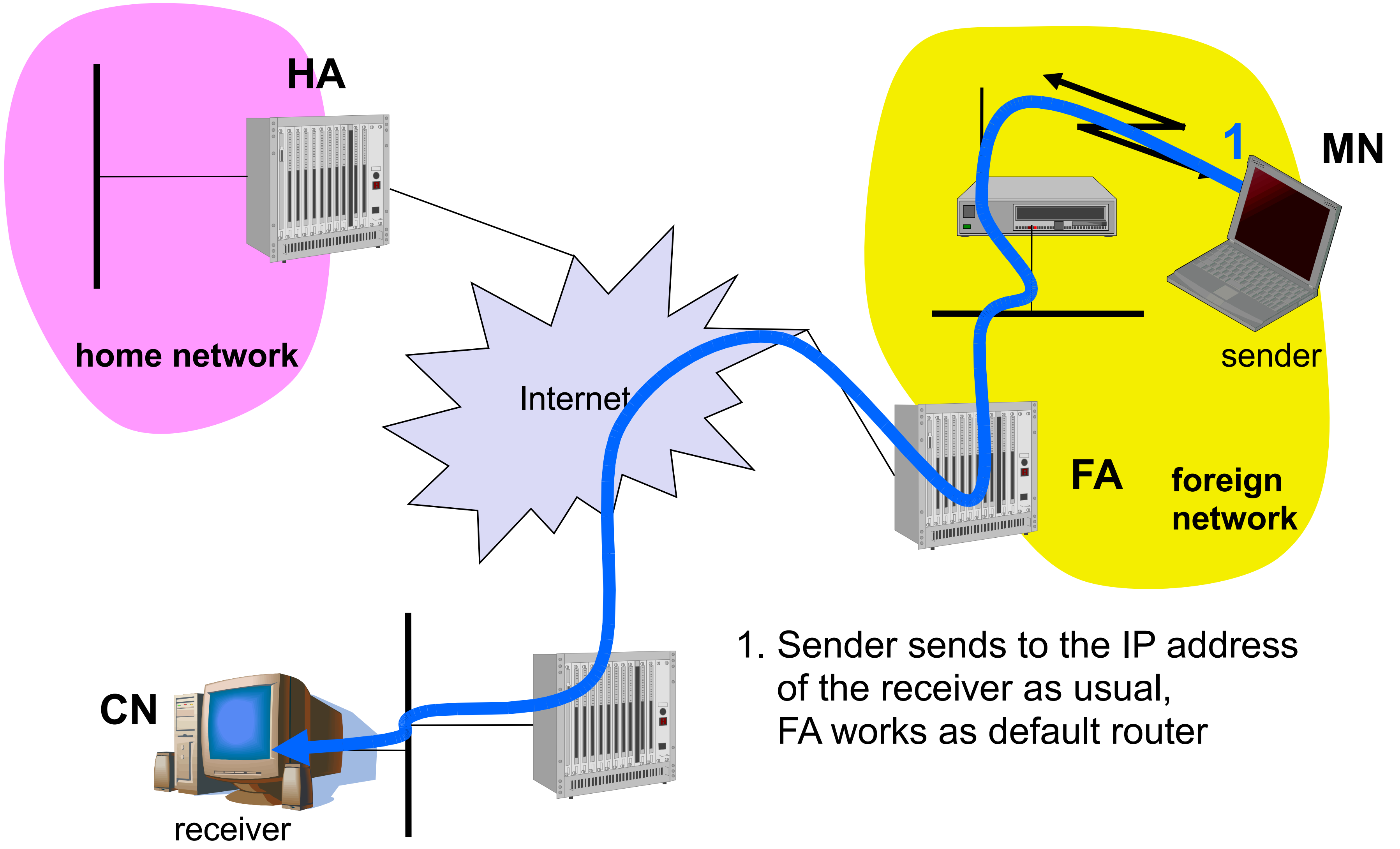
Data transfer to the mobile system



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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

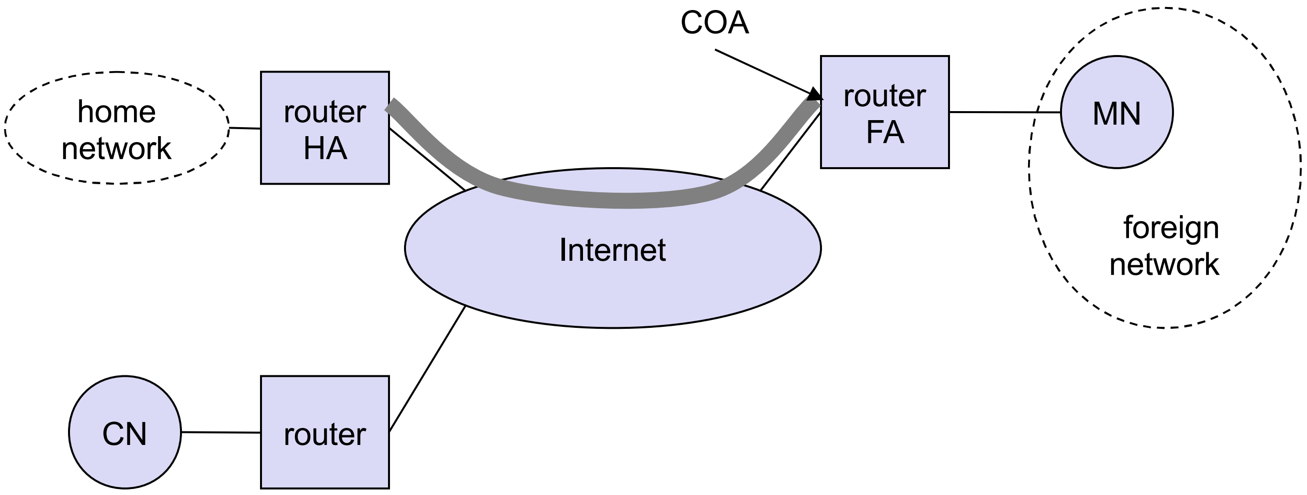
Data transfer from the mobile system

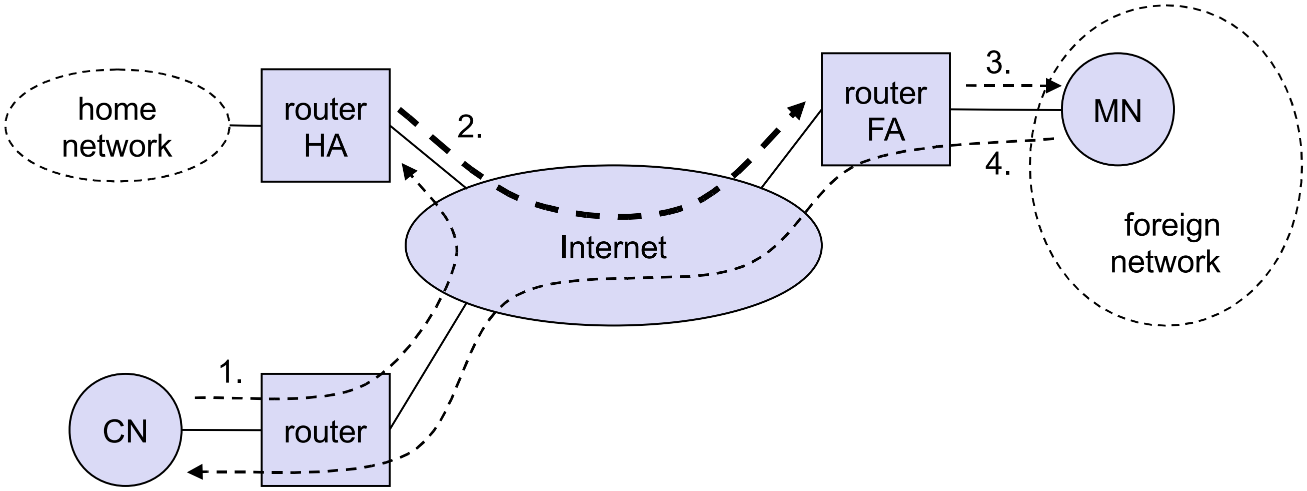


1. Sender sends to the IP address of the receiver as usual, FA works as default router

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Overview





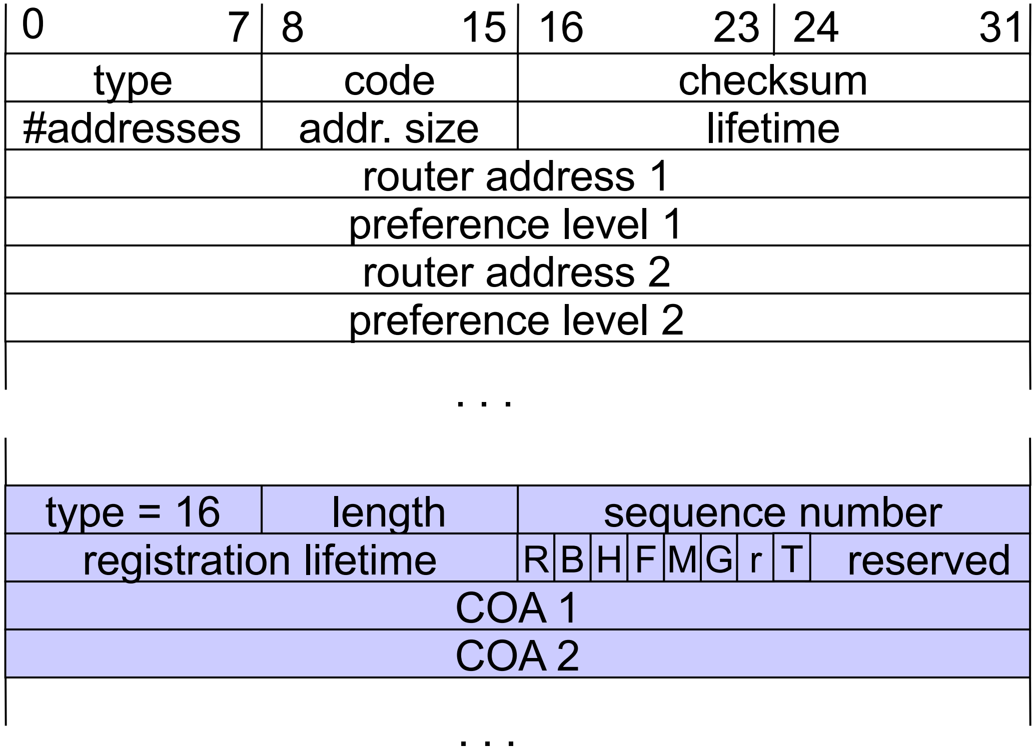
courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

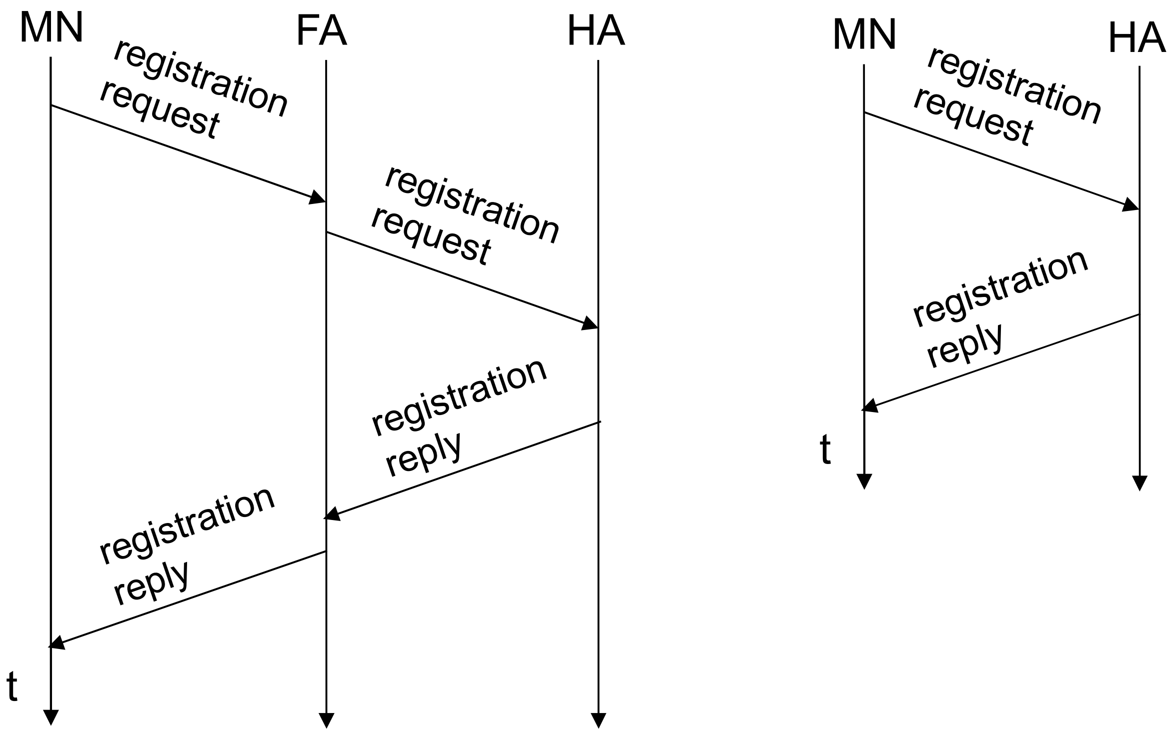
Agent advertisement



0 7	8 15	16 23	24 31
type	code	checksum	
#addresses	addr. size	lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			
. . .			
type = 16	length	sequence number	
registration lifetime		R B H F M G r T	reserved
COA 1			
COA 2			
. . .			

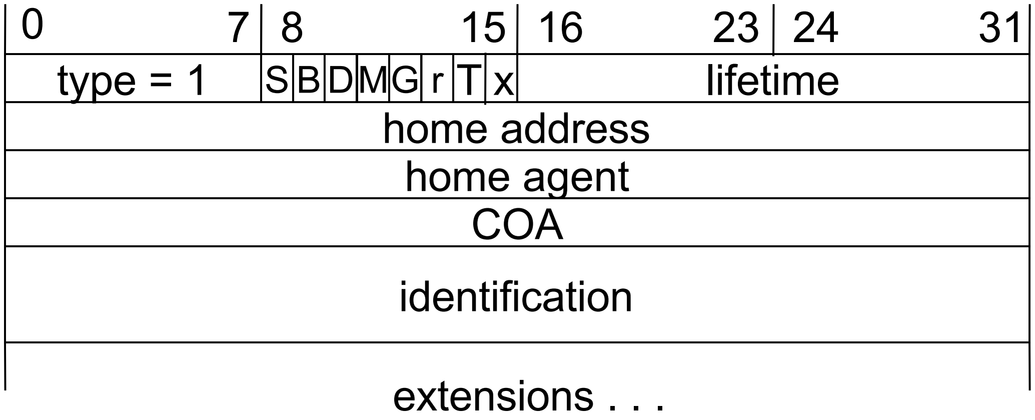
type = 16
length = 6 + 4 * #COAs
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Registration



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Mobile IP registration request


0 7 8 15 16 23 24 31

type = 1 | S | B | D | M | G | r | T | x | lifetime

home address

home agent

COA

identification

extensions . . .

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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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

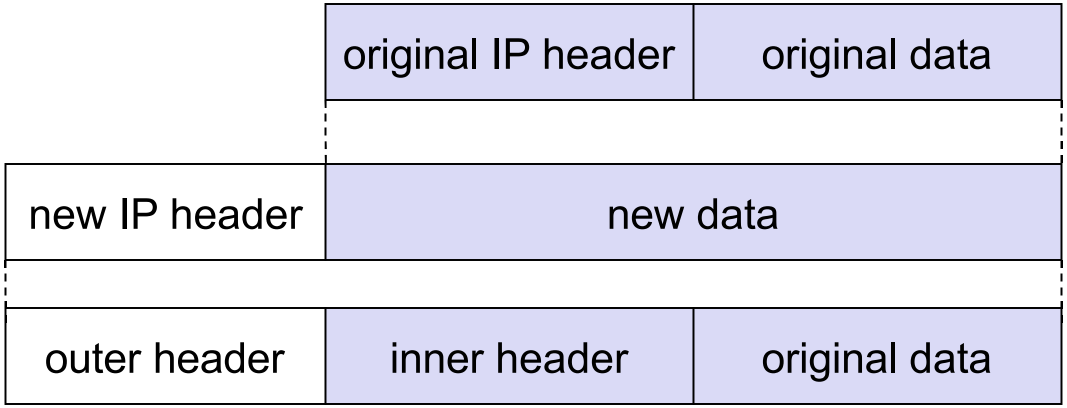
129 administratively prohibited

131 mobile node failed authentication

133 registration Identification mismatch

135 too many simultaneous mobility bindings

Encapsulation



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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>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><i>IP-in-IP</i></td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5"><b>IP address of HA</b></td></tr>
<tr><td colspan="5"><b>Care-of address COA</b></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"><b>IP address of CN</b></td></tr>
<tr><td colspan="5"><b>IP address of MN</b></td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

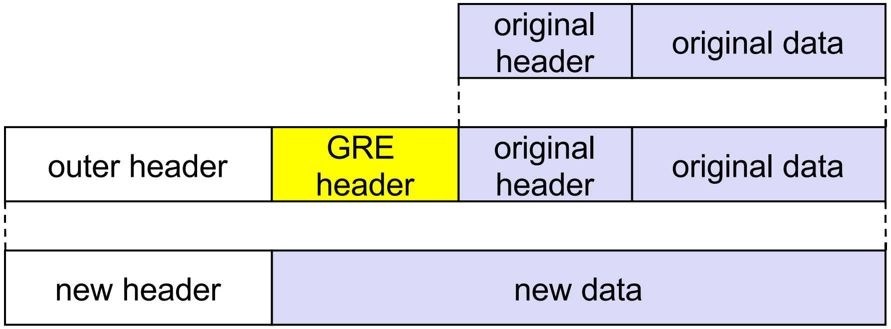
Encapsulation II

- 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 colspan="2">ver.</td><td colspan="2">IHL</td><td colspan="4">DS (TOS)</td><td colspan="8">length</td></tr>
<tr><td colspan="8">IP identification</td><td colspan="2">flags</td><td colspan="6">fragment offset</td></tr>
<tr><td colspan="4">TTL</td><td colspan="4"><i>min. encap.</i></td><td colspan="8">IP checksum</td></tr>
<tr><td colspan="16"><b>IP address of HA</b></td></tr>
<tr><td colspan="16"><b>care-of address COA</b></td></tr>
<tr><td colspan="4">lay. 4 protoc.</td><td colspan="1">S</td><td colspan="3">reserved</td><td colspan="8">IP checksum</td></tr>
<tr><td colspan="16"><b>IP address of MN</b></td></tr>
<tr><td colspan="16"><b>original sender IP address</b> (if S=1)</td></tr>
<tr><td colspan="16">TCP/UDP/ ... payload</td></tr>
</table>

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Generic Routing Encapsulation



original header | original data

outer header | GRE header | original header | original data

new header | new data

RFC 1701

<table>
<tr><td colspan="4">ver.</td><td colspan="2">IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="8">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="2"><i>GRE</i></td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="10"><b>IP address of HA</b></td></tr>
<tr><td colspan="10"><b>Care-of address COA</b></td></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>s</td><td>rec.</td><td>rsv.</td><td>ver.</td><td colspan="2">protocol</td></tr>
<tr><td colspan="8">checksum (optional)</td><td colspan="2">offset (optional)</td></tr>
<tr><td colspan="10">key (optional)</td></tr>
<tr><td colspan="10">sequence number (optional)</td></tr>
<tr><td colspan="10">routing (optional)</td></tr>
<tr><td colspan="4">ver.</td><td colspan="2">IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="8">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="2">lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="10"><b>IP address of CN</b></td></tr>
<tr><td colspan="10"><b>IP address of MN</b></td></tr>
<tr><td colspan="10">TCP/UDP/ ... payload</td></tr>
</table>

RFC 2784 (updated by 2890)

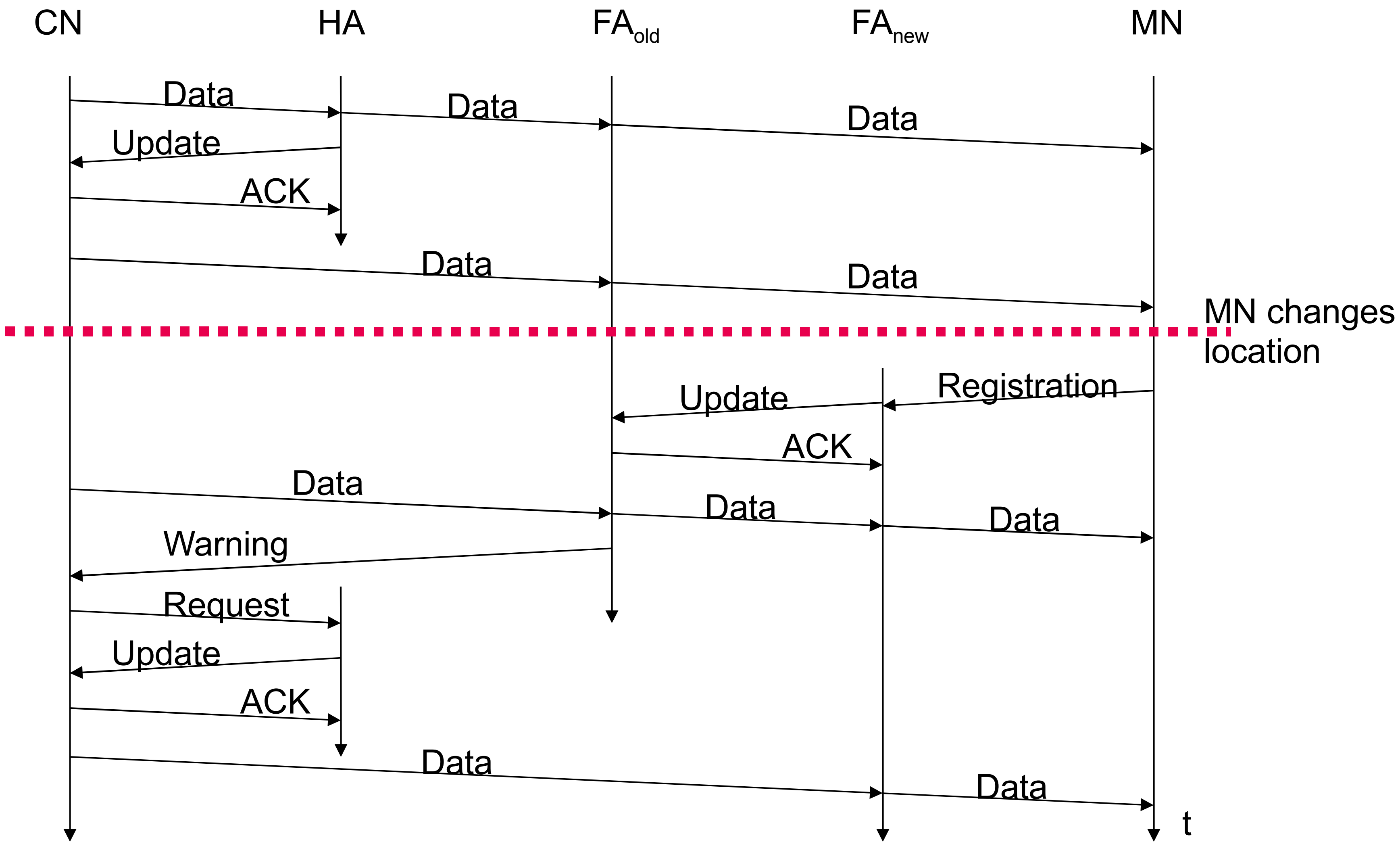
<table>
<tr><td>C</td><td>reserved0</td><td>ver.</td><td>protocol</td></tr>
<tr><td colspan="3">checksum (optional)</td><td>reserved1 (=0)</td></tr>
</table>

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Optimization of packet forwarding

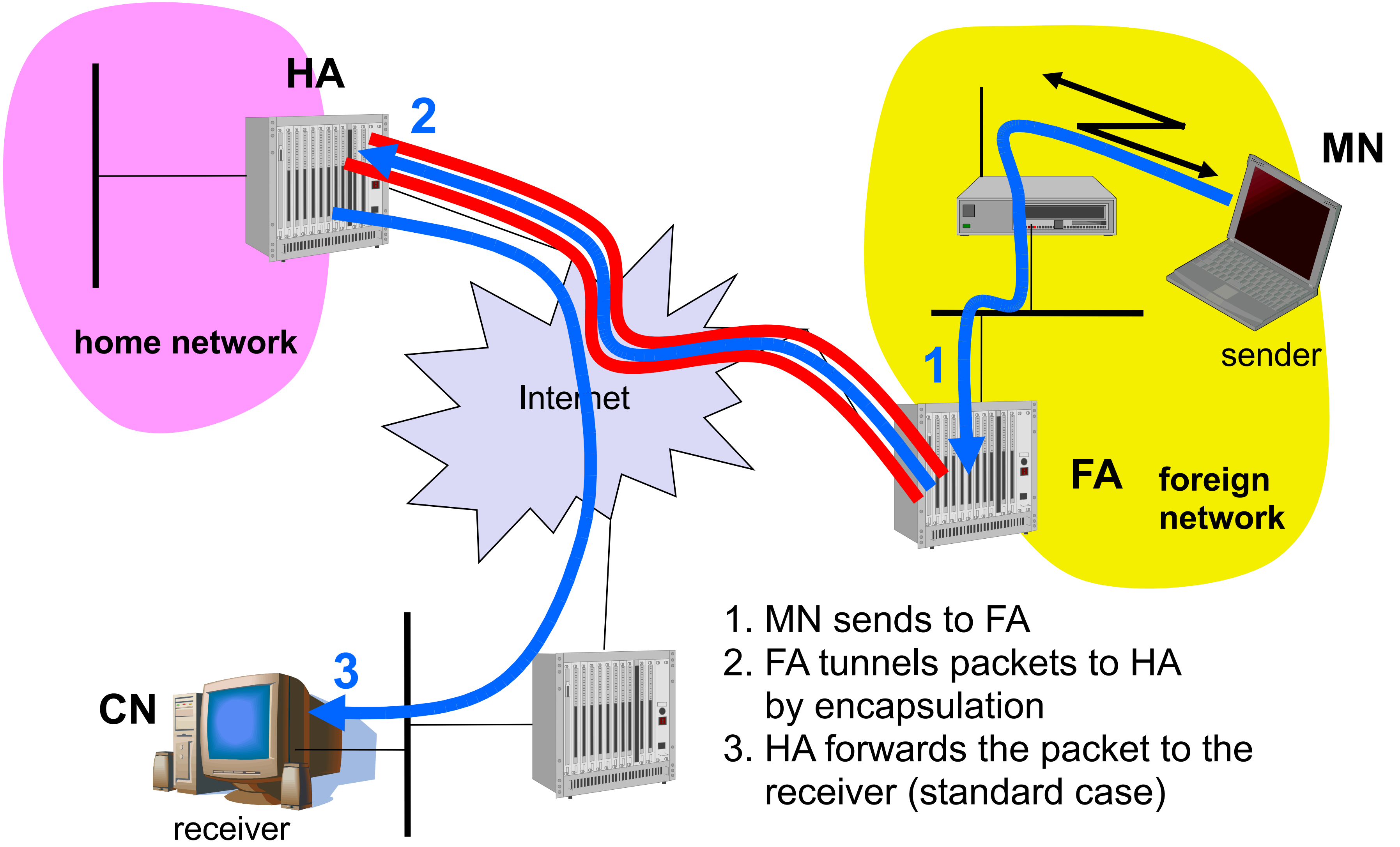
- Problem: Triangular Routing
  - sender sends all packets via HA to MN
  - higher latency and network load
- “Solutions”
  - sender learns the current location of MN
  - direct tunneling to this location
  - HA informs a sender about the location of MN
  - big security problems!
- Change of FA
  - packets 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



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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)

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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

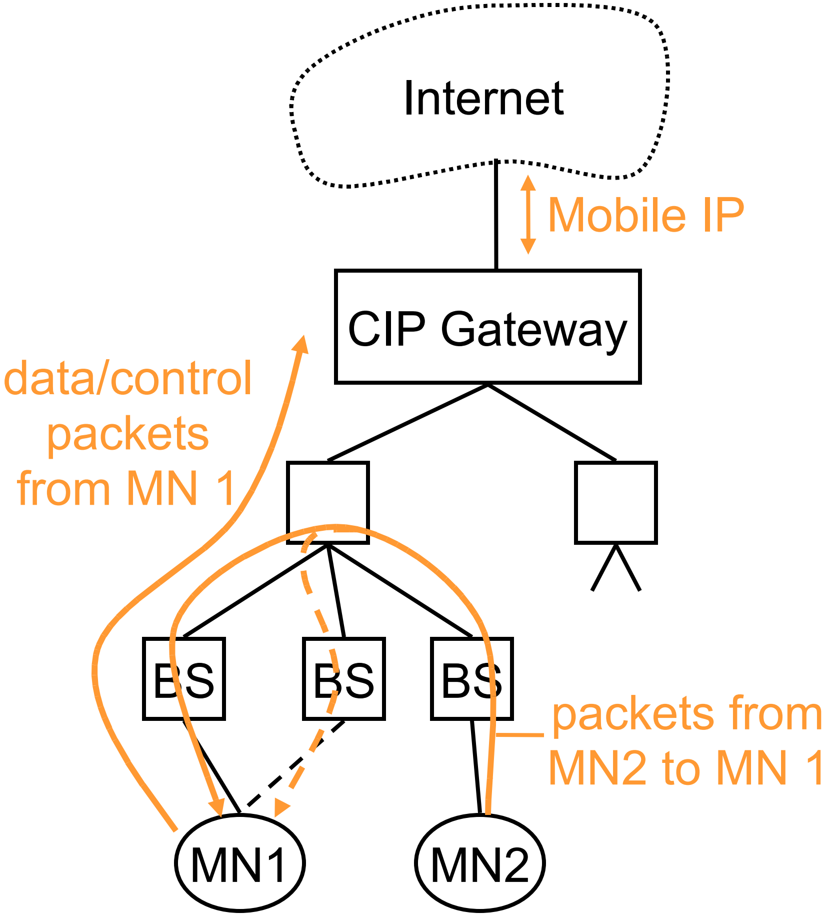
IP Micro-mobility support

- 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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Cellular IP: Other issues

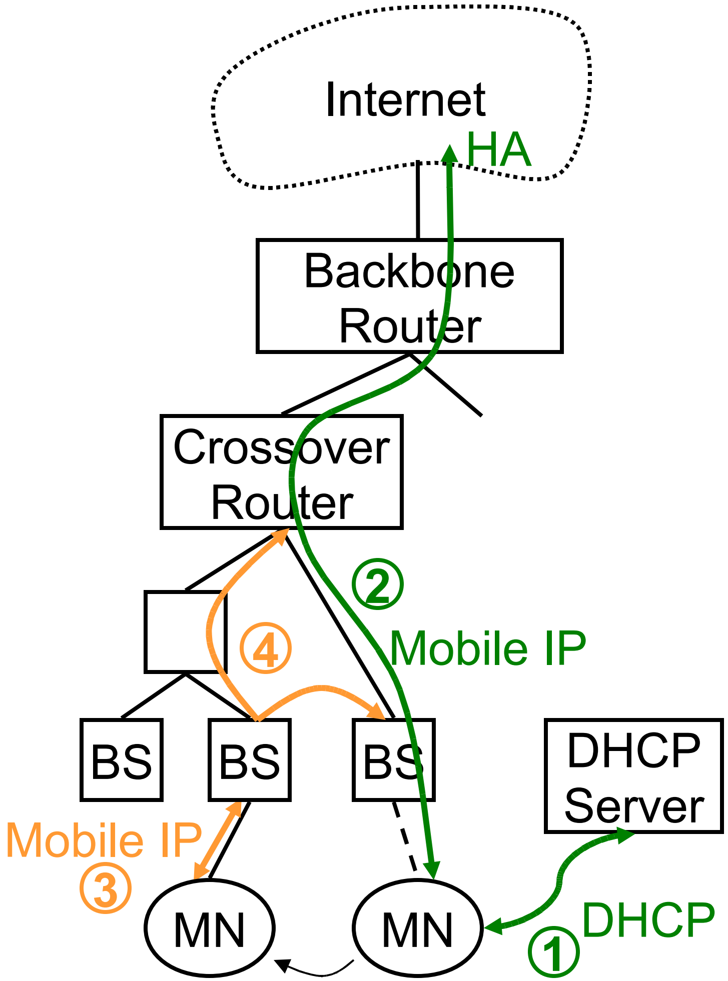
- Advantages:
    - Simple and elegant architecture
    - Mostly self-configuring (little management needed)
    - Integration with firewalls / private address support possible

- 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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

HAWAII

- Operation:
  - MN obtains co-located COA ① and registers with HA ②
  - Handover: MN keeps COA, ③ new BS answers Reg. Request ④ and updates routers
  - MN views BS as foreign agent
- Security provisions:
  - MN-FA authentication mandatory
  - Challenge/Response Extensions mandatory



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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

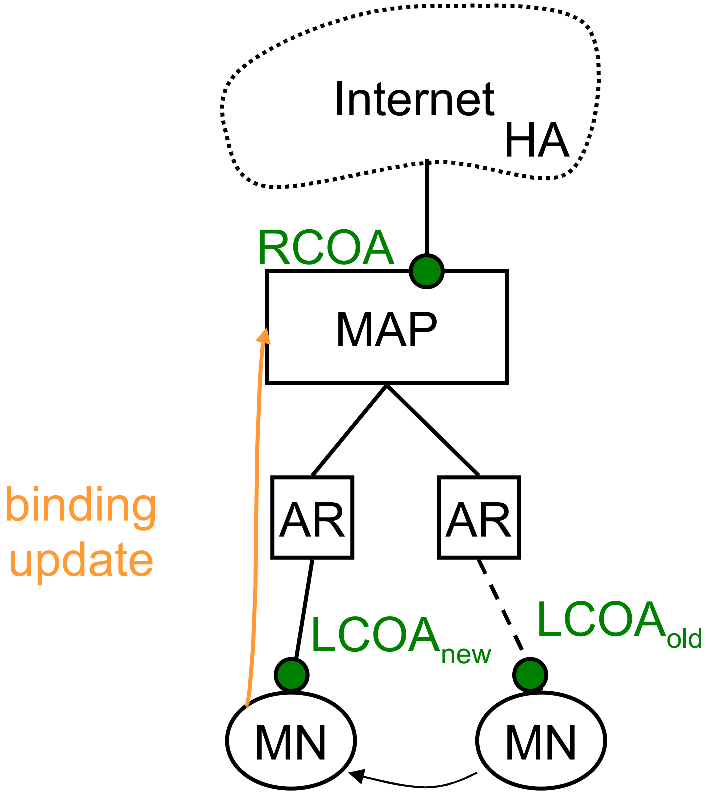
- Potential problems:
  - Mixture of co-located COA and FA concepts may not be supported by some MN implementations
  - No private address support possible
    because of co-located COA

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Hierarchical Mobile IP: Security

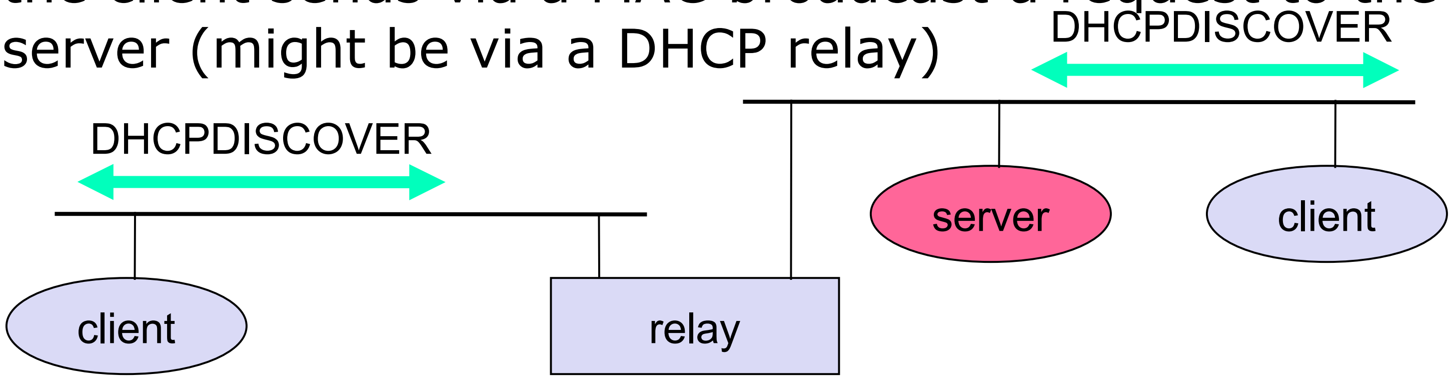
- Advantages:
  - Local COAs can be hidden,
    which provides at least some location privacy
  - Direct routing between CNs sharing the same link is possible (but might be dangerous)
  - The extended mode of HMIPv6 supports both mobile nodes and mobile networks

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

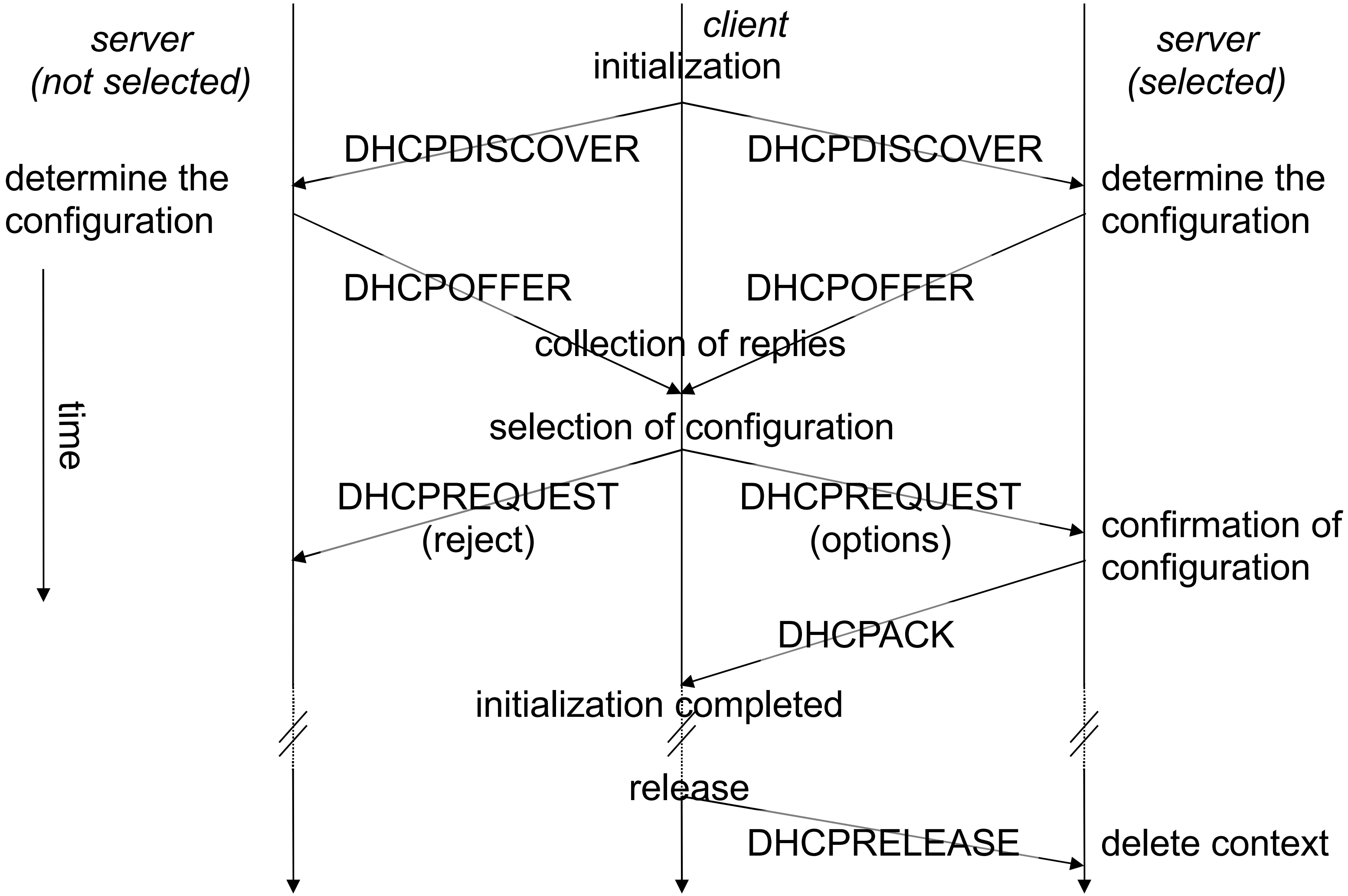
courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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)



DHCP - protocol mechanisms



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

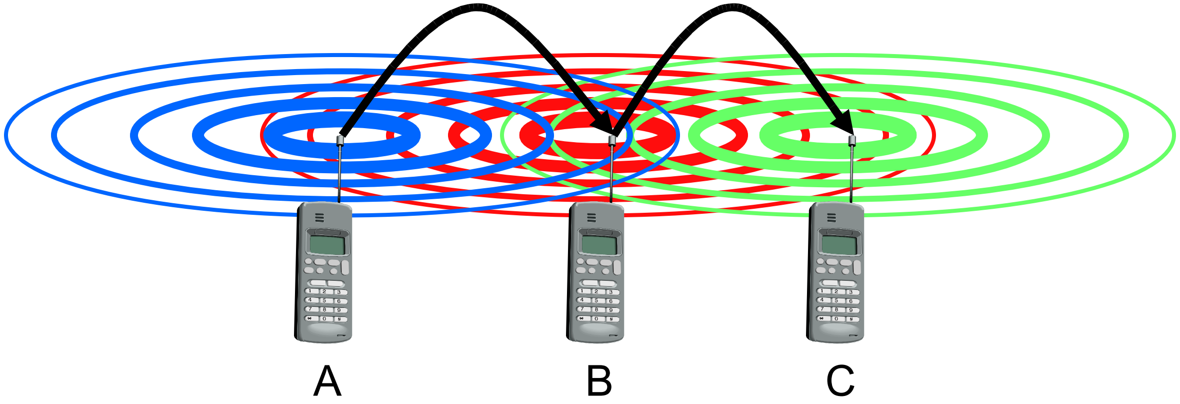
DHCP characteristics

- 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)

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Mobile ad hoc networks

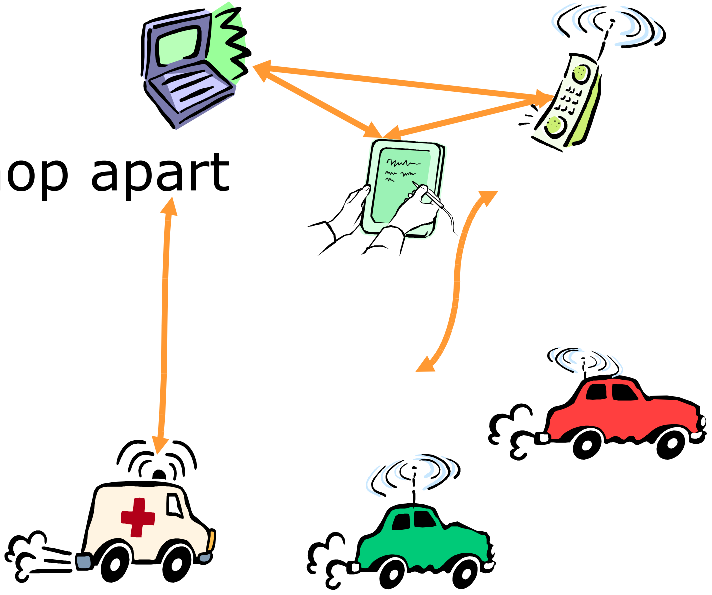
- Standard Mobile IP needs an infrastructure
  - Home Agent/Foreign Agent in the fixed network
  - DNS, routing etc. are not designed for mobility
- Sometimes there is no infrastructure!
  - remote areas, ad-hoc meetings, disaster areas
  - cost can also be an argument against an infrastructure!
- Main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



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Solution: Wireless ad-hoc networks

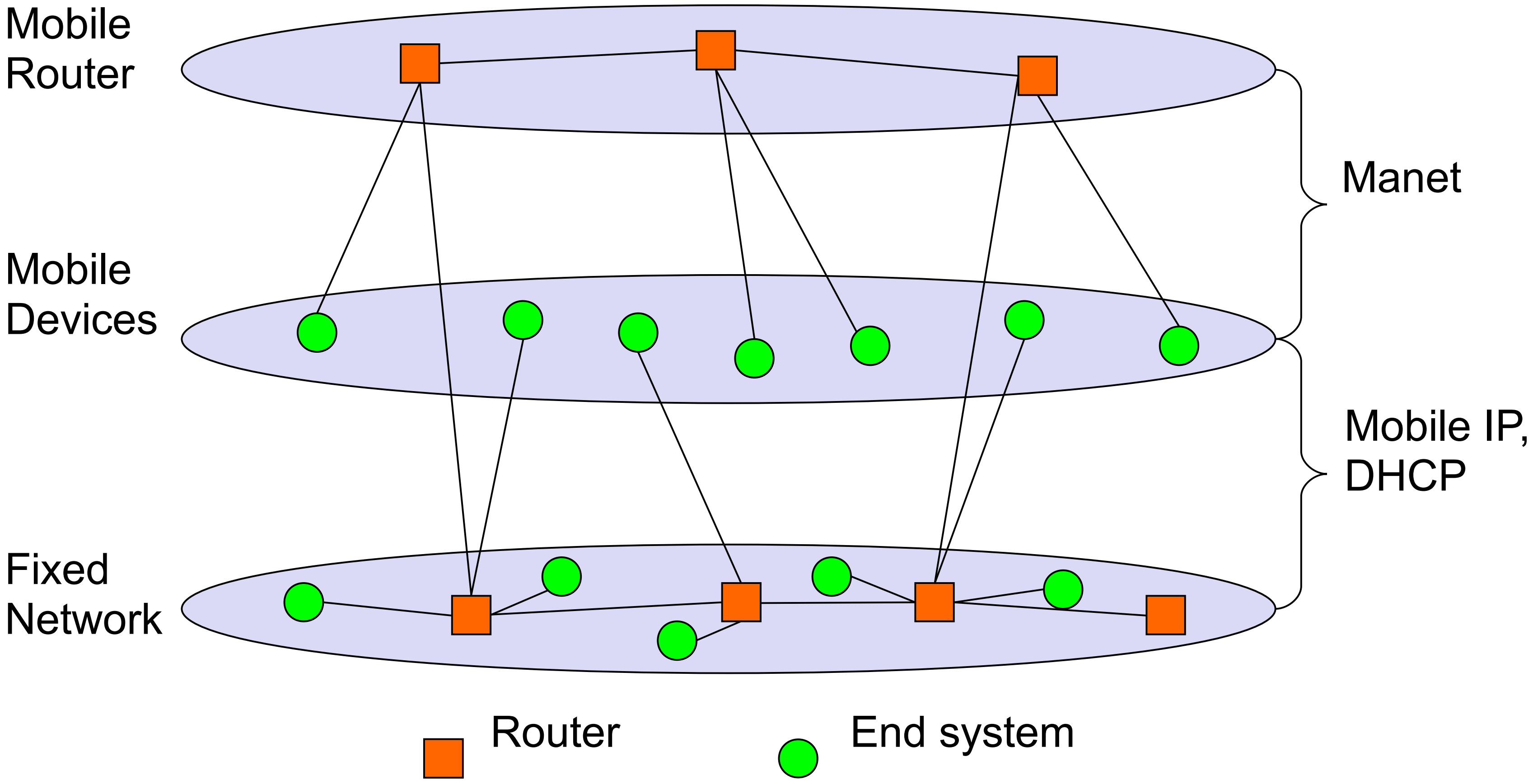
- Network without infrastructure
  - Use components of participants for networking
- Examples
  - Single-hop: All partners max. one hop apart
    - Bluetooth piconet, PDAs in a room, gaming devices…



  - Multi-hop: Cover larger distances, circumvent obstacles
    - Bluetooth scatternet, TETRA police network, car-to-car networks…
- Internet: MANET (Mobile Ad-hoc Networking) group

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

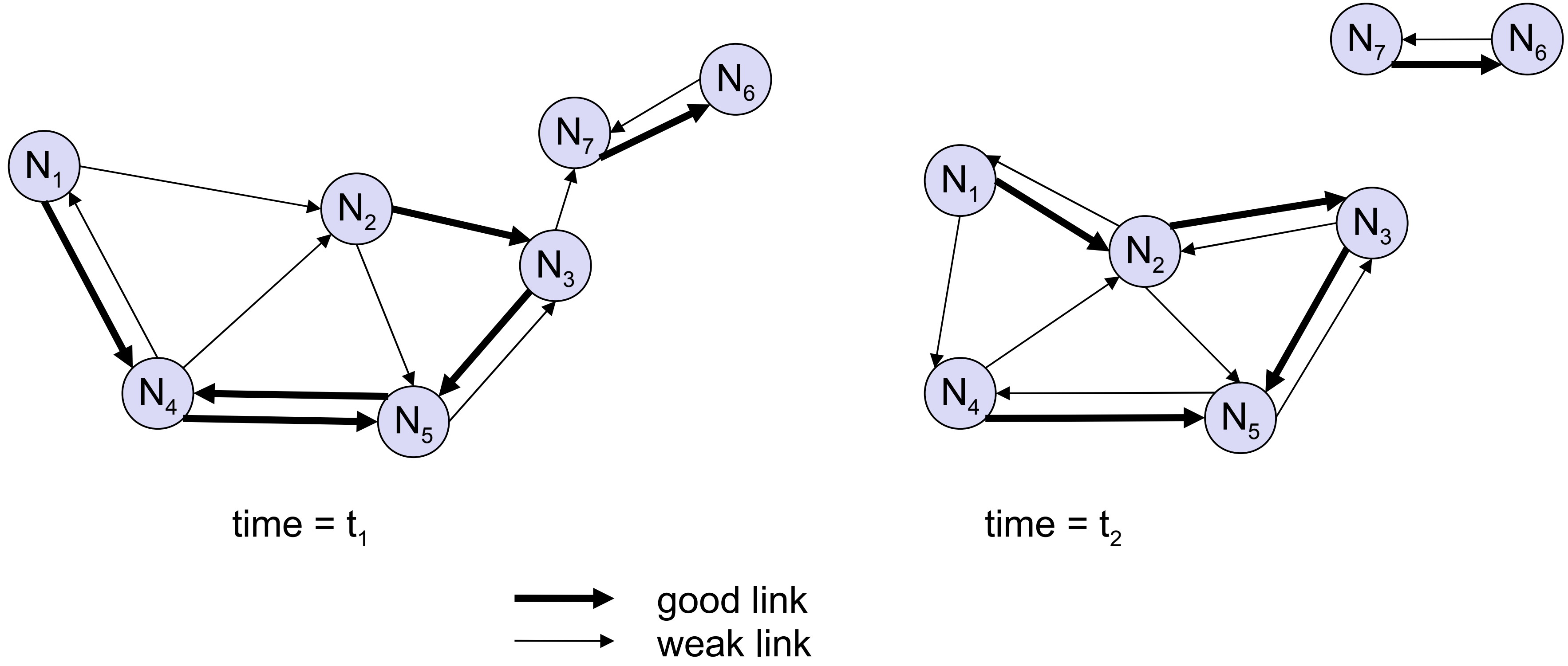
Manet: Mobile Ad-hoc Networking



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Problem No. 1: Routing

- Highly dynamic network topology
  - Device mobility plus varying channel quality
  - Separation and merging of networks possible
  - Asymmetric connections possible



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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 the 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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

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 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

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

DSDV (Destination Sequenced Distance Vector, historical)

- Early work
  - on demand version: AODV
- Expansion of distance vector routing
- 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)

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Dynamic source routing I

- Split routing into discovering a path and maintaining a path

- Discover a path
  - only if a path for sending packets to a certain destination is needed and no path is currently available

- Maintaining a path
  - only while the path is in use one has to make sure that it can be used continuously

- No periodic updates needed!

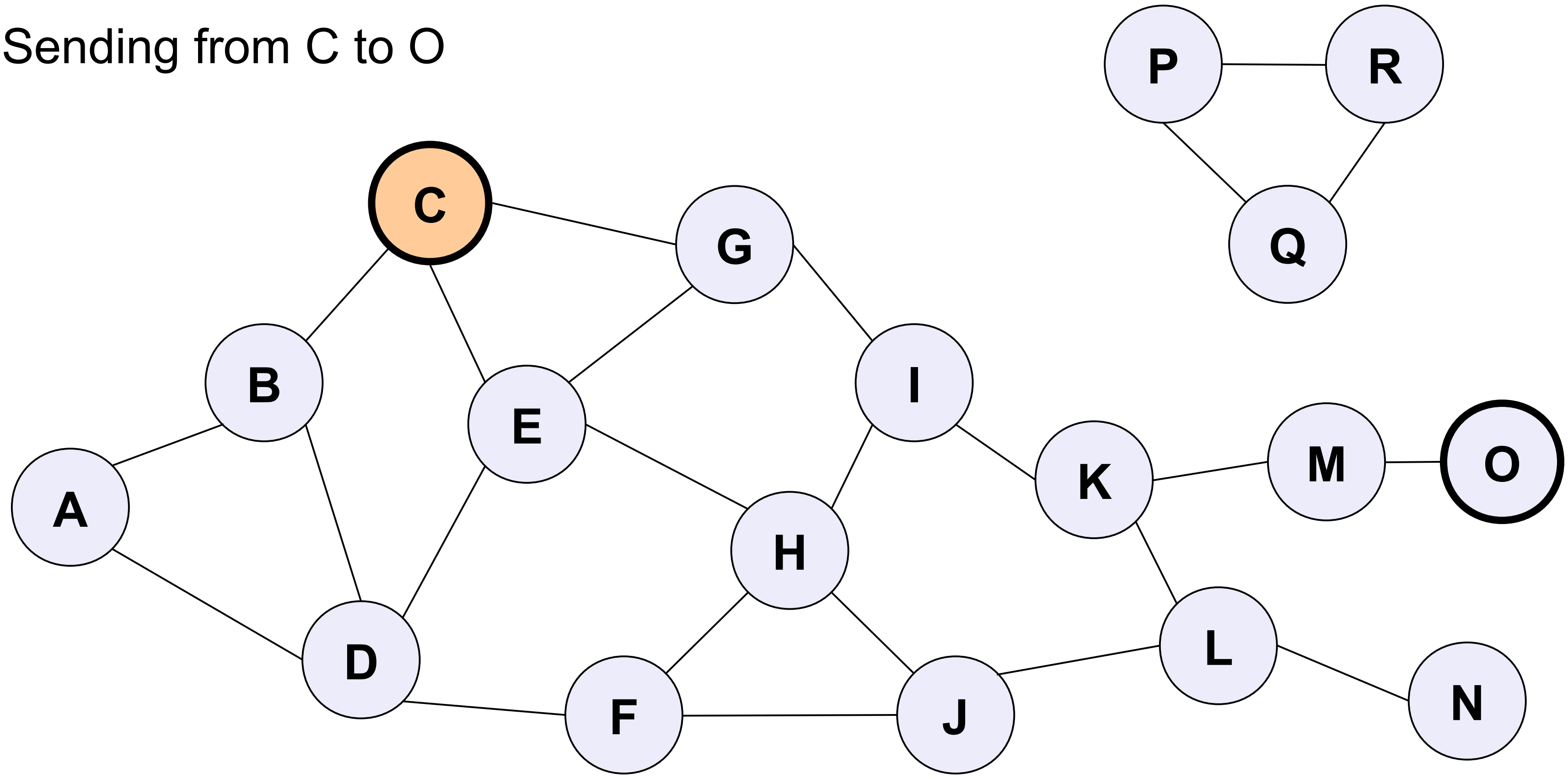
Dynamic source routing II

- 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
  - 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)

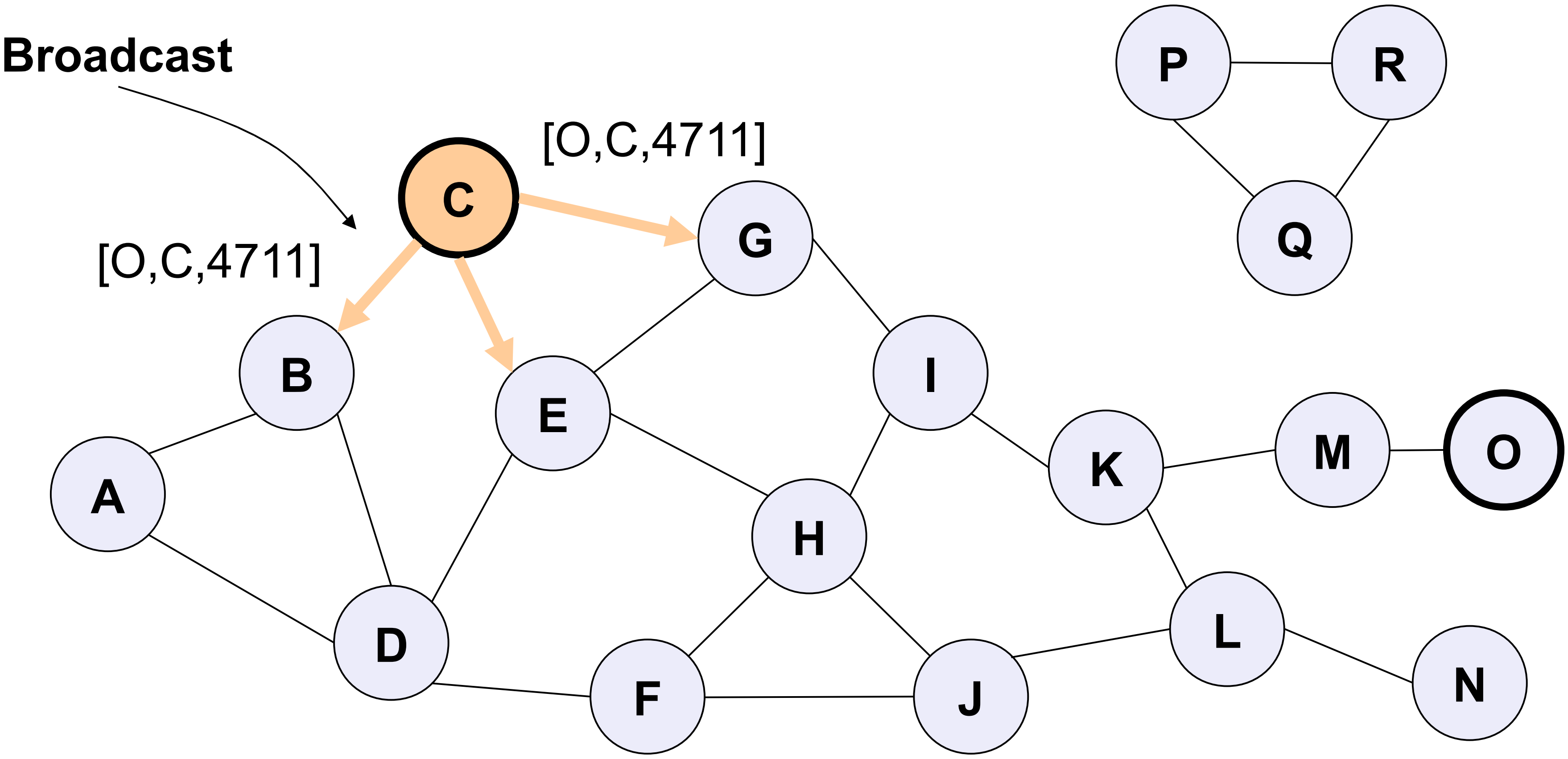
DSR: Route Discovery

Sending from C to O



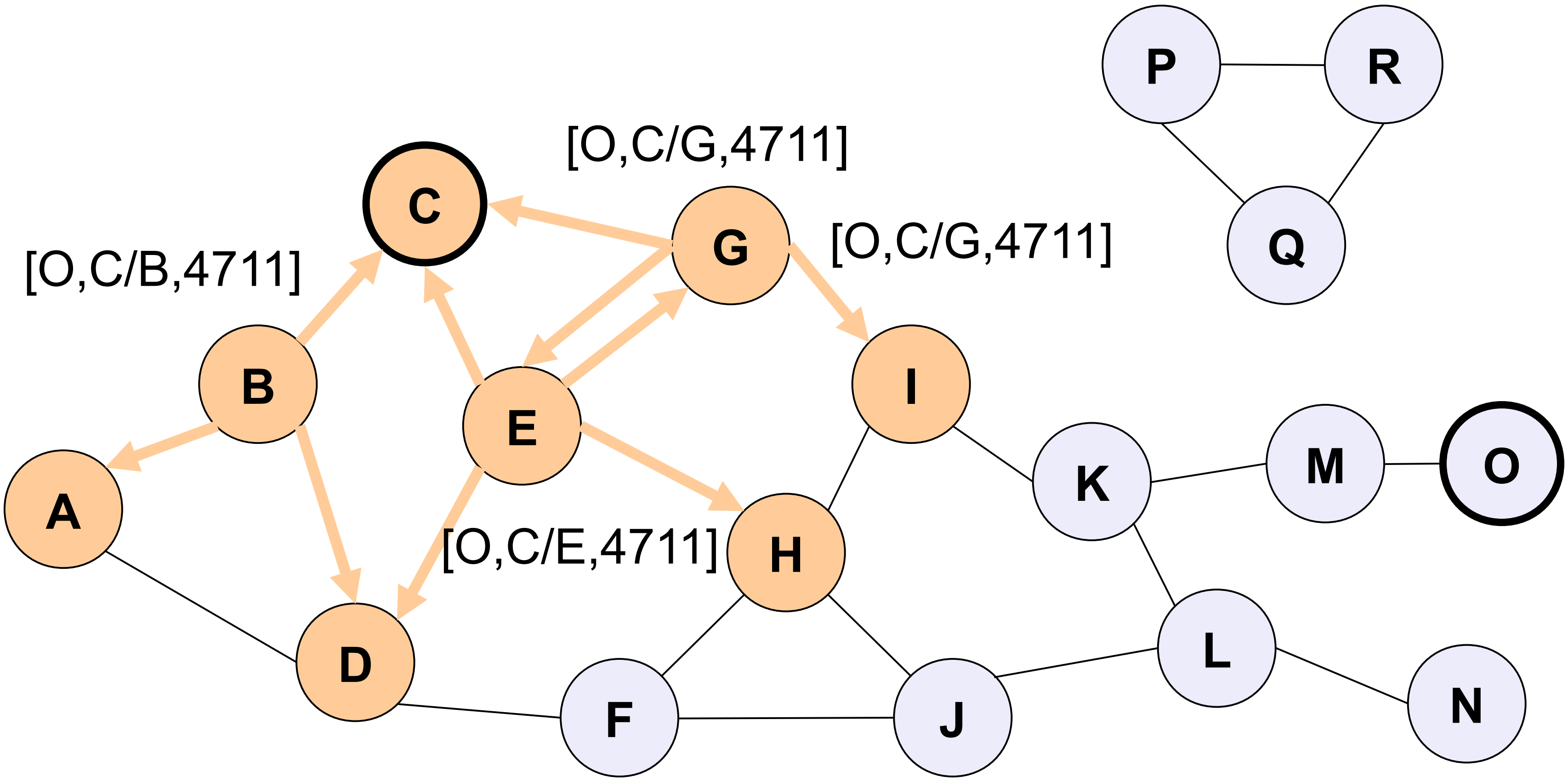
courtesy from Prof. Dr.-Ing. Jochen H. Schiller

DSR: Route Discovery



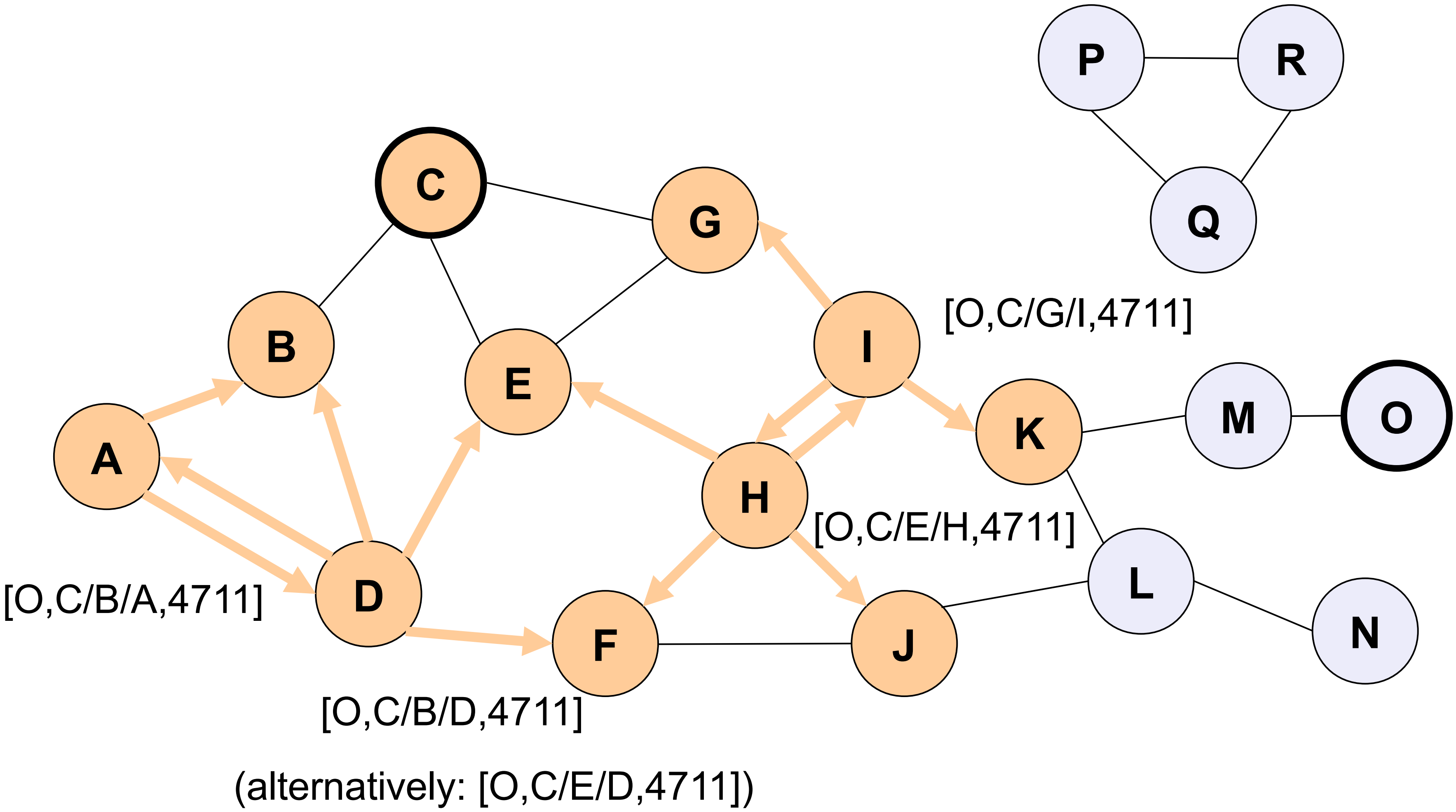
courtesy from Prof. Dr.-Ing. Jochen H. Schiller

DSR: Route Discovery



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

DSR: Route Discovery



[O,C/G/I,4711]

[O,C/E/H,4711]

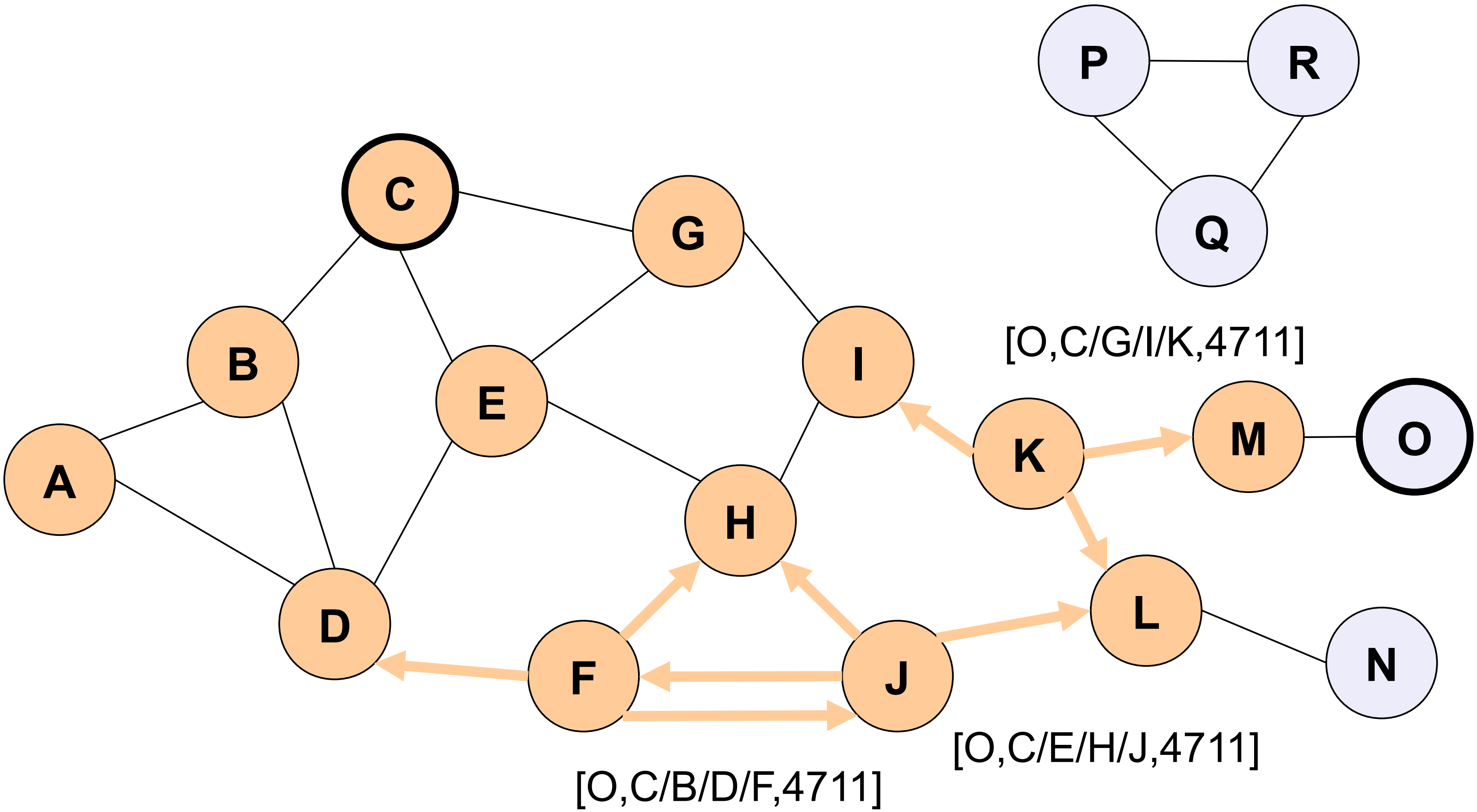
[O,C/B/A,4711]

[O,C/B/D,4711]

(alternatively: [O,C/E/D,4711])

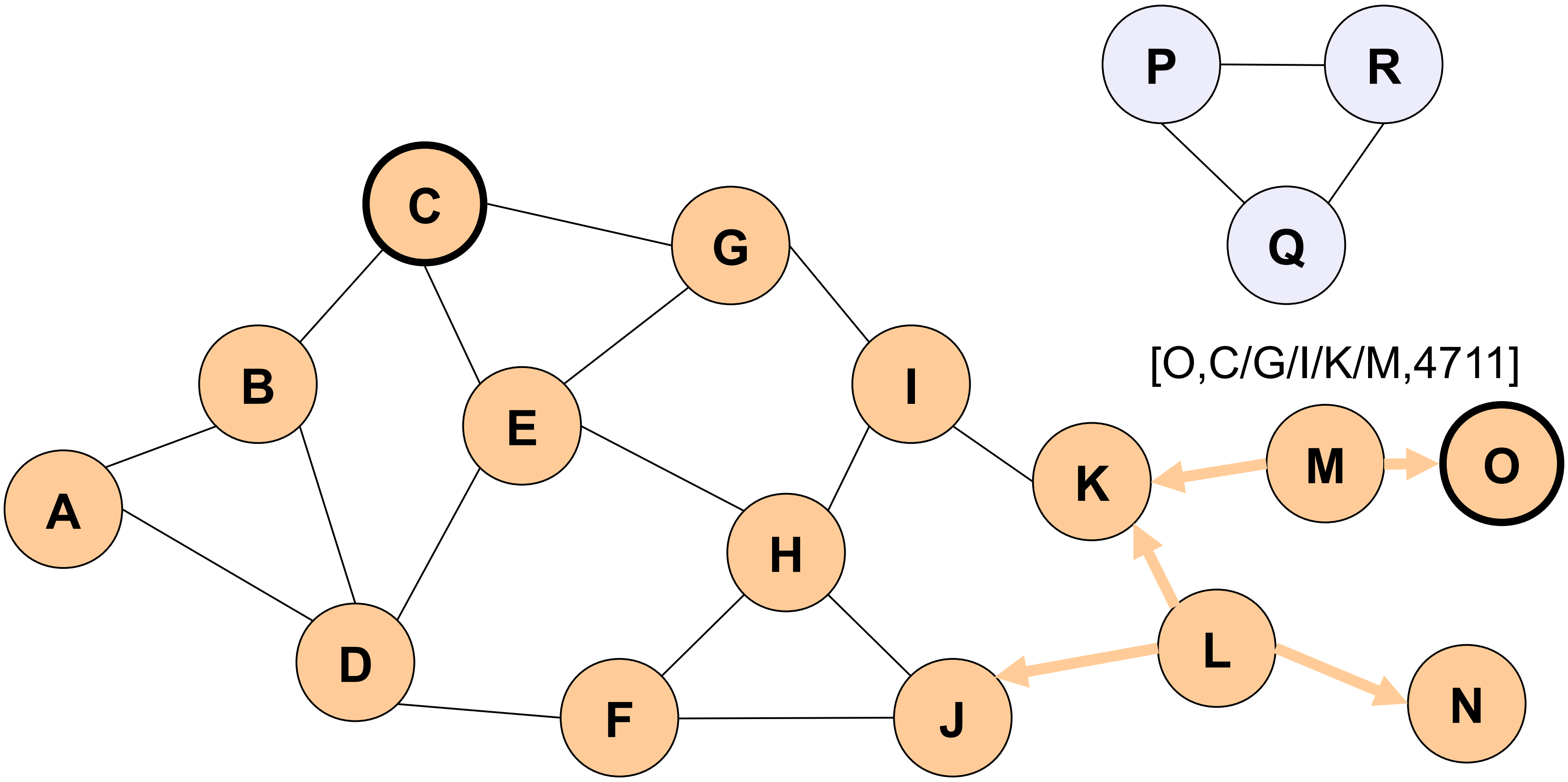
courtesy from Prof. Dr.-Ing. Jochen H. Schiller

DSR: Route Discovery



courtesy from Prof. Dr.-Ing. Jochen H. Schiller

DSR: Route Discovery



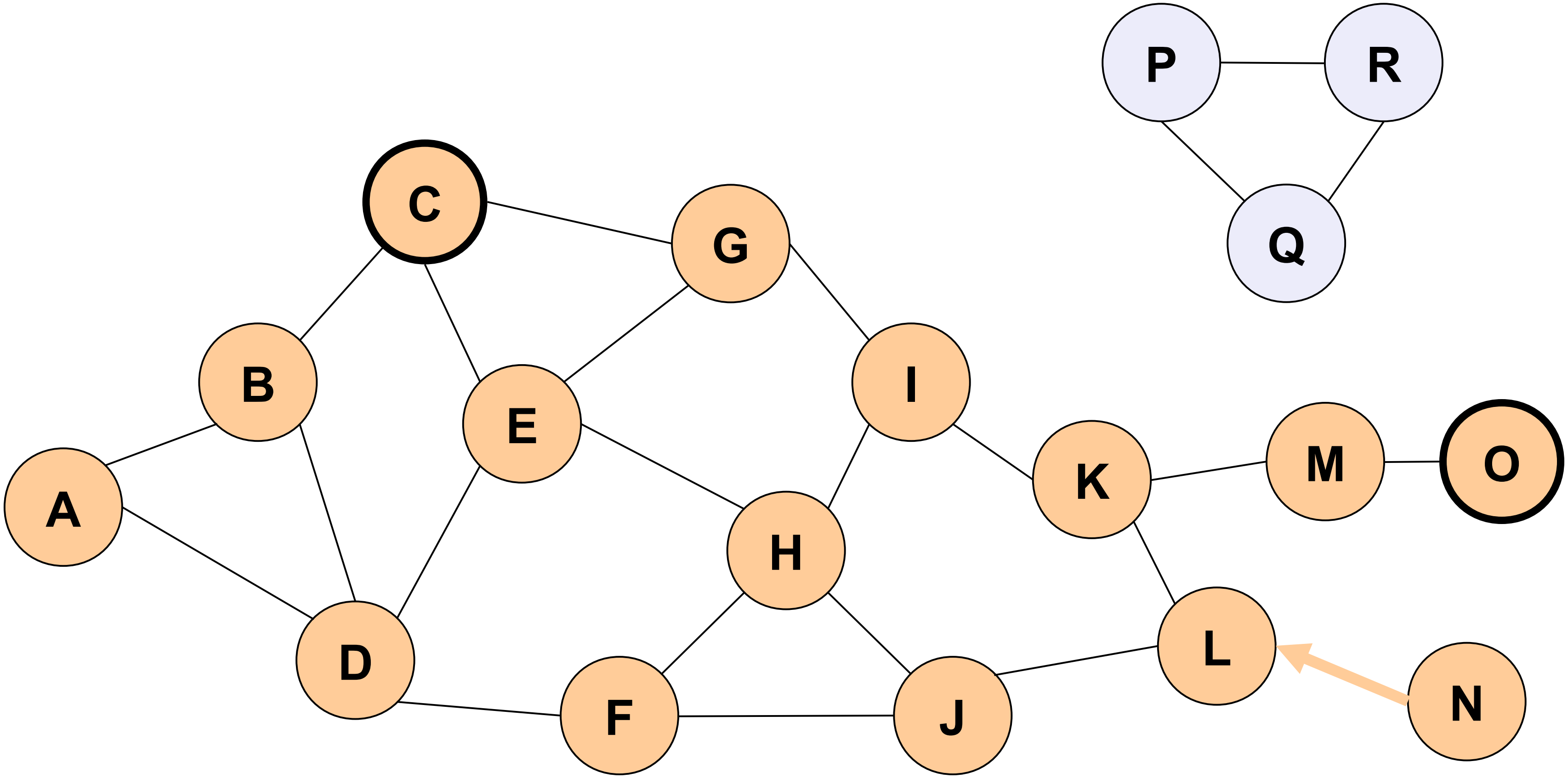
[O,C/G/I/K/M,4711]

[O,C/E/H/J/L,4711]

(alternatively: [O,C/G/I/K/L,4711])

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

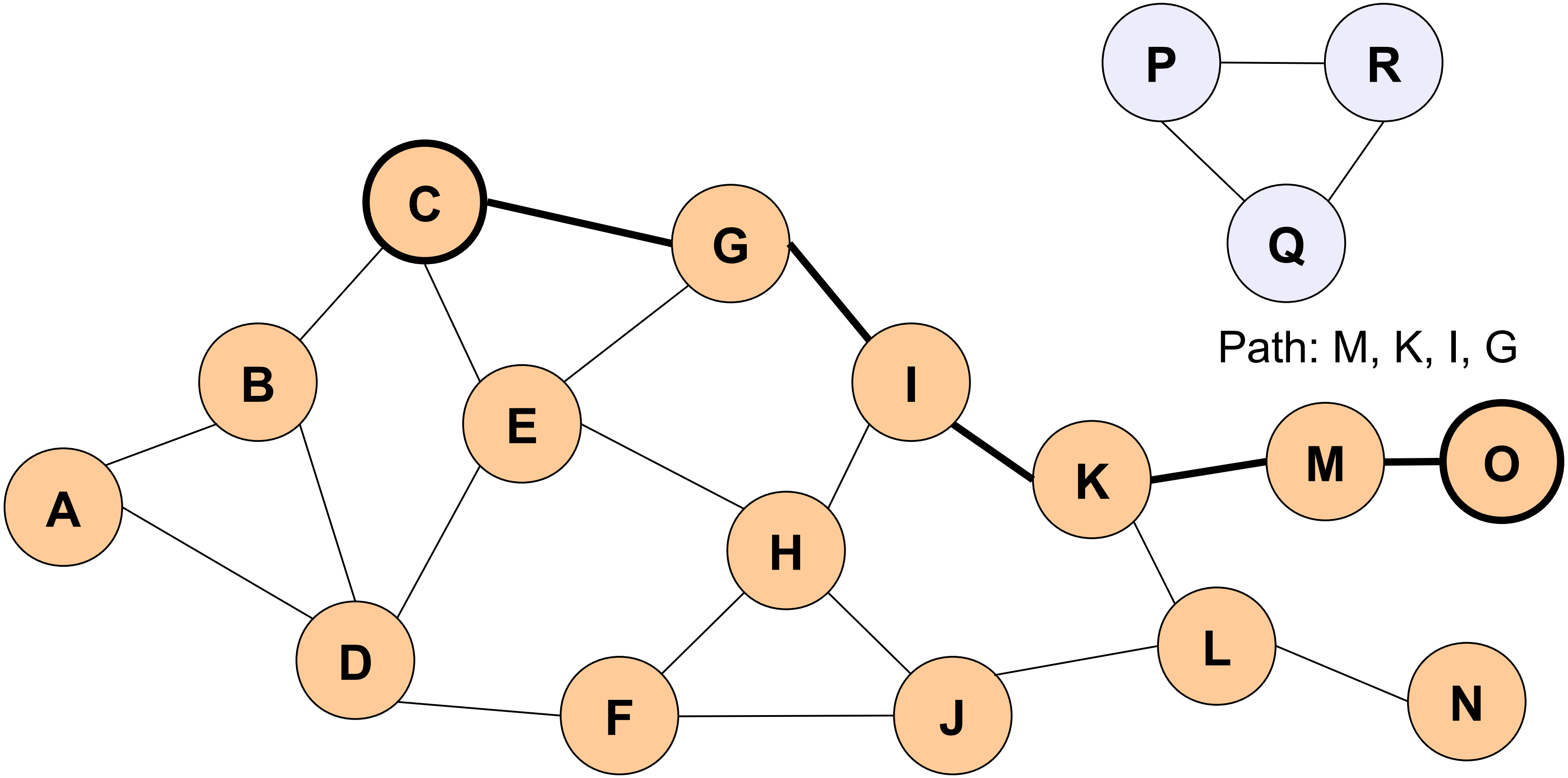
DSR: Route Discovery



[O,C/E/H/J/L/N,4711]

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

DSR: Route Discovery



Path: M, K, I, G

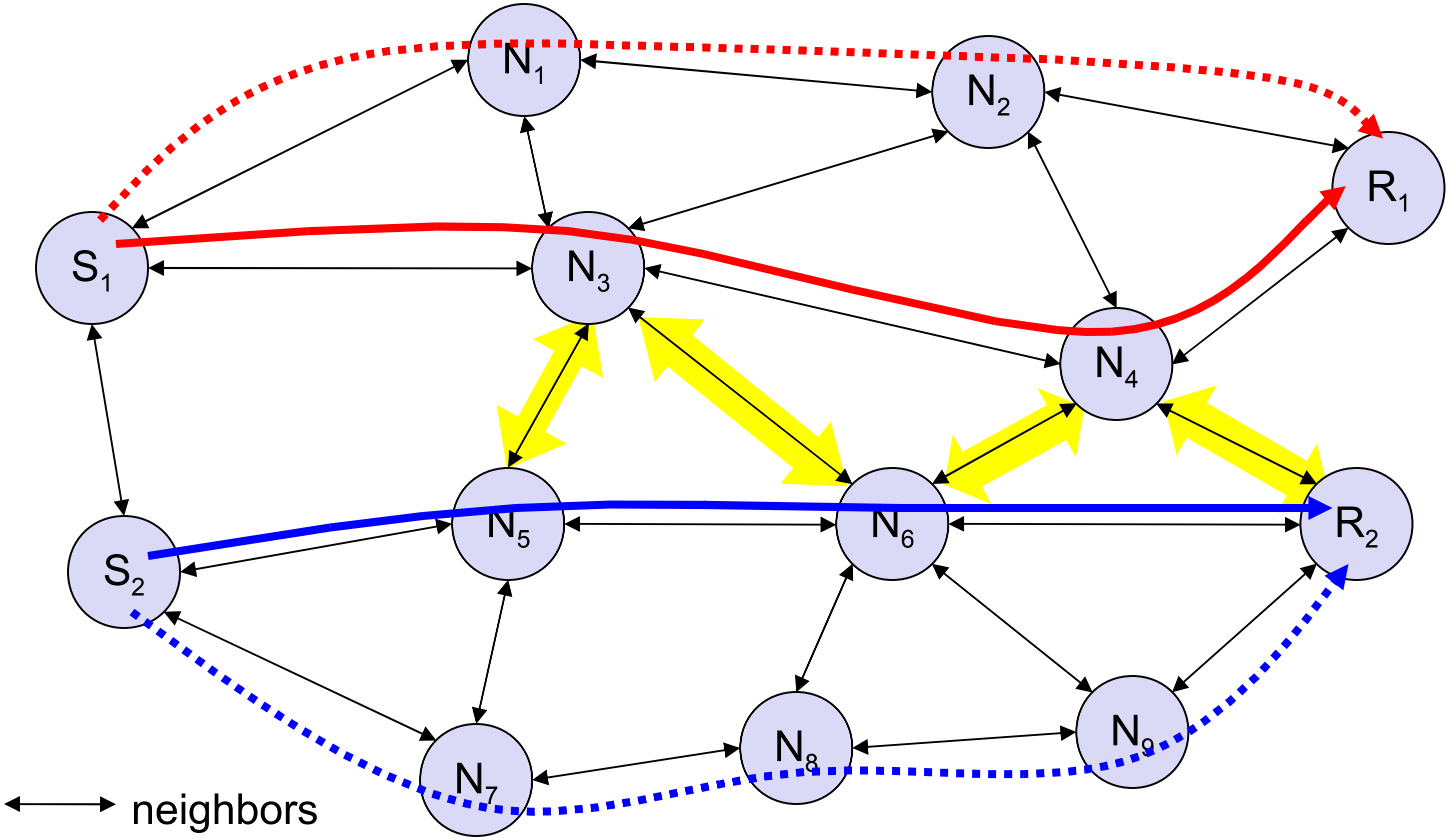
courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Dynamic Source Routing III

- Maintaining paths
  - after sending a packet
    - wait for a layer 2 acknowledgement (if applicable)
    - listen into the medium to detect if other stations forward the packet (if possible)
    - request an explicit acknowledgement
  - if a station encounters problems it can inform the sender of a packet or look-up a new path locally

Interference-based routing

- Routing based on assumptions about interference between signals



neighbors
(i.e. within radio range)

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Examples for interference based routing

- Least Interference Routing (LIR)
  - calculate the cost of a path based on the number of stations that can receive a transmission
- Max-Min Residual Capacity Routing (MMRCR)
  - calculate the cost of a path based on a probability function of successful transmissions and interference
- Least Resistance Routing (LRR)
  - calculate the cost of a path based on interference, jamming and other transmissions

- LIR is very simple to implement, only information from direct neighbors is necessary

A plethora of ad hoc routing protocols

- Flat
  - **proactive**
    - FSLS – Fuzzy Sighted Link State
    - FSR – Fisheye State Routing
    - **OLSR** – Optimized Link State Routing Protocol (RFC 3626)
    - TBRPF – Topology Broadcast Based on Reverse Path Forwarding
  - reactive
    - **AODV** – Ad hoc On demand Distance Vector (RFC 3561)
    - **DSR** – Dynamic Source Routing (RFC 4728)
    - **DYMO** – Dynamic MANET On-demand
- Hierarchical
  - CGSR – Clusterhead-Gateway Switch Routing
  - HSR – Hierarchical State Routing
  - LANMAR – Landmark Ad Hoc Routing
  - ZRP – Zone Routing Protocol
- Geographic position assisted
  - DREAM – Distance Routing Effect Algorithm for Mobility
  - GeoCast – Geographic Addressing and Routing
  - GPSR – Greedy Perimeter Stateless Routing
  - LAR – Location-Aided Routing

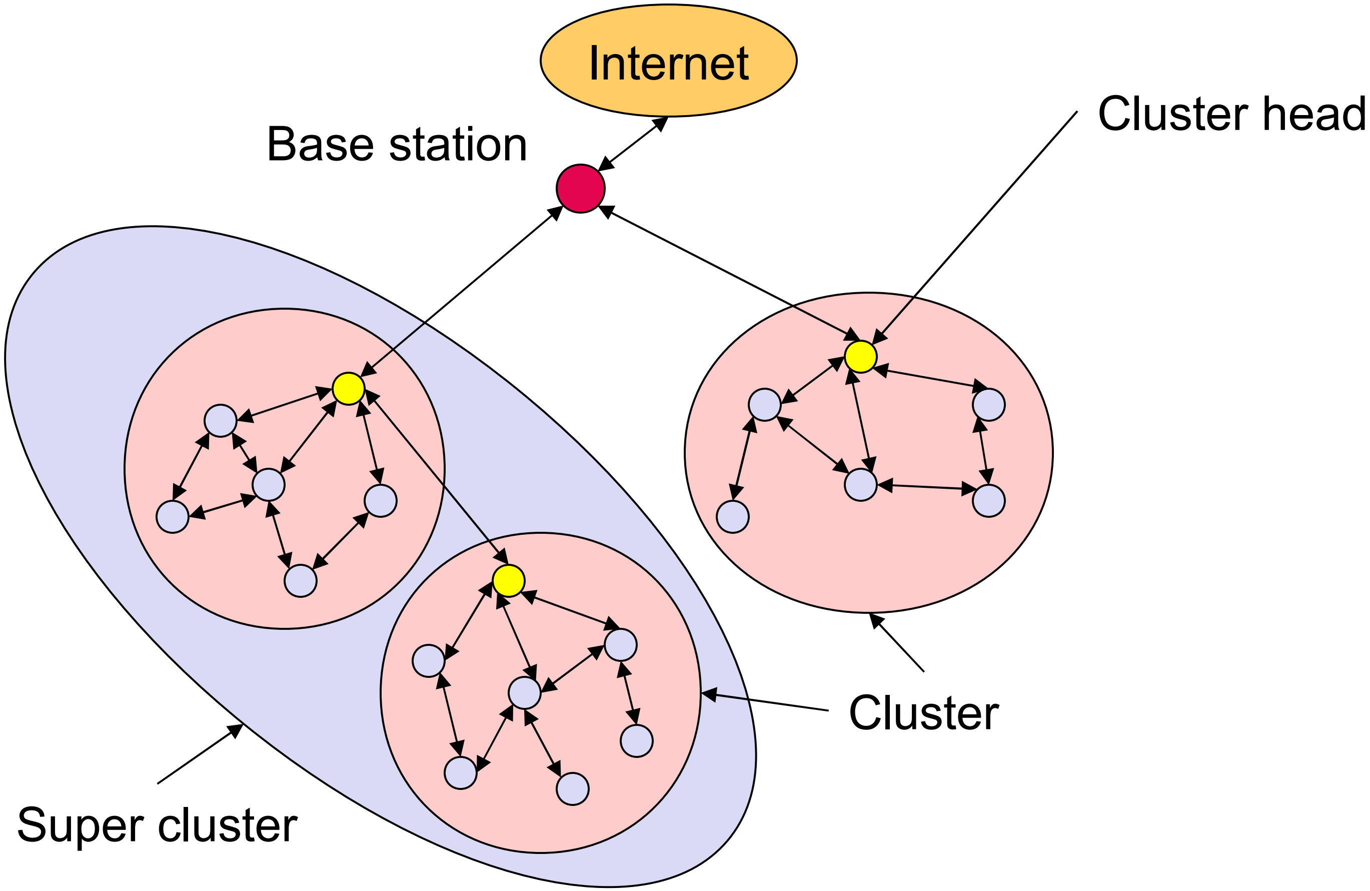
Two promising candidates: OLSRv2 and DYMO

courtesy from Prof. Dr.-Ing. Jochen H. Schiller

Further difficulties and research areas

- Auto-Configuration
  - Assignment of addresses, function, profile, program, …
- Service discovery
  - Discovery of services and service providers
- Multicast
  - Transmission to a selected group of receivers
- Quality-of-Service
  - Maintenance of a certain transmission quality
- Power control
  - Minimizing interference, energy conservation mechanisms
- Security
  - Data integrity, protection from attacks (e.g. Denial of Service)
- Scalability
  - 10 nodes? 100 nodes? 1000 nodes? 10000 nodes?
- Integration with fixed networks

Clustering of ad-hoc networks



courtesy from Prof. Dr.-Ing. Jochen H. Schiller