Mobility Support
(Network Layer)

Problem Exposition

Routing in the Internet works

- ❑ based on IP destination address (e.g. 129.13.42.99) ---> network prefix (in this case 129.13.42) determines physical subnet (home net of receiver)
- ➔ change of physical subnet implies change of IP address
- ➔ It always needs a *topological correct address*

Changing the IP-address?

- ❑ adjust the host IP address depending on the current location (e.g. using DHCP)
- ➔ almost impossible to find a mobile system
- ➔ only useful to act as client of services (e.g. accessing WWW)
- ➔ no complete integration

- ❑ use dynamic DNS to update actual IP address
- ➔ DNS updates take to long time (up to one day)
- ➔ TCP connections break, security problems etc

Requirements to Mobile IP

Transparency
- to protocols of higher layers (e.g. TCP) and applications (in principle)
- ➔ mobile end-systems keep their IP address

Compatibility
- to protocols of higher layers (e.g. TCP) and applications (e.g. WWW browser)
- changes to routers should be not required
- support of the same layer 2 protocols as IP
- access to other existing Internet servers should be not affected

Security
- authentication of all messages used to manage mobility (e.g. registration)

Efficiency and scalability
- only few additional messages necessary to manage mobility (connection typically via a low bandwidth radio link)

Roles and Definitions

Mobile Node (MN)

- node that can change the point of connection to the network without changing its IP address

Correspondent Node (CN)

- communication partner

Home Agent (HA)

- system in the home network of the MN, typically the subnet router
- registers the location of the MN, tunnels IP datagrams to the COA representing the end-point of the tunnel

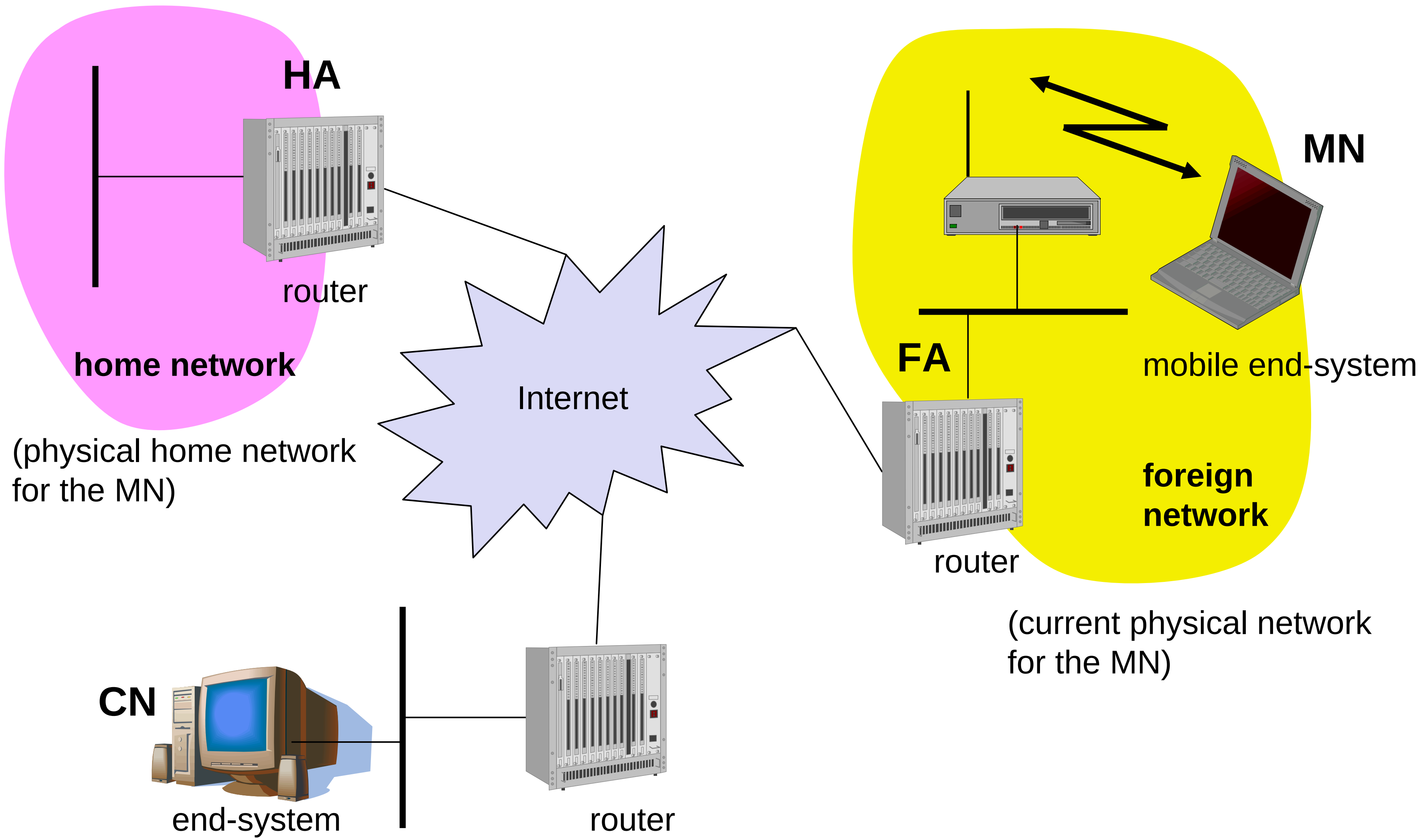
Foreign Agent (FA)

- 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 for messages sent by the MN while being in the foreign network

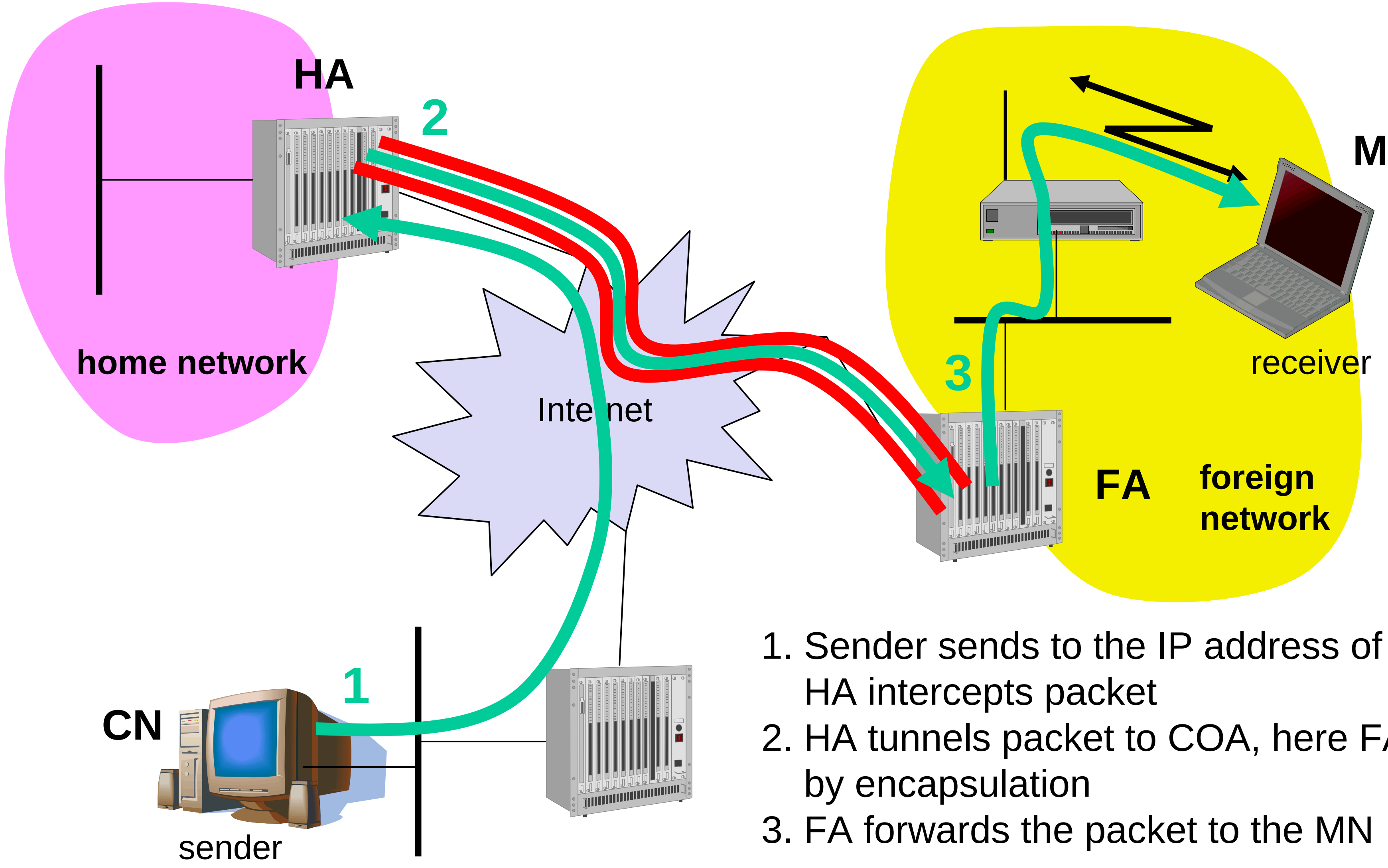
Care-of Address (COA)

- address of the current tunnel end-point for the MN (at FA or MN)
- actual location of the MN from an IP point of view

Example scenario for Mobile IP

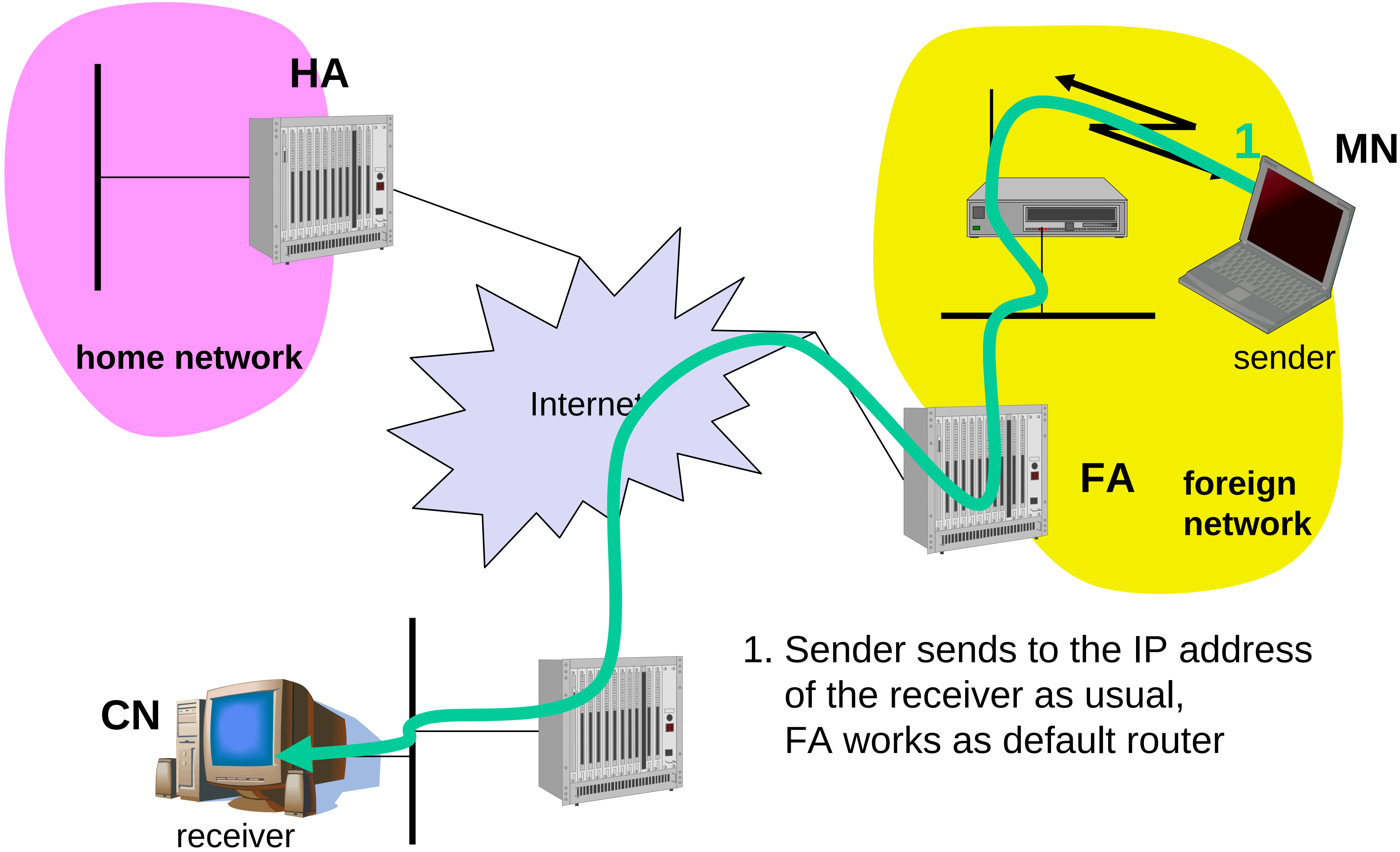


Data transfer to the MN



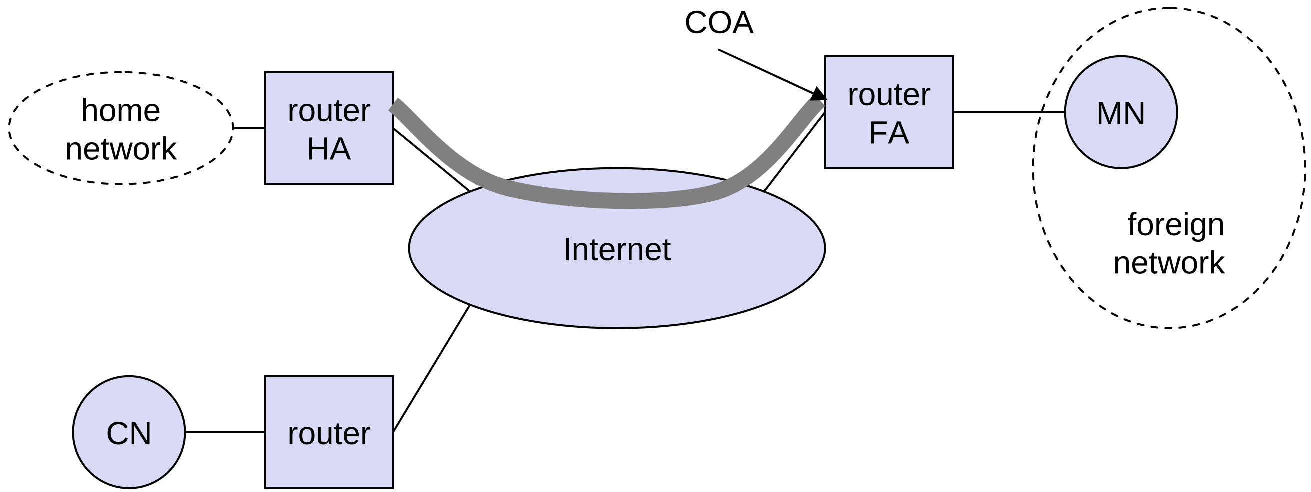
1. Sender sends to the IP address of MN, HA intercepts packet
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the MN

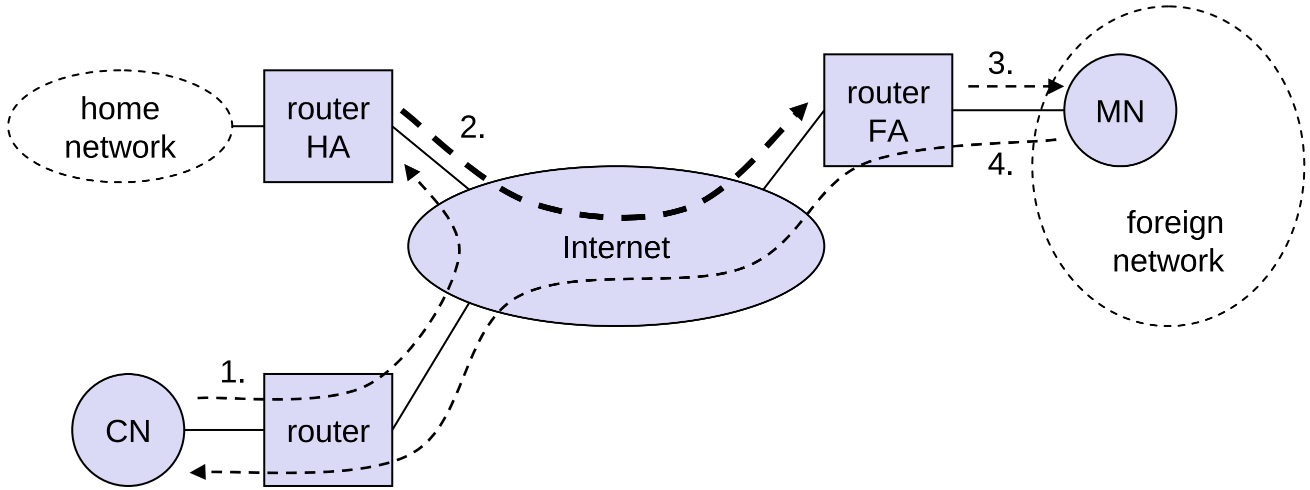


1. Sender sends to the IP address of the receiver as usual, FA works as default router

Overview



COA
home
network
router
HA
router
FA
MN
Internet
foreign
network
CN
router



home
network
router
HA
2.
router
FA
3.
MN
4.
Internet
foreign
network
1.
CN
router

Network integration

Agent Advertisement

- HA and FA periodically send advertisement messages into their physical subnets (Agent Advertisement Messages)
- MN listens to these messages and detects, if it is in a foreign network
- MN reads a COA from the FA advertisement messages

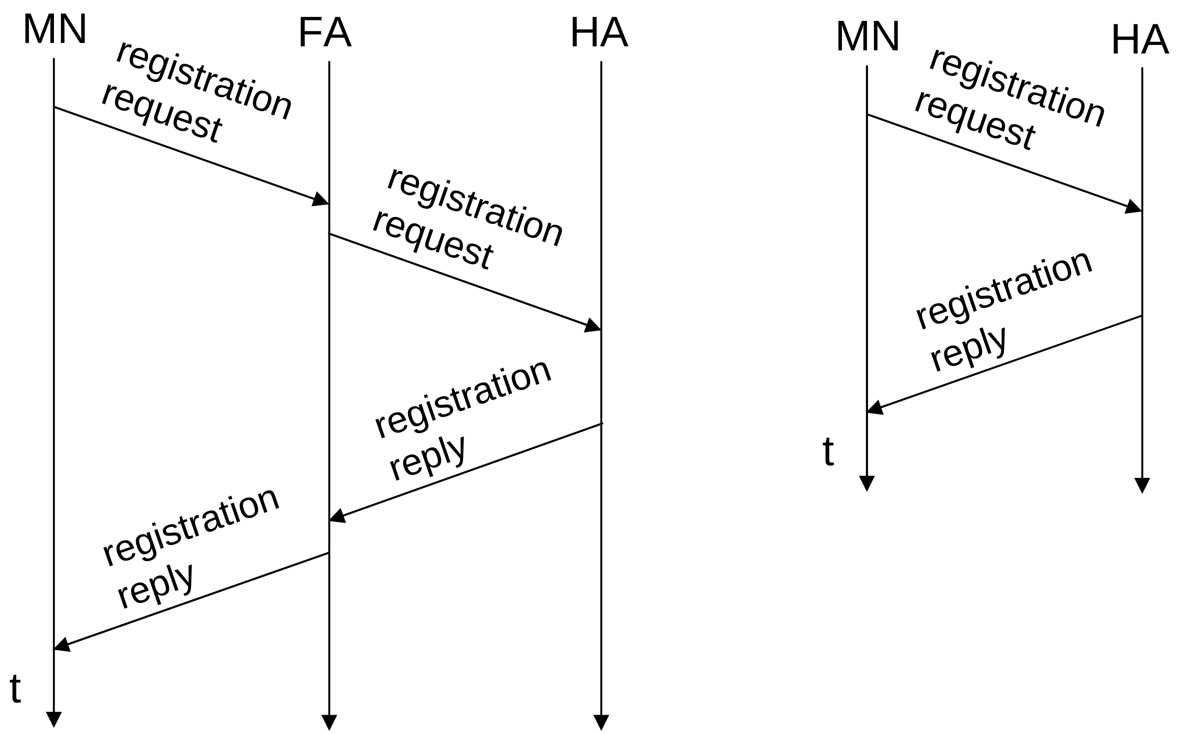
Agent Solicitation

- MN periodically sends solicitation messages to find potential FA's
- MN gets a COA from the responding FA

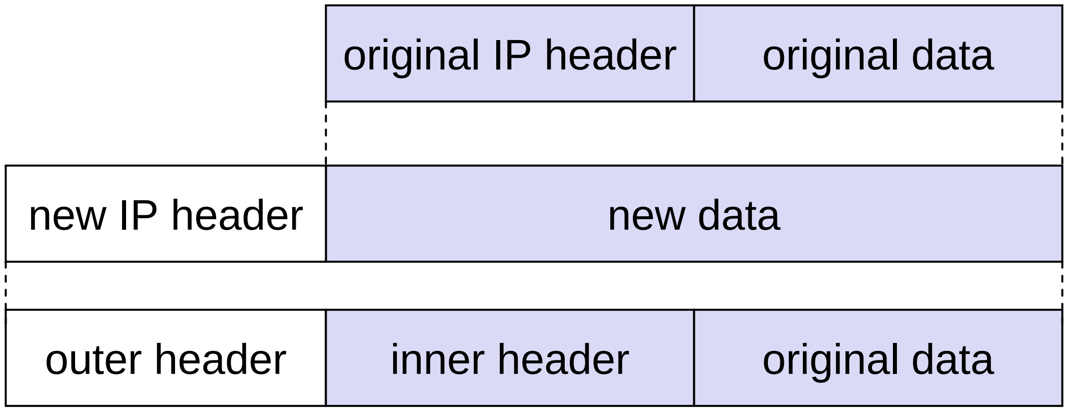
Registration (always limited lifetime!)

- MN signals COA to the HA via the FA, HA acknowledges via FA to MN
- these actions have to be secured by authentication

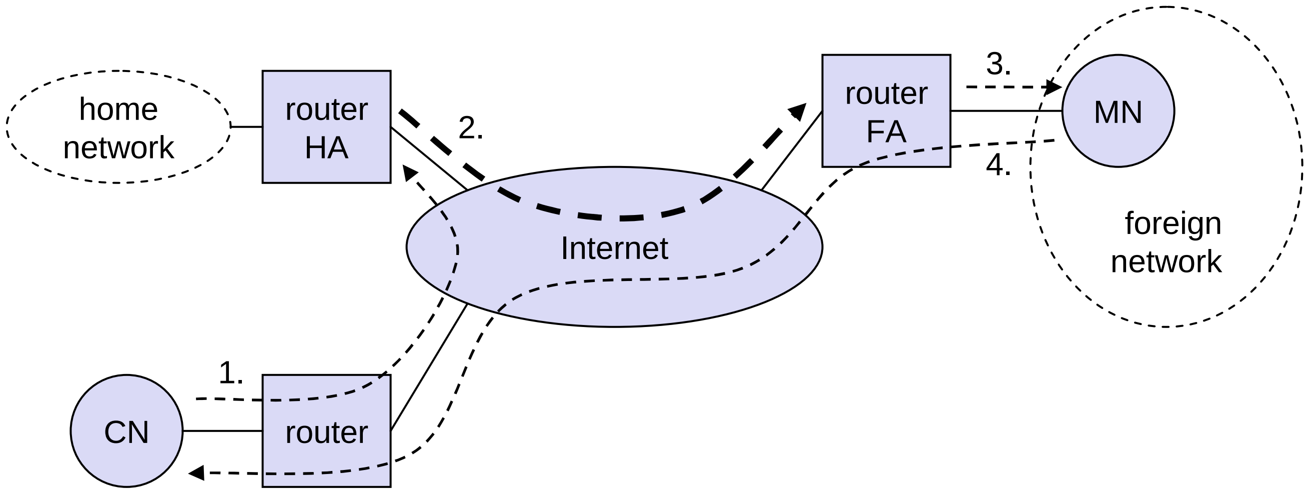
Registration



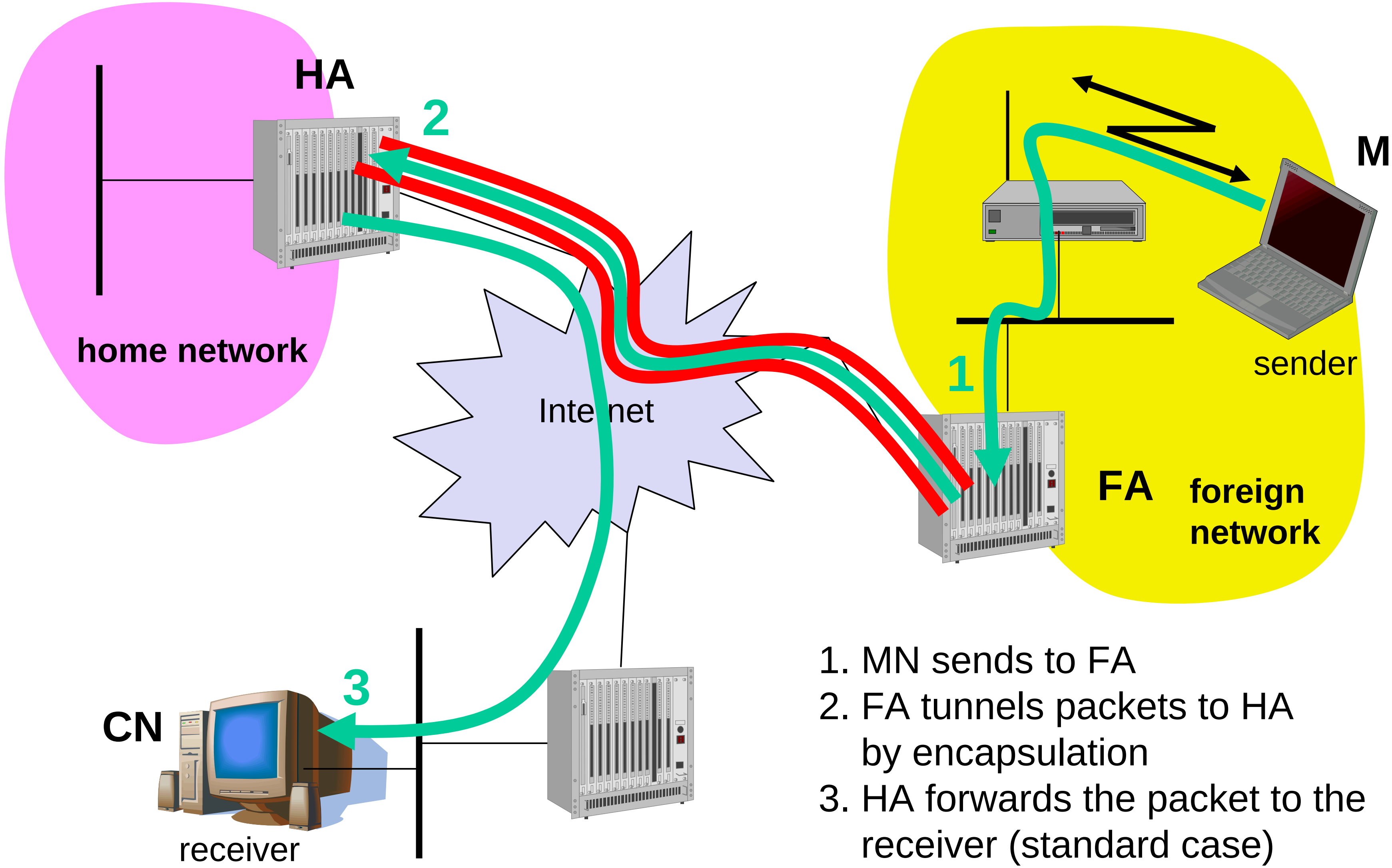
Encapsulation



Overview


home
network
router
HA
2.
router
FA
3.
MN
4.
Internet
foreign
network
1.
CN
router

Mobile IP with reverse tunneling



1. MN sends to FA
2. FA tunnels packets to HA by encapsulation
3. HA forwards the packet to the receiver (standard case)

Security Problems with mobile IP

- authentication with FA during registration is problematic, for the FA typically belongs to another organization
- no protocol for key management and key distribution has been standardized in the Internet
- typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling) but .....

Security is a hot topic of current research and development!

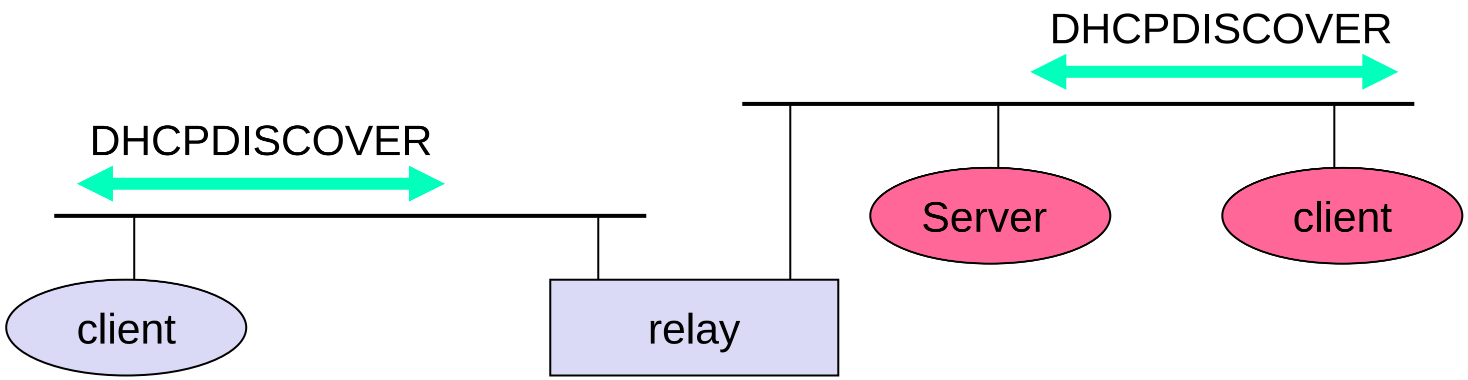
DHCP: Dynamic Host Configuration Protocol

Application

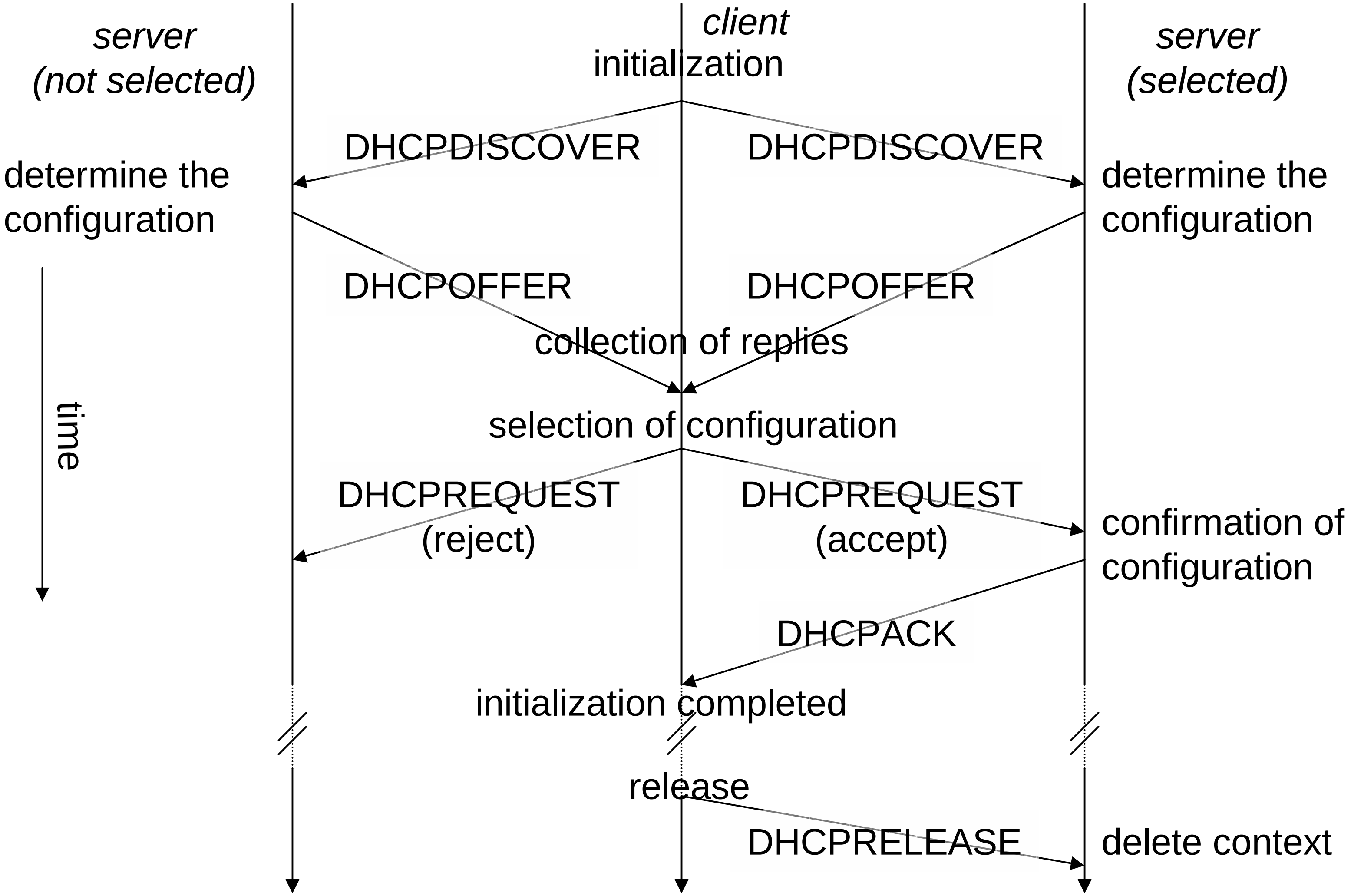
- simplification of installation and maintenance of networked computers
- supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
- enables automatic integration of systems into an Intranet or the Internet, can be used to 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

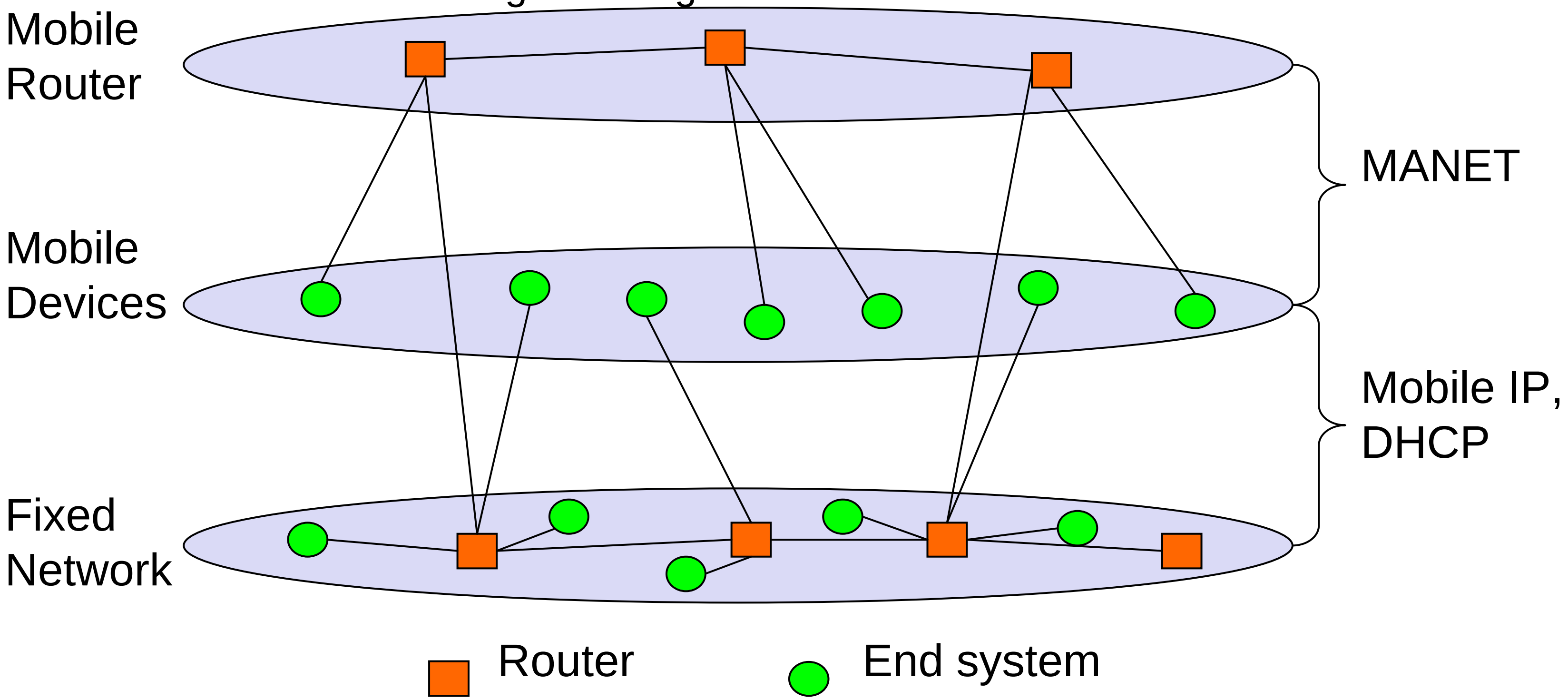


Standard Mobile IP needs an infrastructure

- Home Agent/Foreign Agent, tunnels in the fixed network

Sometimes there is no infrastructure!

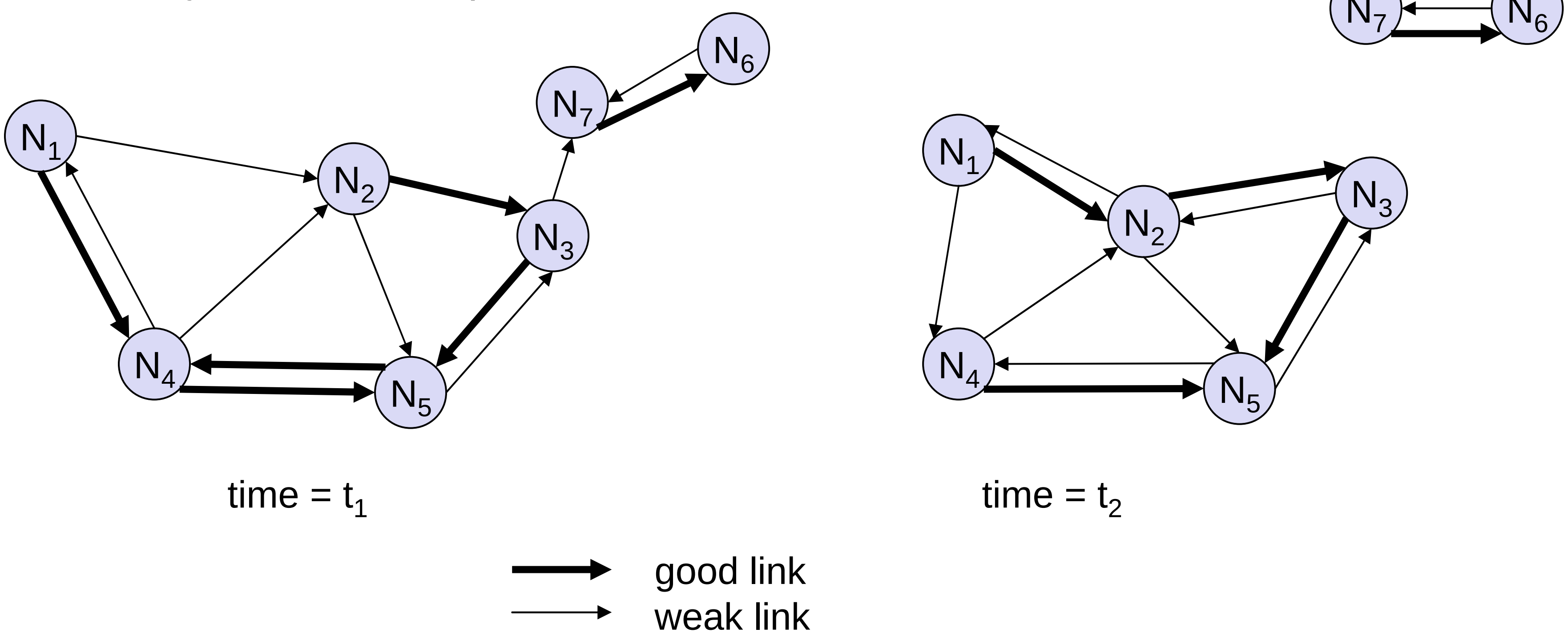
- remote areas, ad-hoc meetings, disaster areas, military operations
- cost can also be an argument against an infrastructure!



Central Problem : Routing

Highly dynamic network topology

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



Fundamental differences to wired networks

- Links can be asymmetric, i.e., they can have a direction dependent transmission quality
- Links can be very redundant ---> making efficient routing complex
- Unplanned connections: Interferences
- Most important: Highly dynamic network topology

----------->:

- Classical routing in wired networks does not work
- Information from lower layers (e.g. signal strength,interference) needed
- Centralized methods do not work
- Connection-oriented approaches like TCP to increase reliability do not work
- Flooding may always be a last option
- Hierarchical clustering may help

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
  - Battery run-time, time of connectivity …

DSDV (Destination Sequenced Distance Vector)

(Original) Distance Vector Routing in wired networks:

- 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

DSDV adds:

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)

DSR (Dynamic Source Routing) I

Problem: What, if packets are sent only from time to time?

---> constantly updating routing information is overkill!

Idea: 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!

DSR (Dynamic Source Routing) II

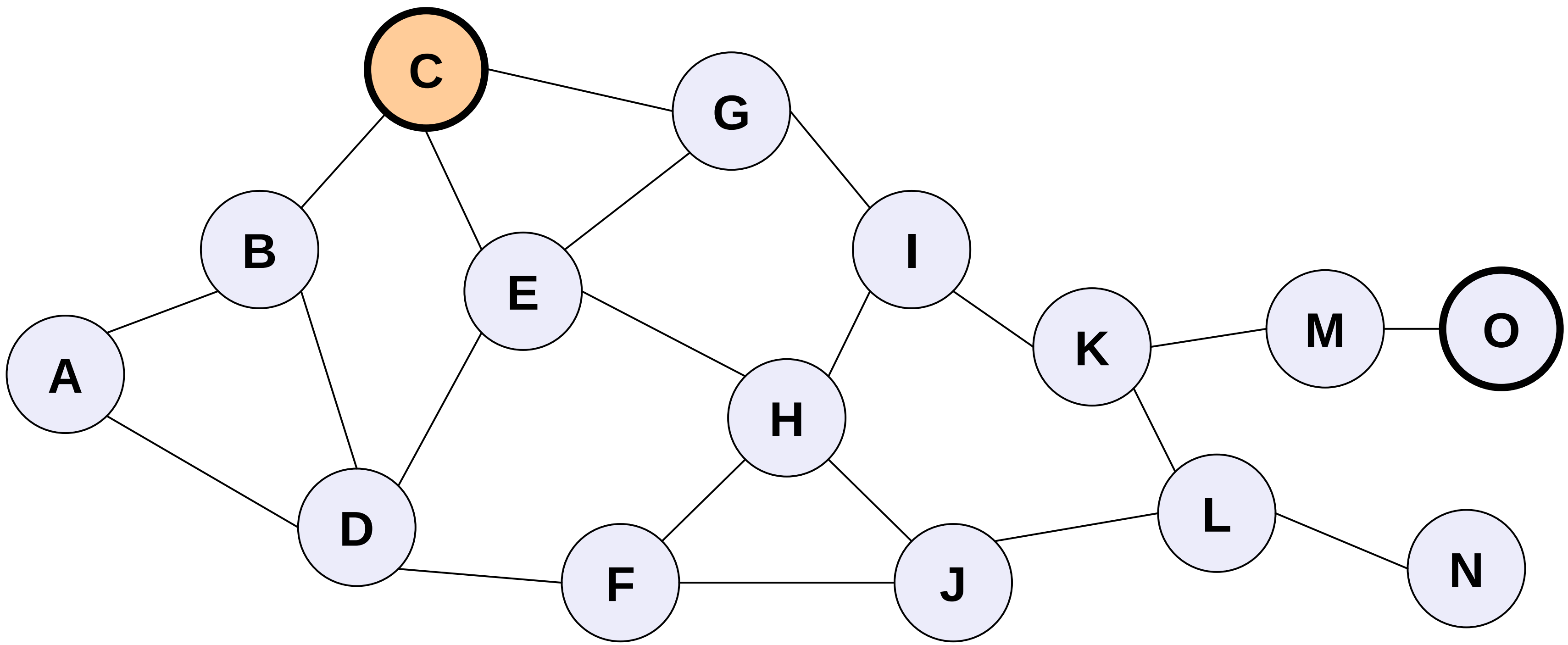
Path discovery

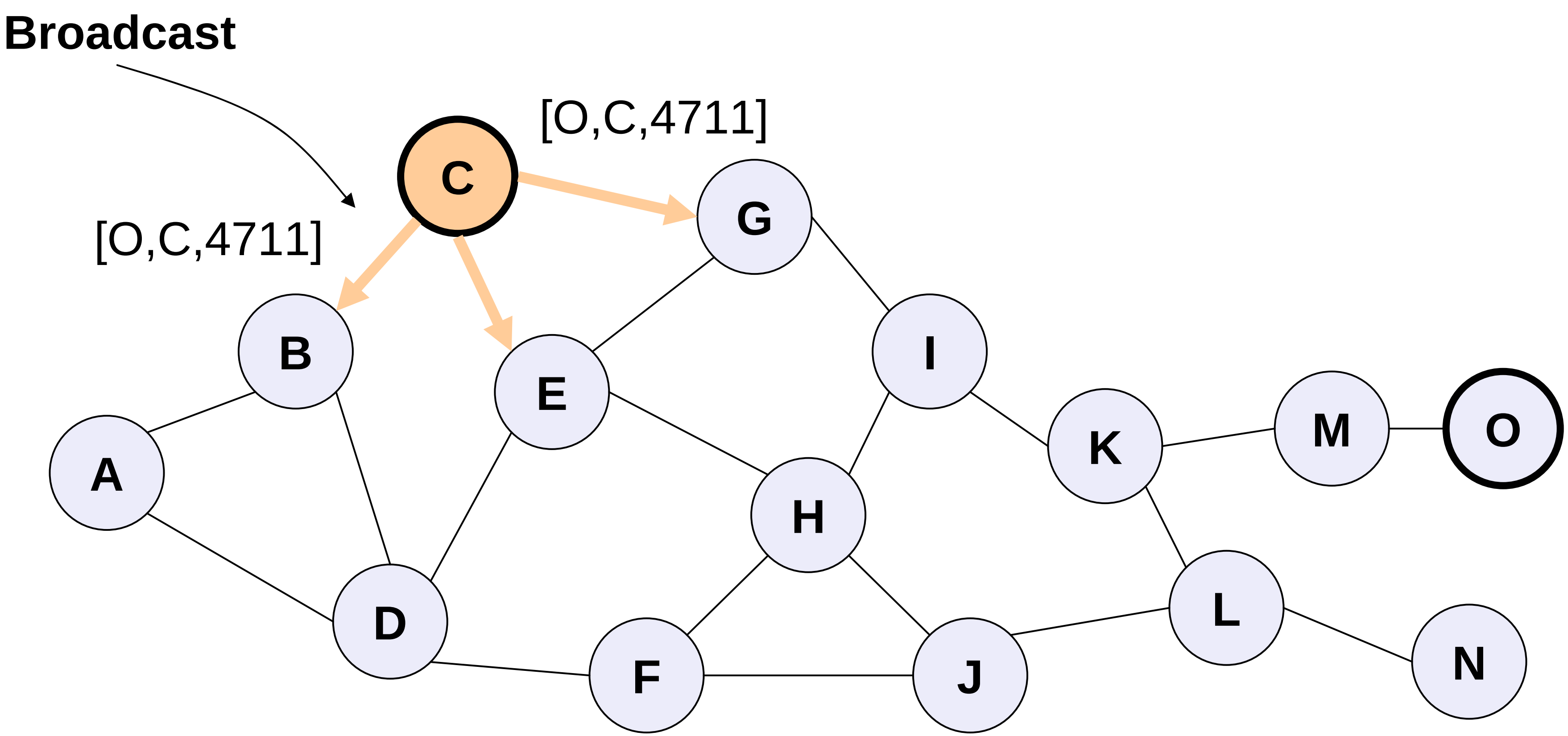
- broadcast a packet with destination address and unique ID
- if a station receives a broadcast packet it acts as follows:
  - if the station is **not** the receiver, append own address to the packet and broadcast it
  - if the packet has already been received earlier (identified via ID) then discard it
  - if the station is the receiver (i.e., has the correct destination address),then return the packet (including now the complete path) to the sender
- sender eventually receives packet with the current complete path (address list)

Optimizations

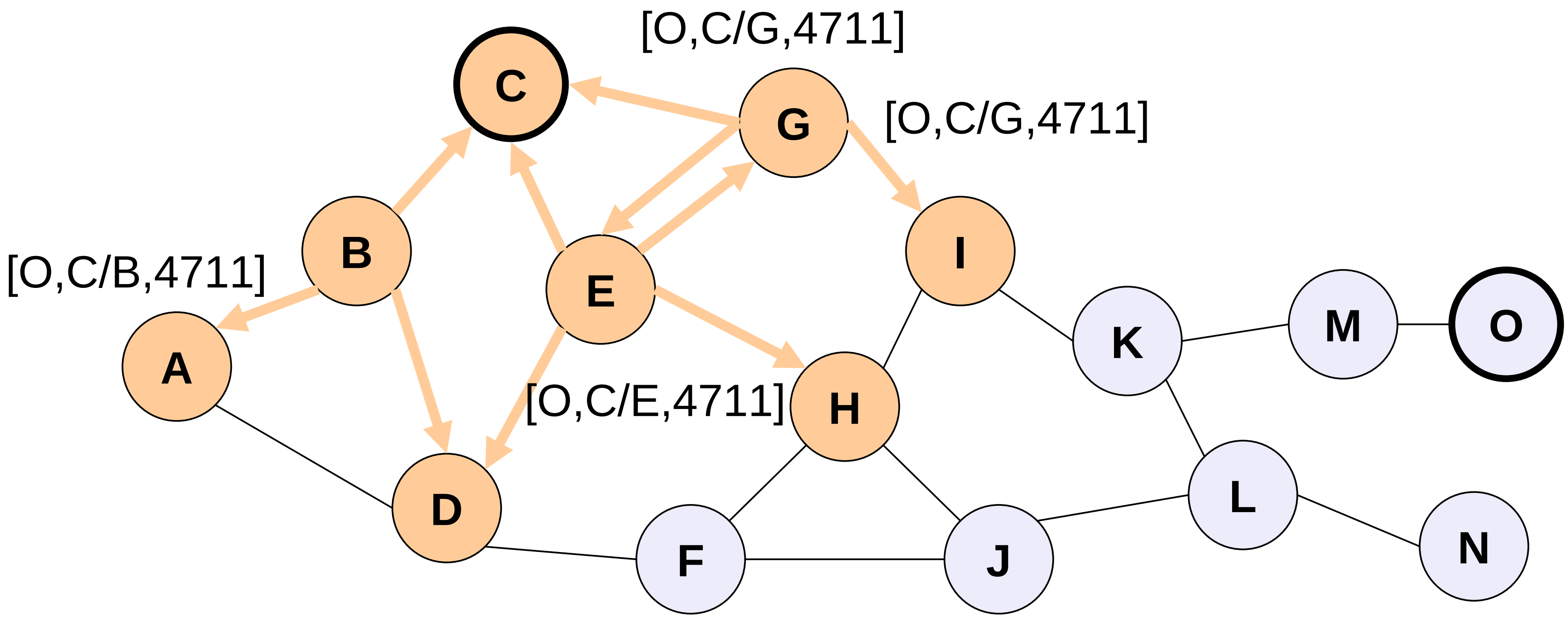
- limit broadcasting if maximum diameter of the network is known
- caching of address lists (i.e. paths) with help of passing packets
  - stations can use the cached information for path discovery (own paths or paths for other hosts)

Sending from C to O:

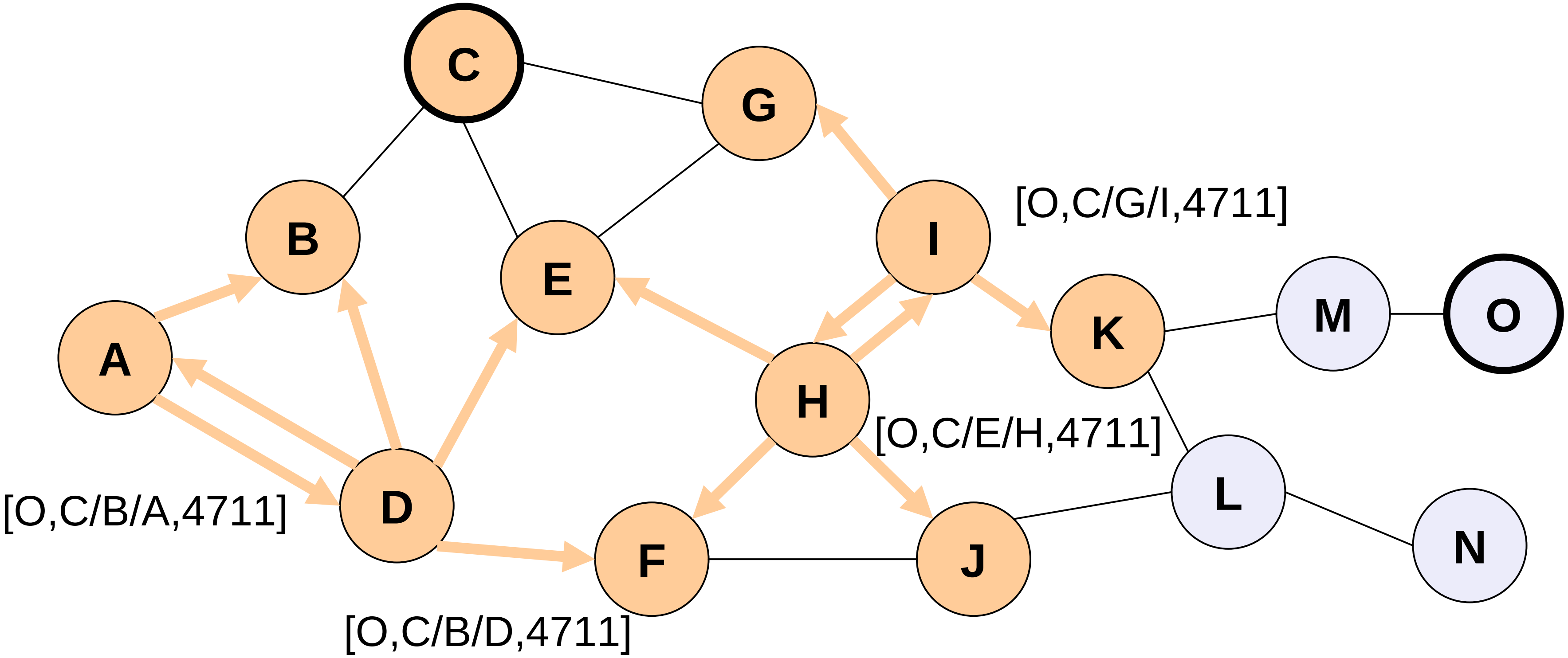



Broadcast
[O,C,4711]
[O,C,4711]
C
G
B
E
I
A
K
M
O
H
D
L
F
J
N

DSR: Route Discovery

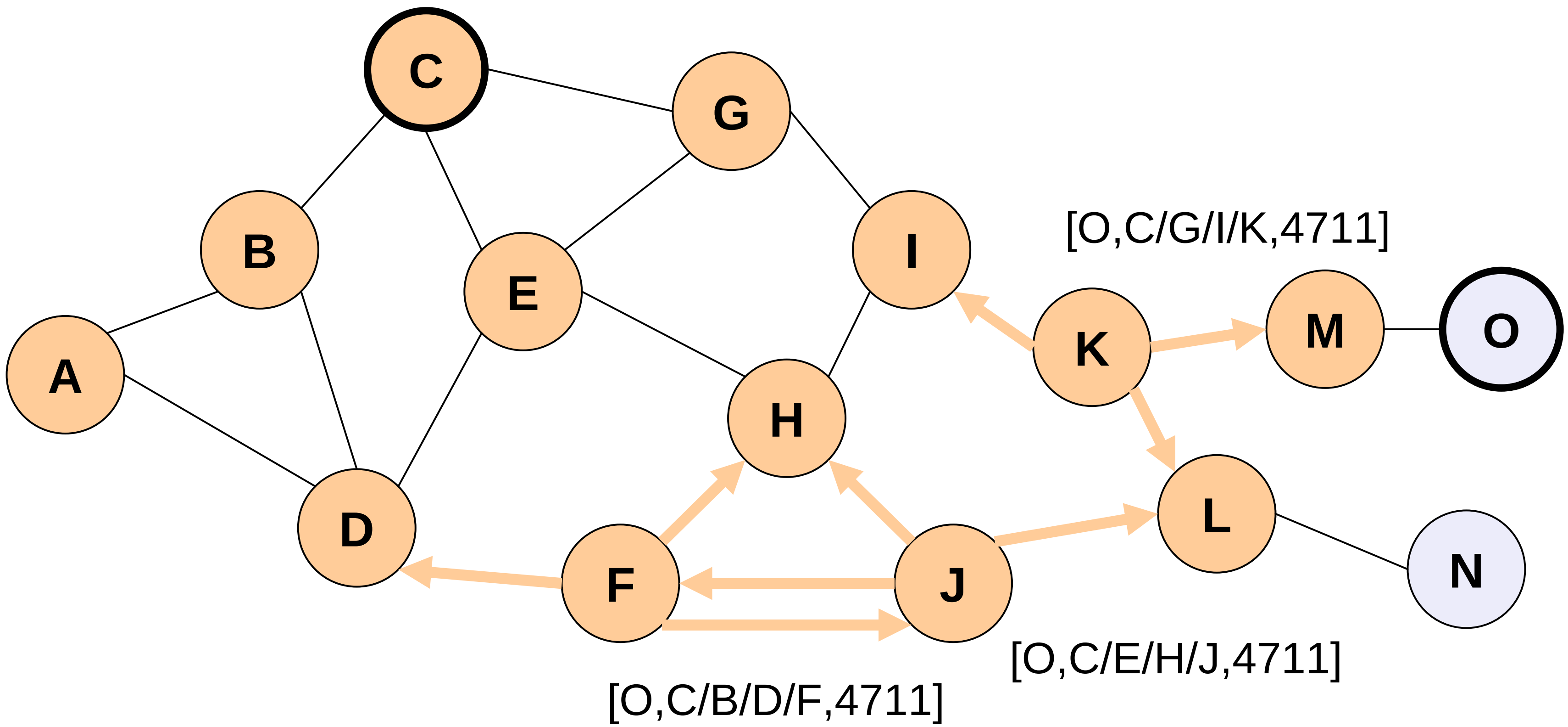


DSR: Route Discovery

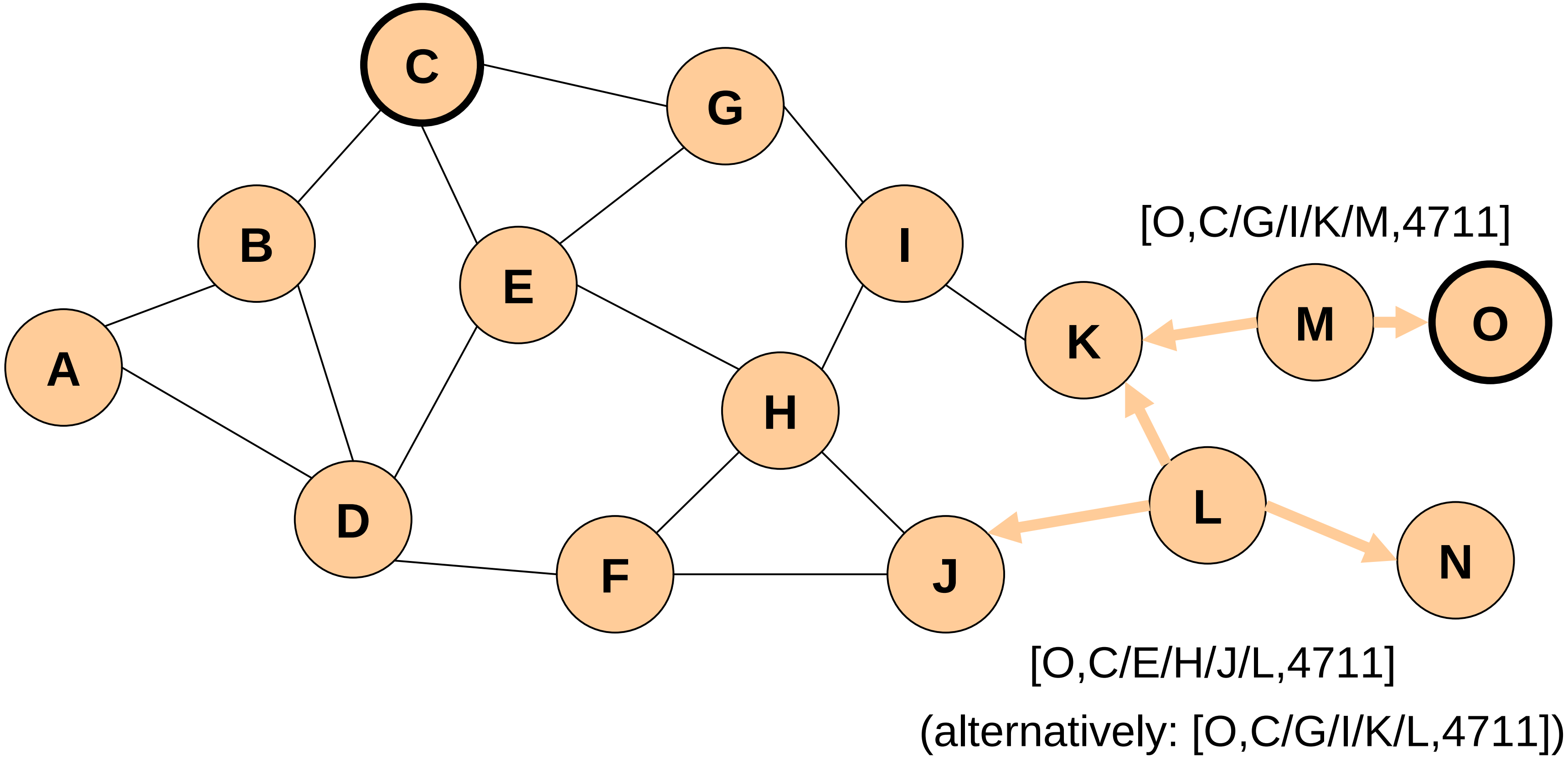


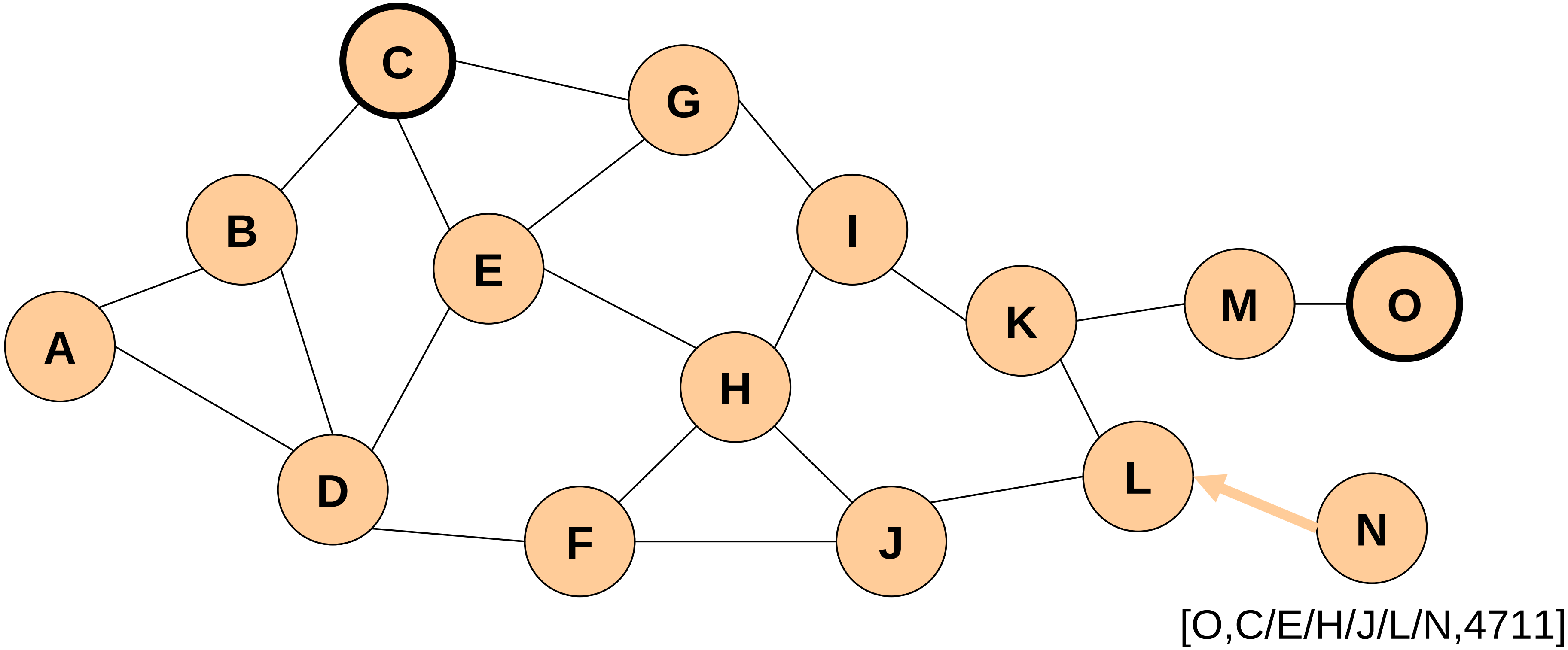
(alternatively: [O,C/E/D,4711])

DSR: Route Discovery

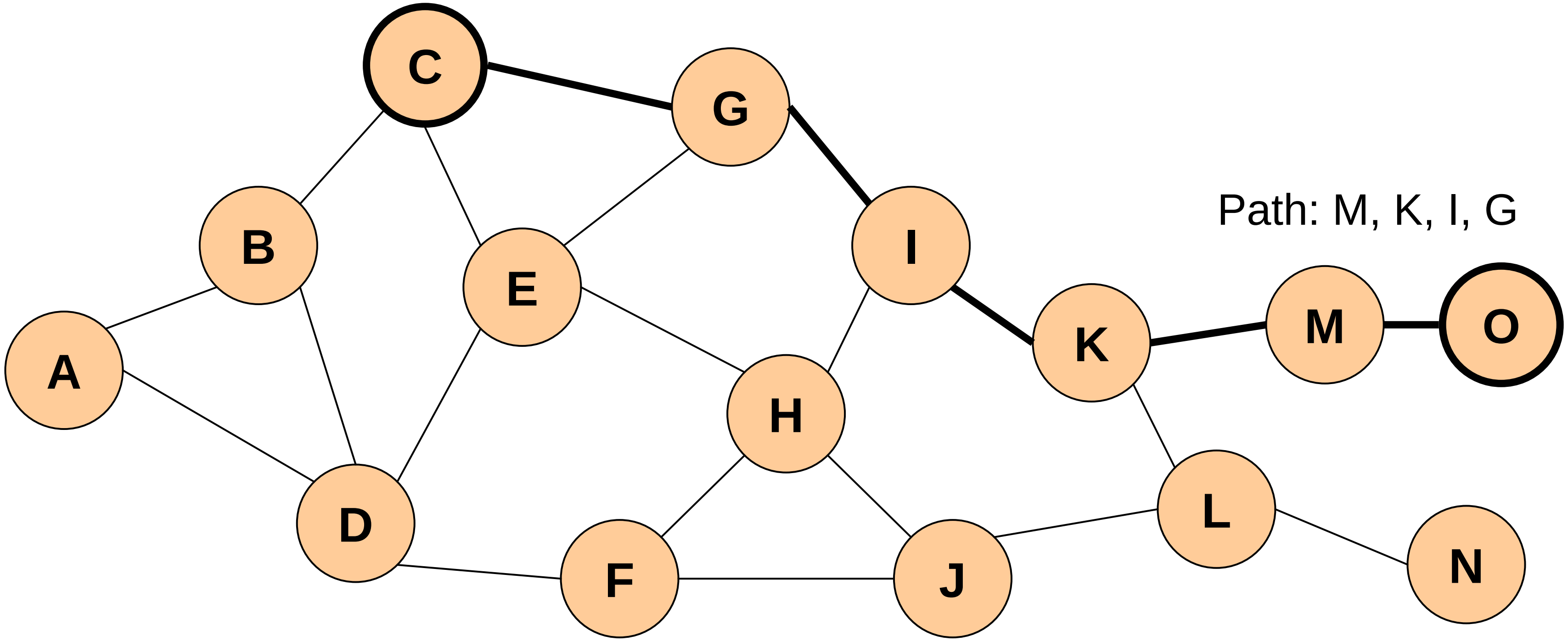


DSR: Route Discovery




C
G
B
E
I
A
K
M
O
H
D
L
F
J
N
[O,C/E/H/J/L/N,4711]

DSR: Route Discovery



DSR (Dynamic Source Routing) III

Maintaining paths:

after sending a packet several mechanisms can be used:

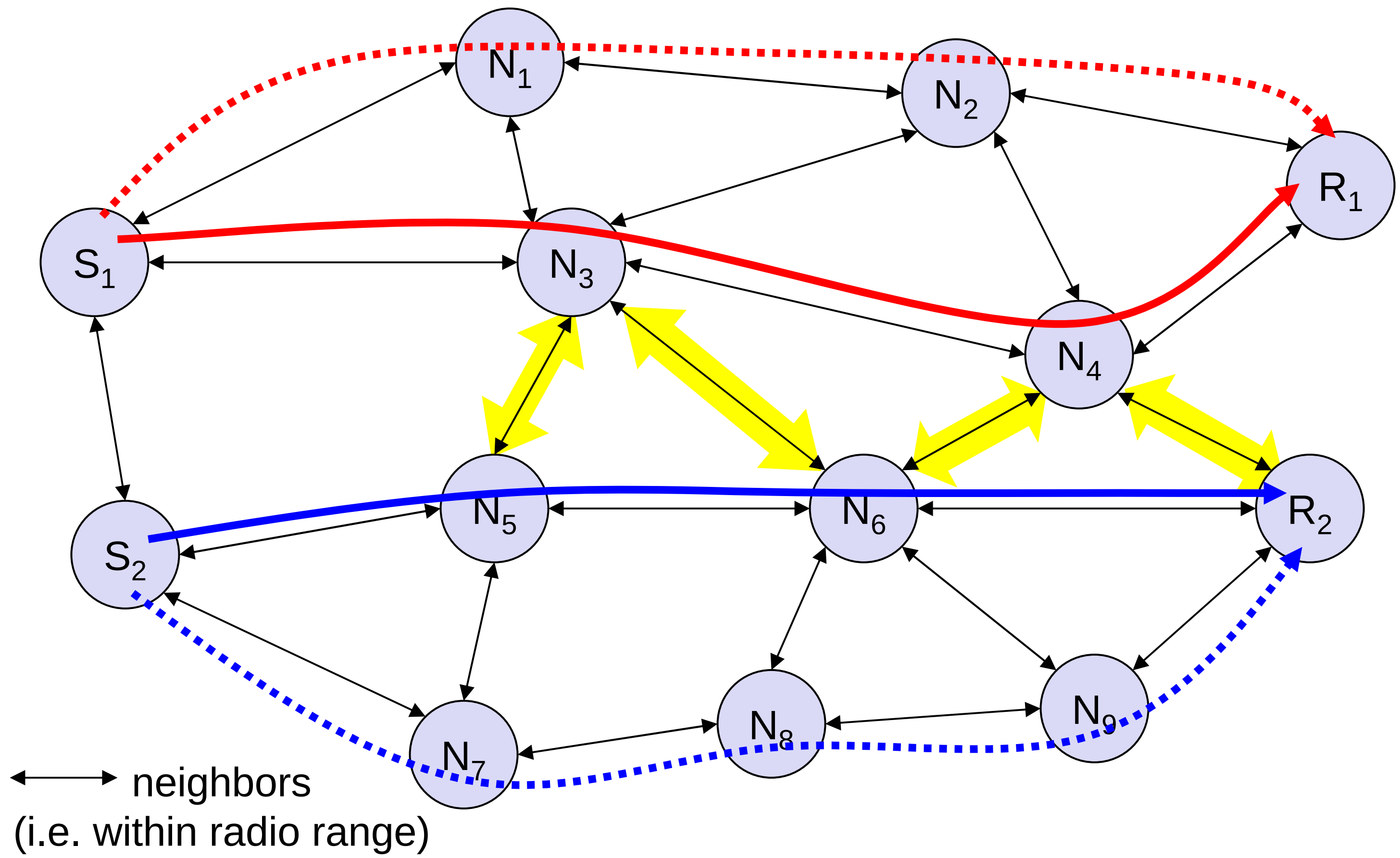
- wait for a layer 2 acknowledgement (if applicable)
- listen into the medium to detect if other stations forward the packet (if possible)
- request an explicit acknowledgement

if a station encounters problems it can inform the sender of a packet or itself looks up for a new path locally.

LIR: Alternative to hops as metric for optimal routing

Idea: Routing based on assumptions about interference between signals

Example of Least Interference Routing (LIR):



An overview of ad - hoc routing protocols

Flat

- proactive
  - FSLS – Fuzzy Sighted Link State
  - FSR – Fisheye State Routing
  - OLSR – Optimised Link State Routing Protocol
  - TBRPF – Topology Broadcast Based on Reverse Path Forwarding
- reactive
  - **AODV** – Ad hoc On demand Distance Vector
  - DSR – Dynamic Source Routing

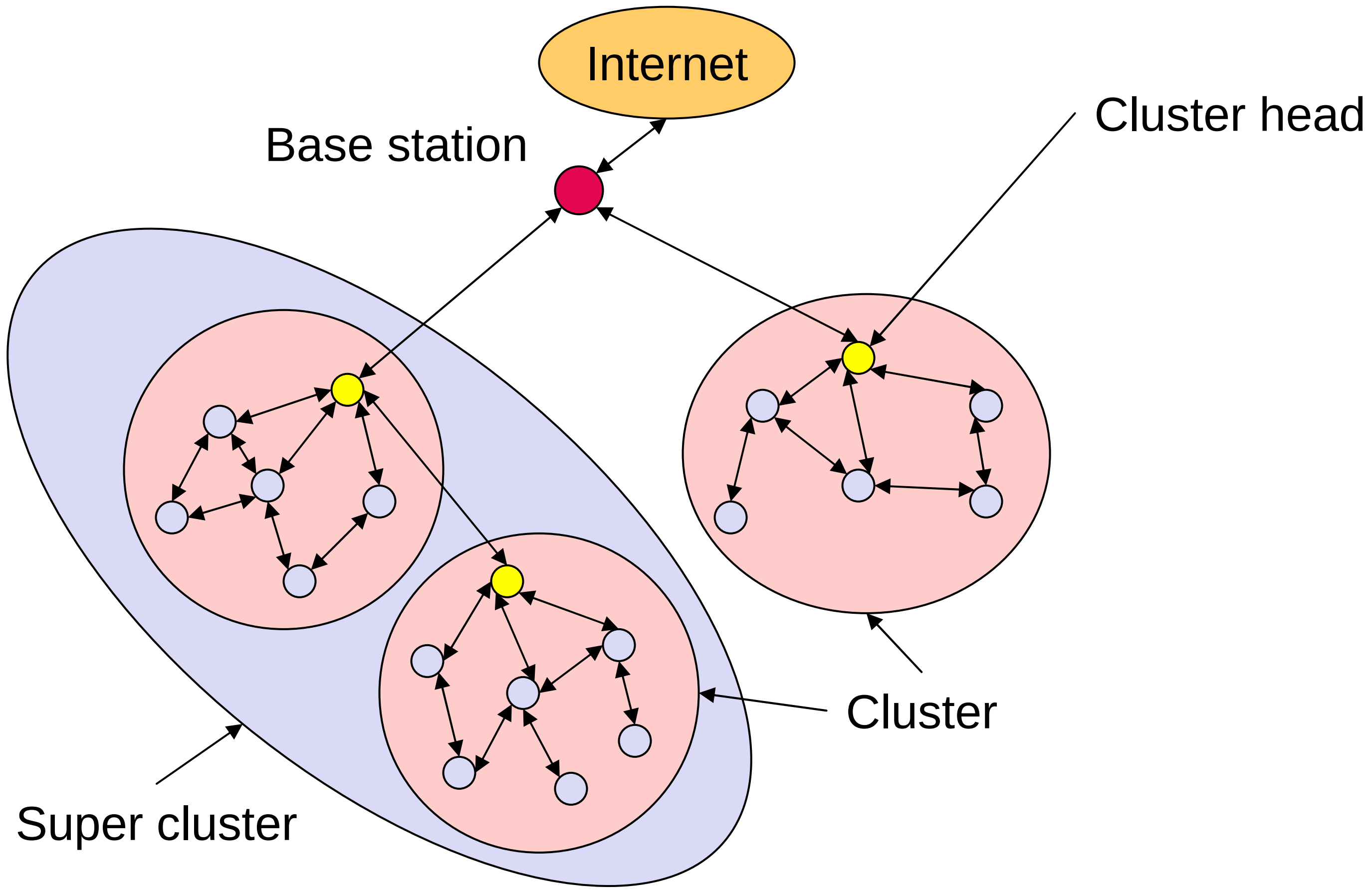
Hierarchical

- 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

Clustering of ad-hoc networks



Summary

Mobile IP:

- All nodes of a network should be able to communicate with each other also if different communication technologies are used
- Open problems: QoS (esp. security), efficiency of packet transmission

DHCP:

- Simple mechanism to integrate a mobile station into a network

Ad-Hoc Networks:

- Communicating over larger distances without relying on existent infrastructure
- Routing is the main aspect
  - needs information from lower layers
  - Providing QoS is the main issue
  - Applications?
- Meshed Networks: in-between infrastructure and ad-hoc
- Considering mobility of whole networks

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