

# Mobile Communications

## Chapter 8: Network Protocols/Mobile IP

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

*Prof. Jó Ueyama*

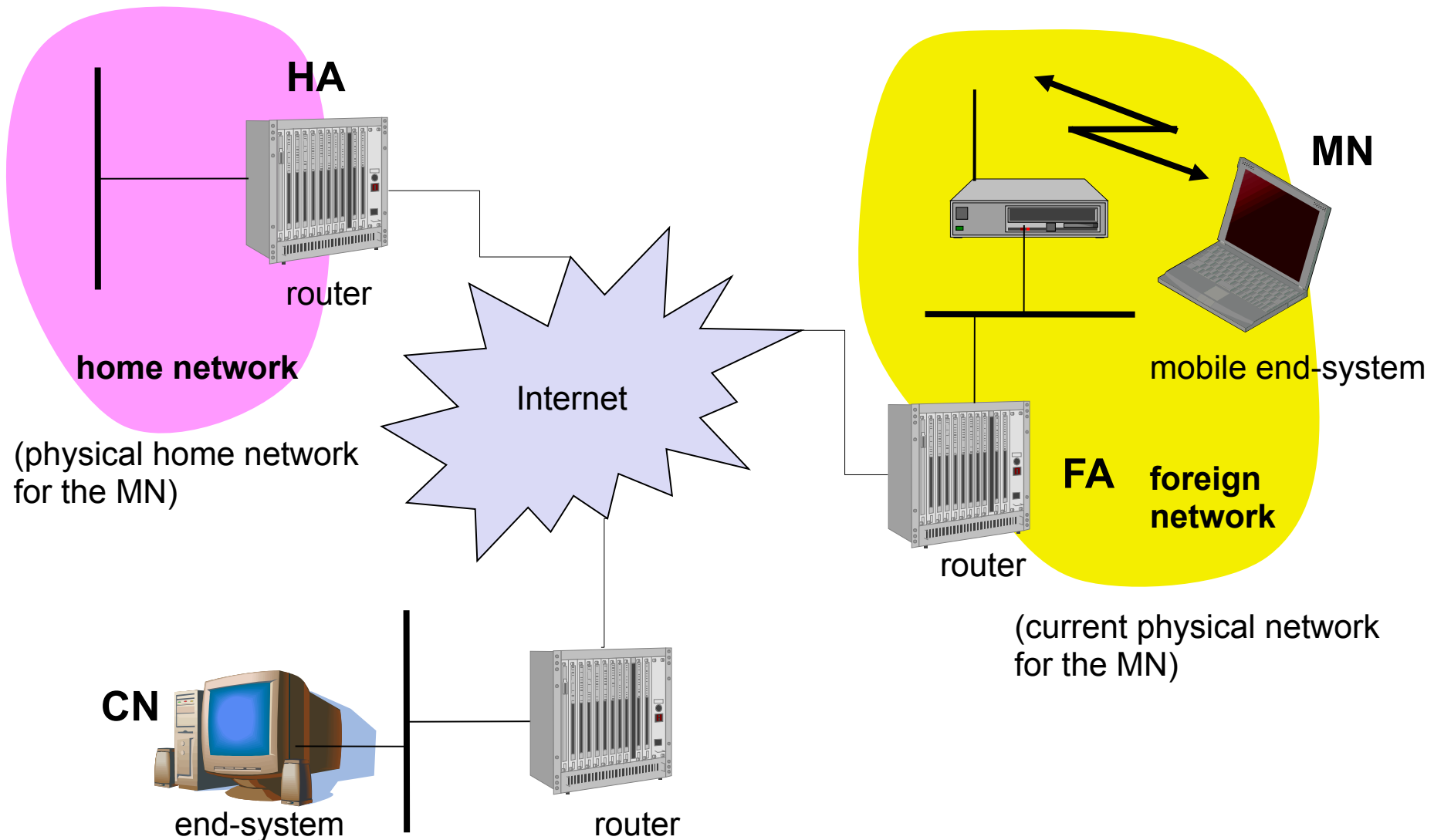
- Routing
  - based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
  - change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables
- Specific routes to end-systems?
  - 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

- 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

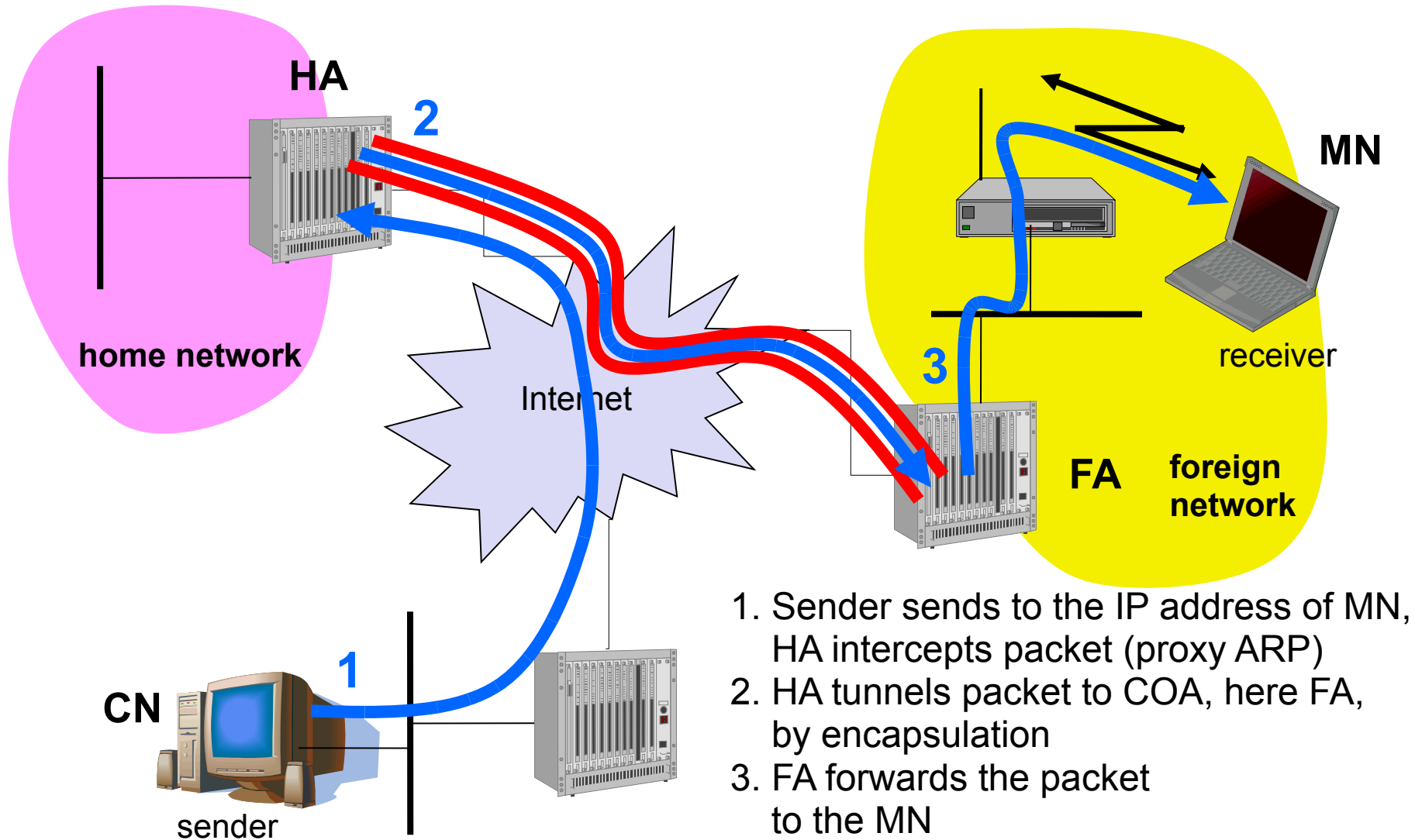
- Mobile Node (MN)
  - system (node) that can change the point of connection to the network without changing its IP address
- Home Agent (HA)
  - system in the home network of the MN, typically a router
  - registers the location of the MN, tunnels IP datagrams to the COA
- Foreign Agent (FA)
  - system 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



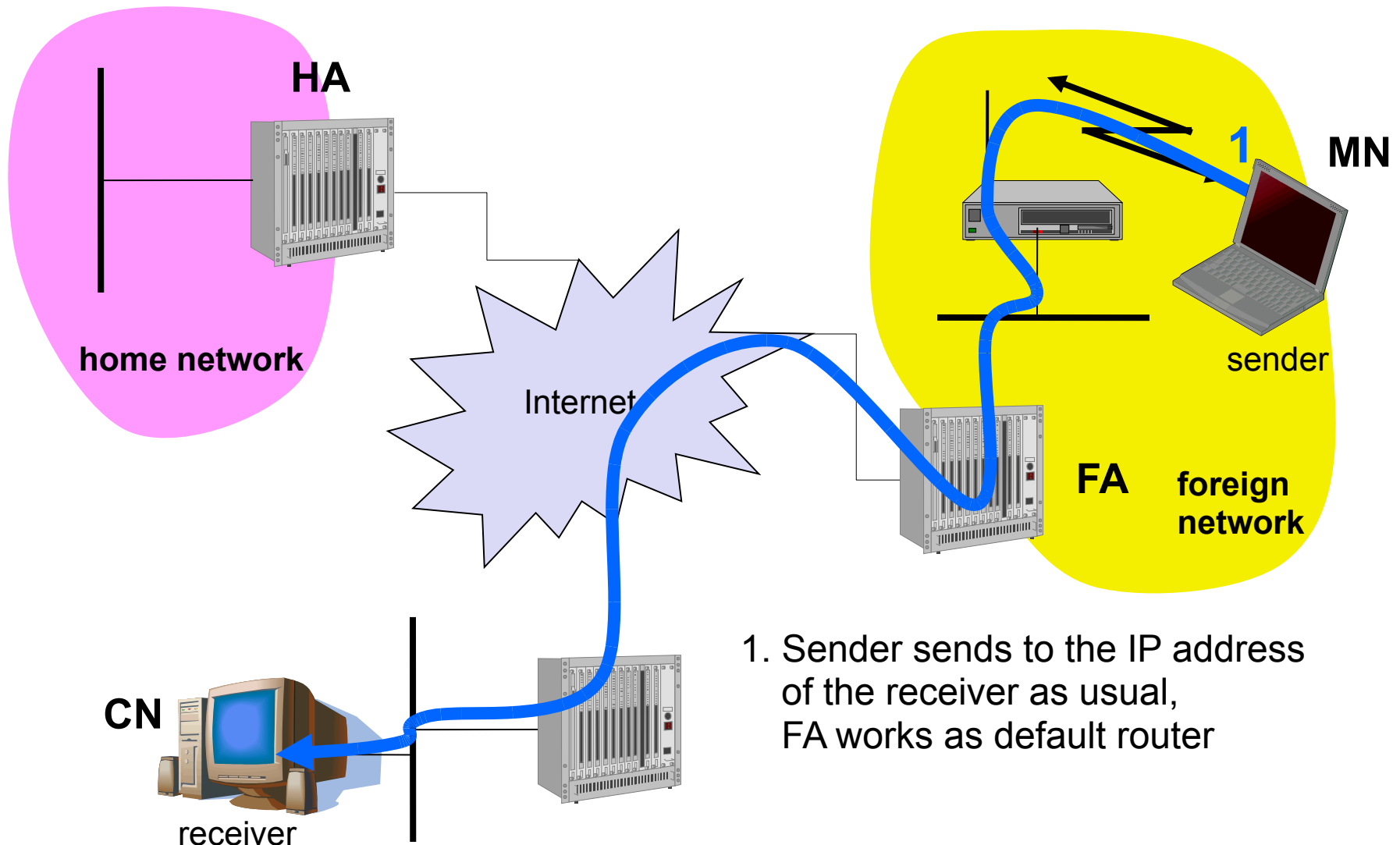
# Example network



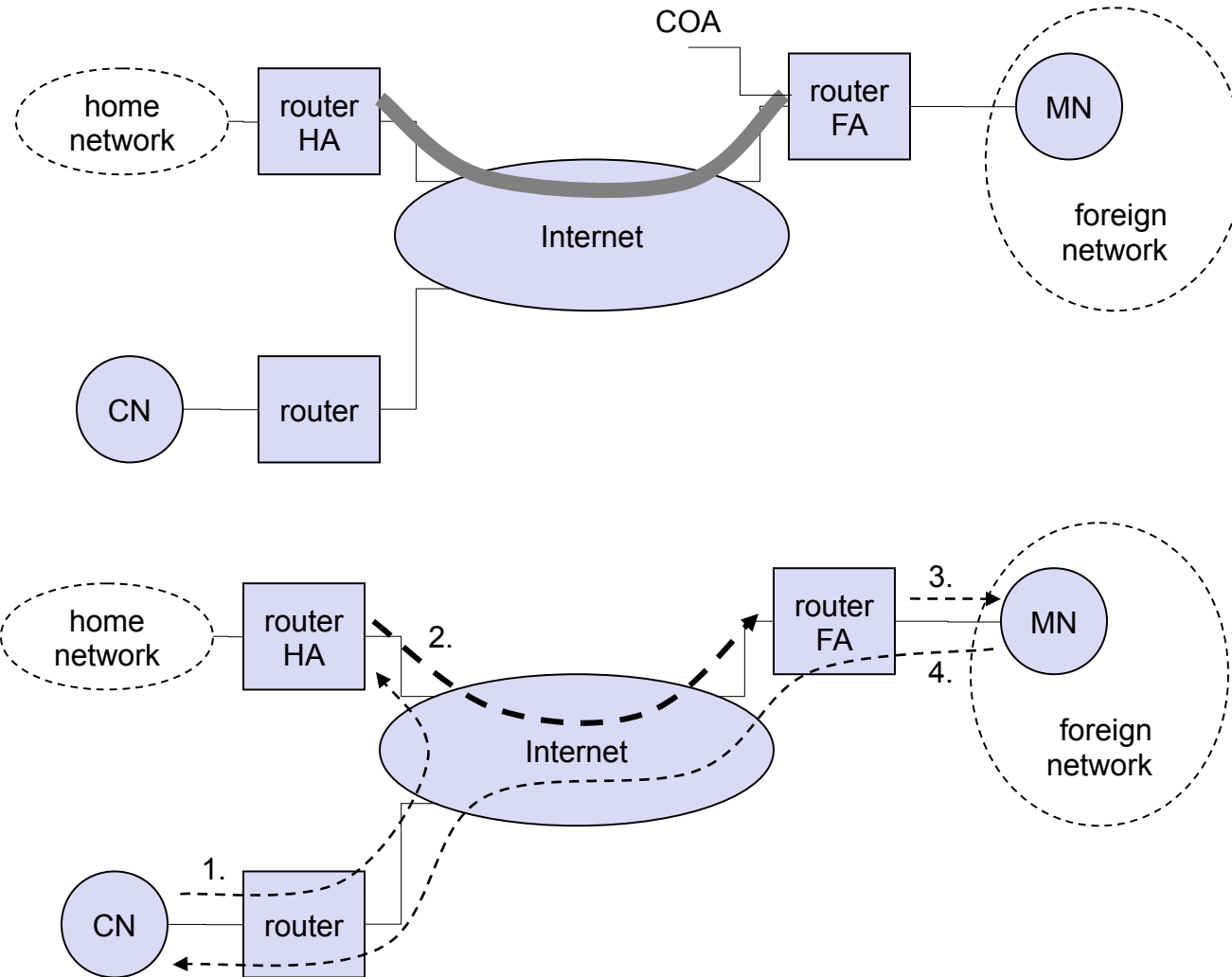
# Data transfer to the mobile system



# Data transfer from the mobile system



# Overview





- 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

|                       |   |            |    |                 |    |    |                |
|-----------------------|---|------------|----|-----------------|----|----|----------------|
| 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

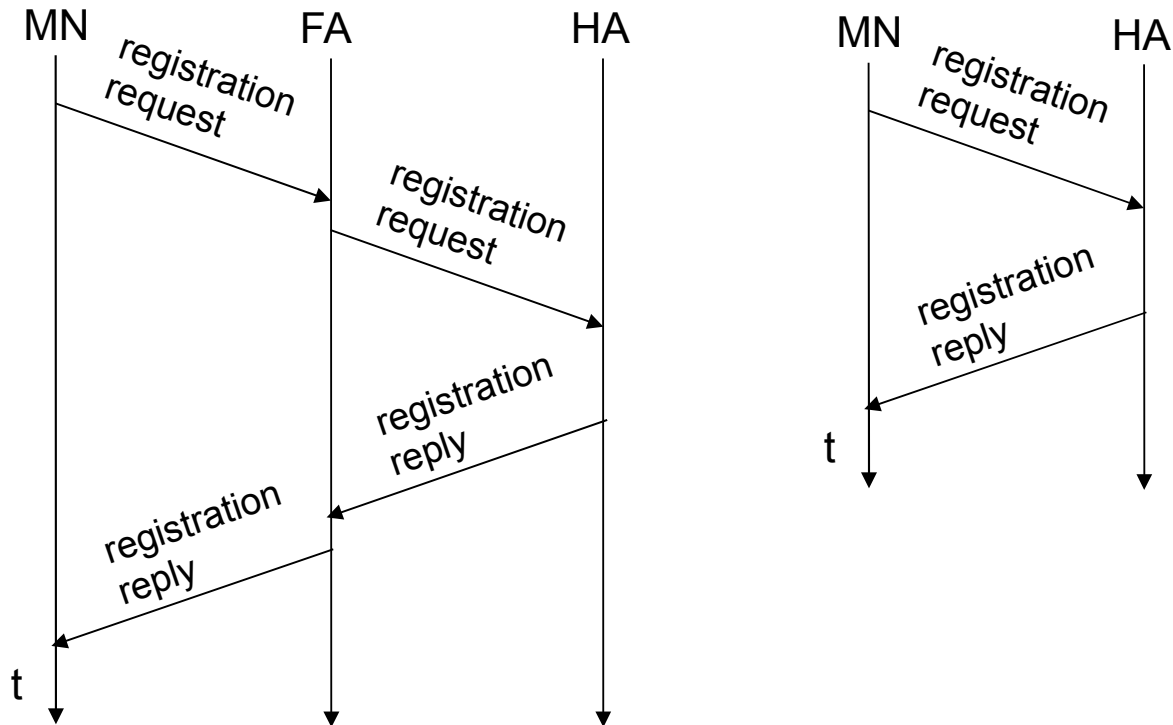
r: =0, ignored (former Van Jacobson compression)

T: FA supports reverse tunneling

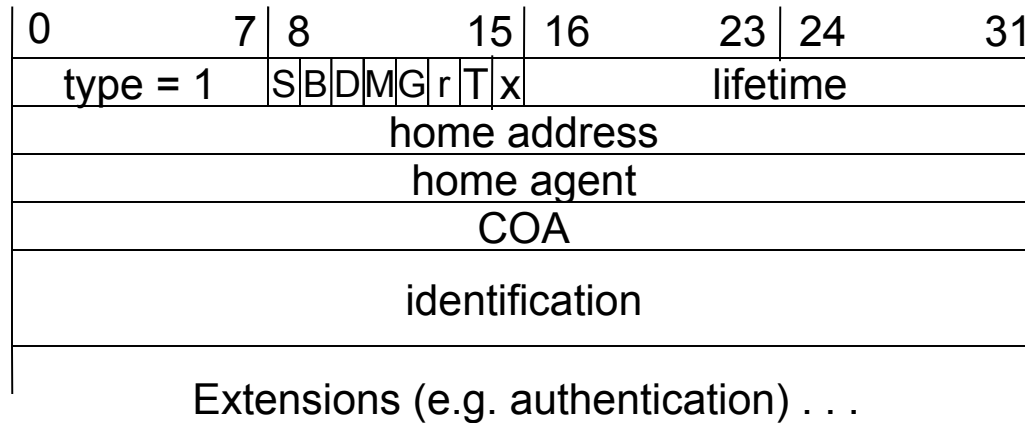
reserved: =0, ignored

- Agent Advertisement Packet Frame
  - Type: 16 indicates agent advertisement
  - Length: number in bytes excluding Type and Length fields;  $6 + 4 * \# \text{ COAs}$
  - Sequence number: count of agent advertisement messages since agent was initialized
  - R Bit, indicates that the registration is required even if the mobile node has already registered with this network; or already has a CO-COA
  - H Bit: This agent offers services as a home agent on this network
  - F Bit: This agent offers services as a foreign agent on this network

# Registration via FA or directly with the HA



# Mobile IP registration request



S: simultaneous bindings (requests that multiple copies of packet are sent to each registered COA)

B: broadcast datagrams

D: decapsulation by MN (If Co-located COA is adopted)

M: minimal encapsulation

G: GRE encapsulation

r: =0, ignored

T: reverse tunneling requested

x: =0, ignored

Type 1 → registration request

# 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

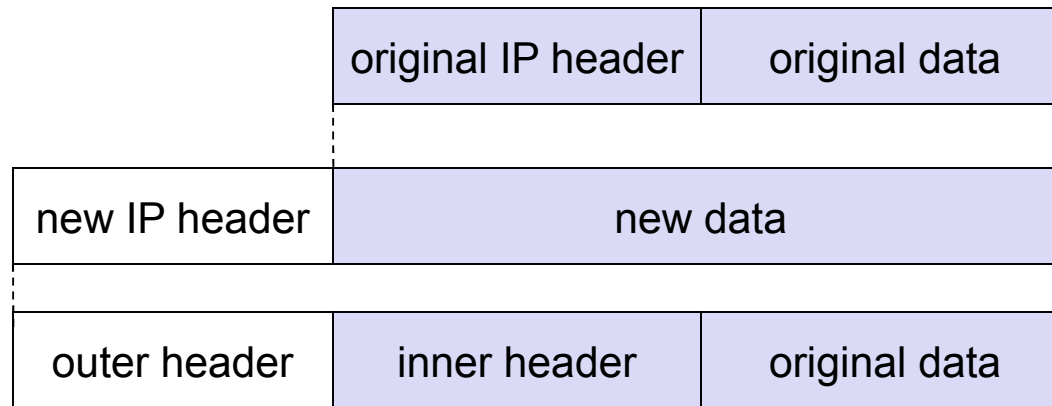
131 mobile node failed authentication

133 registration Identification mismatch

135 too many simultaneous mobility bindings

Type 3 → resposta do home agente

# 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     |  |
| <b>IP address of HA</b>    |     |                 |                 |  |
| <b>Care-of address COA</b> |     |                 |                 |  |
| ver.                       | IHL | DS (TOS)        | length          |  |
| IP identification          |     | flags           | fragment offset |  |
| TTL                        |     | lay. 4 prot.    | IP checksum     |  |
| <b>IP address of CN</b>    |     |                 |                 |  |
| <b>IP address of MN</b>    |     |                 |                 |  |
| TCP/UDP/ ... payload       |     |                 |                 |  |



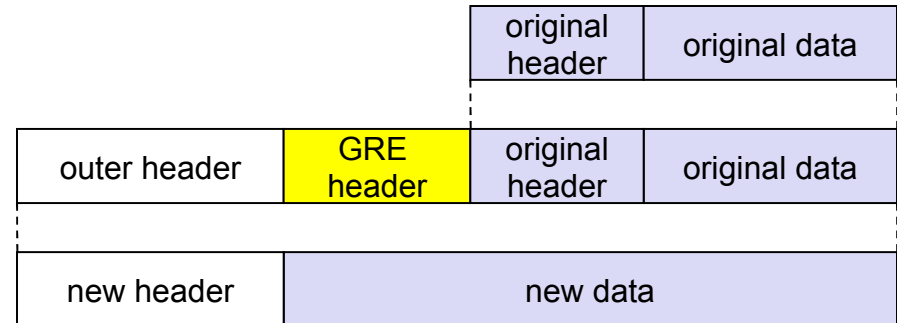
- Minimal encapsulation (optional)
  - avoids repetition of identical fields
  - e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
  - only applicable for non fragmented packets, no space left for fragment identification

|  |                    |          |                 |  |
|--|--------------------|----------|-----------------|--|
| ver.                                       | IHL                | DS (TOS) | length          |  |
| IP identification                          |                    | flags    | fragment offset |  |
| TTL  | <i>min. encap.</i> |          | IP checksum     |  |
| <b>IP address of HA</b>                    |                    |          |                 |  |
| <b>care-of address COA</b>                 |                    |          |                 |  |
| lay. 4 protoc.                             | S                  | reserved | IP checksum     |  |
| <b>IP address of MN</b>                    |                    |          |                 |  |
| <b>original sender IP address (if S=1)</b> |                    |          |                 |  |
| TCP/UDP/ ... payload                       |                    |          |                 |  |

# 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) |          |

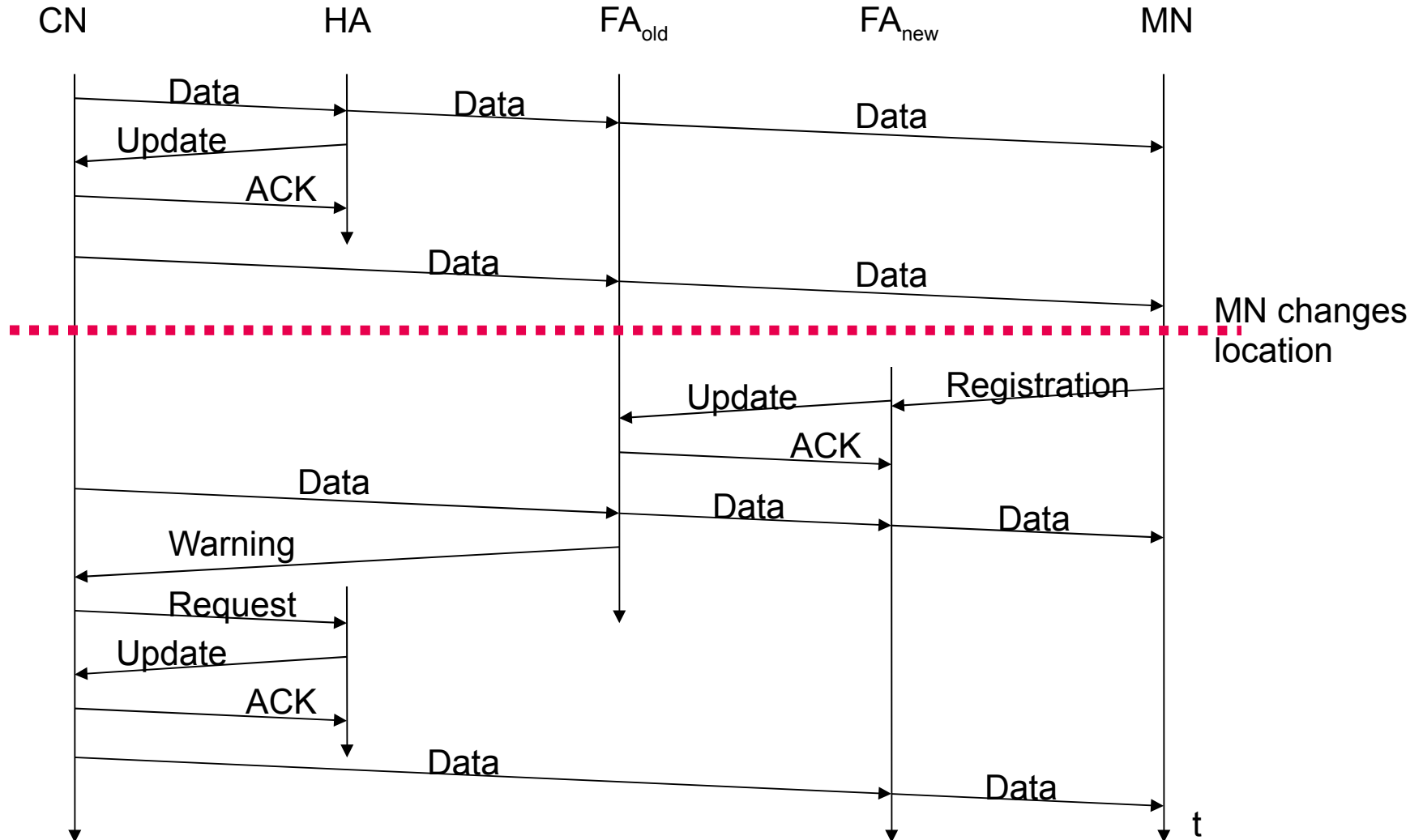
# Generic Routing Encapsulation

- C: is checksum available?
- R: offset and routing available and valid information?
- K: key field present for authentication?
- S: sequence number available? If so, strict sequence must be obeyed to restore packet order
- rec.: it determines the number of recursive encapsulations; default is 0 (only one level)
- rsv.: reserved; set to 0
- Protocol: Ethernet? Mobile IP?

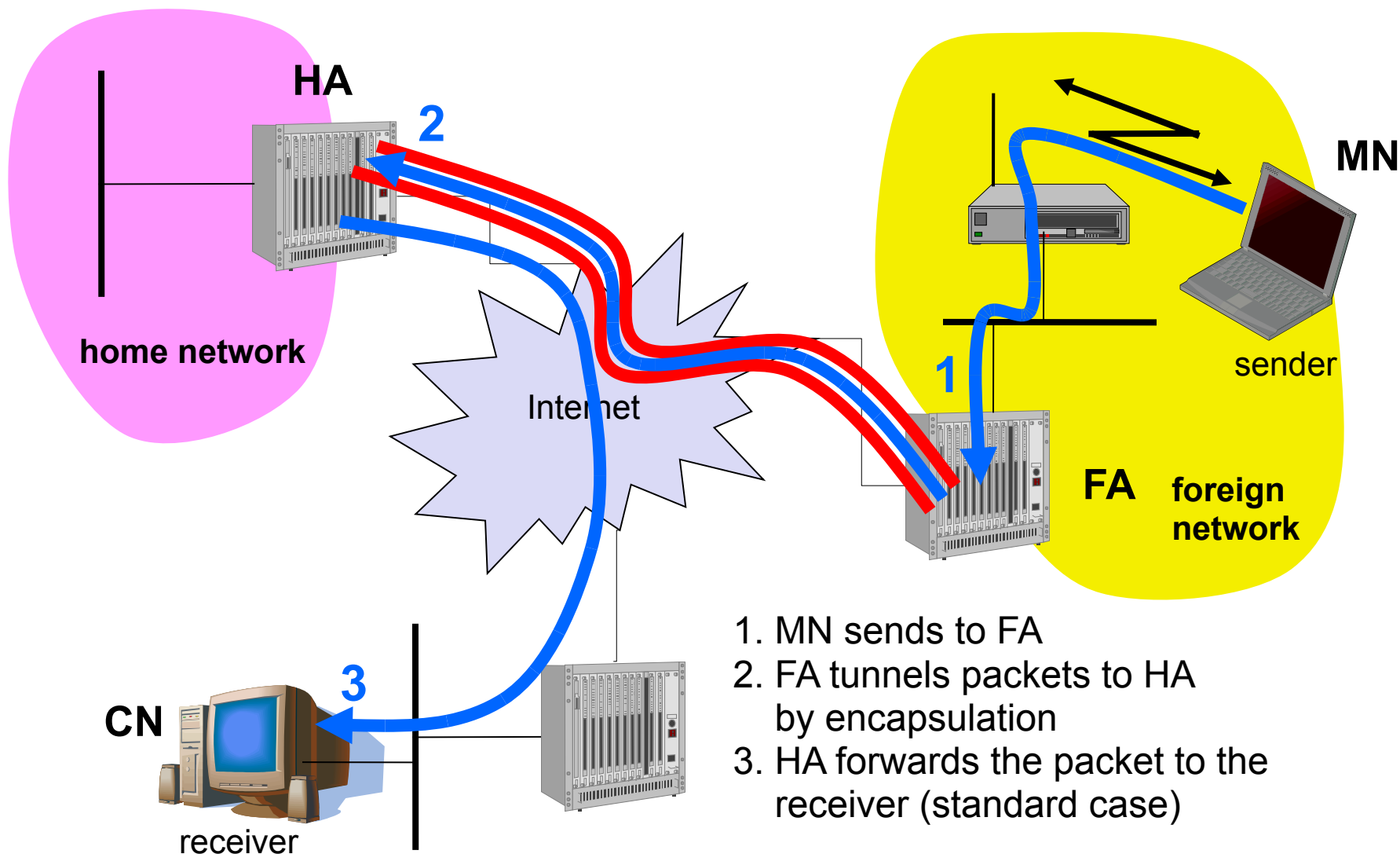
# Optimization of packet forwarding

- 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)



# 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 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 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

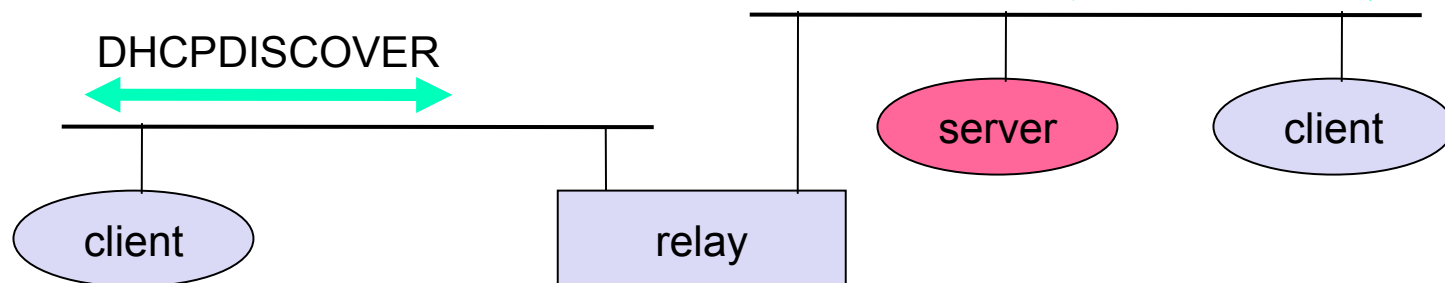
# Mobile IP and IPv6 (RFC 3775)

- 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

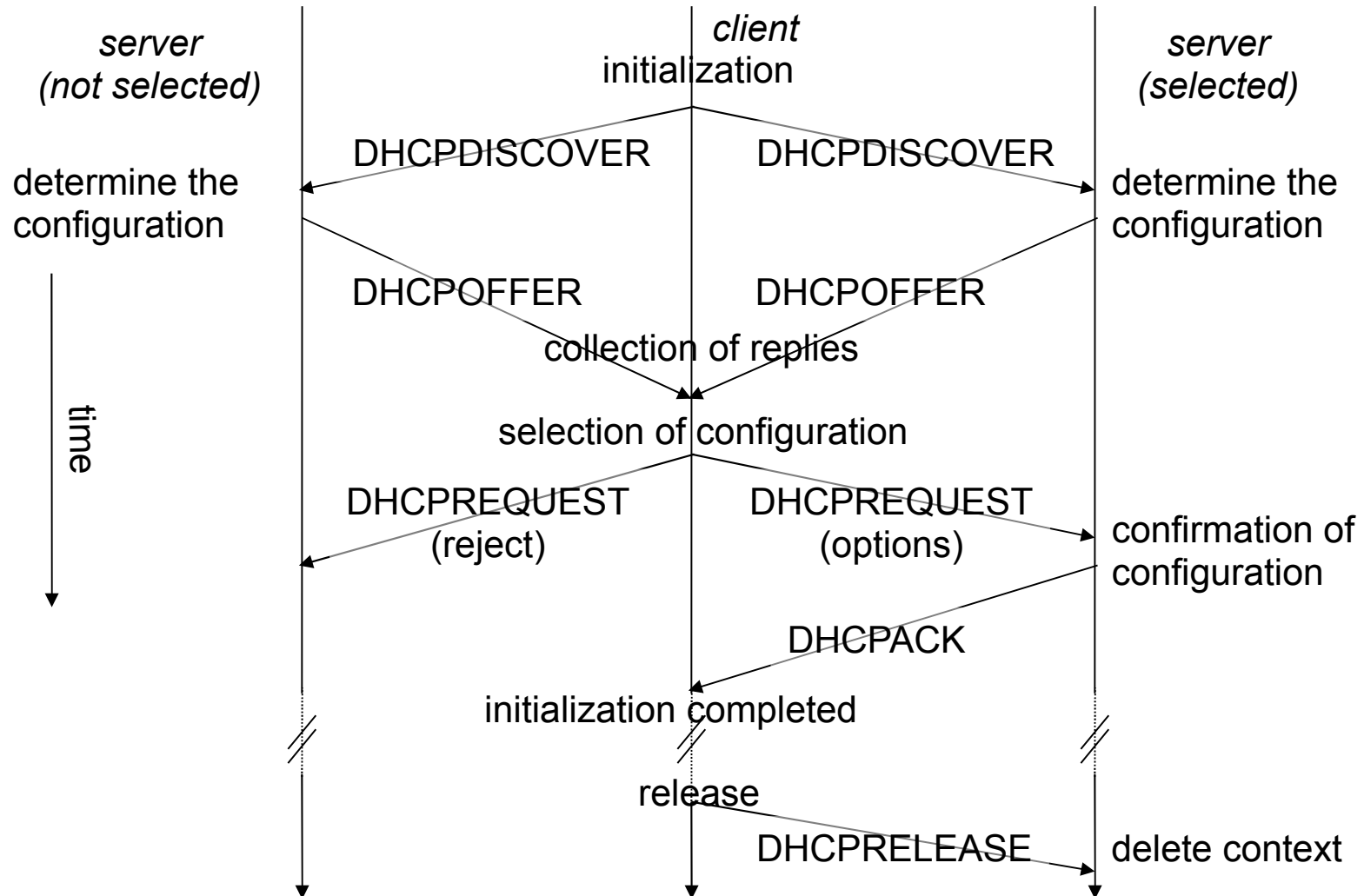


- Security
  - authentication with FA problematic, for the FA typically belongs to another organization
  - no protocol for key management and key distribution has been standardized in the Internet
- Firewalls
  - typically mobile IP cannot be used together with firewalls, special set-ups are needed (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

- 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)



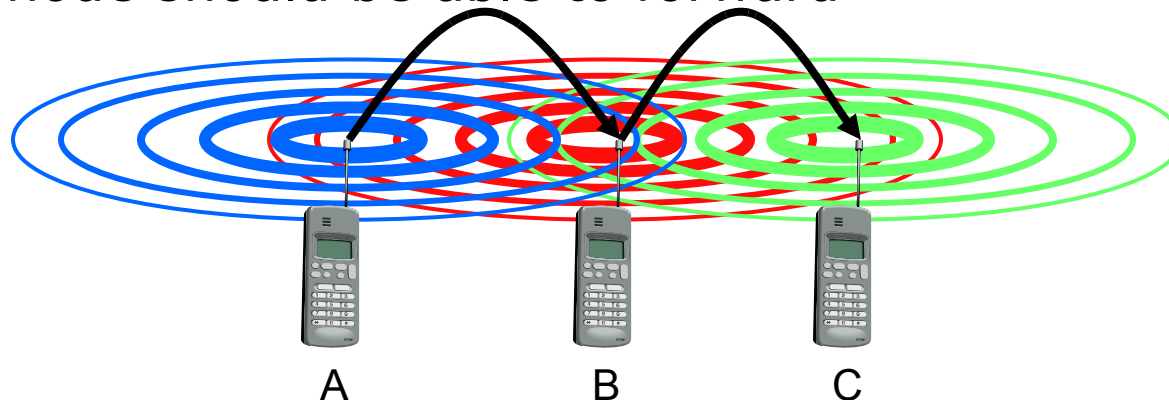
# DHCP - protocol mechanisms



- 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

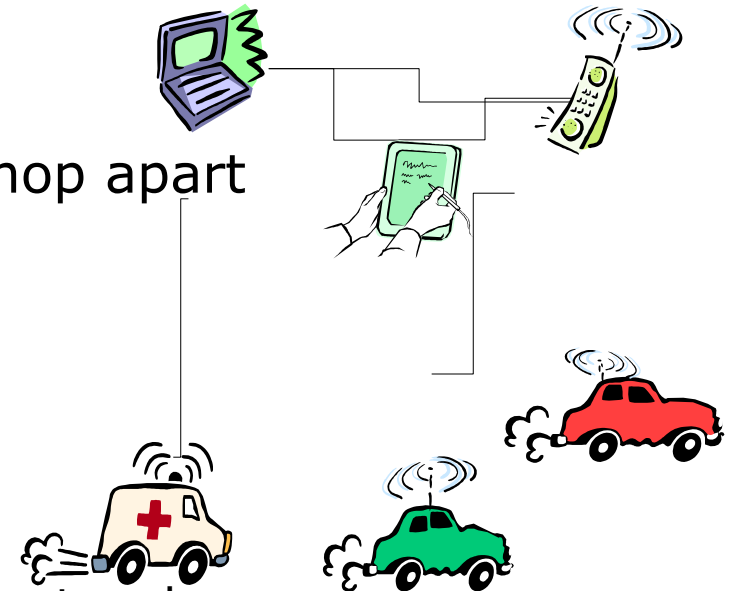


# Solution: Wireless ad-hoc networks

- Network without infrastructure
  - Use components of participants for networking

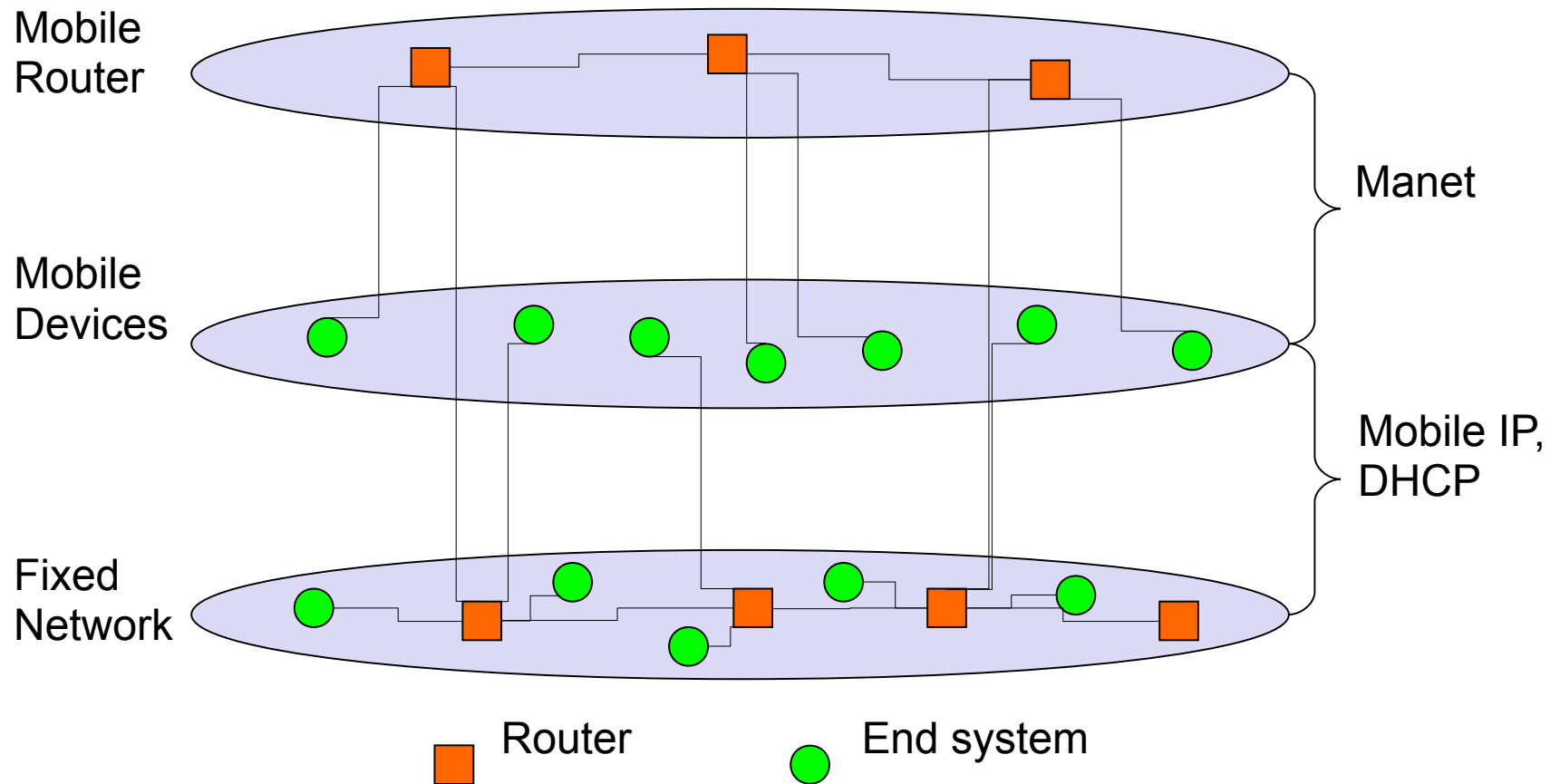
- Examples

- 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...



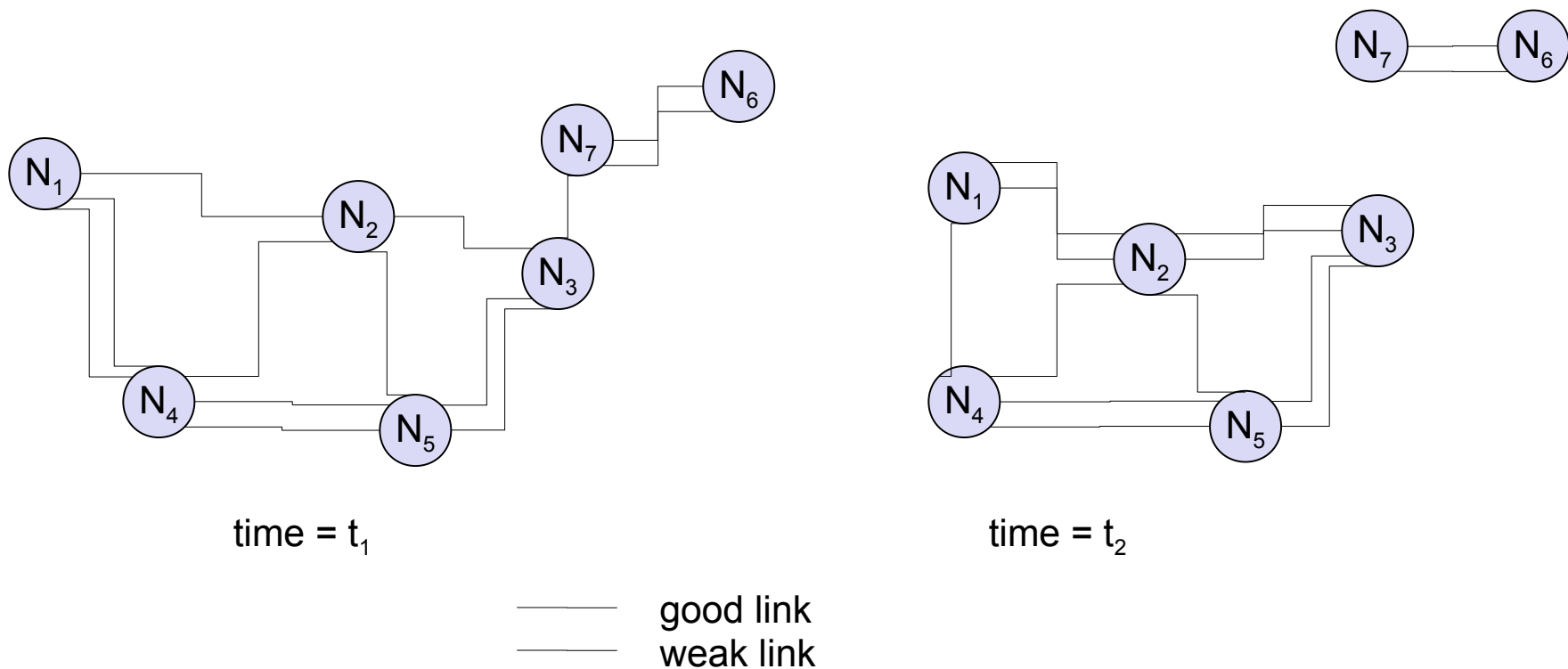
- Internet: MANET (Mobile Ad-hoc Networking) group

# Manet: Mobile Ad-hoc Networking



# Problem No. 1: Routing

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





# 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

# 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 ...

- 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

# DSDV (Destination Sequenced Distance Vector, historical)

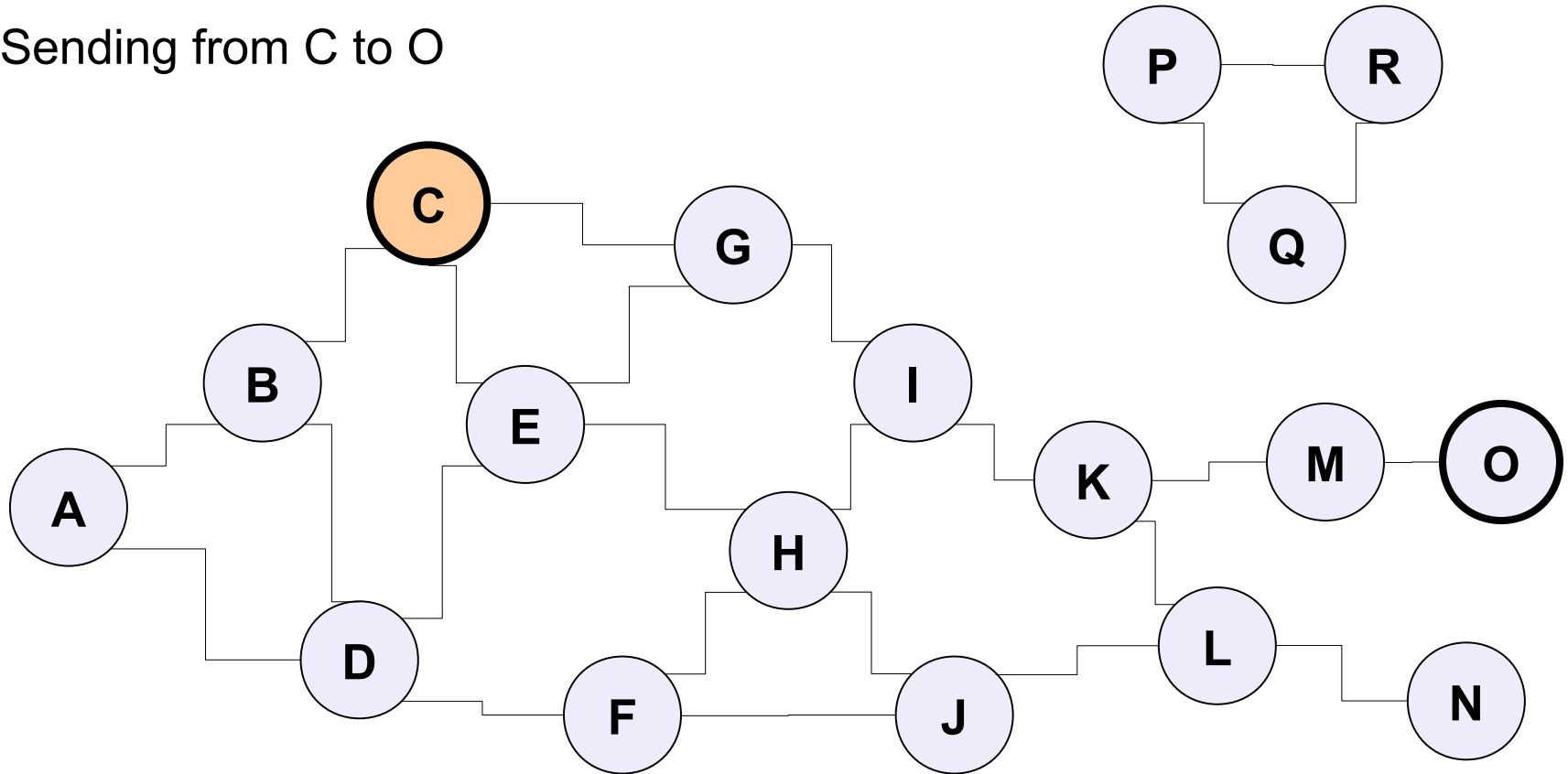
- Early work
  - on demand version: AODV
- Expansion of distance vector routing
- Sequence numbers for all routing updates
  - assures in-order execution of all updates
  - avoids loops and inconsistencies
- Decrease of update frequency
  - store time between first and best announcement of a path
  - inhibit update if it seems to be unstable (based on the stored time values)

- 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!

- 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)

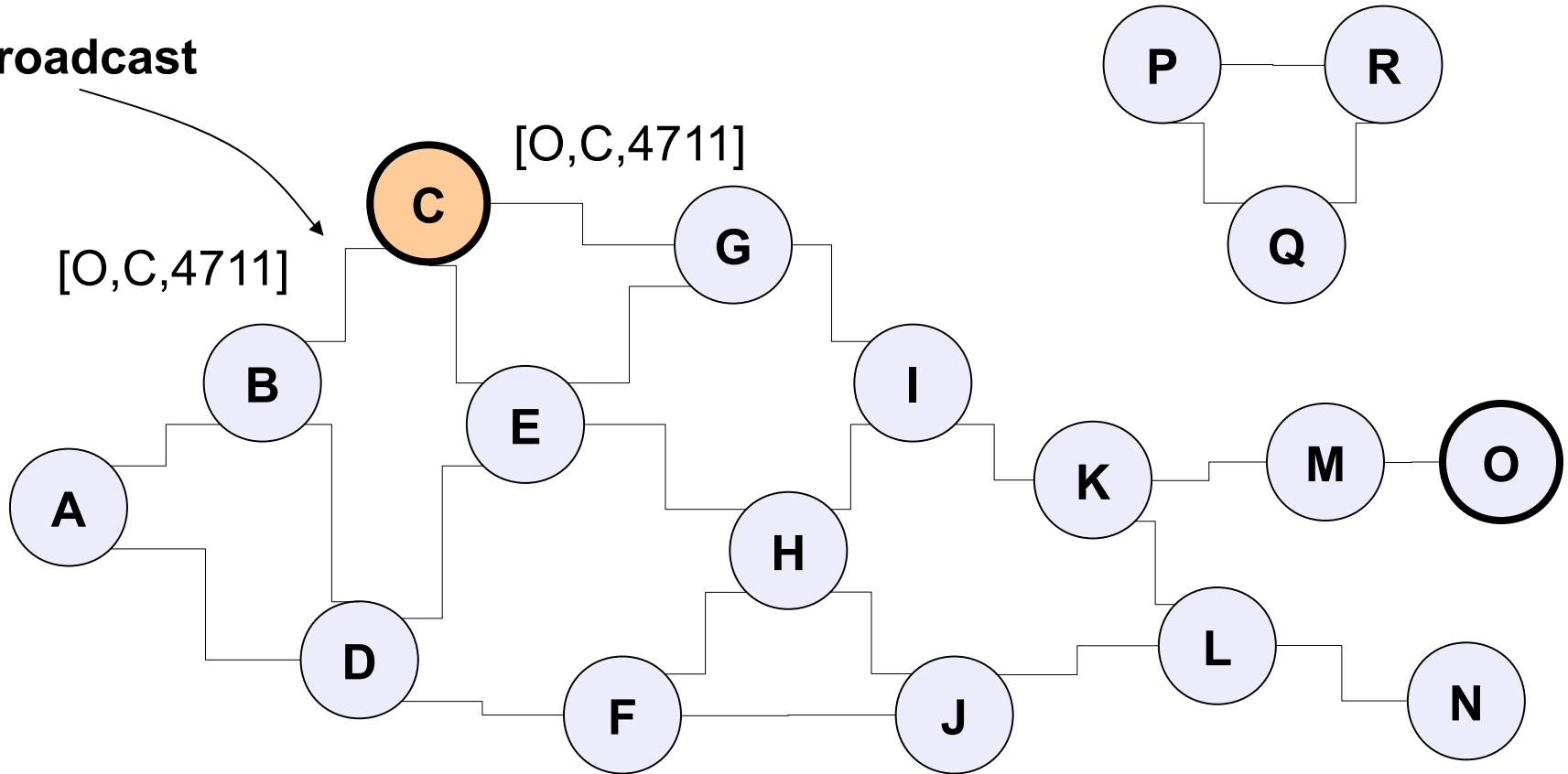
# DSR: Route Discovery

Sending from C to O



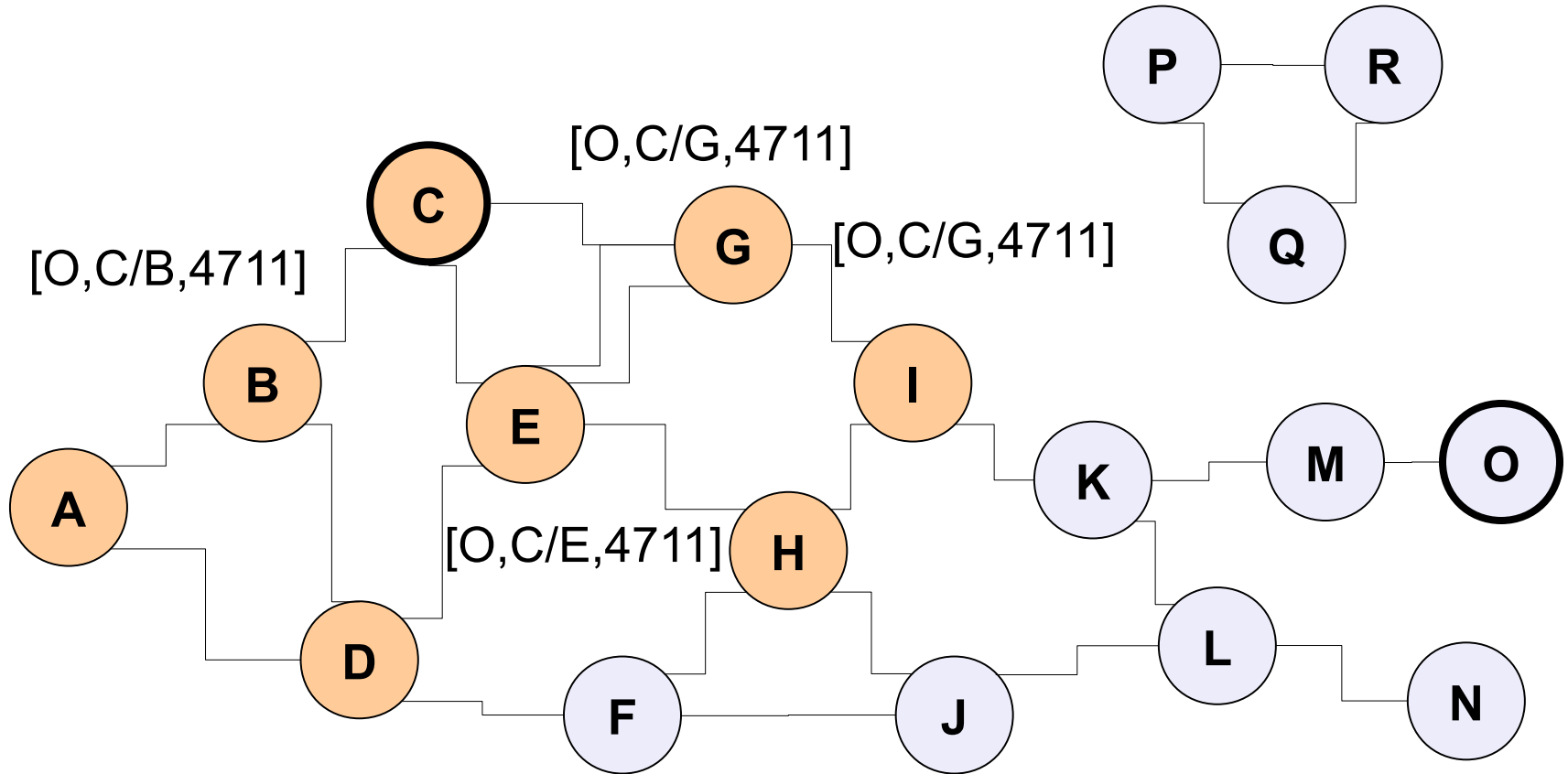
# DSR: Route Discovery

Broadcast

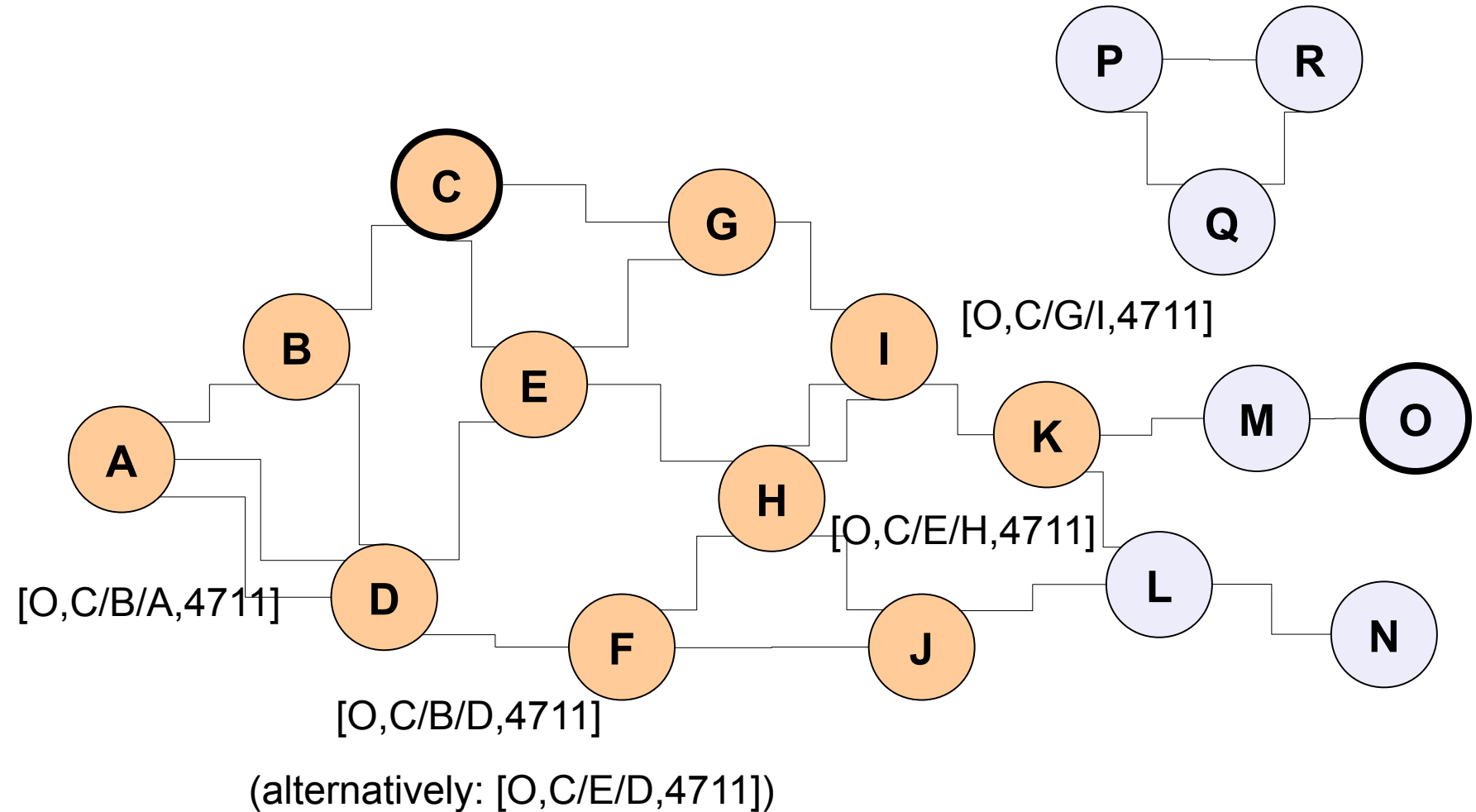




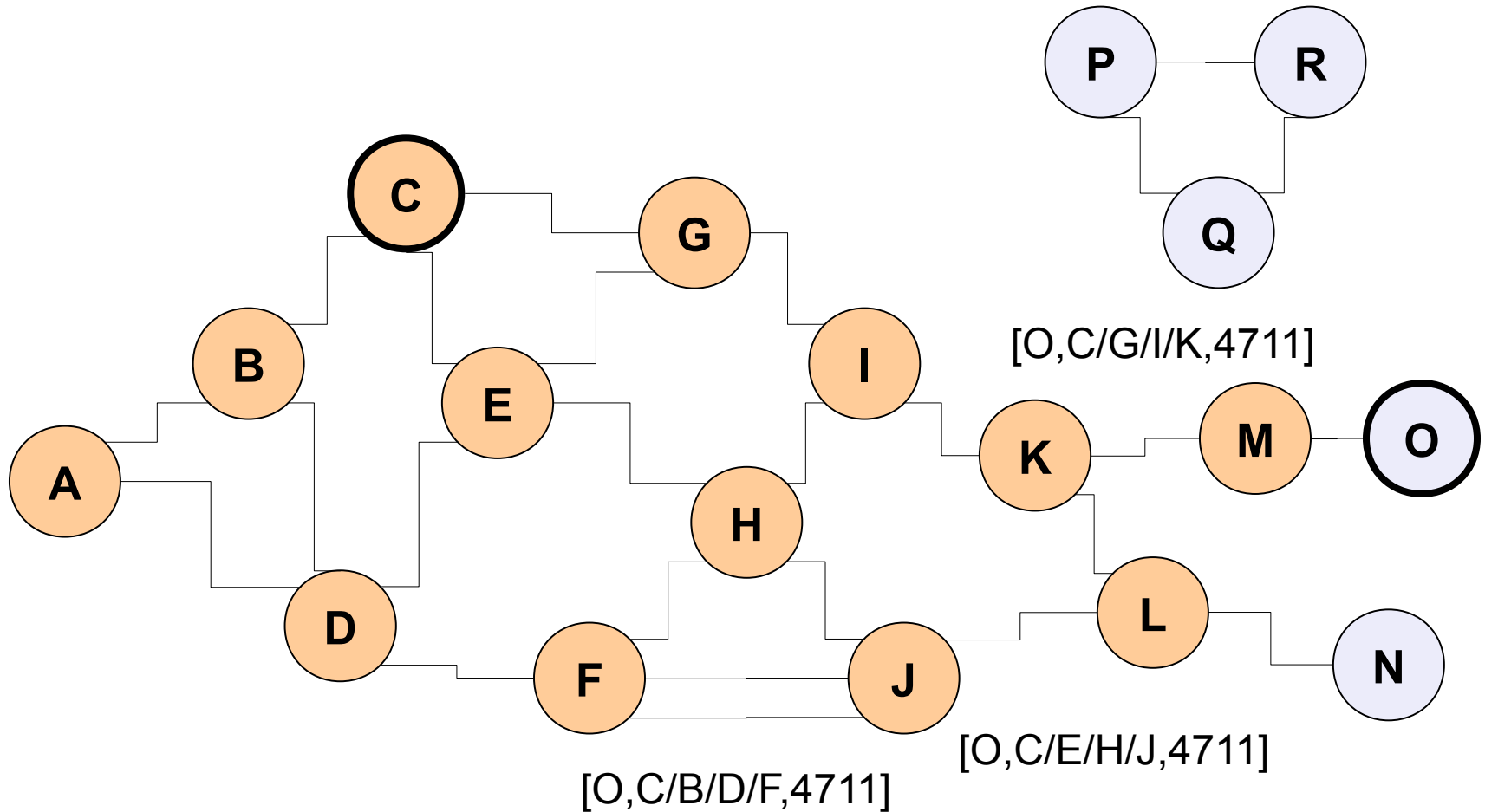
# DSR: Route Discovery



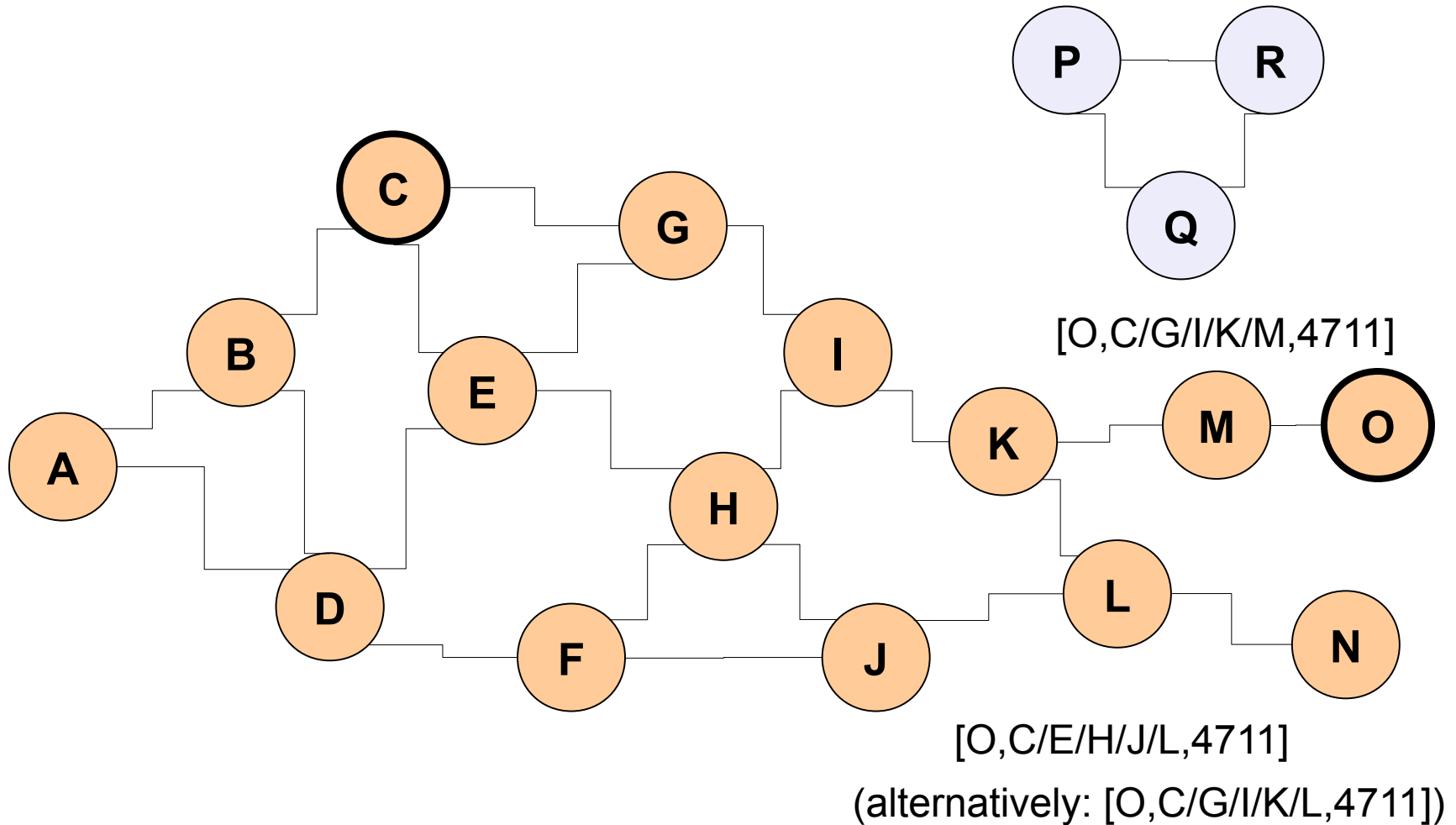
# DSR: Route Discovery



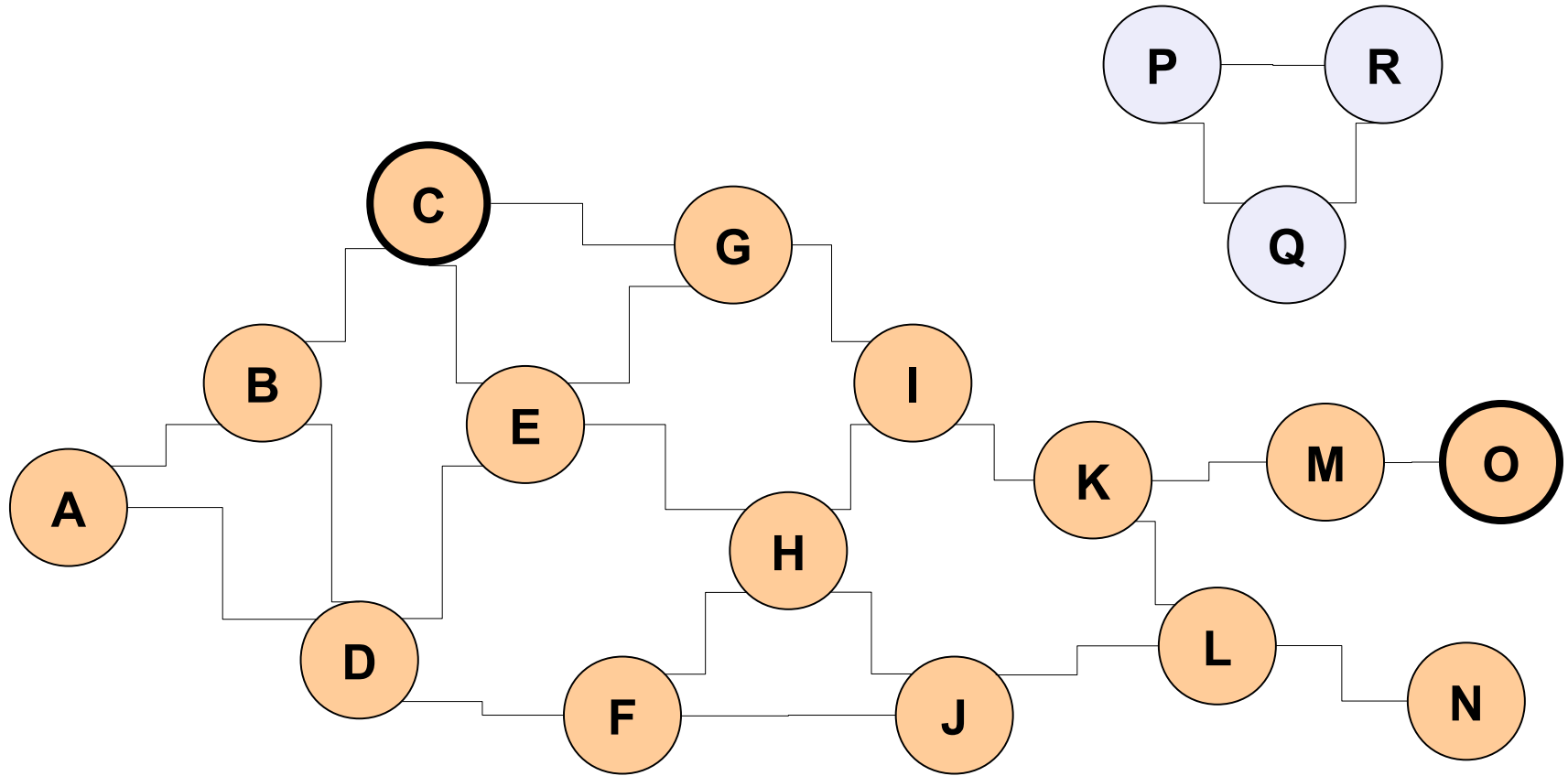
# DSR: Route Discovery



# DSR: Route Discovery

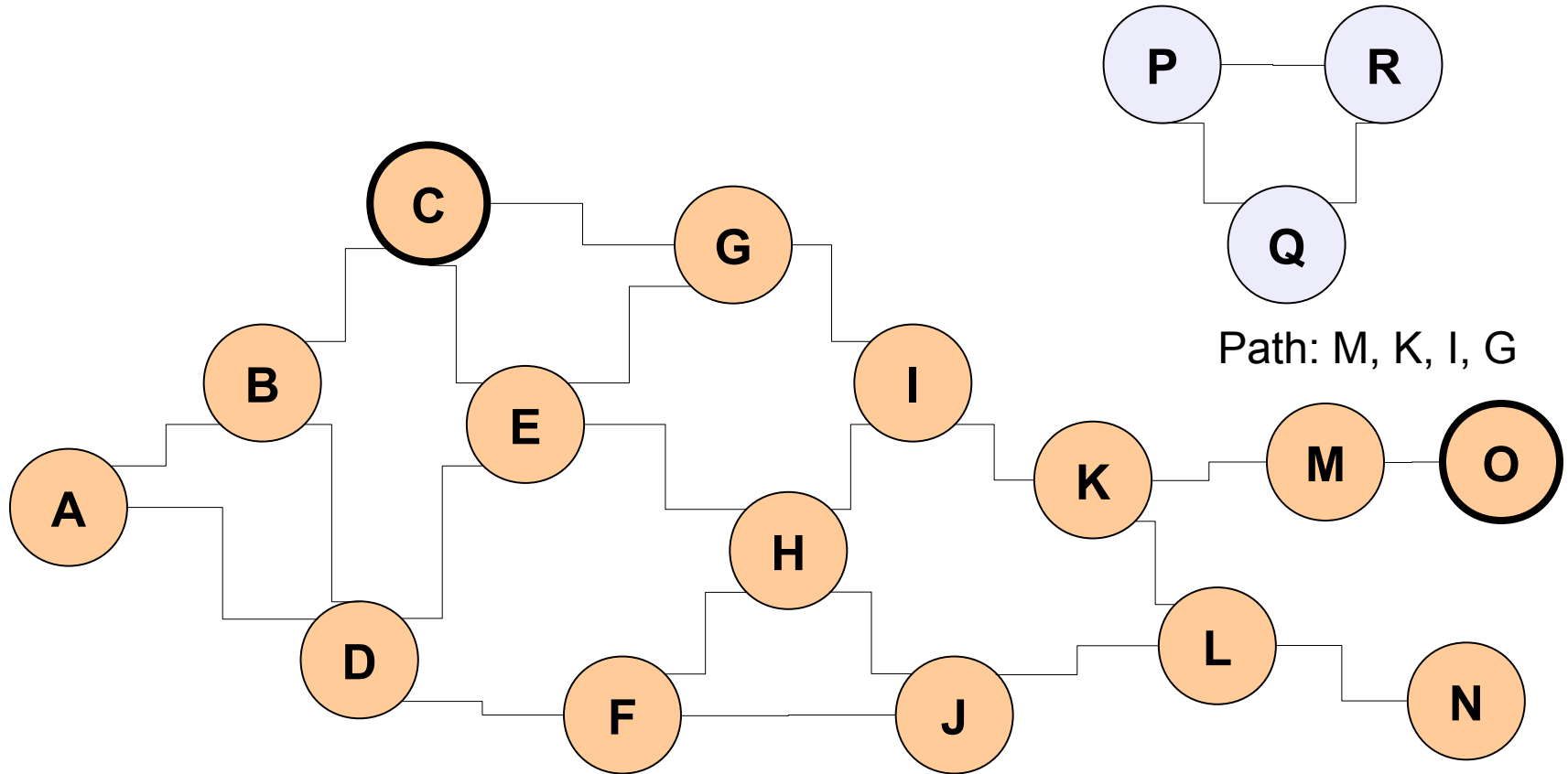


# DSR: Route Discovery



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

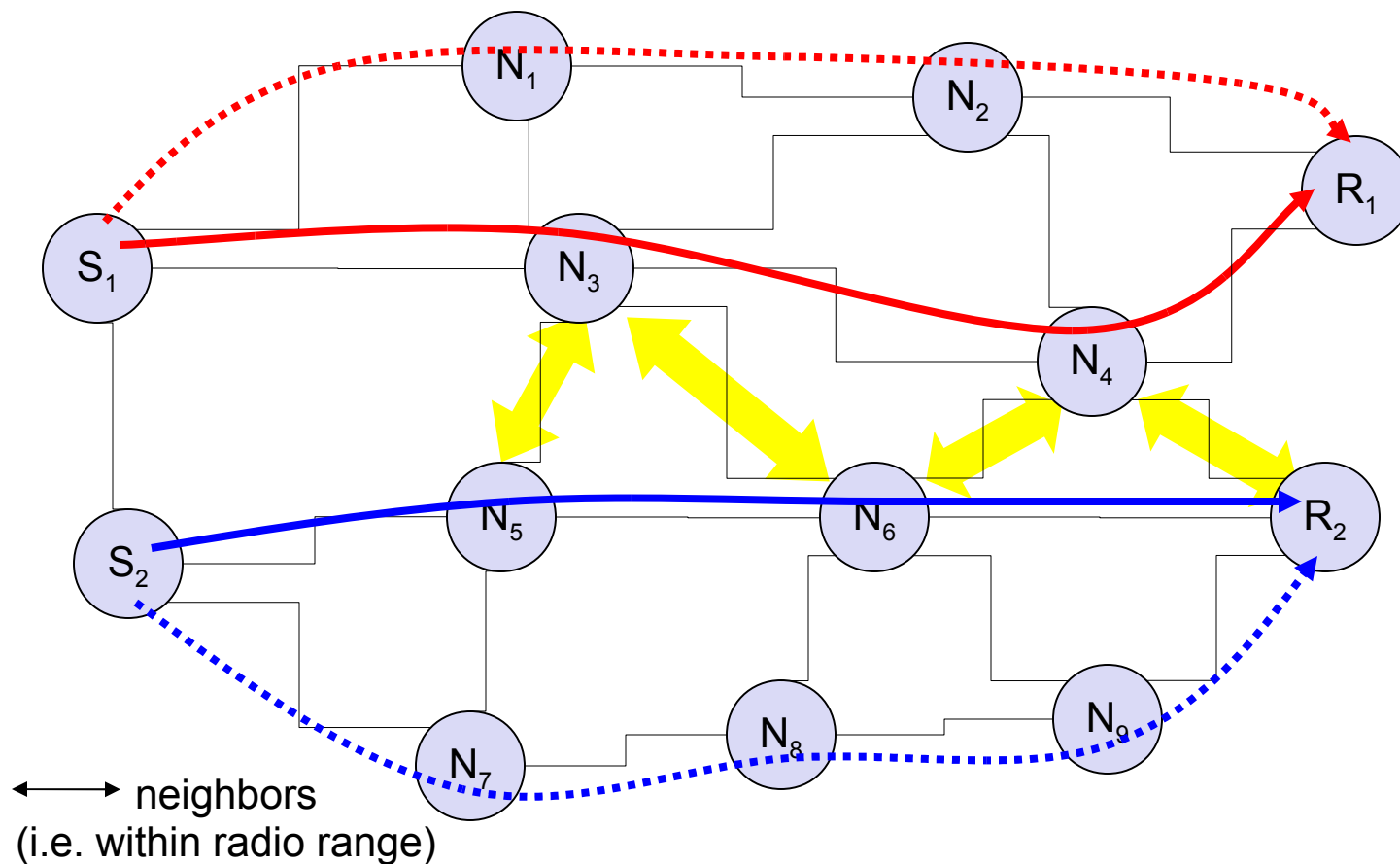
# DSR: Route Discovery



- 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





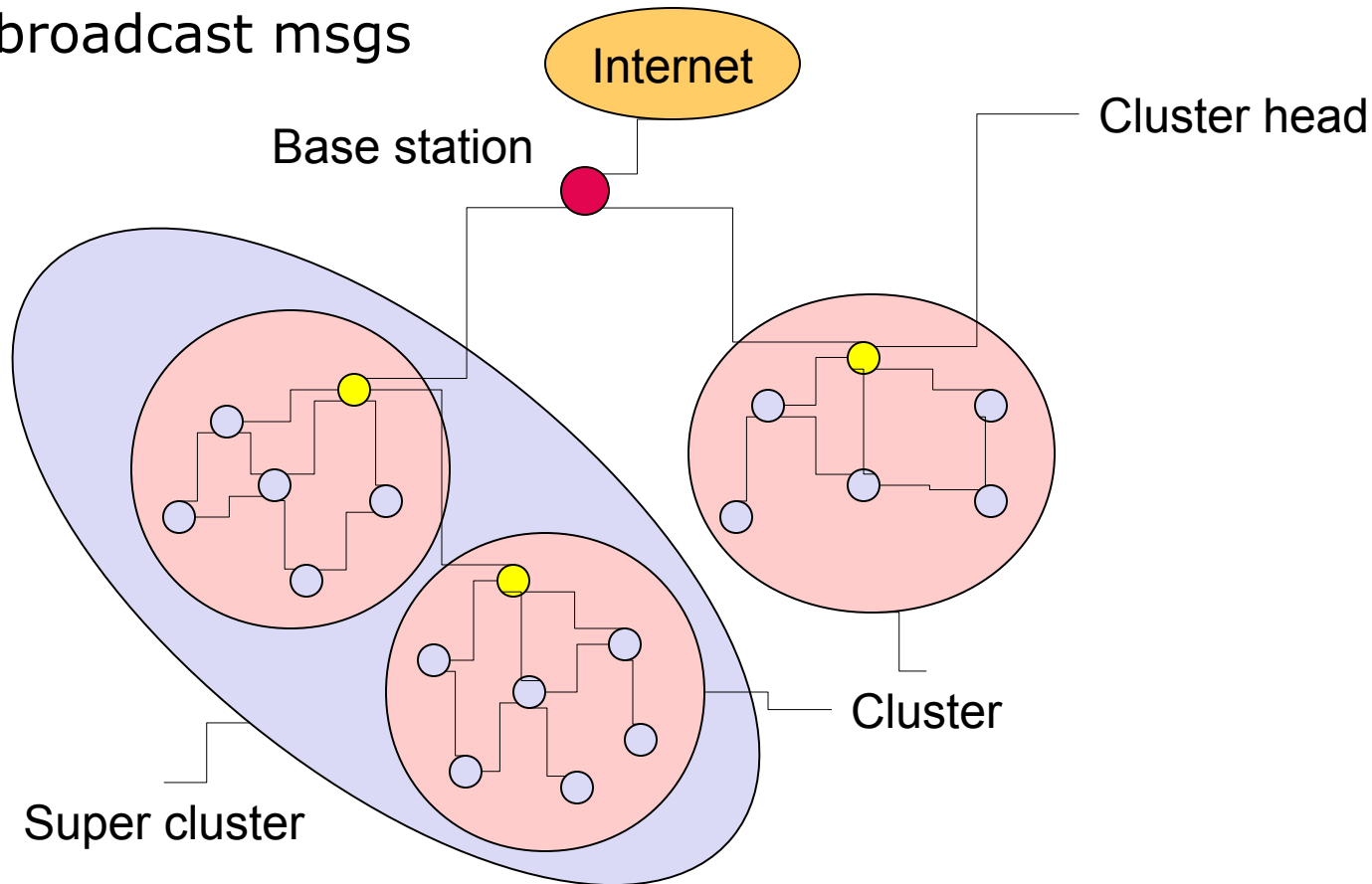
- Least Interference Routing (LIR)
  - calculate the cost of a path based on the number of stations that can receive a transmission
- Max-Min Residual Capacity Routing (MMRCR)
  - calculate the cost of a path based on a probability function of successful transmissions and interference
- Least Resistance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

# 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 (advantages?)

- Locality property
- Less broadcast msgs



# Finalizando...

- Fim do capítulo Mobile network layer
- Leiam o capítulo 8
- Próxima aula trataremos sobre a camada de transporte em ambientes móveis