Prof. Dr.-Ing Jochen H. Schiller
Inst. of Computer Science
Freie Universität Berlin
Germany

Freie Universität Berlin

Mobile Communications
Chapter 6: Internet Protocols

Mobile IP, Security, MIPv6, PMIPv6
Micro mobility support, Locator/ID split
Ad-hoc networks, Routing protocols, WSN/IoT

TCP-mechanisms
Classical approaches, PEPs in general
Additional optimizations

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 to long time
- TCP connections break, security problems

Requirements for Mobile IPv4 (RFC 5944 was: 3344, was: 3220, was: …, updated by: …)

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 few 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

Terminology

Mobile Node (MN)
- system (node) that can change the point of connection to the network without changing its IP address

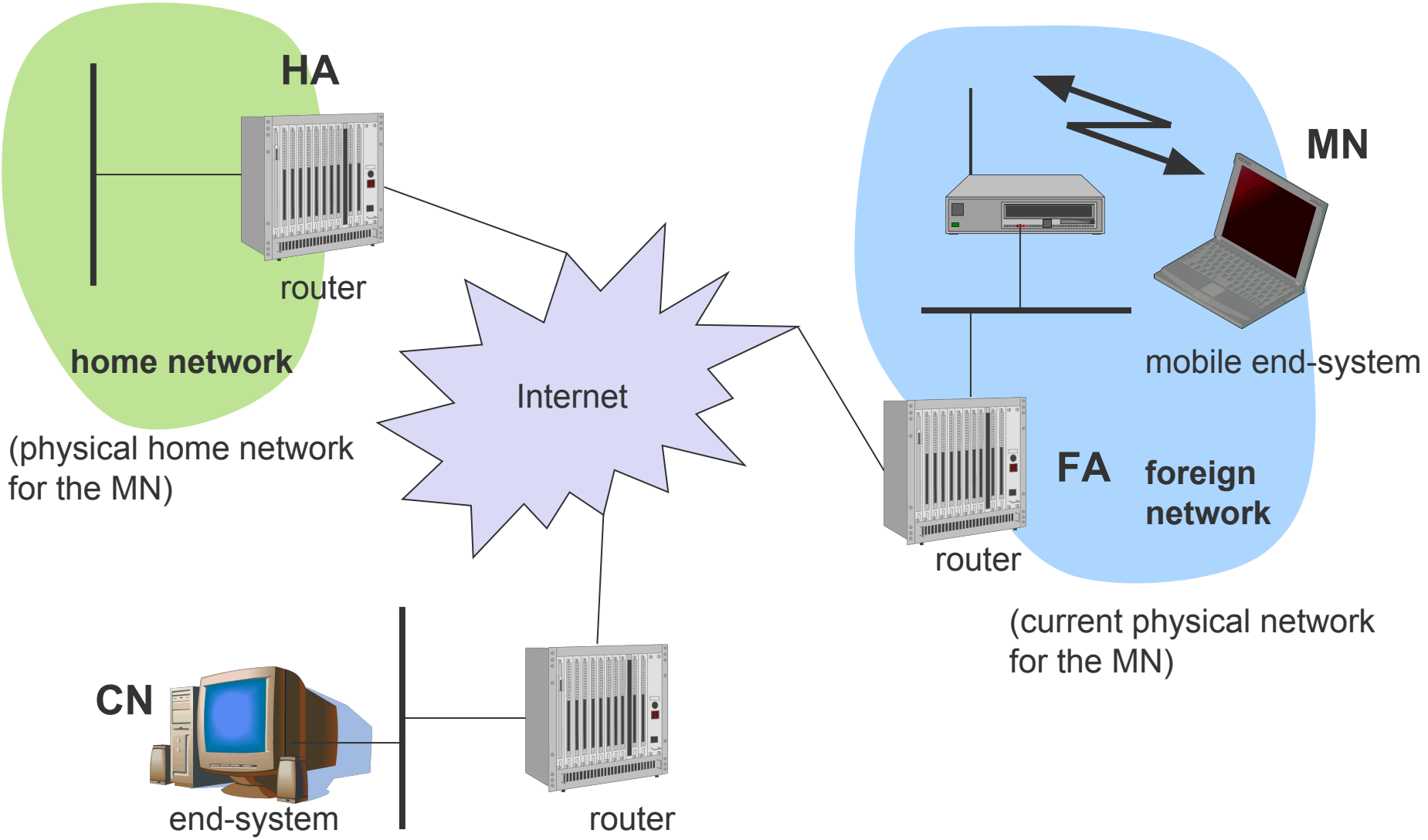
Home Agent (HA)
- system in the home network of the MN, typically a router
- registers the location of the MN, tunnels IP datagrams to the COA

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

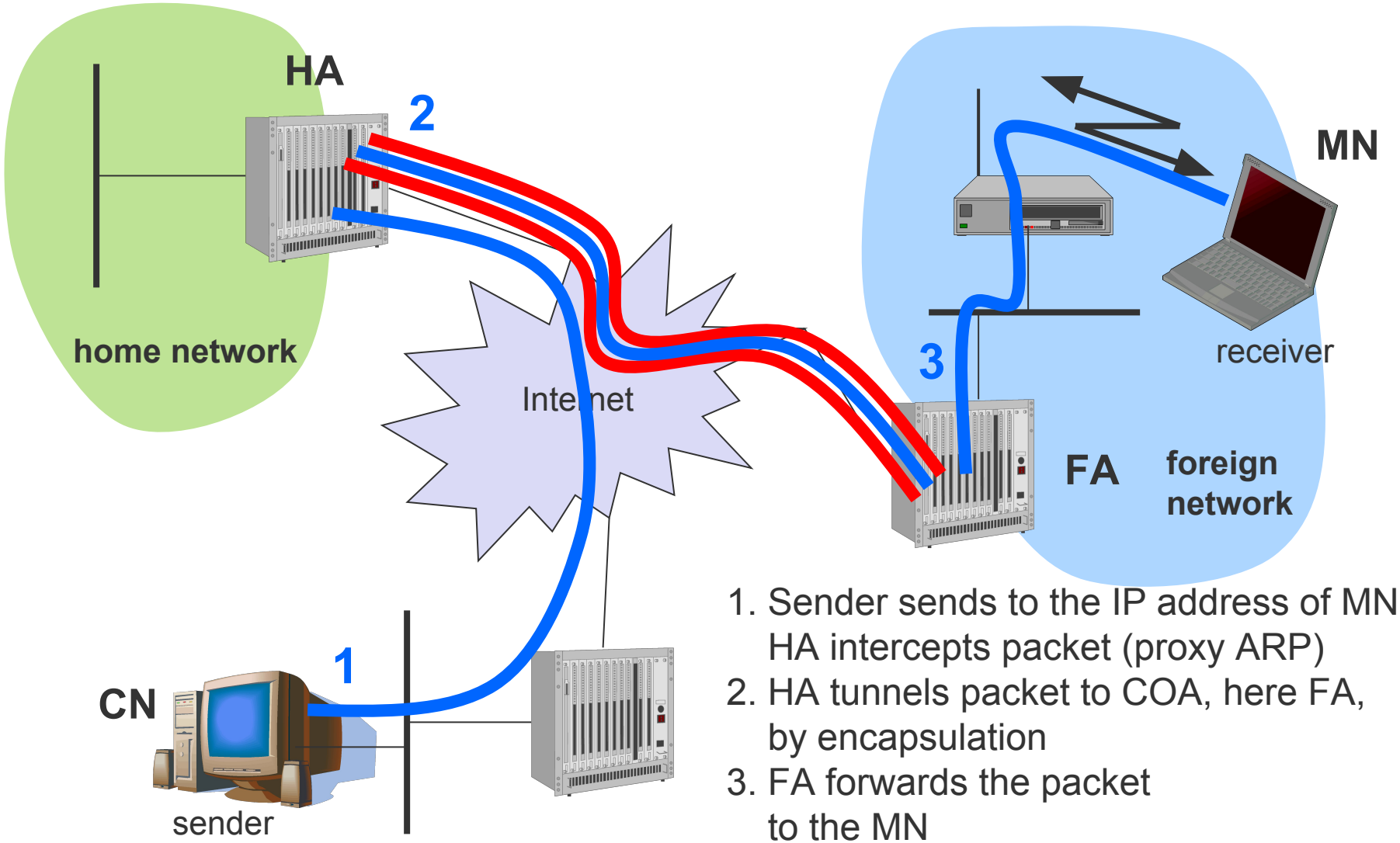
Care-of Address (COA)
- address of the current tunnel end-point for the MN (at FA or MN)
- actual location of the MN from an IP point of view
- can be chosen, e.g., via DHCP

Correspondent Node (CN)
- communication partner

Example network

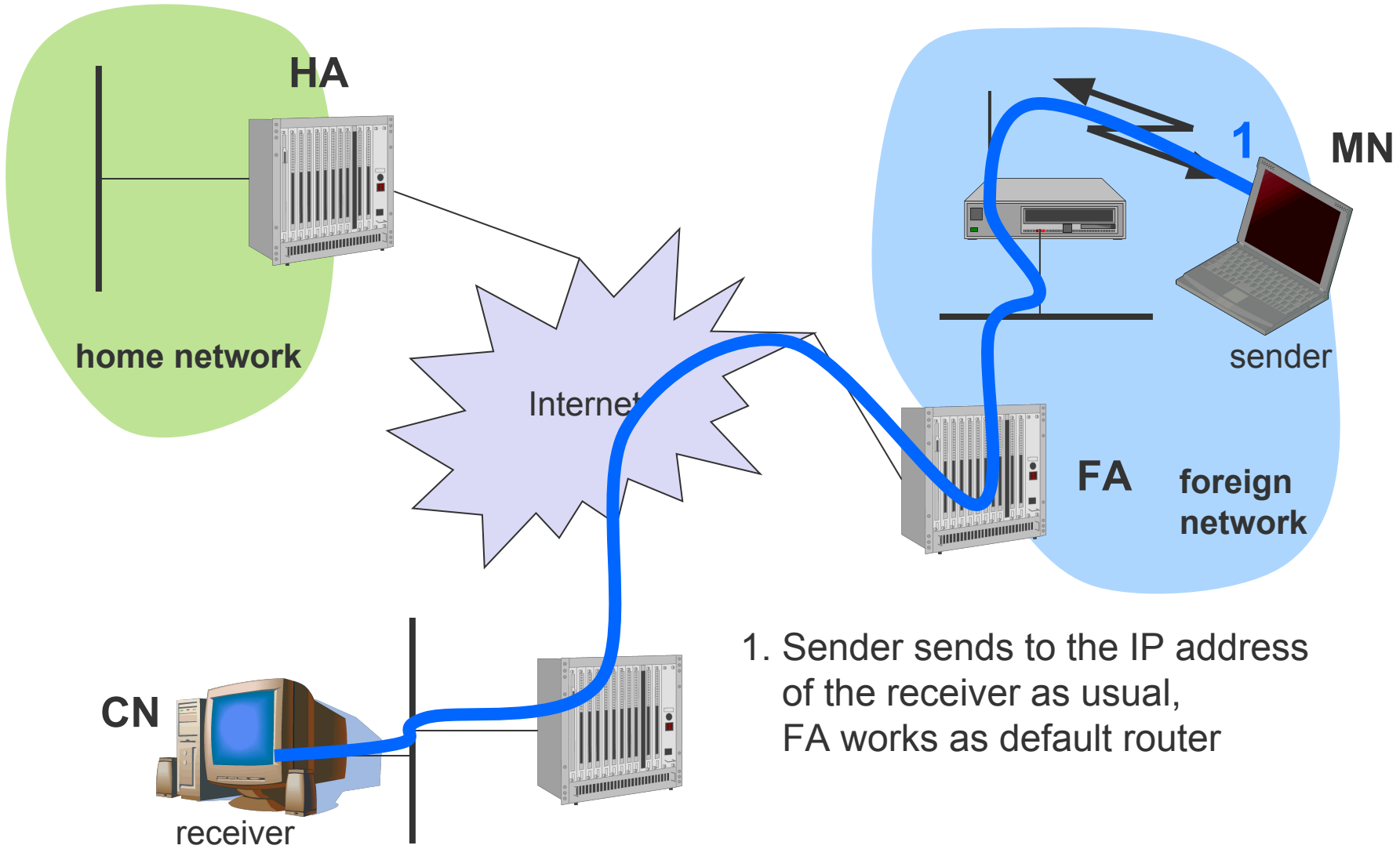


Data transfer to the mobile system

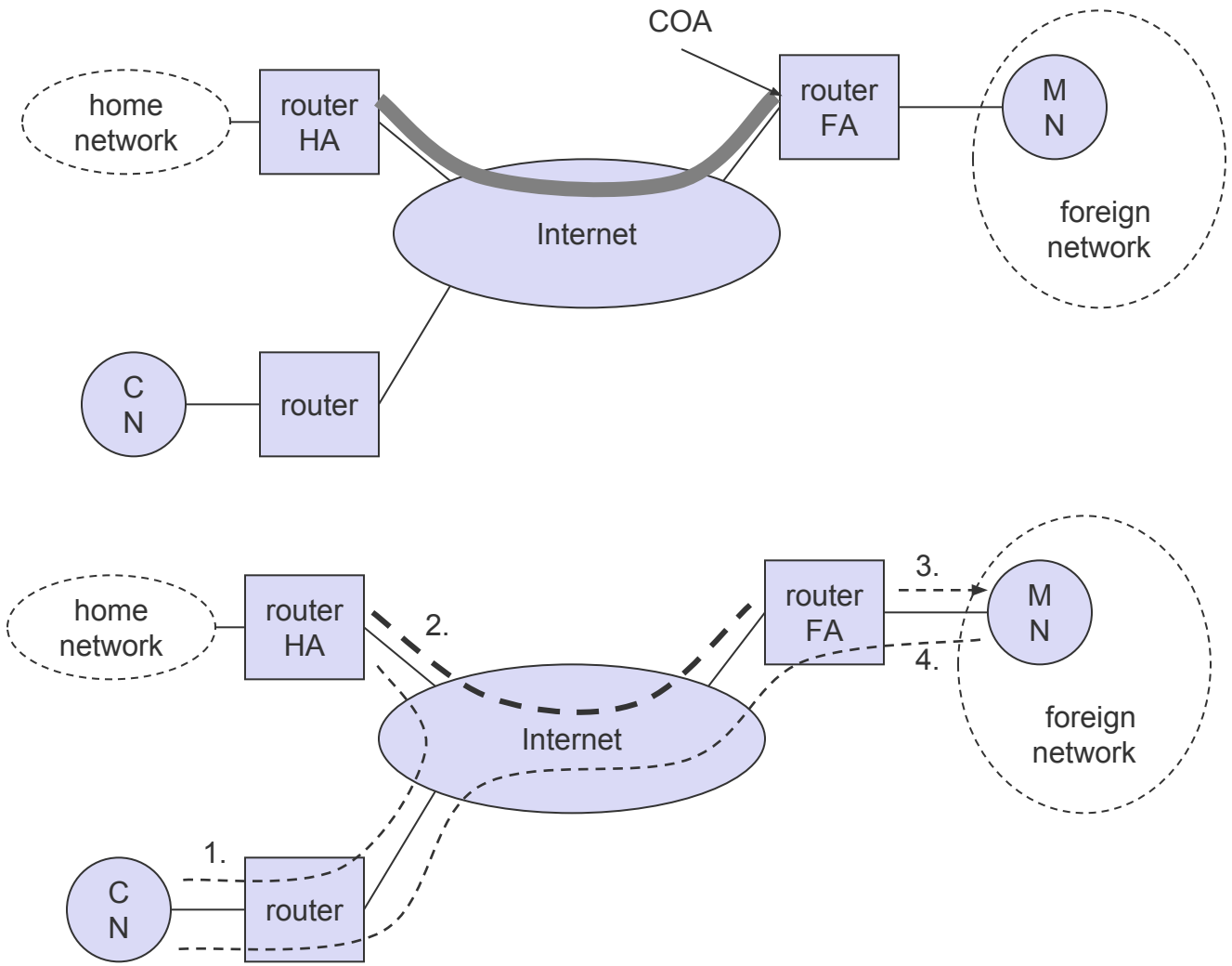


1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



Overview


COA
home network
router HA
router FA
M N
Internet
foreign network
C N
router
home network
router HA
2.
router FA
3.
M N
4.
Internet
foreign network
1.
C N
router

Questions & Tasks

- What is the key motivation for the classical Mobile IP?
- Why can we use mobile systems without any Mobile IP?
- What is triangular routing? Potential performance issues?

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!)

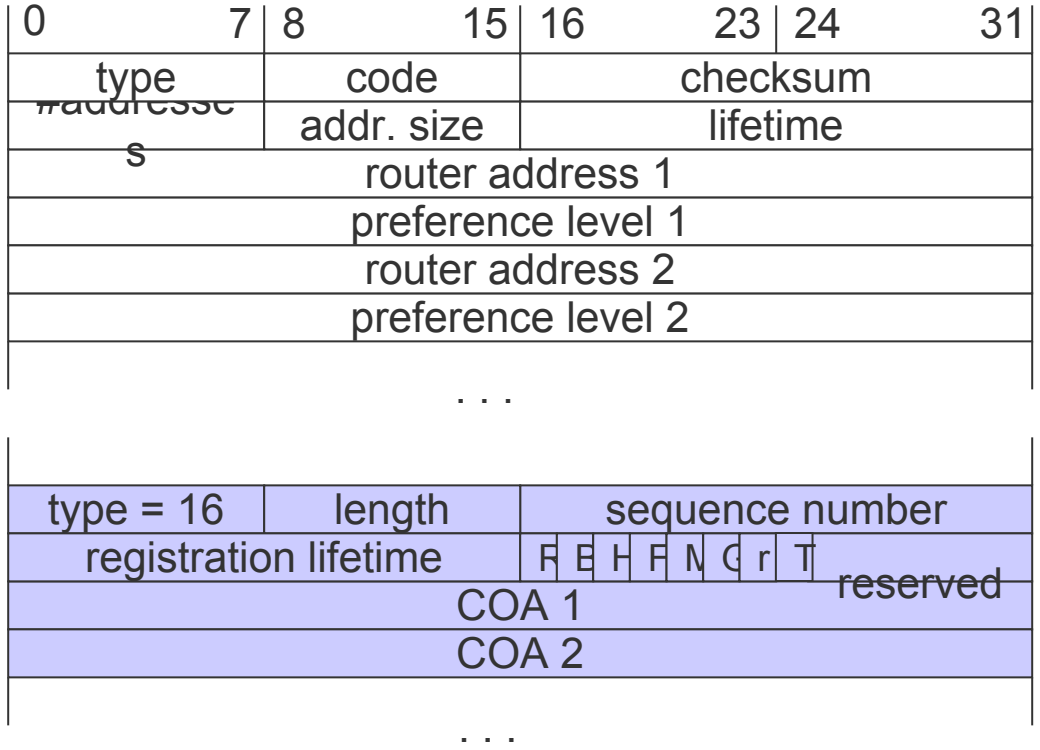
- MN signals COA to the HA via the FA, HA acknowledges via FA to MN
- these actions have to be secured by authentication

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

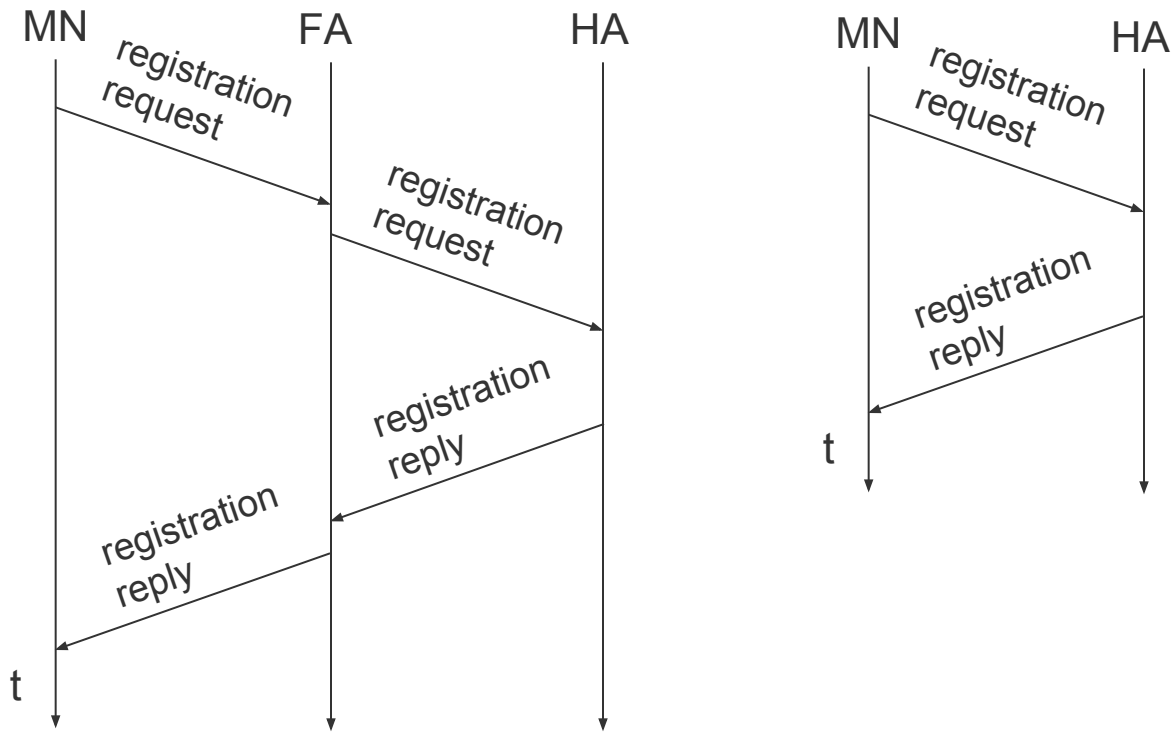
Agent advertisement

Extended ICMP Router Advertisements

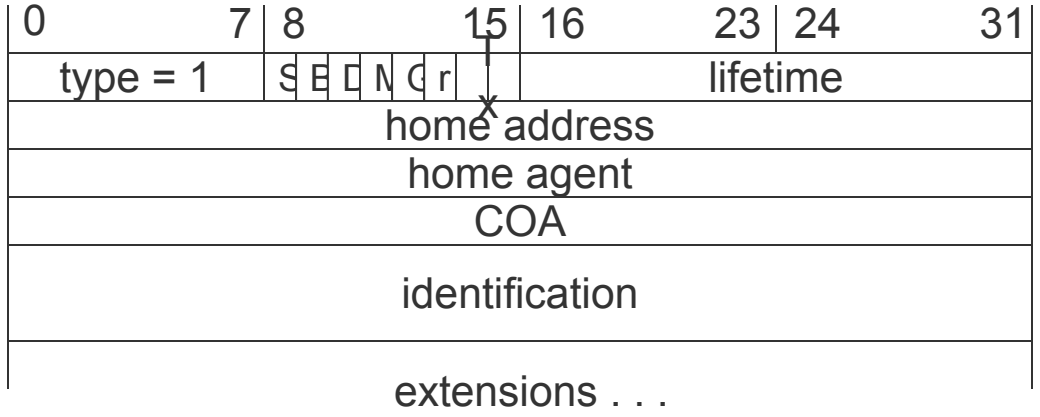


type = 16
length = 6 + 4 * #COAs
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Registration

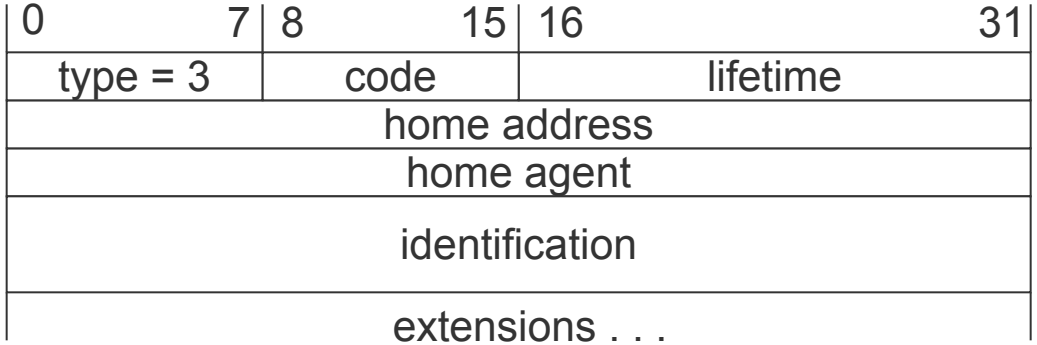


Mobile IP registration request



S: simultaneous bindings
B: broadcast datagrams
D: decapsulation by MN
M mininal encapsulation
G: GRE encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored

Mobile IP registration reply



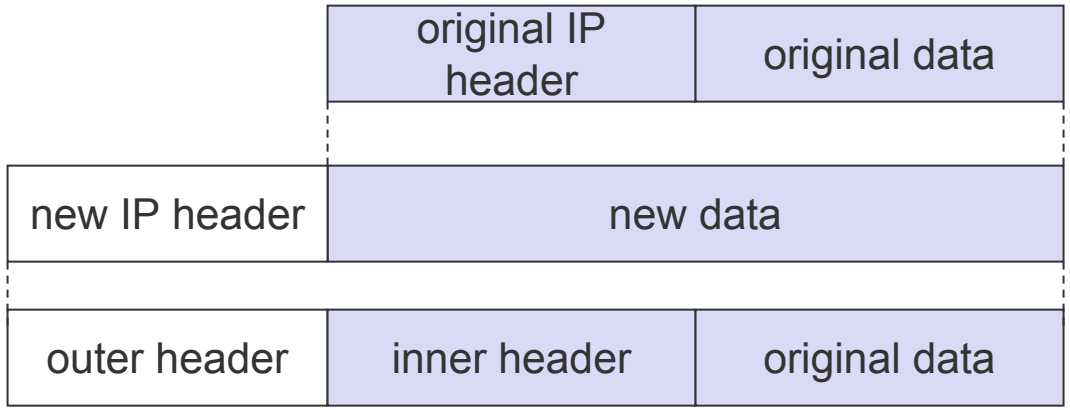
Example codes:

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 – needed for the tunnel HA-CoA



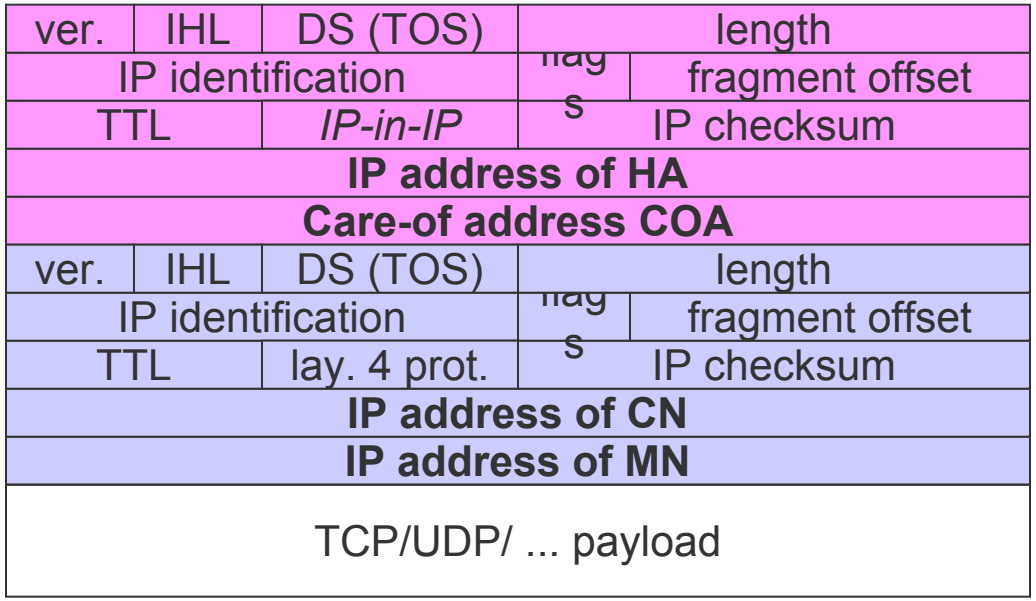
Encapsulation

Encapsulation of one packet into another as payload

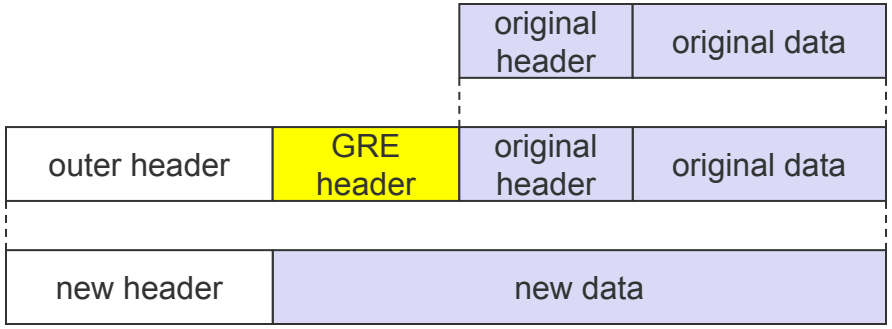
- e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
- here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)

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

- tunnel between HA and COA



Optional: 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)

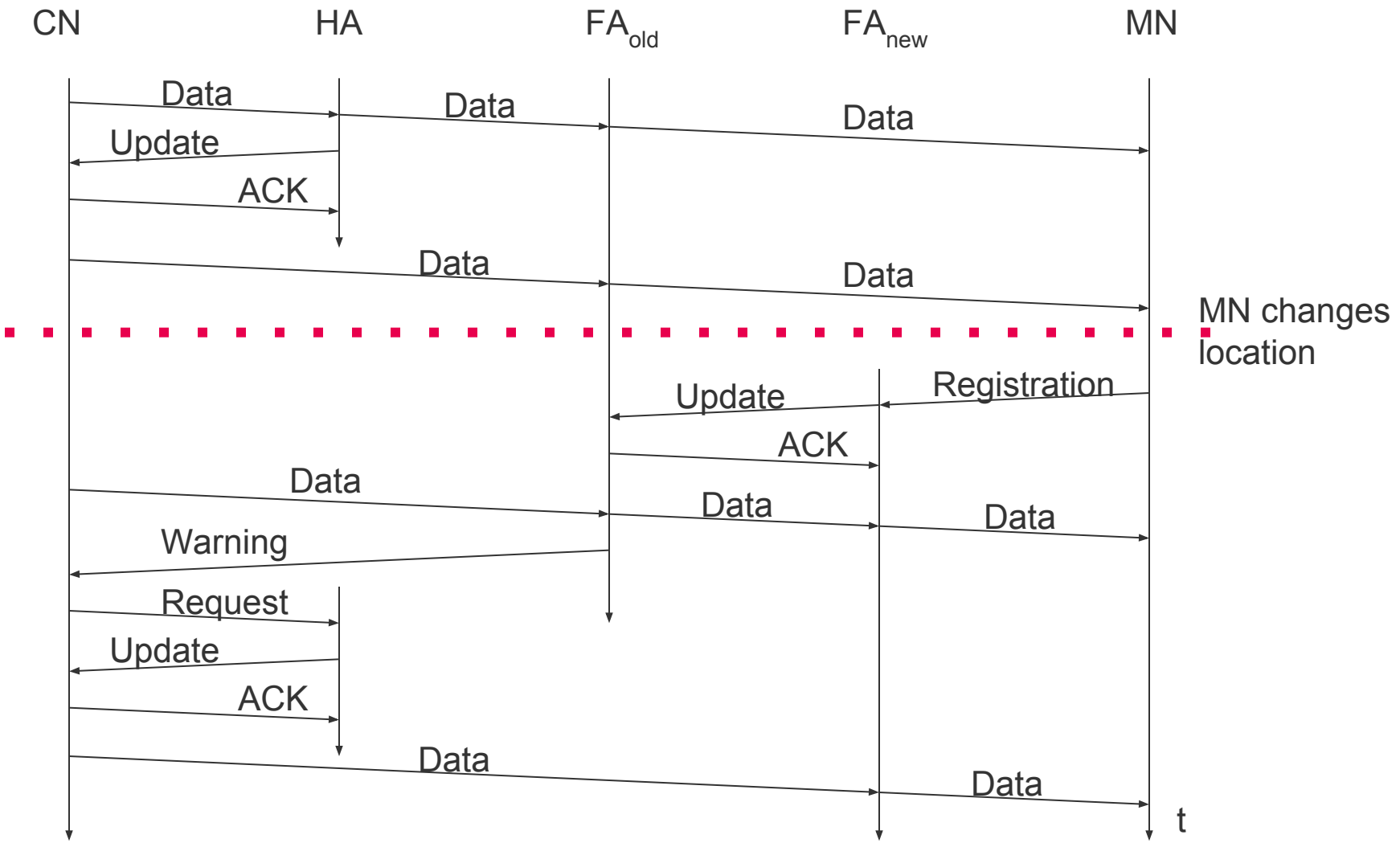
Optimization of packet forwarding

Problem: Triangular Routing
- sender sends all packets via HA to MN
- higher latency and network load

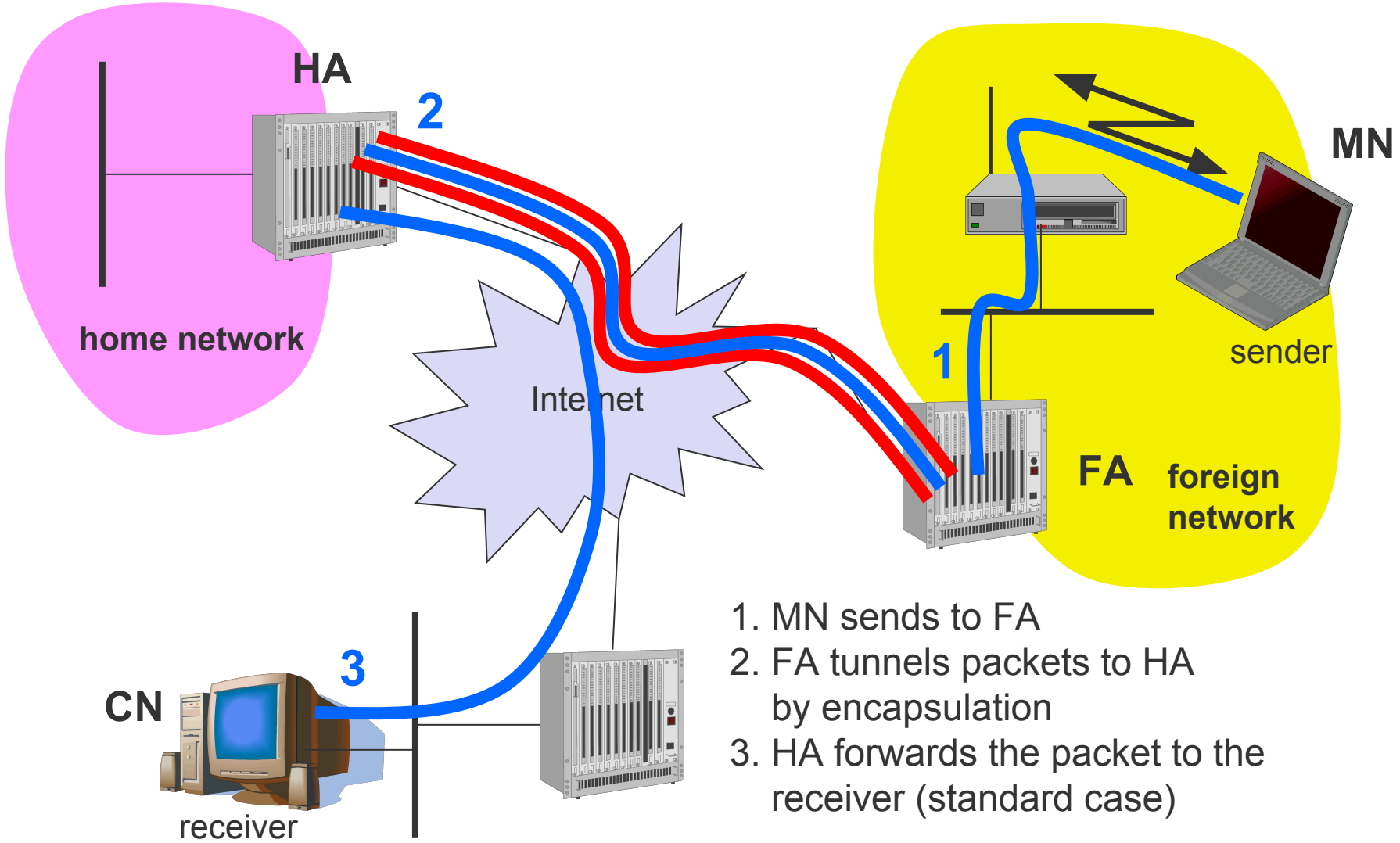
“Solutions”
- sender learns the current location of MN
- direct tunneling to this location
- HA informs a sender about the location of MN
- big security problems!

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)



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

Mobile IP with reverse tunneling

Router accept 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

Problems with mobile IP

Security
- authentication with FA problematic, for the FA typically belongs to another organization
- no common protocol for key management and key distribution widely accepted 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 resource reservation protocols
- tunneling makes it hard to give a flow of packets a special treatment needed for the QoS

Security, firewalls, QoS etc. are always topics of research and discussions…

Questions & Tasks

- How does an MN detect that it is not “at home”?
- What is the difference of a co-located COA and a COA at the FA?
- How to optimize triangular routing?
- Why may reverse tunneling be needed? Performance issues?
- Which security issues come with mobile IP?

Mobile IP and IPv6 (RFC 6275, was: 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

All routers perform router advertisement
- can be used instead of the special agent advertisement, no need for a separate FA

Addresses are always co-located
- MN can signal a sender directly the COA, sending via HA not needed in this case
- this allows for an automatic path optimization

„Soft“ hand-over
- no packet loss due to change of subnets
- 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

IP Micro-mobility support

What happens if, e.g., a student changes subnets on a campus frequently?

- Involvement of the HA each time
- Reveals precise “location”

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

Lot of research, not everything in products

Important criteria:
Security Efficiency, Scalability, Transparency, Manageability

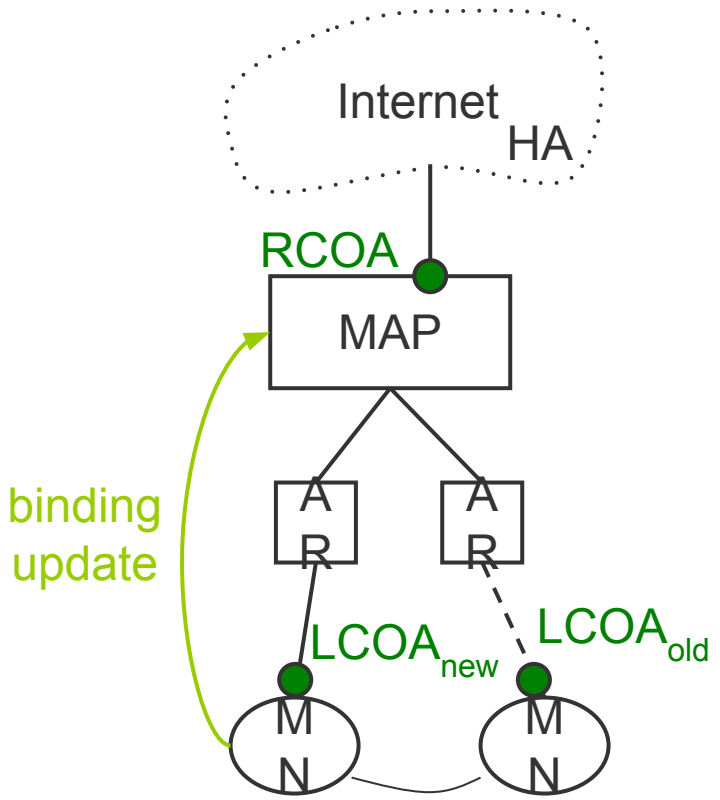
Hierarchical Mobile IPv6 (RFC 5380, was: 4140)

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



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)
- Handover requires minimum number of overall changes to routing tables

Potential problems:

- Decentralized security-critical functionality (handover processing) in mobility anchor points
- MNs can (must!) directly influence routing entries via binding updates (authentication necessary)
- Not transparent to MNs
- Handover efficiency in wireless mobile scenarios:
  - All routing reconfiguration messages sent over wireless link

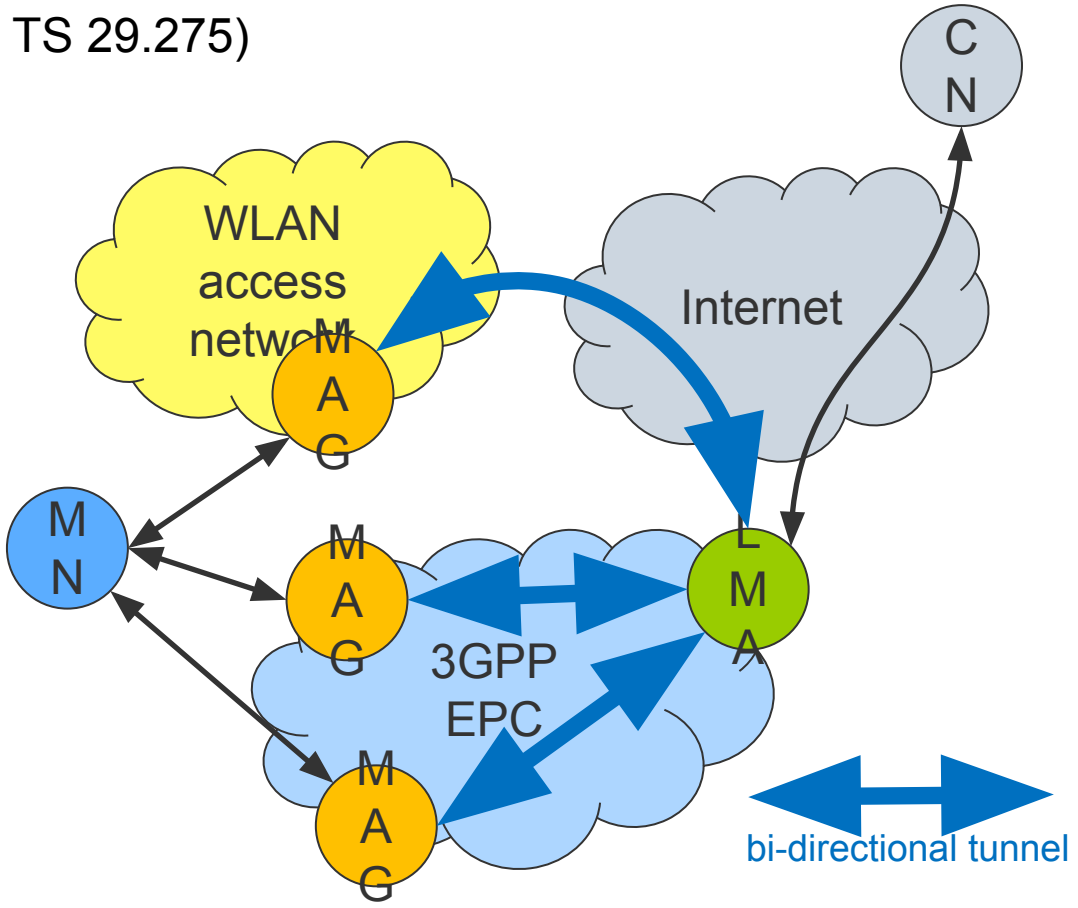
Proxy Mobile IPv6 (PMIPv6)

Network-based mobility management protocol, RFC5213, updated by RFC6543, RFC7864
- enables IP mobility for a host *without* requiring its participation in any mobility-related signaling
- the network manages the IP mobility, no software change in clients needed
- adopted by 3GPP in LTE (LMA is in the PDN Gateway, 3GPP TS 29.275)

Local Mobility Anchor (LMA)
- acts as MIPv6 Home Agent
- anchor for MN's network prefix(es)

Mobile Access Gateway (MAG)
- function on access routers, tracks MN's mobility
- performs the signaling in the network with the LMA
- does the mobility management on behalf of the MN
- compatible to MIPv6 enabled MNs

IP traffic offloading possible



Split the two roles of an IP address: localization and identification

Host Identity Protocol v2 (HIPv2, RFC 7401, was: 5201, updated by 6253, 8002)

- Introduction of HIP layer between routing and transport, Alternative to Mobile IP
- IP addresses for routing only, change depending on location (must be topological correct!)
- Identification via Host Identity Tag, used e.g. for TCP connection identification instead of IP address
- Host Identity Tag based on public keys
  - Communication requires Diffie Hellman key exchange
- Pro
  - No intermediate agent, normal IP routing
- Con
  - Extra RTT due to key exchange, firewalls, extra layer
- See also RFCs 5202, 5203, 5204, 5205, 5206, 5207, 5770…

Locator/ID Separation Protocol (LISP, RFC 6830)

- New routing concept, tunneling for data transport, no changes to hosts or core
- RLOC (Routing Locator): topologically assigned, used for routing
- EID (Endpoint Identifier): administratively assigned, used for identification

Questions & Tasks

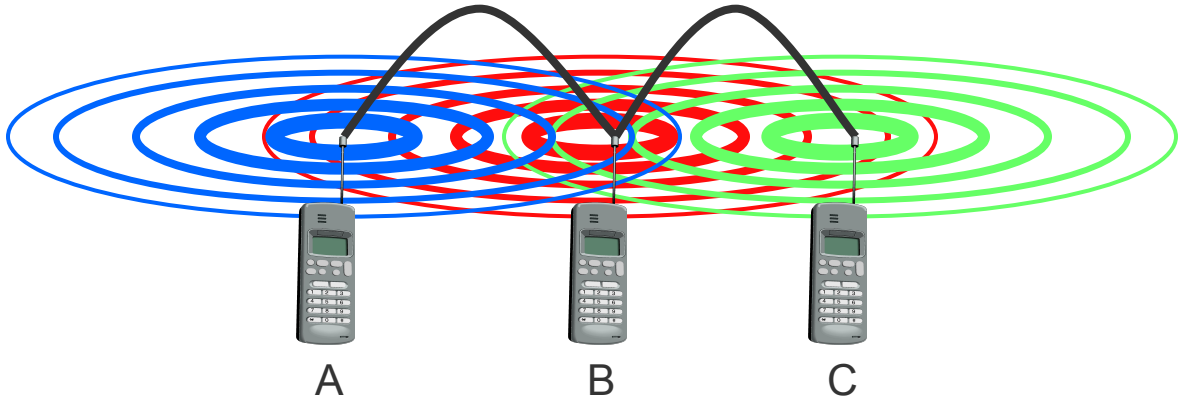
- How does IPv6 simplify Mobile IP?
- What is the motivation of micro-mobility support?
- What is a big advantage of PMIPv6?
- Which two roles does an IP address have? Why can this be problematic? Solutions?

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!

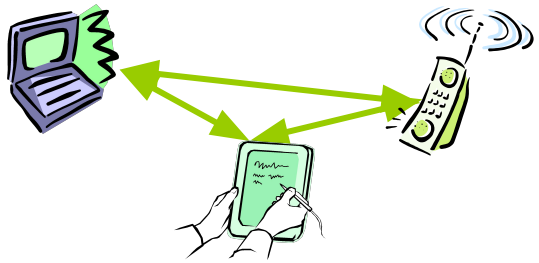
Main topic: routing
- no default router available
- every node should be able to forward



Solution: Wireless ad-hoc networks

Network without infrastructure
- Use components of participants for networking

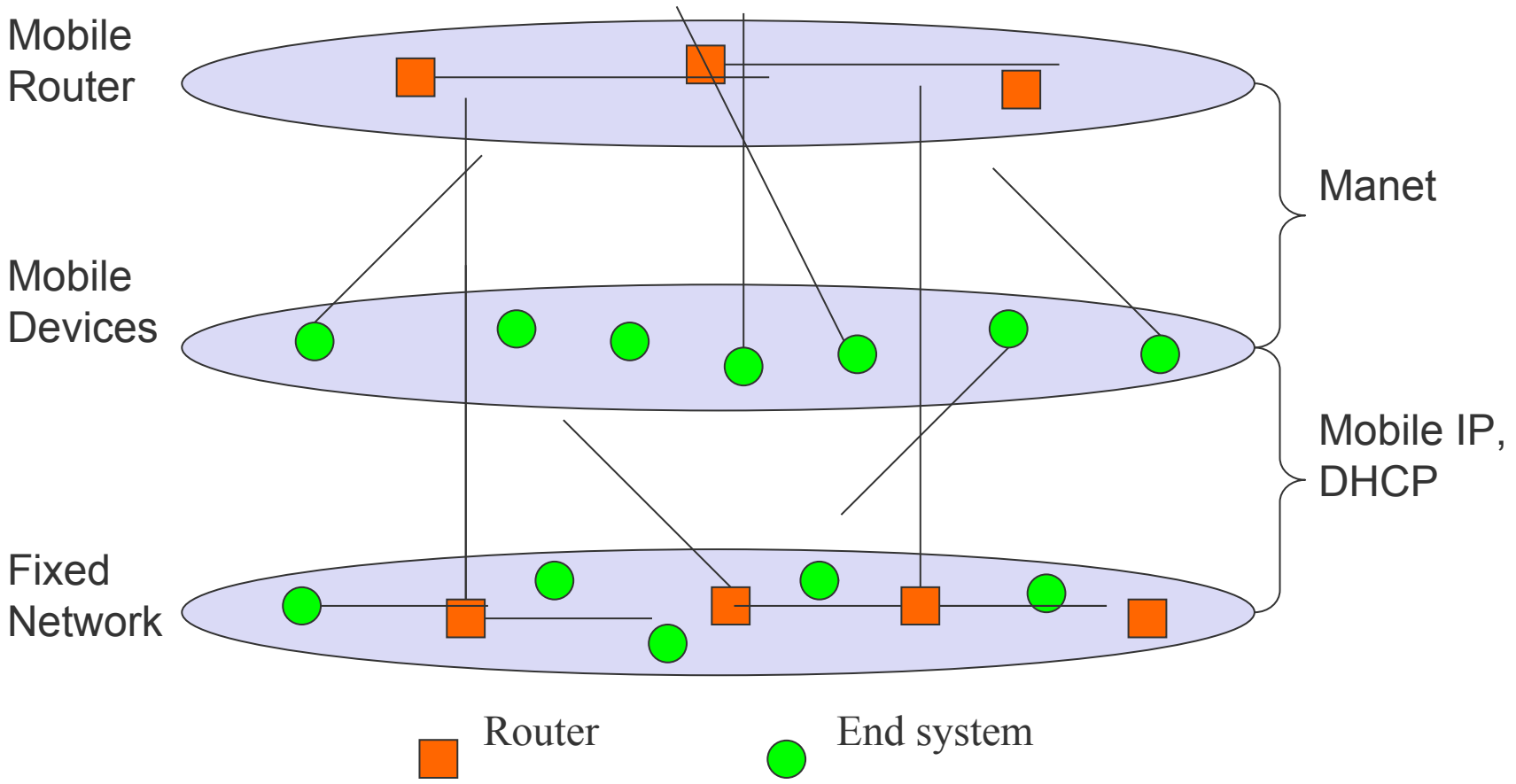
Examples
- Single-hop: All partners max. one hop apart
  - Bluetooth piconet, tablets in a room, gaming devices…



- Multi-hop: Cover larger distances, circumvent obstacles
  - Bluetooth scatternet, TETRA police network, car-to-car networks…

Internet: MANET (Mobile Ad-hoc Networking) group
- IEEE mesh networks solve similar issues on layer 2 – but think of layer 2 vs. layer 3 addresses!

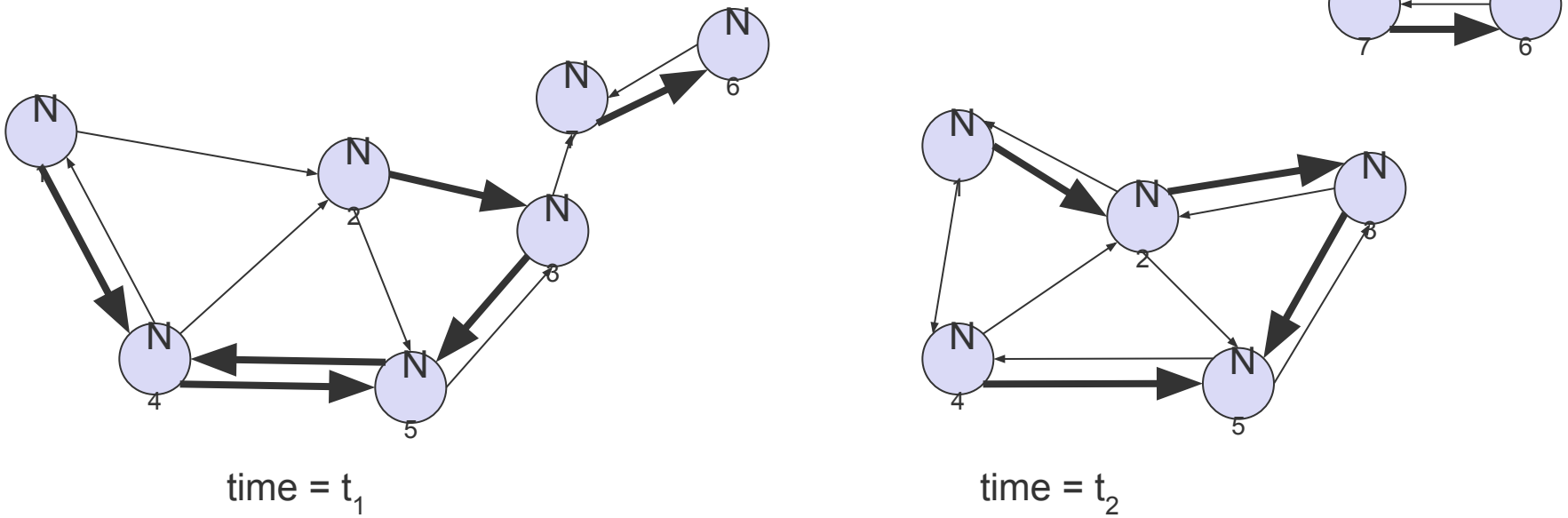
Manet: Mobile Ad-hoc Networking



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

Was THE big topic in many research projects
- Far more than 50, 100, 150, … different proposals exist
- The most simple 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

A simple example: 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! It is a so-called reactive routing protocol.

A simple example: Dynamic source routing II

Path discovery

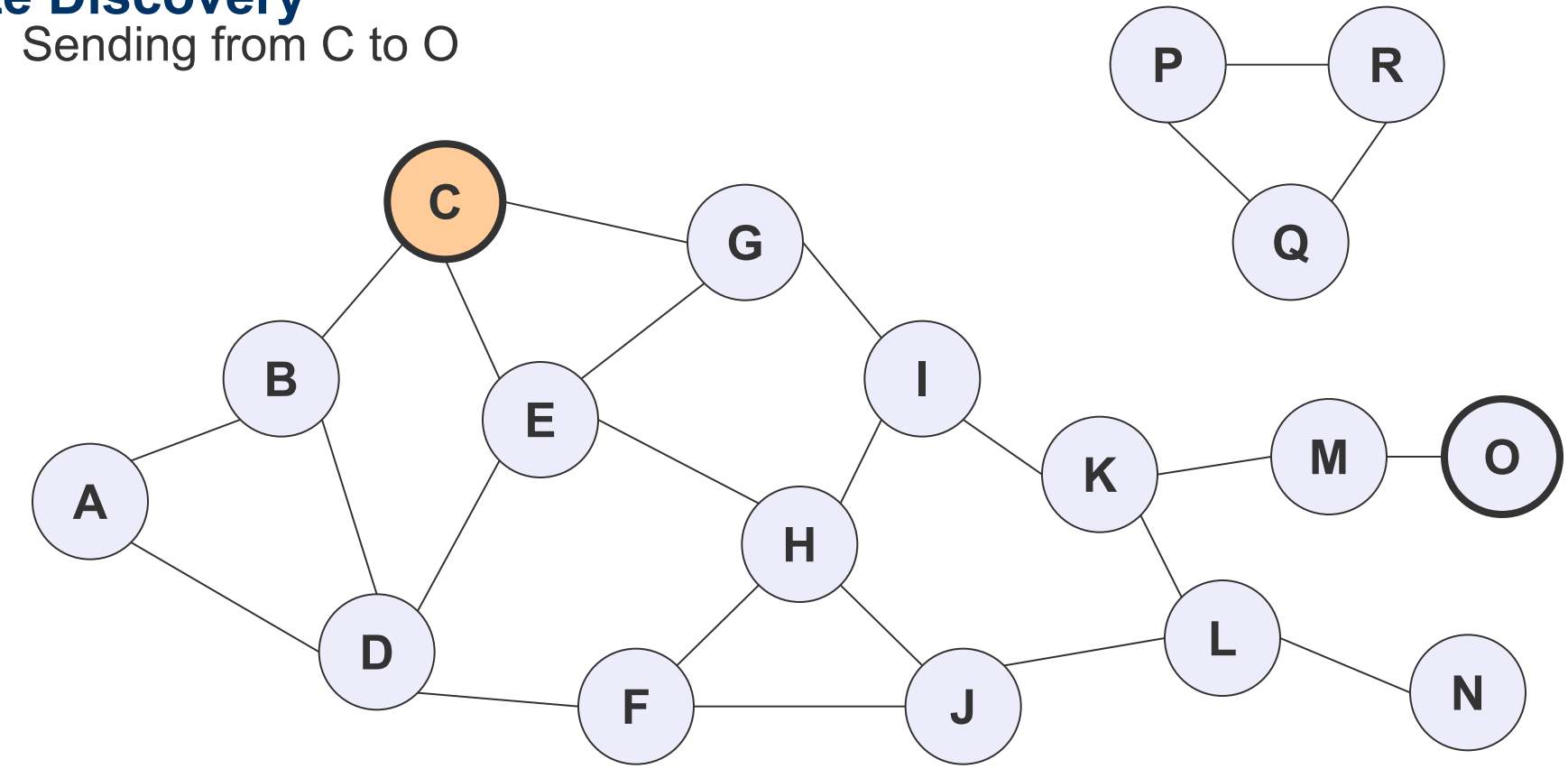
- broadcast a packet with destination address and unique ID
- if a station receives a broadcast packet
  - if the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet)
  - if the packet has already been received earlier (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)

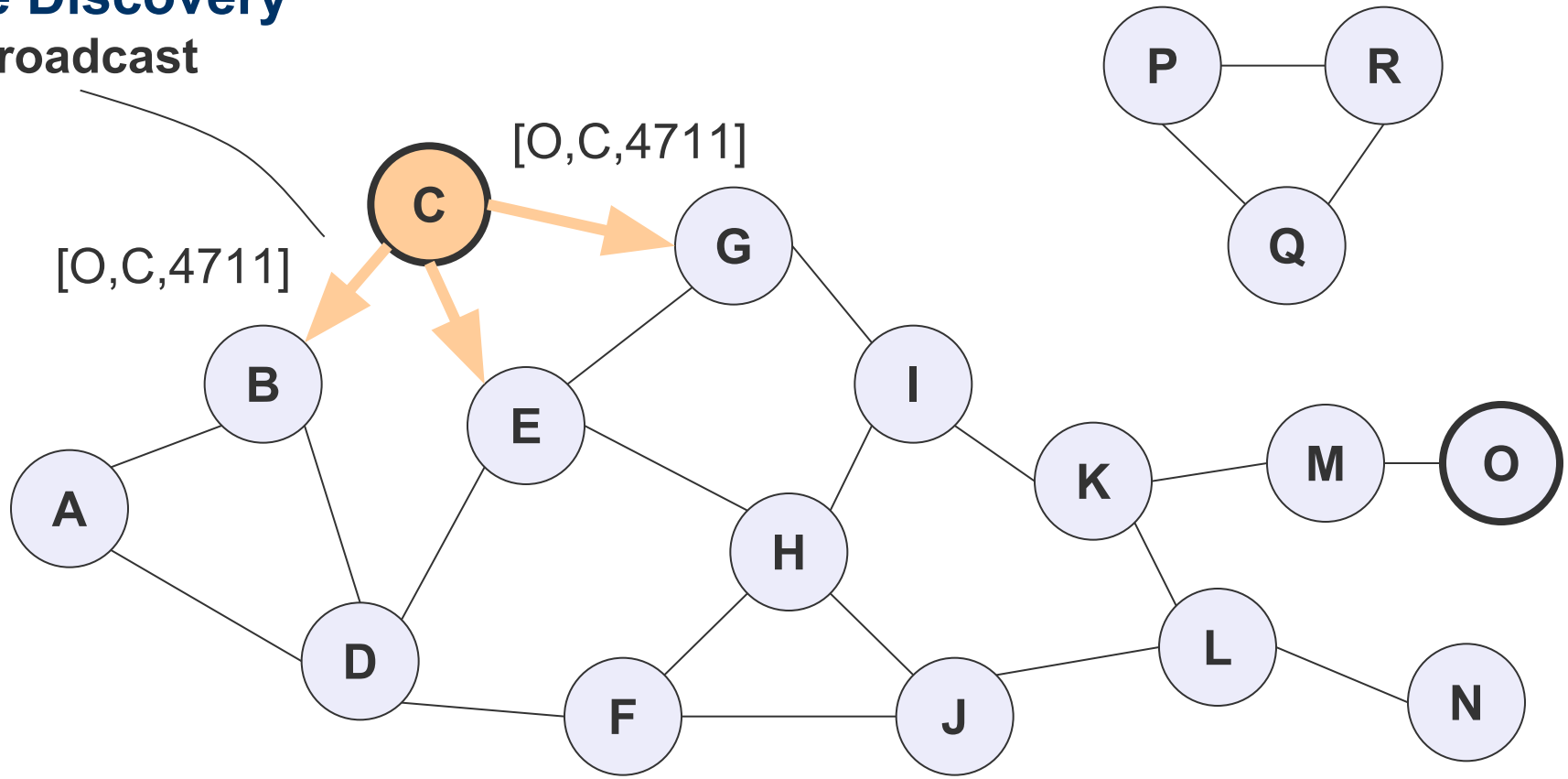
DSR: Route Discovery

Sending from C to O

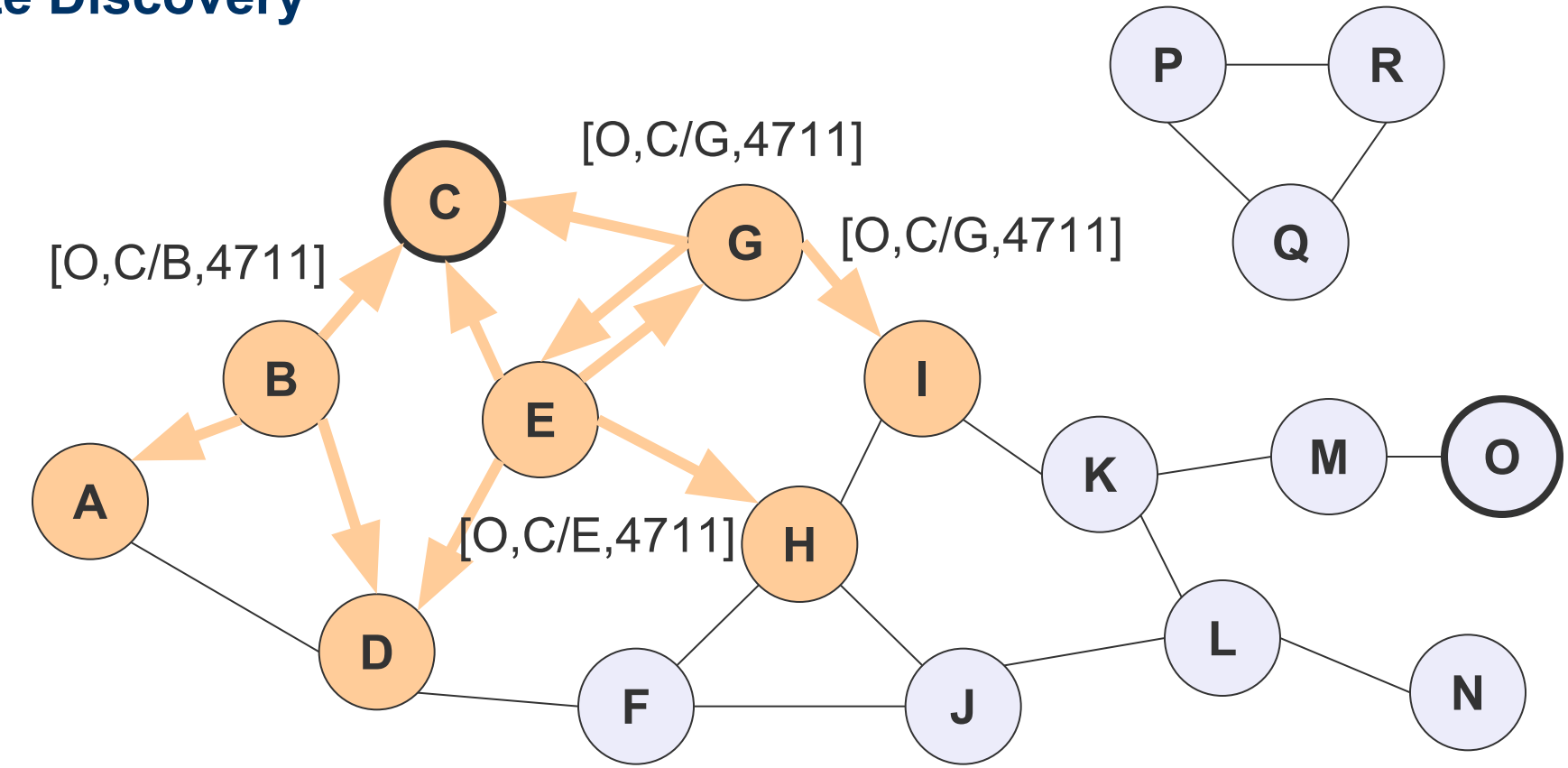


DSR: Route Discovery

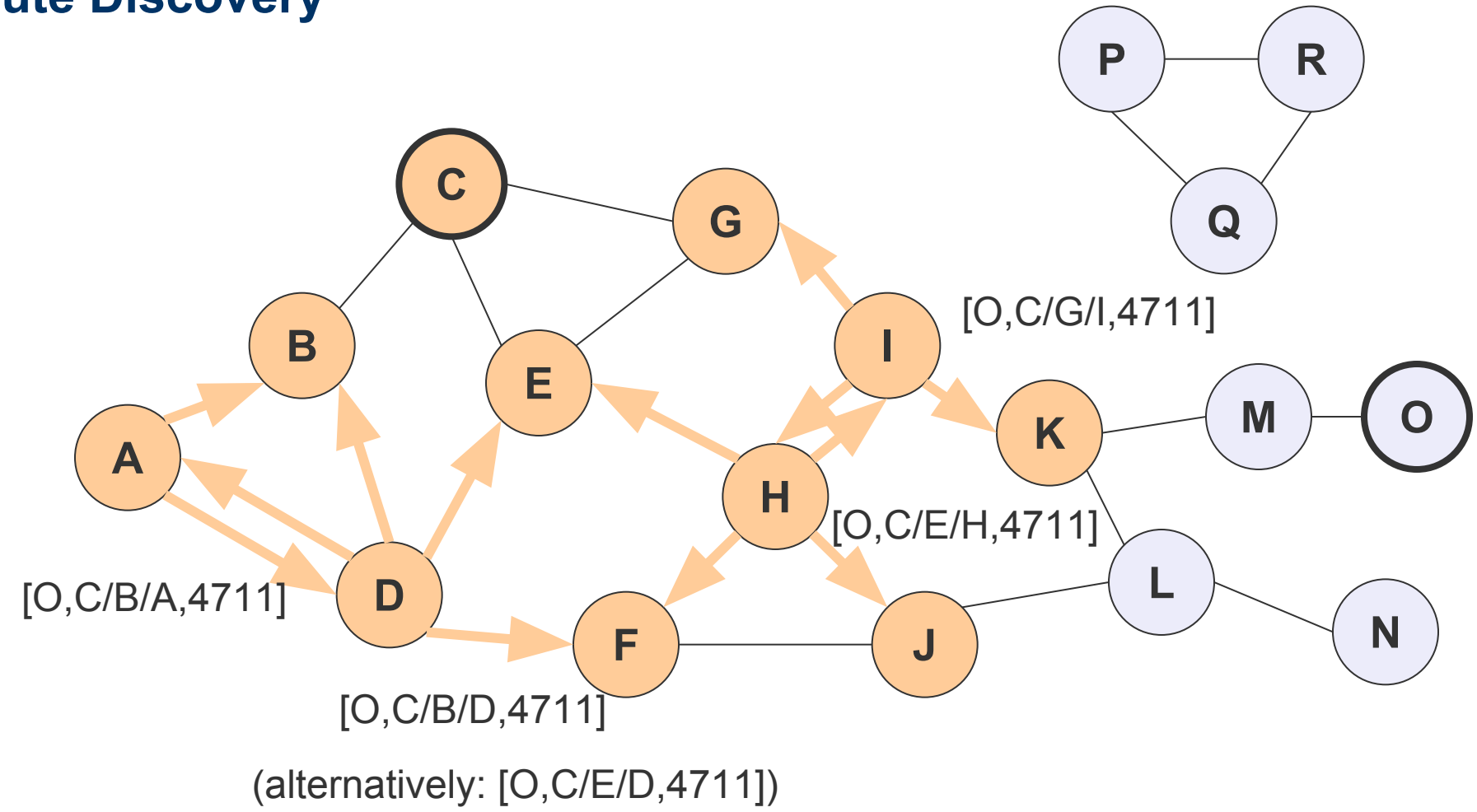
Broadcast



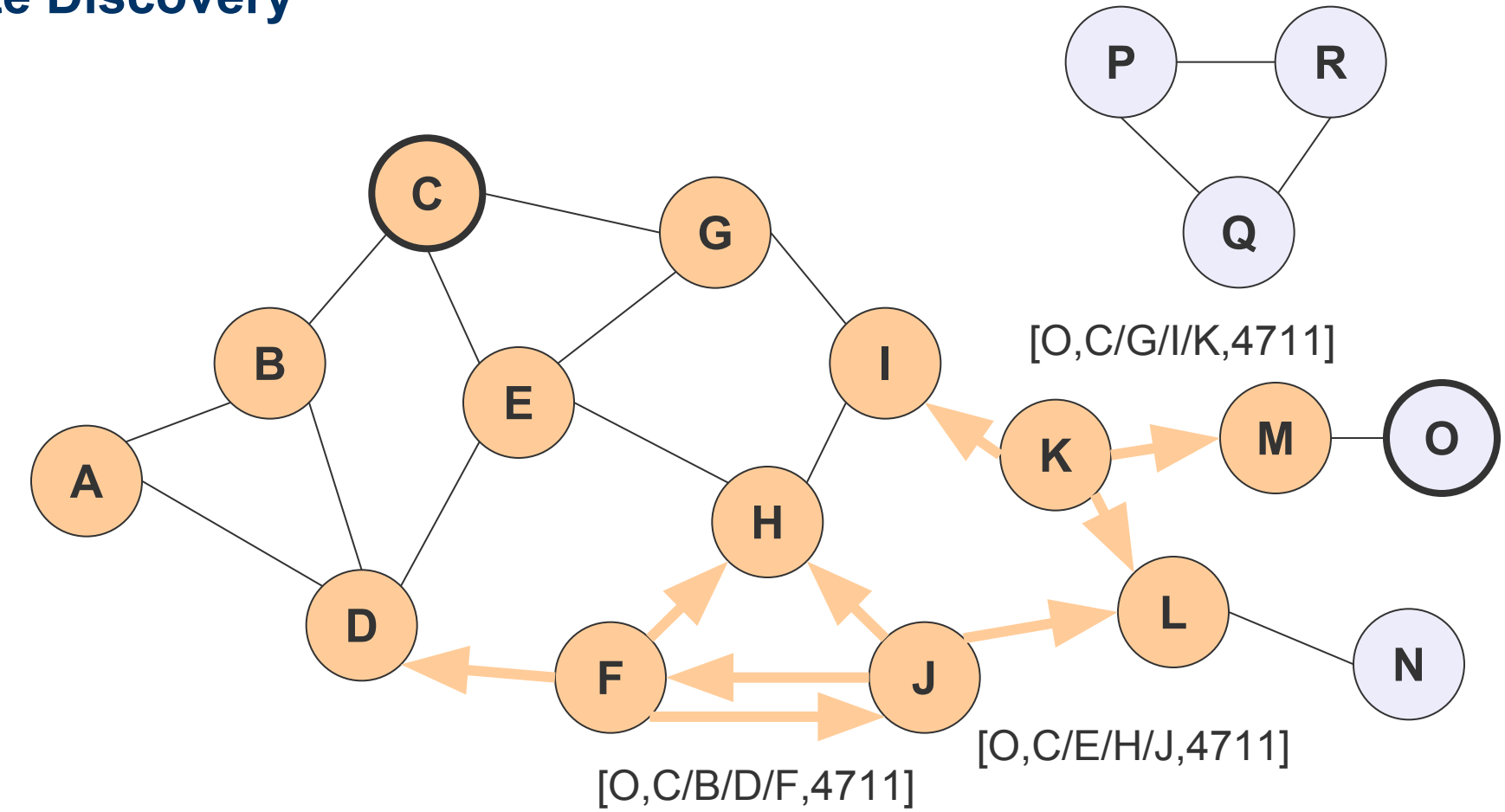
DSR: Route Discovery



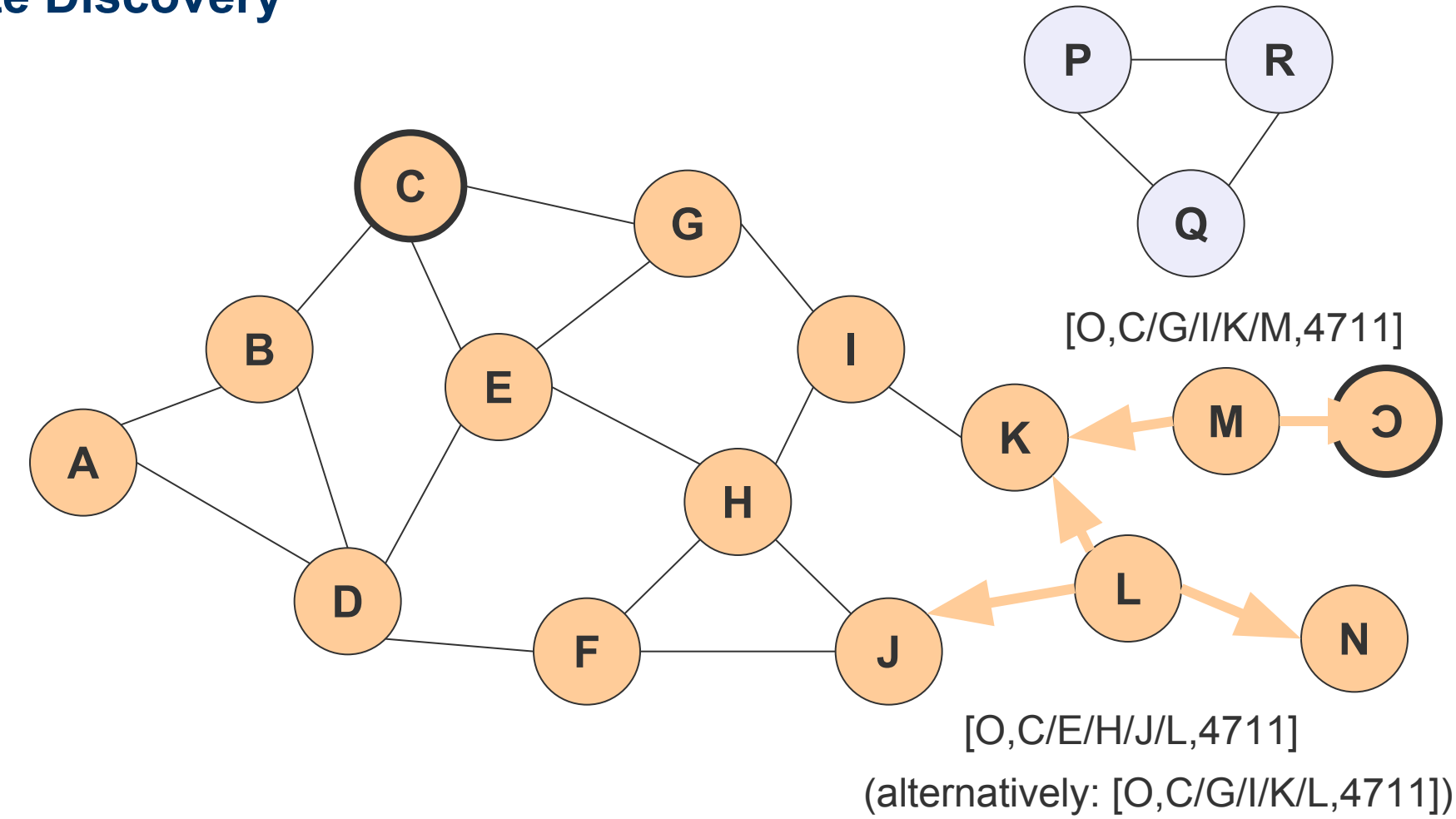
DSR: Route Discovery



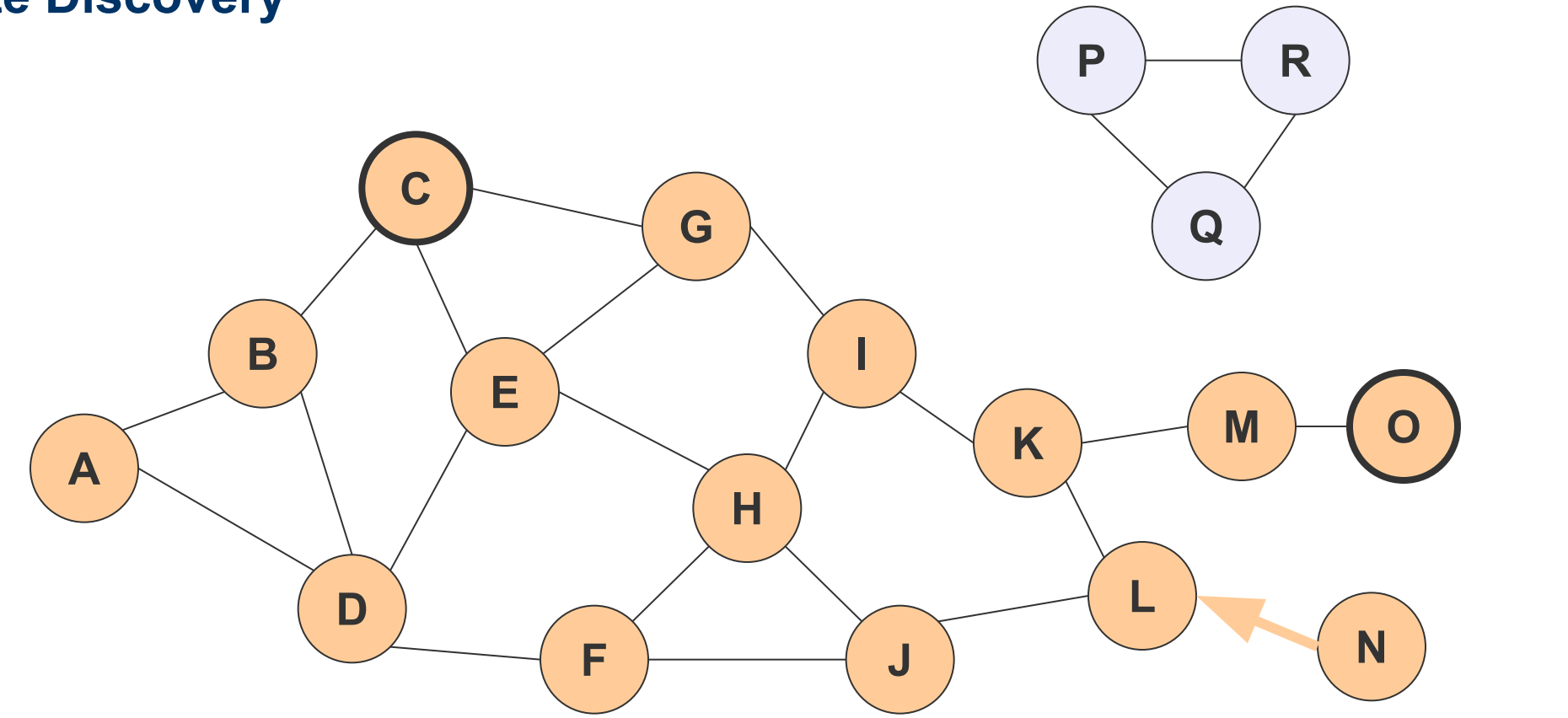
DSR: Route Discovery



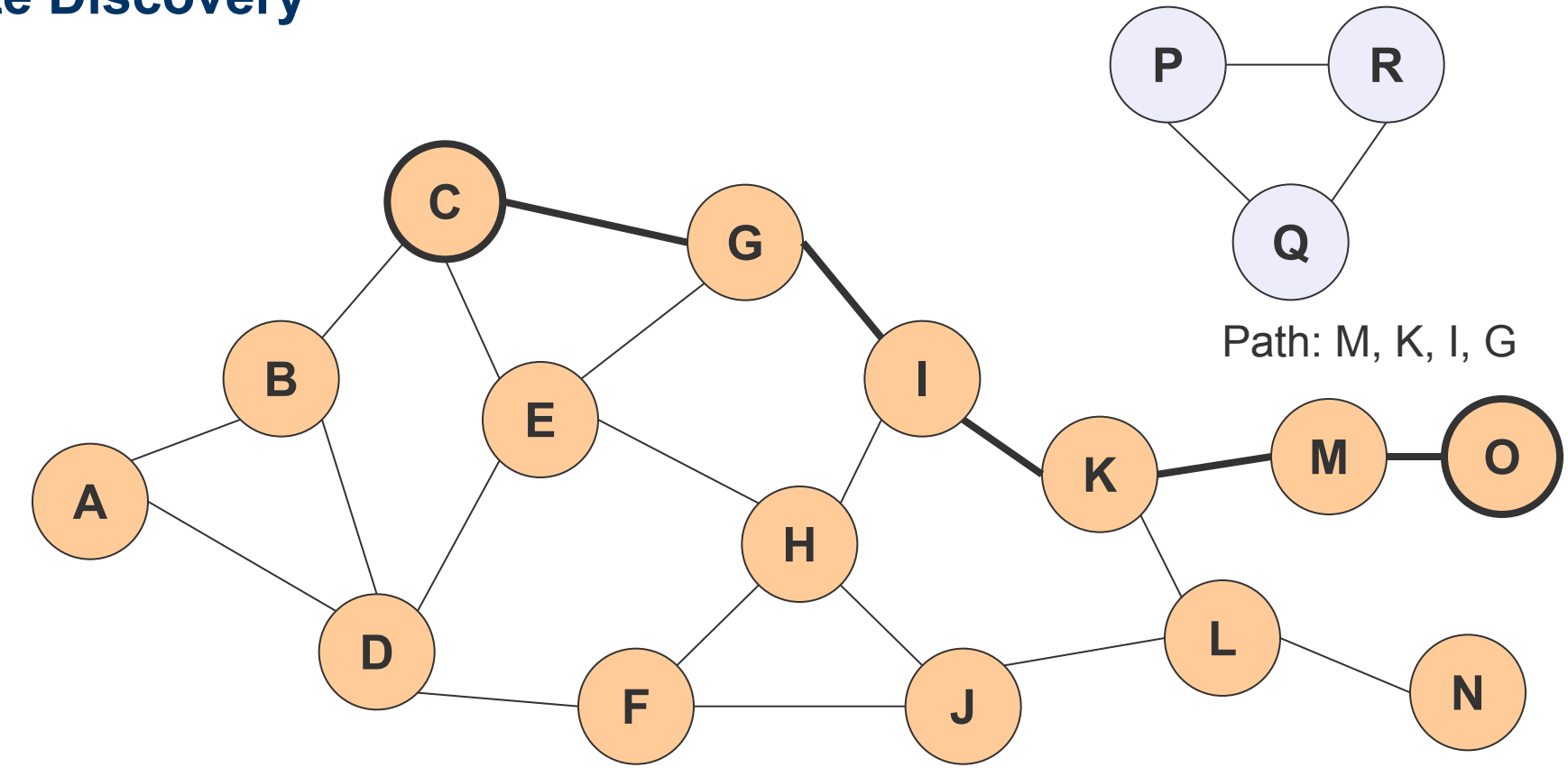
DSR: Route Discovery



DSR: Route Discovery



DSR: Route Discovery



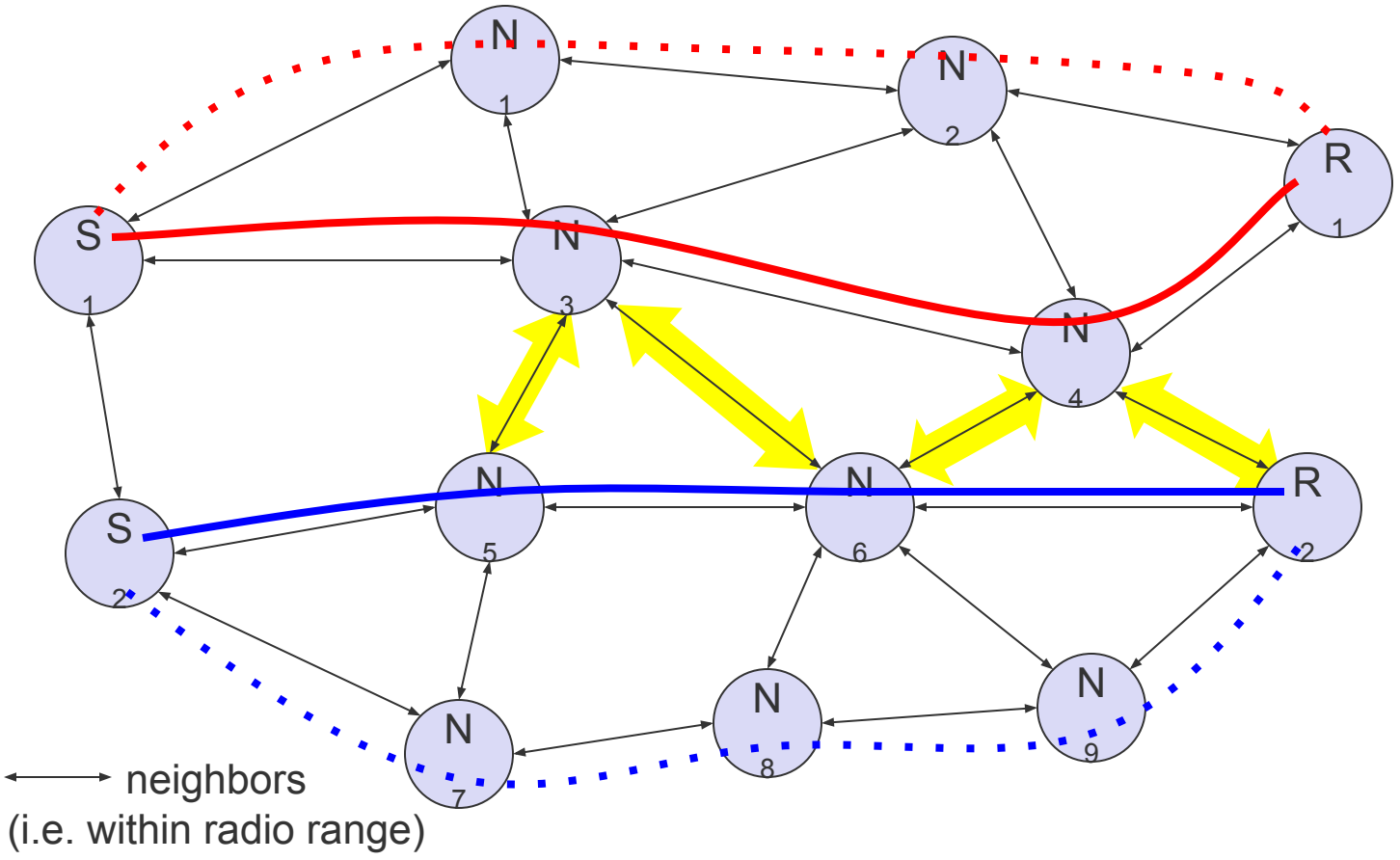
A simple example: Dynamic Source Routing III

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



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

OLSRv2: RFC 7181
- updated by 7183, 7187, 7188, 7466
- table-driven, proactive
- optimization of classic link state routing
- selection of multipoint-relays (MPRs): each 2-hop neighbor must be reachable
- flooding of topology messages only via MPRs
- different link metrics possible

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

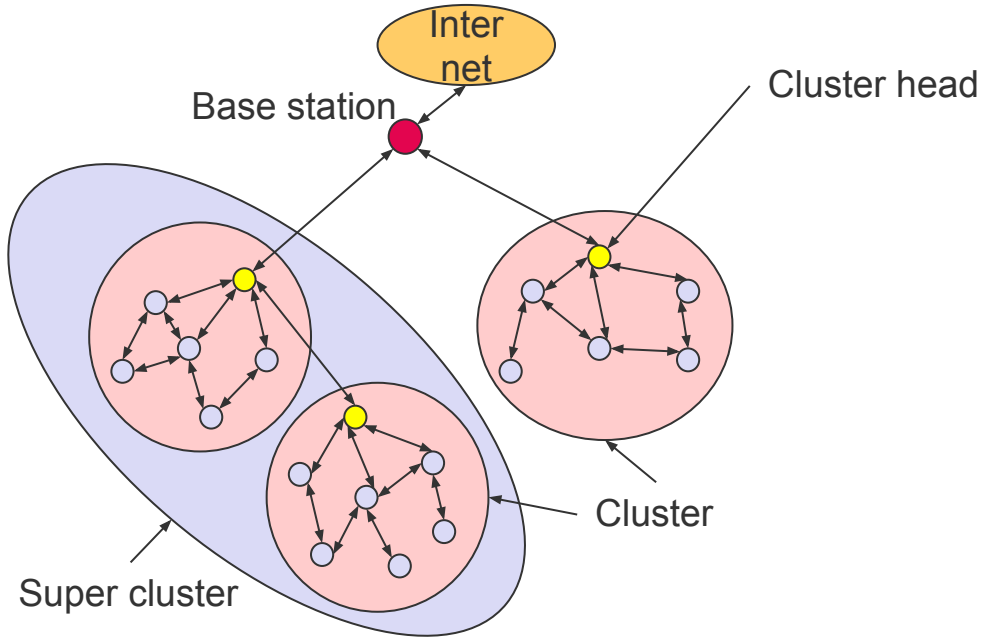
Quality-of-Service
- Maintenance of a certain transmission quality

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?

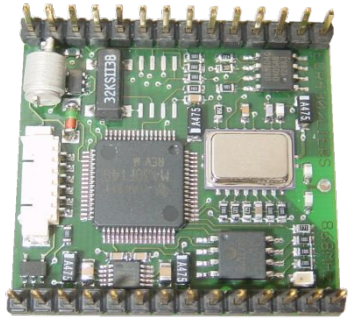
Integration with fixed networks



Questions & Tasks

- What makes routing so difficult in ad-hoc networks?
- Which problems do traditional routing algorithms have in wireless ad-hoc networks?
- What is the difference between proactive and reactive routing protocols?
- What are metrics for wireless ad-hoc routing?

The next step: Wireless Sensor Networks (WSN)



Commonalities with MANETs

- Self-organization, multi-hop
- Typically wireless, should be energy efficient

Differences to MANETs

- *Applications:* MANET more powerful, more general ↔ WSN more specific
- *Devices:* MANET more powerful, higher data rates, more resources ↔ WSN rather limited, embedded, interacting with environment
- *Scale:* MANET rather small (some dozen devices) ↔ WSN can be large (thousands)
- *Basic paradigms:* MANET individual node important, ID centric ↔ WSN network important, individual node may be dispensable, data centric
- Mobility patterns, Quality-of Service, Energy, **Cost per node** …

Properties of wireless sensor networks

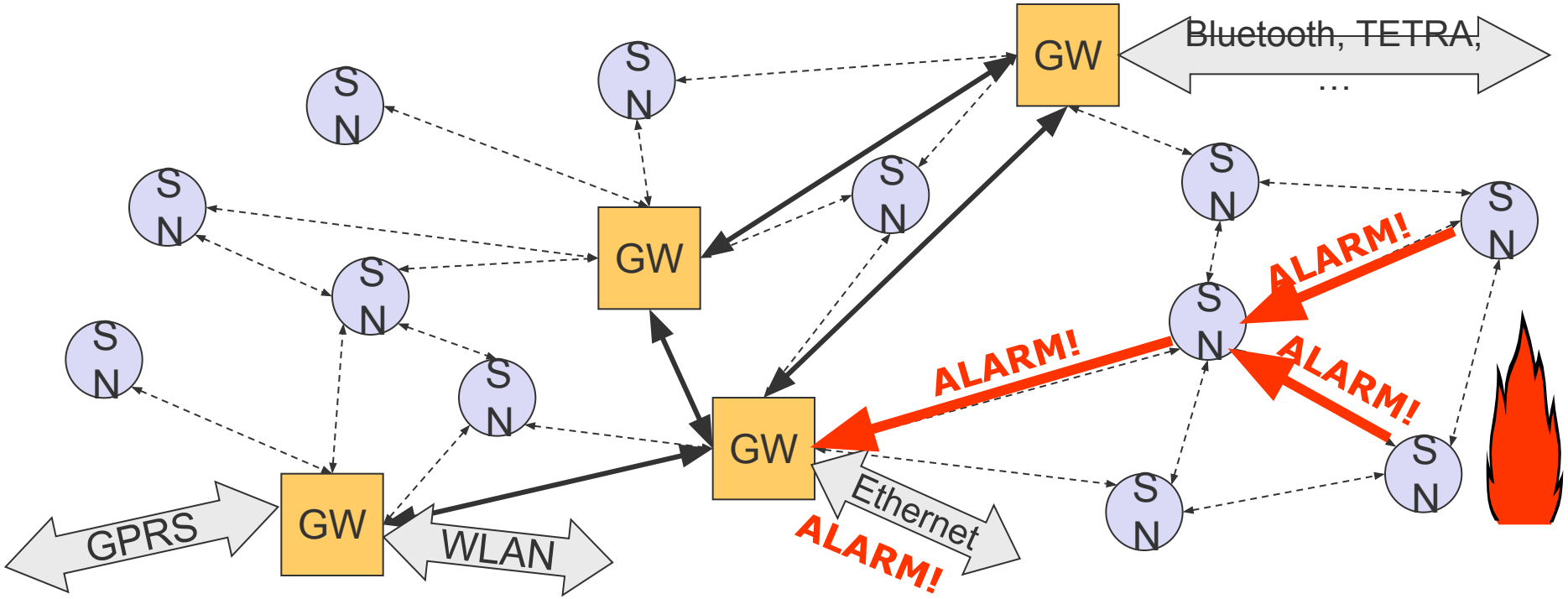
Sensor nodes (SN) monitor and control the environment

Nodes process data and forward data via radio

Integration into the environment, typically attached to other networks over a gateway (GW)

Network is self-organizing and energy efficient

Potentially high number of nodes at very low cost per node



Promising applications for WSNs

Machine and vehicle monitoring
- Sensor nodes in moveable parts
- Monitoring of hub temperatures, fluid levels …

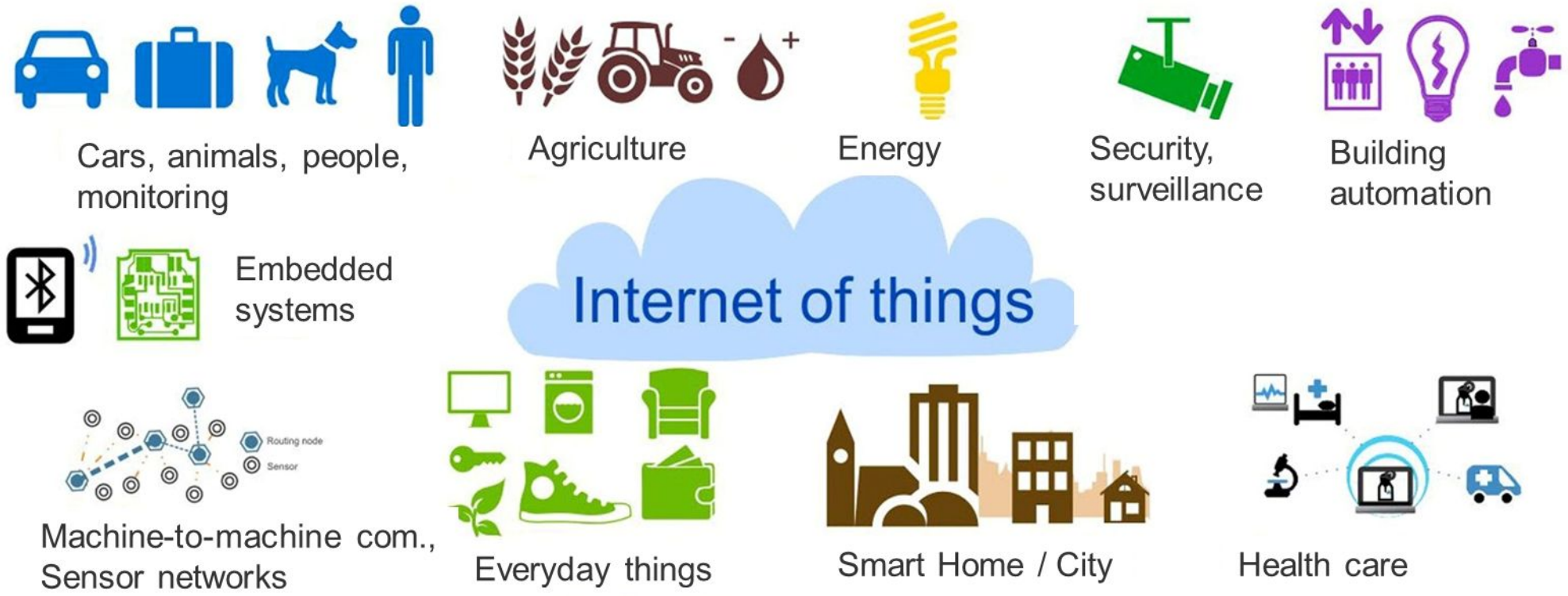
Health & medicine
- Long-term monitoring of patients with minimal restrictions
- Intensive care with relative great freedom of movement

Intelligent buildings, building monitoring
- Intrusion detection, mechanical stress detection
- Precision HVAC with individual climate

Environmental monitoring, person tracking
- Monitoring of wildlife and national parks
- Cheap and (almost) invisible person monitoring
- Monitoring waste dumps, demilitarized zones

… and many more: logistics (total asset management, RFID), telematics …
- WSNs are quite often complimentary to fixed networks!

And now… the Internet of Things!



Source: The Telecare Blog, thetelecareblog.blogspot.de, 24.10.14

One common technology for everything!

Internet of Things – is it really new?

1991: Mark Weiser

- *The Computer for the 21st Century,* ubiquitous use of IT, disappearing computer

1999: Kevin Ashton

- Coined the term *Internet of Things* in the context of logistics/supply chains, enhanced radio tags

Network of inter-connected, embedded mini computers

- Collecting and distributing data, Internet technologies as common platform, comprises enhanced RFIDs, wireless sensor networks, actors, mobile communications, “smart” objects, cyber physical systems, …
- Next generation embedded systems + wireless sensor networks + actors + Internet protocols + …

Already today, there are many more communicating systems compared to people – more than 10 billion

In the future:

- Some estimate > 25 billion end of 2020, others estimate > 50 billion – ok, there will be MANY…
- As always great expectations: 202x - 1 trillion $ revenue p.a. estimated by GSMA

Internet of Things: What is really new?

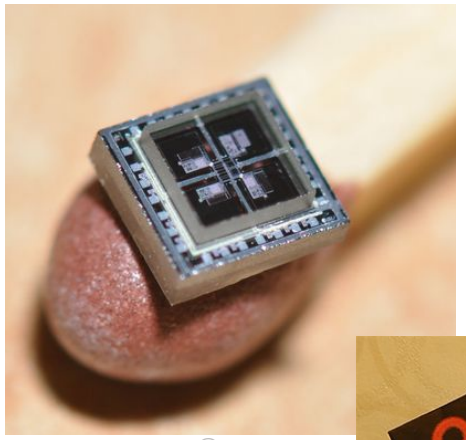
Miniaturization
- MEMS, smart everything, embedded objects

Availability of many “new” technologies
- Cloud/edge computing, big data, IPv6, 6LoWPAN, content centric networking, adapted operating systems…

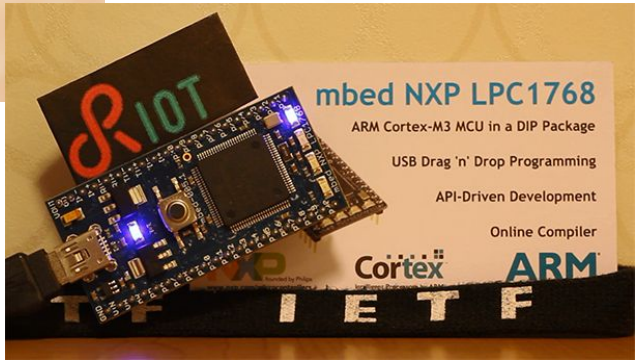
Restricted devices
- At least at the beginning wrt. firewalls, antivirus, …
- BUT we all use the same or similar protocols and interfaces

Complexity
- function(#nodes, topology, traffic pattern, stability, legacy, ?)

 All this comes together now! Possibilities and vulnerabilities…



© iecetech.org



Source: RIOT OS, www.riot-os.org
1,5 kByte RAM, 5 kByte ROM, real-time, multi-threaded

6LoWPAN

IPv6 over Low power Wireless Personal Area Networks

- RFCs (updates): 4919, 4944 (6282, 6775, 8025, 8066), 6282 (8066), 6775 (8505), 6606, 6568

Assumptions: IEEE 802.15.4 devices are limited in power/memory/energy, have long sleep cycles, are unreliable, ad-hoc deployment is typical, large number of devices will be seen, …

Problem:

- MAC layer offers only max. 81 byte for data due to PHY limits plus security mechanisms
- IPv6 header requires 40 byte, UDP additional 8 byte, leaving only 33 byte for applications

Solution:

- Compression of IPv6 and UDP headers down to 7 byte (ideal case)
- Fragmentation of packets as IPv6 requires at least 1280 byte message size
- Adaptation layer between link and network layer

D: dispatch, defines packet type (e.g., IPv6 adr., fragment, mesh…)

Questions & Tasks

- Think of mobile and wireless communications – what are specific challenges of WSNs or IoT in general?
- Which problems arise using the classical Internet protocols together with e.g. 802.15.4/ZigBee?

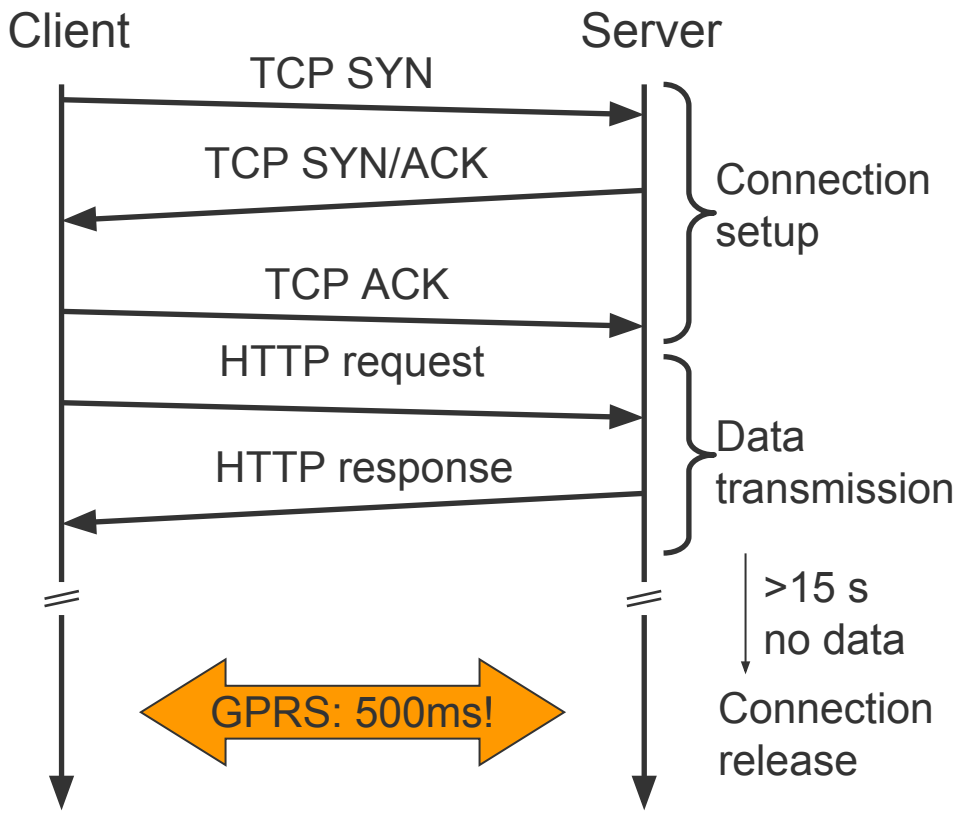
The Transport Layer

Example: HTTP (used by web services) typically uses TCP
- Reliable transport between client and server required

TCP
- Steam oriented, not transaction oriented
- Network friendly: time-out
  - congestion
  - slow down transmission

Well known – TCP guesses quite often wrong in wireless and mobile networks
- Packet loss due to transmission errors
- Packet loss due to change of network

Result
- Severe performance degradation



Motivation I

Transport protocols typically designed for
- Fixed end-systems
- Fixed, wired networks

Research activities
- Performance
- Congestion control
- Efficient retransmissions

TCP congestion control
- packet loss in fixed networks typically due to (temporary) overload situations
- router have to discard packets as soon as the buffers are full
- TCP recognizes congestion only indirect via missing acknowledgements, retransmissions unwise, they would only contribute to the congestion and make it even worse
- slow-start algorithm as reaction

Motivation II

TCP slow-start algorithm

- sender calculates a congestion window for a receiver
- start with a congestion window size equal to one segment
- exponential increase of the congestion window up to the congestion threshold, then linear increase
- missing acknowledgement causes the reduction of the congestion threshold to one half of the current congestion window
- congestion window starts again with one segment

TCP fast retransmit/fast recovery

- TCP sends an acknowledgement only after receiving a packet
- if a sender receives several acknowledgements for the same packet, this is due to a gap in received packets at the receiver
- however, the receiver got all packets up to the gap and is actually receiving packets
- therefore, packet loss is not due to congestion, continue with current congestion window (do not use slow-start)

Influences of mobility on TCP-mechanisms

TCP assumes congestion if packets are dropped

- typically wrong in wireless networks, here we often have packet loss due to *transmission errors*
- furthermore, *mobility* itself can cause packet loss, if e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while there are still packets in transit to the wrong access point and forwarding is not possible

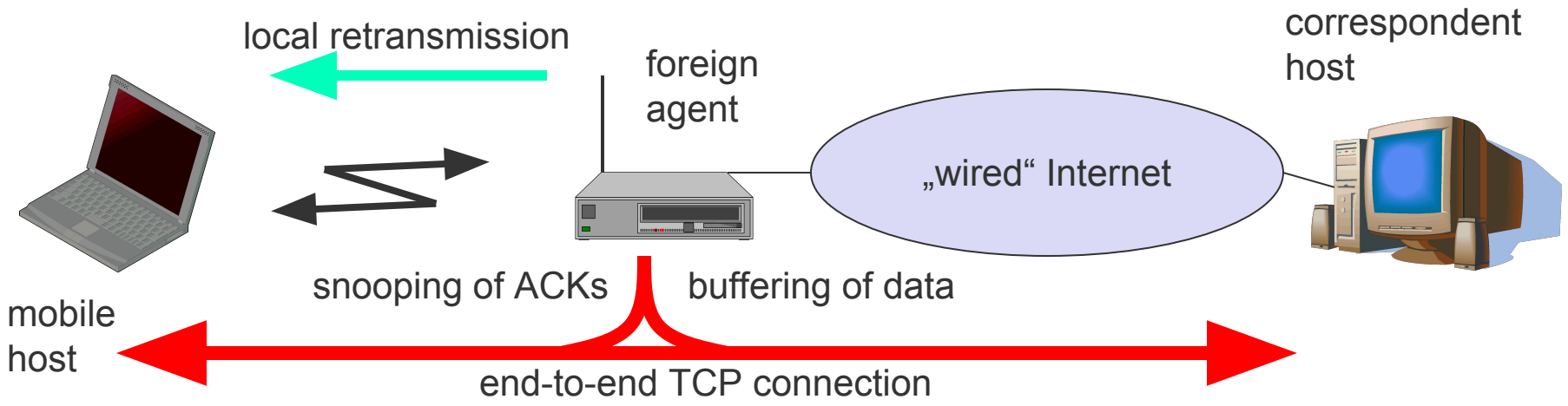
The performance of an unchanged TCP can degrade severely

- however, TCP cannot be changed fundamentally due to the large base of installations in the fixed network, TCP for mobility has to remain compatible
- the basic TCP mechanisms keep the whole Internet together

Early approach: Snooping TCP I

"Transparent" extension of TCP within the foreign agent

- buffering of packets sent to the mobile host
- lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called "local" retransmission)
- the foreign agent therefore "snoops" the packet flow and recognizes acknowledgements in both directions, it also filters ACKs
- changes of TCP only within the foreign agent



Early approach: Snooping TCP II

Data transfer to the mobile host

- FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
- fast retransmission possible, transparent for the fixed network

Data transfer from the mobile host

- FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
- MH can now retransmit data with only a very short delay

Integration of the MAC layer

- MAC layer often has similar mechanisms to those of TCP
- thus, the MAC layer can already detect duplicated packets due to retransmissions and discard them

Problems

- snooping TCP does not isolate the wireless link as good as other approaches (e.g. Indirect-TCP)
- snooping might be useless depending on encryption schemes

Fast retransmit/fast recovery

Change of foreign agent often results in packet loss

- TCP reacts with slow-start although there is no congestion

Forced fast retransmit

- as soon as the mobile host has registered with a new foreign agent, the MH sends duplicated acknowledgements on purpose
- this forces the fast retransmit mode at the communication partners
- additionally, the TCP on the MH is forced to continue sending with the actual window size and not to go into slow-start after registration

Advantage

- simple changes result in significant higher performance

Disadvantage

- further mix of IP and TCP, no transparent approach

Transmission/time-out freezing

Mobile hosts can be disconnected for a longer time
- no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or multiplexing with higher priority traffic
- TCP disconnects after time-out completely

TCP freezing
- MAC layer is often able to detect interruption in advance
- MAC can inform TCP layer of upcoming loss of connection
- TCP stops sending, but does now not assume a congested link
- MAC layer signals again if reconnected

Advantage
- scheme is independent of data

Disadvantage
- TCP on mobile host has to be changed, mechanism depends on MAC layer

Selective retransmission

TCP acknowledgements are often cumulative

- ACK *n* acknowledges correct and in-sequence receipt of bytes up to *n-1* (byte-stream oriented!)
- if single packets are missing quite often a whole packet sequence beginning at the gap has to be retransmitted (go-back-n), thus wasting bandwidth

Selective retransmission as one solution

- RFC2018 allows for acknowledgements of single packets, not only acknowledgements of in-sequence packet streams without gaps
- sender can now retransmit only the missing packets (i.e. non acknowledged parts of the byte-stream)

Advantage

- much higher efficiency

“Disadvantage”

- more complex software in a receiver, more buffer needed at the receiver
- Might be a problem in really tiny devices…

Comparison of different approaches for a “mobile” TCP

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	isolation of wireless link, simple	loss of TCP semantics, higher latency at handover
Snooping TCP	“snoops” data and acknowledgements, local retransmission	transparent for end-to-end connection, MAC integration possible	problematic with encryption, bad isolation of wireless link
M-TCP	splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast retransmit/ fast recovery	avoids slow-start after roaming	simple and efficient	mixed layers, not transparent
Transmission/ time-out freezing	freezes TCP state at disconnect, resumes after reconnection	independent of content or encryption, works for longer interrupts	changes in TCP required, MAC dependant
Selective retransmission	retransmit only lost data	very efficient	slightly more complex receiver software, more buffer needed
Transaction oriented TCP	combine connection setup/release and data transmission	Efficient for certain applications	changes in TCP required, not transparent

TCP Improvements I

Initial research work
- Indirect TCP, Snoop TCP, M-TCP, T/TCP, SACK, Transmission/time-out freezing, …

$$BW \leq \frac{0.93 * MSS}{RTT * \sqrt{p}}$$

- max. TCP **B**and**W**idth
- **M**ax. **S**egment **S**ize
- **R**ound **T**rip **T**ime
- loss **p**robability

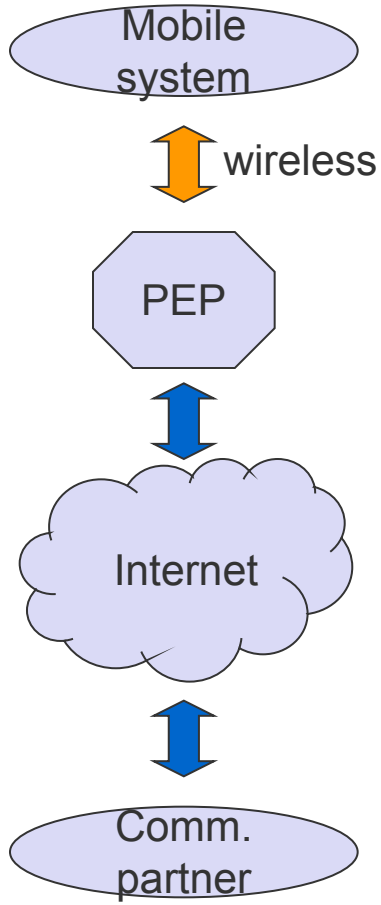
TCP over 2.5/3G wireless networks
- Fine tuning of TCP, RFC3481 – best current practice (BCP 71, 2003)
- Learn to live with *sometimes*
  - Data rates: 64 kbit/s up, 115-384 kbit/s down; asymmetry: 3-6, but also up to 1000 (broadcast systems), periodic allocation/release of channels
  - High latency, high jitter, packet loss
- Suggestions
  - Large (initial) sending windows, large maximum transfer unit, selective acknowledgement, explicit congestion notification, time stamp, no header compression
- Widespread use in adapted protocol stacks
  - "Historical": i-mode running over FOMA, WAP 2.0 ("TCP with wireless profile")

Alternative congestion control algorithms
- TCP Vegas (cong. control with focus on packet delay, rather than packet loss)
- TCP Westwood plus (use ACK stream for better setting cong. control), (New) Reno, Santa Cruz, …

TCP Improvements II

Performance enhancing proxies (PEP, RFC 3135)
- Transport layer
  - Local retransmissions and acknowledgements
- Additionally on the application layer
  - Content filtering, compression, picture downscaling
  - E.g., Internet/WAP gateways
  - Web service gateways?
- Big problem: breaks end-to-end semantics
  - Disables use of IP security
  - Choose between PEP and security!

More open issues
- RFC 3150 / BCP 48 (slow links)
  - Recommends header compression, no timestamp
- RFC 3155 / BCP 50 (links with errors)
  - States that explicit congestion notification cannot be used
- In contrast to 2.5G/3G recommendations!



Questions & Tasks

- What are the problems of using TCP over wireless links?
- Why do many “enhancements” fail or are not wide-spread?
- What should wireless systems optimize in favor of TCP performance?