Introduction to Wireless and Mobile Networking

Lecture: Mobile IP

Hung-Yu Wei
National Taiwan University

Overview of Mobile IP

- IP
  - IP address is widely used
  - IP routing
- Mobile
  - Need to support mobility
- How does mobility affect the protocol design?
  - Delivering IP packets to mobile nodes

Network Layer (Layer-3)

- Routing
  - Important issue in "mobile" network
- IP-based network solution
  - IP dominates the networking world!
- Mobile network routing
  - Mobility management protocols
    - Global mobility management protocols
      - Mobile IP
    - Local mobility management protocols
      - Cellular IP, HAWAII
  - Ad hoc network routing protocols
    - AODV, DSR, OLSR, DSDV…etc

IP-based Mobility

- Mobile IP
  - IETF (www.ietf.org) Internet Engineering Task Force
    - Mobile IP working group
      - RFCs (Request for Comments)
  - Mobile IPv4
    - RFC 3344
  - Mobile IPv6
    - RFC 3775

What is Mobile IP?

- Basic Mobile IP protocol
  - Advertisement
  - Registration
  - Tunneling datagrams
- Extensions
  - Route optimizations
  - Movement detection issues
- Other related protocols
  - DHCP, AAA, micro-mobility

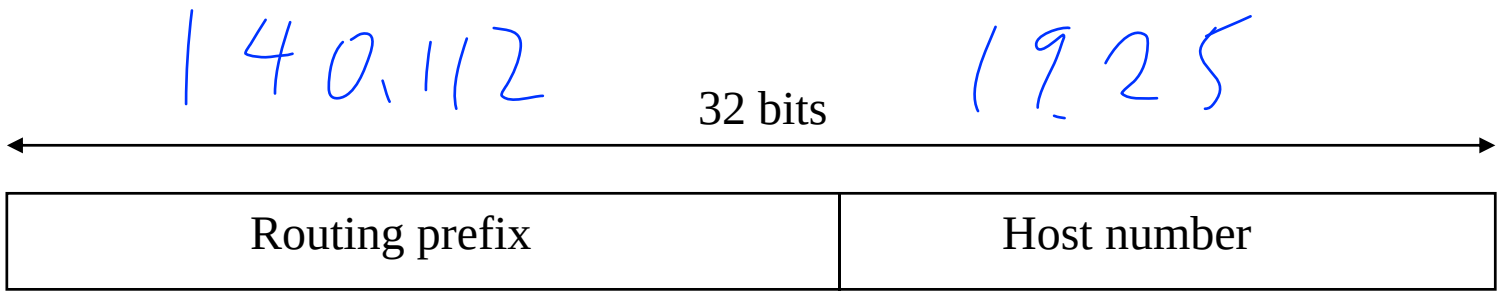
dynamic IP assign

The IP Addressing Problem

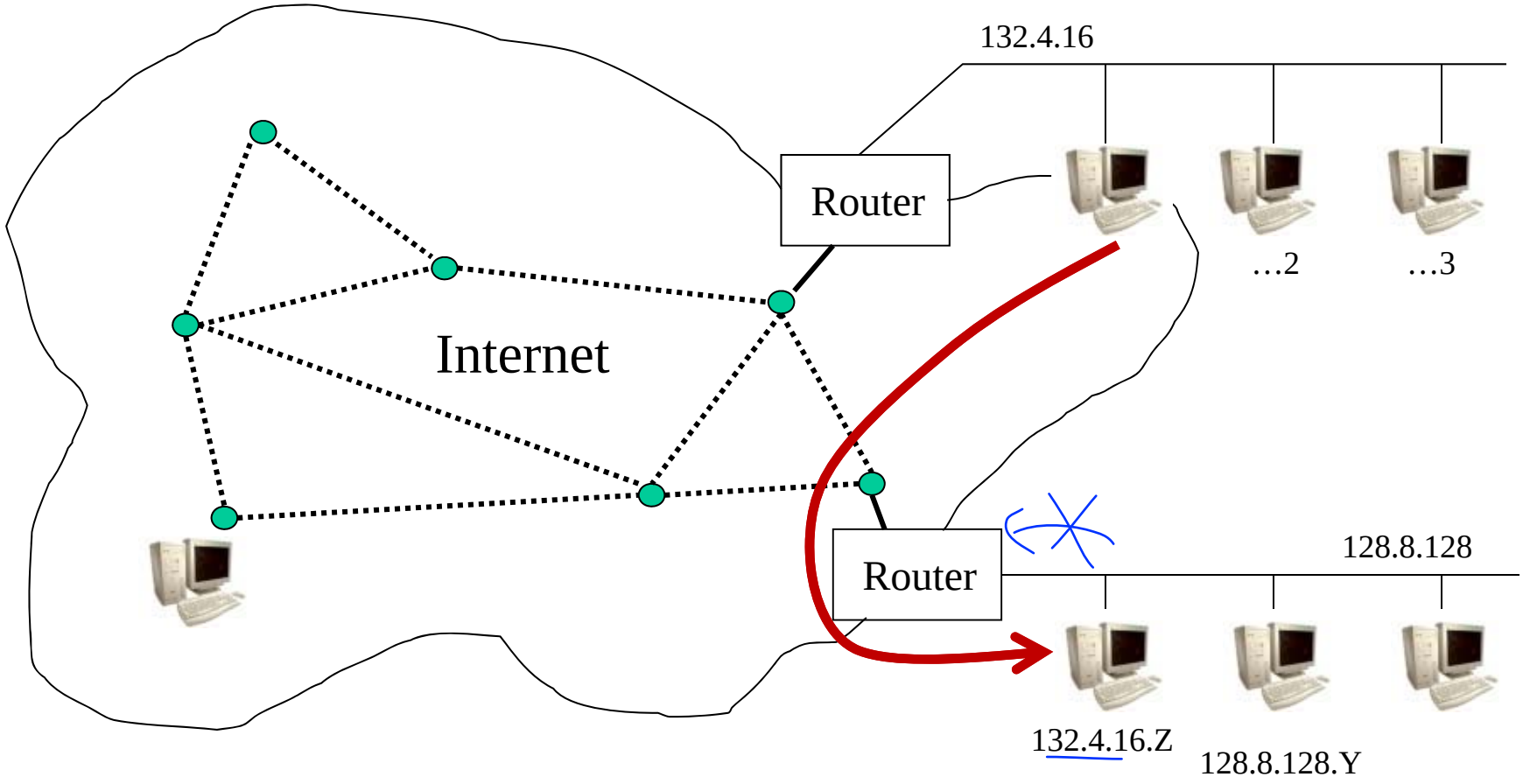
- IP address allocation and administration
  - Assume a close relationship between a computer's IP address and its physical location
- Mobile networks
  - Change of physical locations

Review: IP Address Structure

- Routing prefix
  - defines the network on which the address resides
  - often determined the netmask
  - usually subnet prefix
- Host number
  - fits in the least significant remaining bits of the IP address following the routing prefix

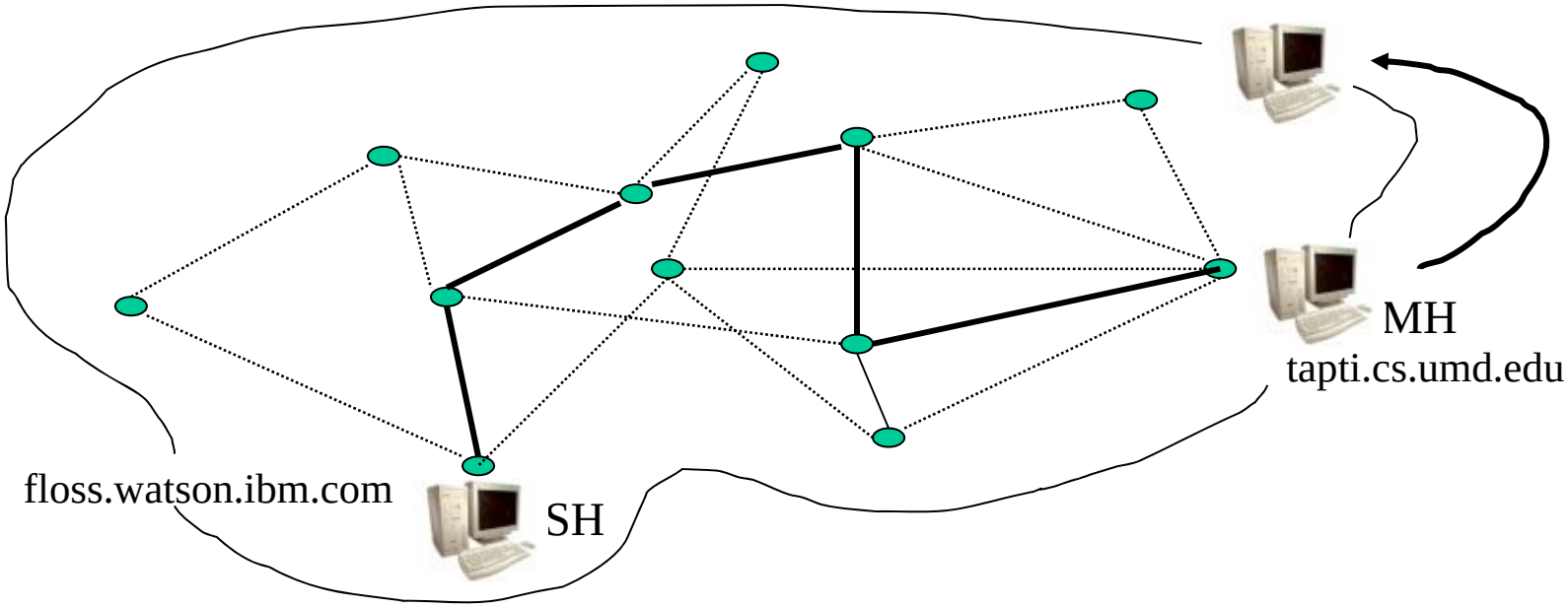


IP Subnet Model vs. Mobility



The Transport Problem: TCP/IP

- TCP uses ports and the IP addresses of the network endpoints to identify a communication channel used for data transfer



Dual use of IP Addresses

- Applications use IP addresses
  - to identify routes by which datagrams my be exchanged between two network nodes
- Applications use IP addresses
  - to identify the endpoints themselves
- Problems due to dual usage
  - Using applications (e.g., TCP) when changing the hosts point of attachment

Solution

- We observe that
  - Applications need an unchanging way to identify the network endpoints
  - Routes between the endpoints must change as they move
- Mobile IP solves this issue
  - by maintaining two addresses; one for each of the dual usage
    - Identification
    - Routing
  - one IP address is used to “locate” the mobile host
  - the other IP address for “identifying” a communications endpoint on the mobile host

Concept: home network and foreign network

- Home network
  - Home address: home network should have the same prefix for mobile nodes' home addresses
- Foreign network
  - A network that is not home network
- Mobility agents
  - Agents that handle IP-mobility
    - Home Agent
    - Foreign Agent

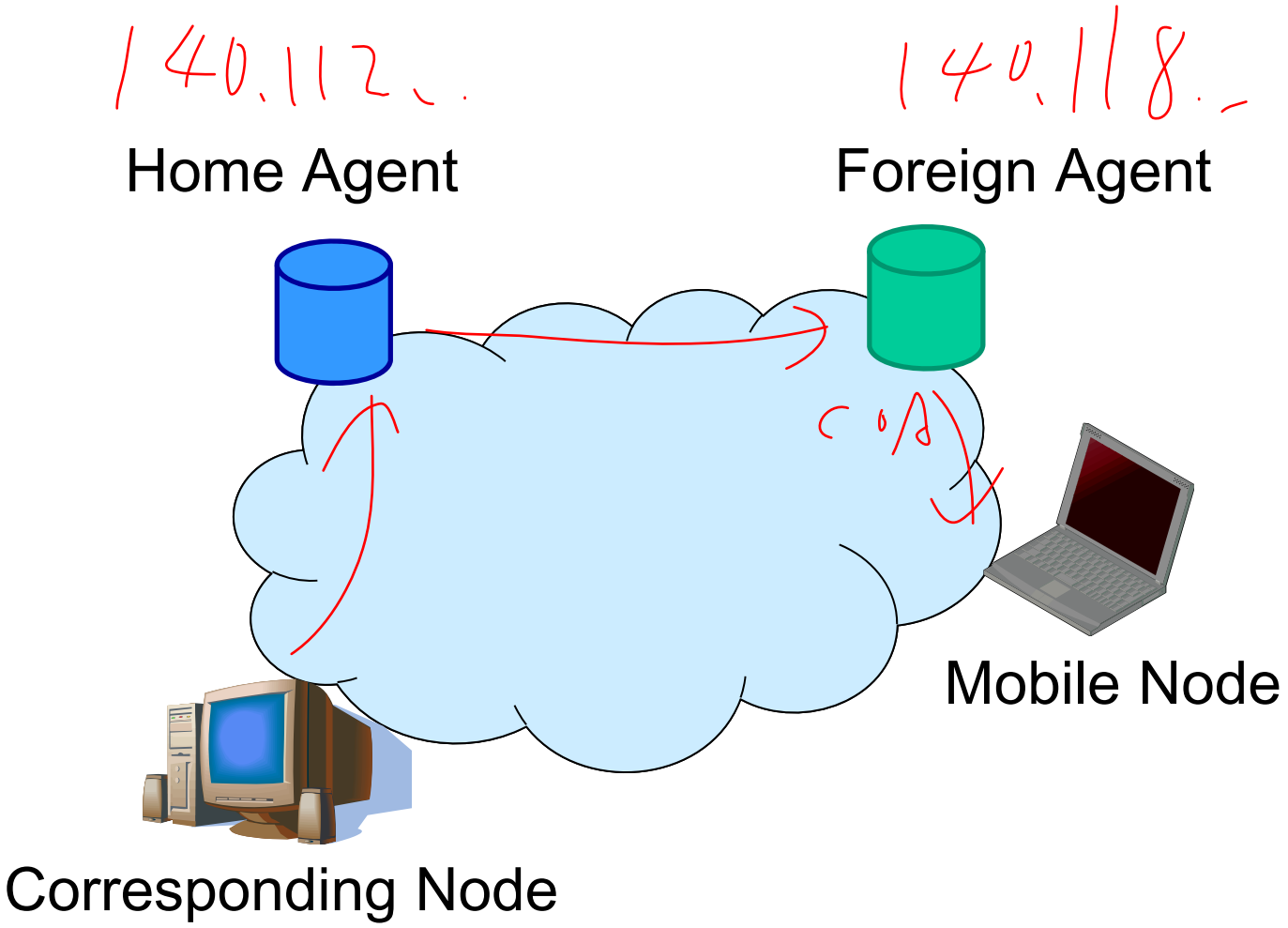
Mobility Management Model

- Home network and Packet Forwarding
  - packets are routed toward the home address
    - source node is unaware of whether the destination is mobile or not; it simply sends to the home address
- Care-of-address (CoA)
  - Care-of-address is used to locate the mobile host's current position
  - "readdressing" is the operation used to change the destination address (home address) to the care-of-address

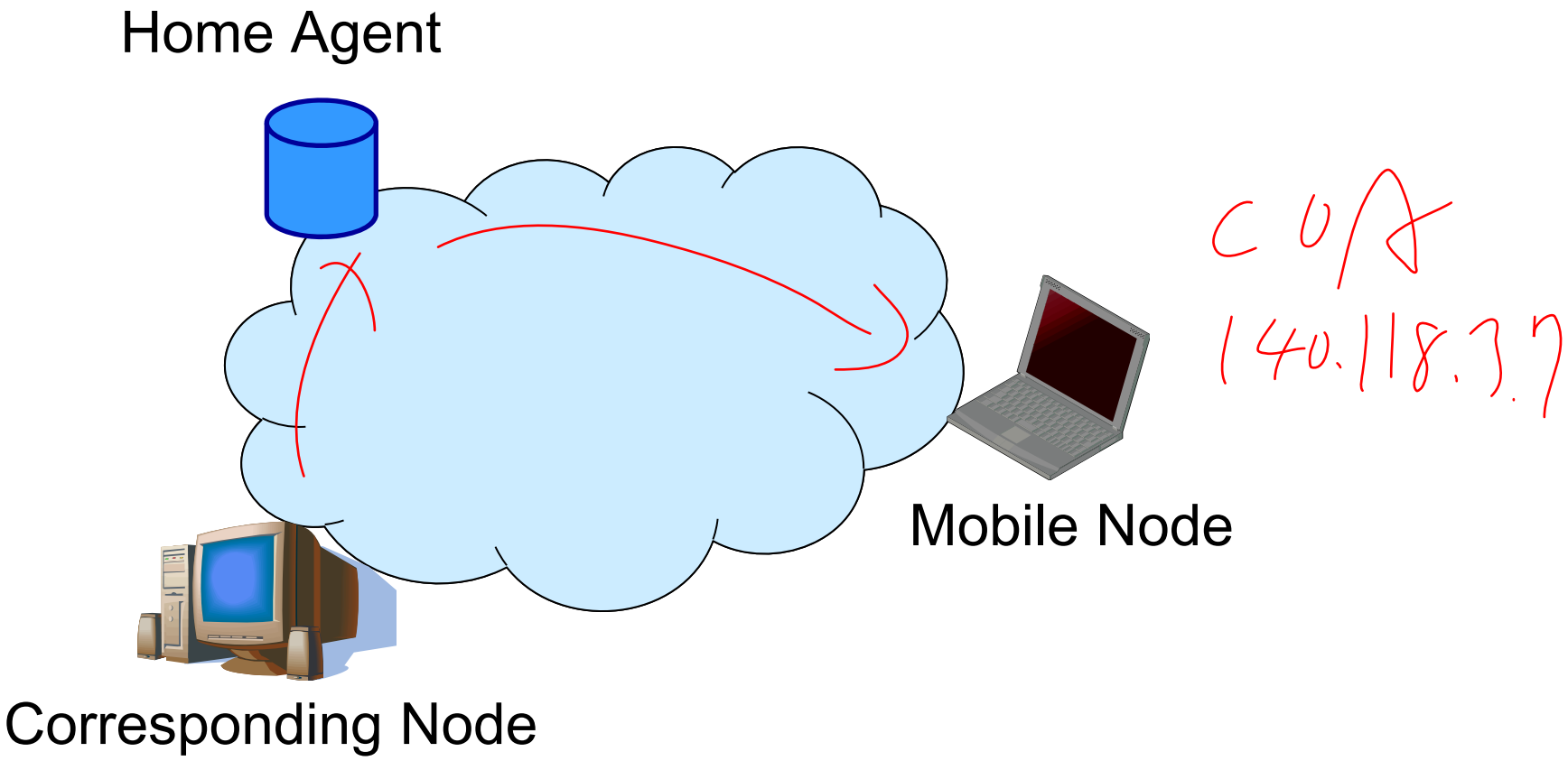
Summary: Terminologies

- 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

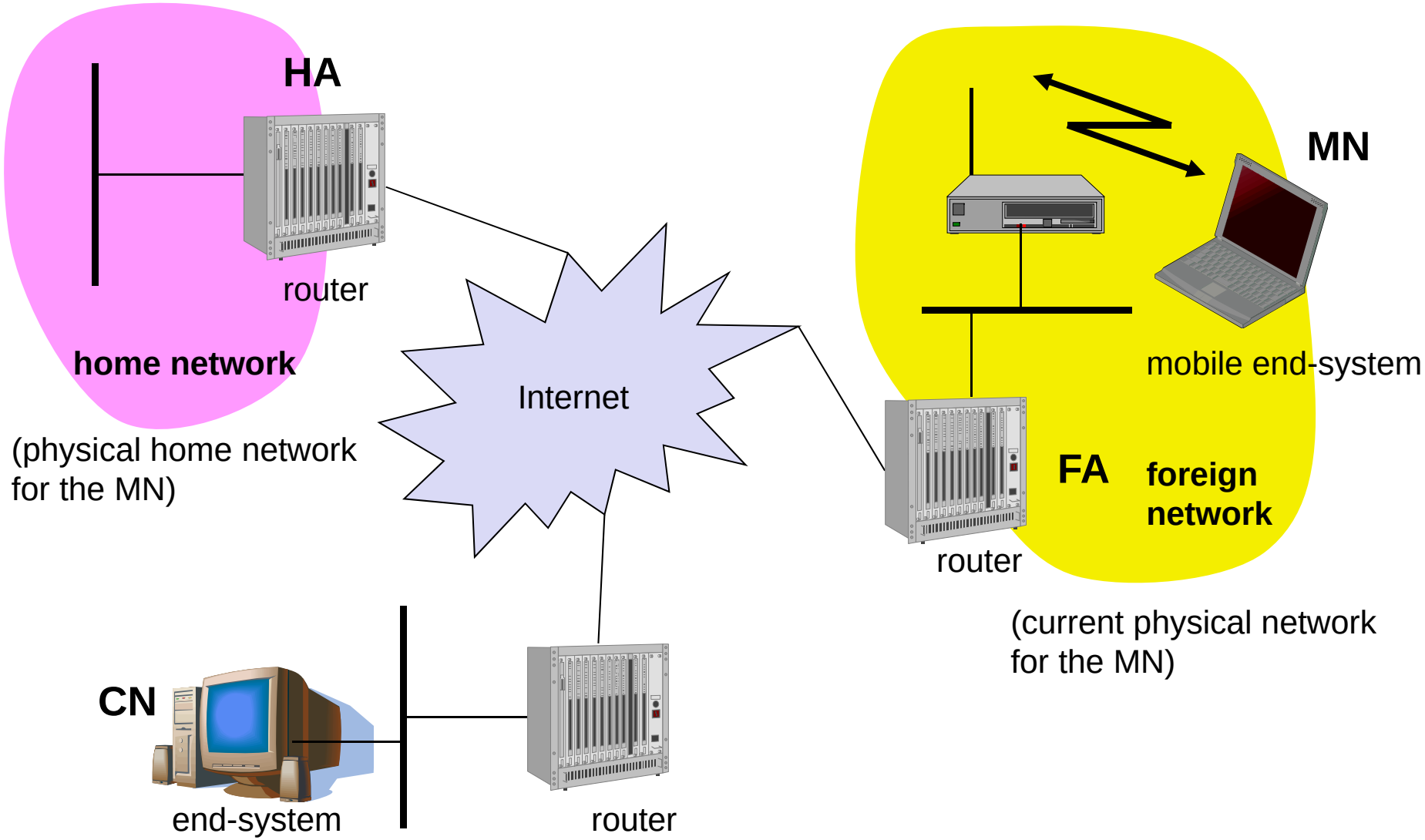
Mobile IP: Foreign Agent Mode



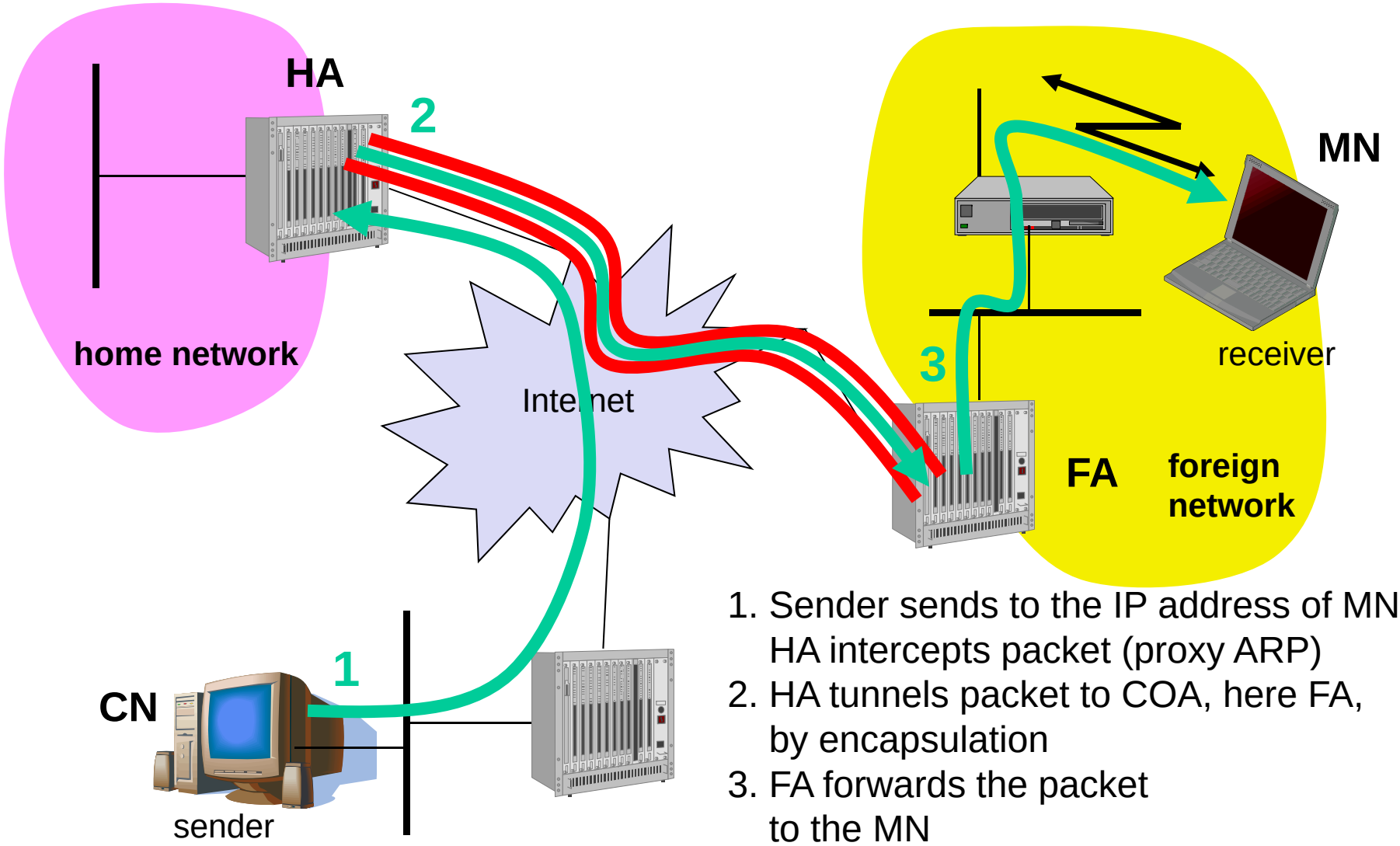
Mobile IP: Co-located CoA



Example network

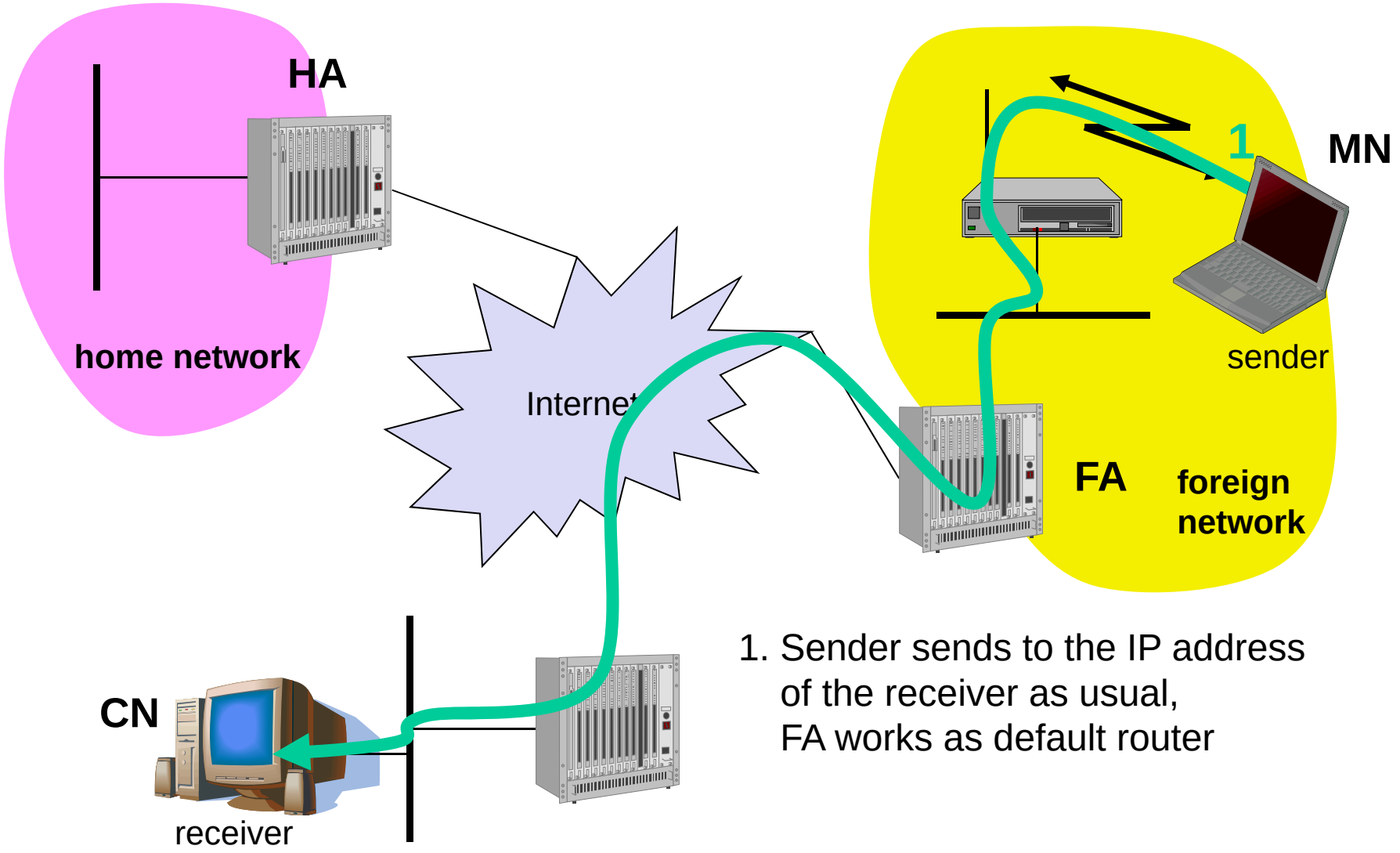


Data transfer to the mobile system



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

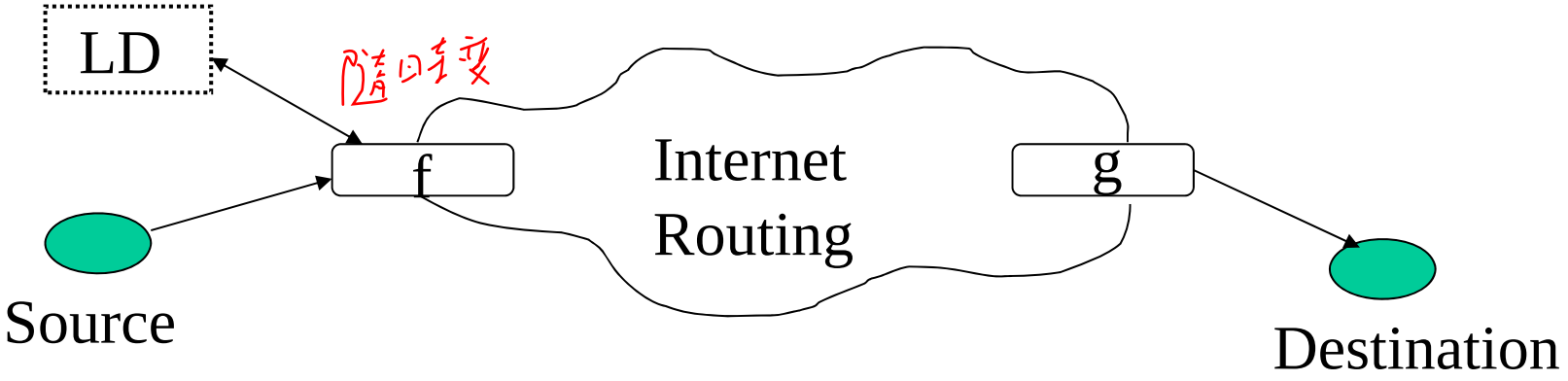
Data transfer from the mobile system



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

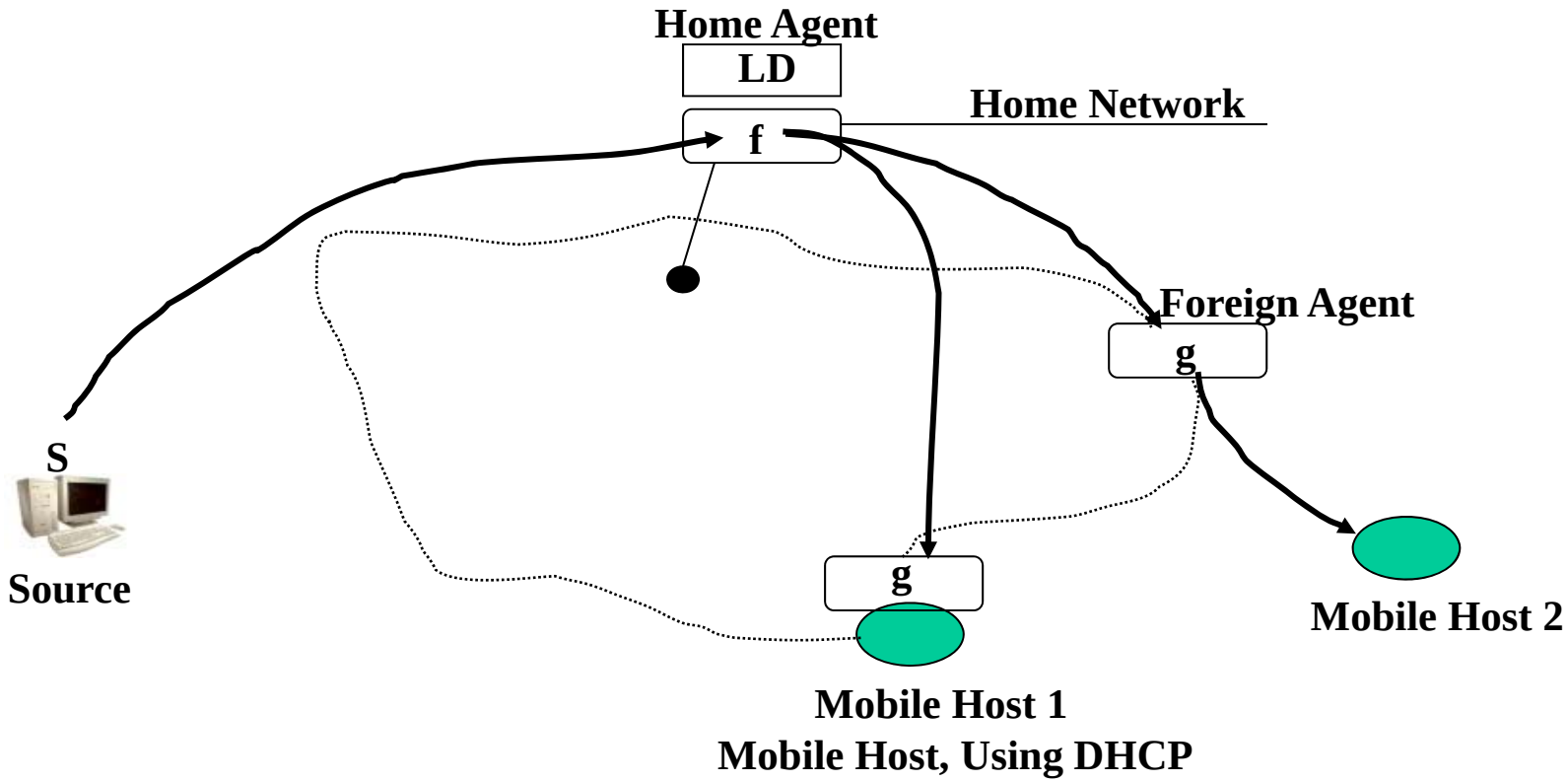
Abstract Model

- Two mapping functions
  - f(home address) → (forwarding address)
  - g(forwarding address) → (home address)
- Readdressing (f) at the home network
  - associating (in the location directory - LD) the home address and the care-of-address of the mobile host and maintaining up to date values for this association
  - delivering the datagram to the care-of-address
- Inverting (g) the readdressing operation once the datagram arrives at the care-of-address



Abstract Model: Mobile IP

- Mobile IPv4
  - (1) Co-located mode
  - (2) FA mode



Overview of Mobile IP operations

Basic Mobile IP Operations

- Operations
  - Agent discovery
    - Advertisement
    - Solicitation
  - Registration
  - Tunneling
- 2 modes (categorize by care-of-address)
  - FA as CoA
  - Co-located CoA

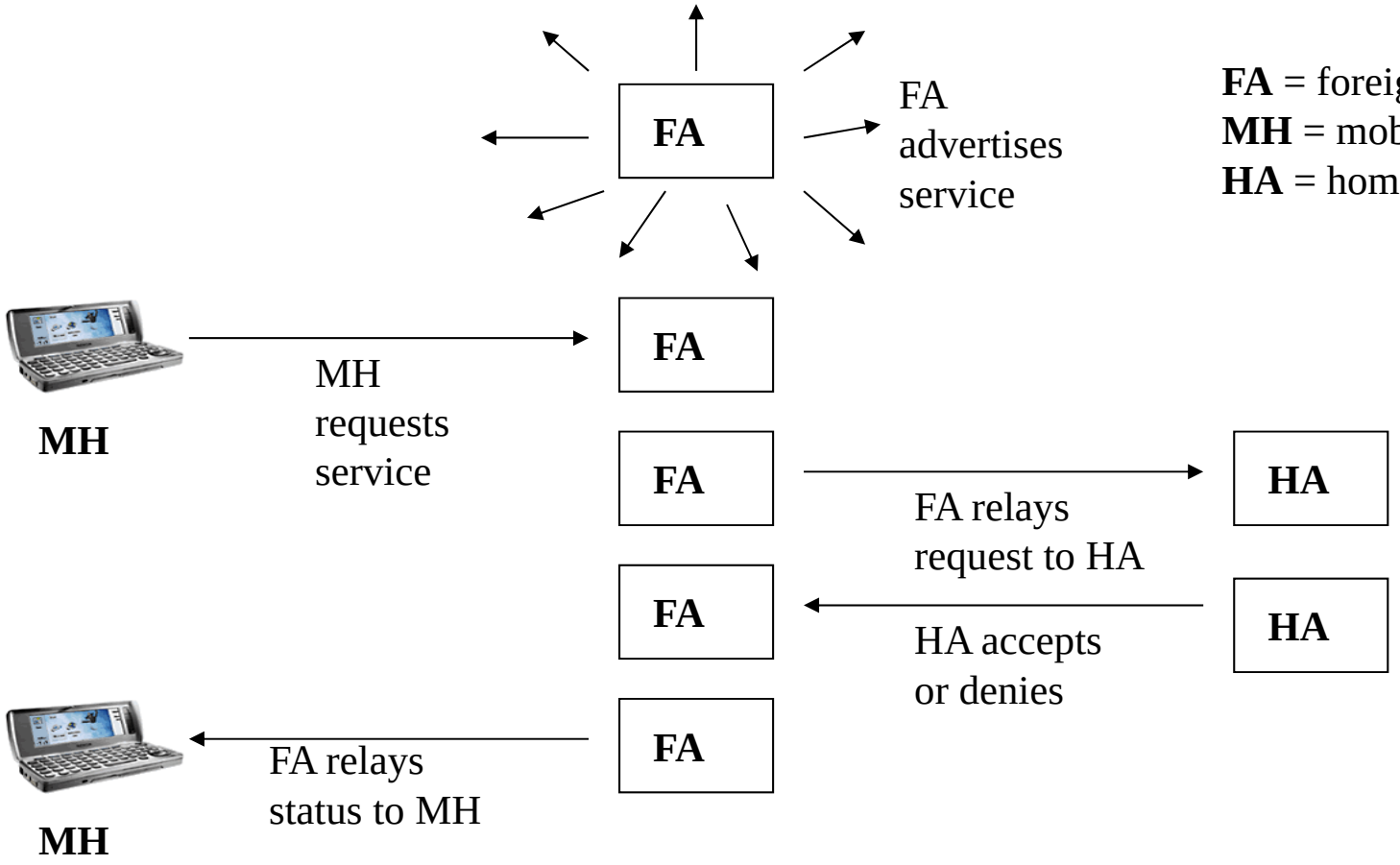
Agent Discovery

- Agent discovery
  - home agent and foreign agents may advertise their availability
  - a newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present
- Types of agent discovery mechanisms
  - HA (or FA) initiated
    - advertisement
  - MN initiated
    - solicitation

Registration

- Registration
  - when the mobile node is away from home, it registers its care of address (CoA) with its home agent
  - depending on its method of attachment, the mobile node will register either
    - Directly with its home agent
    - OR though a foreign agent, which forwards the registration to the home agent

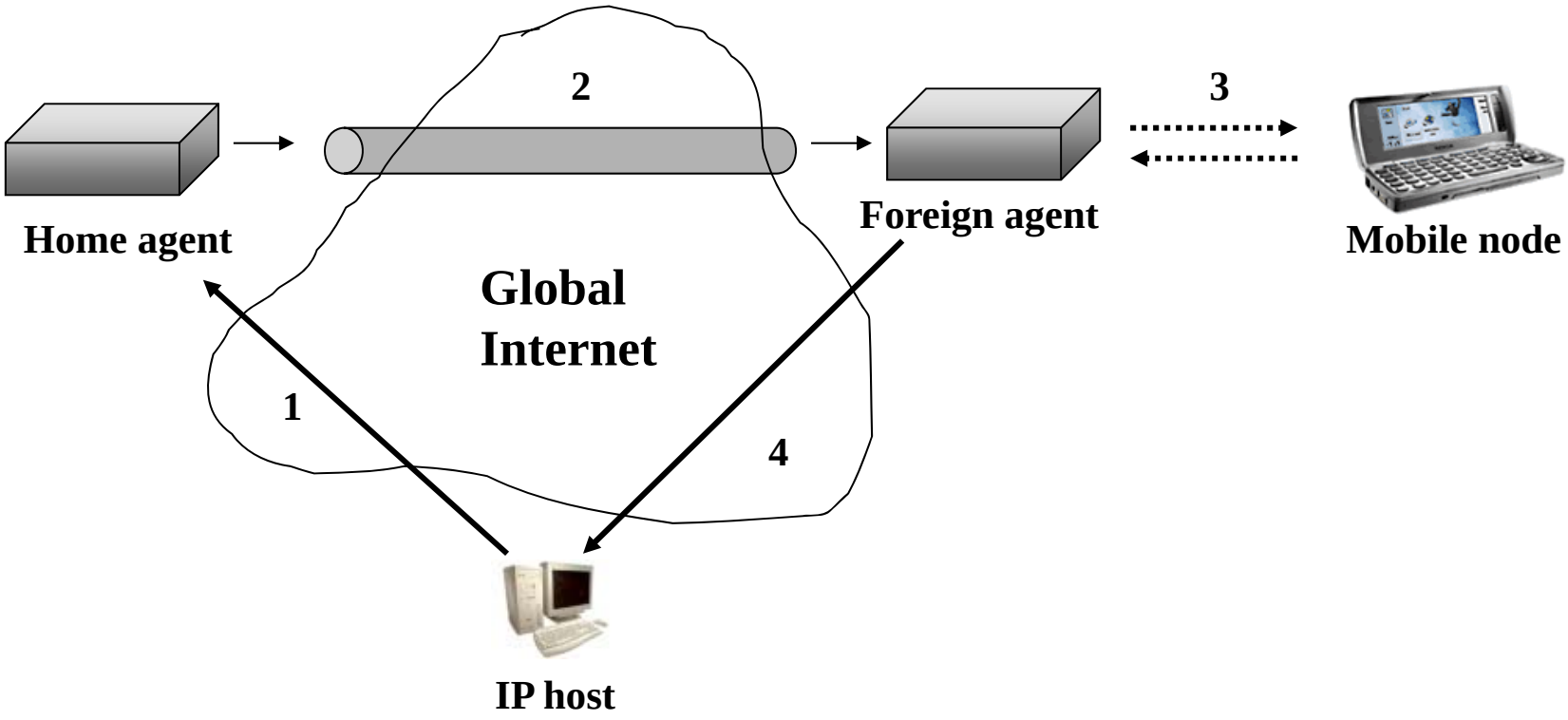
Registration



Tunneling

- Tunneling datagrams
  - Deliver data packets to the MN when it is away from home
    - the home agent has to tunnel the datagram to the care-of-address

Datagram


2
3
Home agent
Foreign agent
Mobile node
Global
Internet
1
4
IP host

Getting a care-of-address (COA)

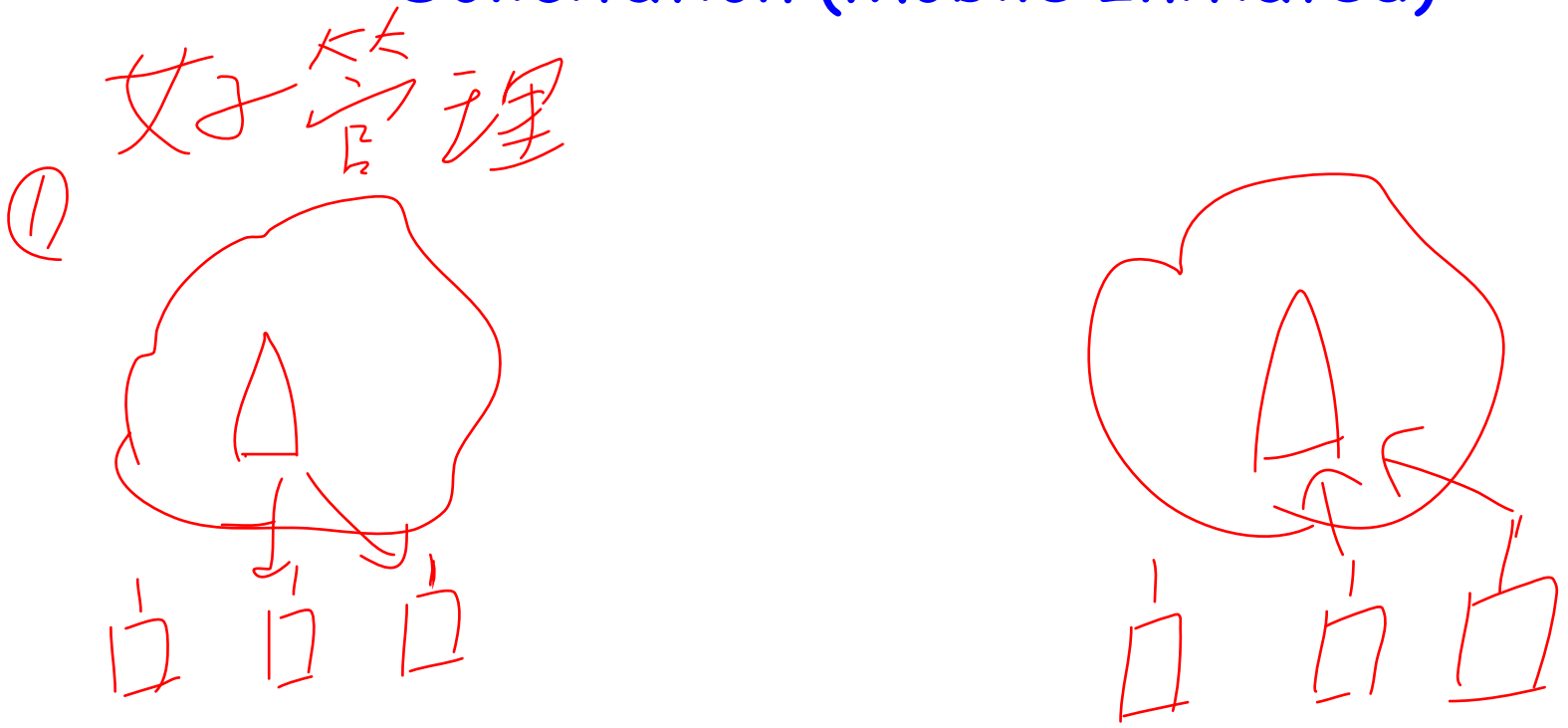
- Two ways to acquire a care-of-address (COA)
  - a **foreign agent COA** is a COA provided by the foreign agent through its agent advertisement messages
    - many nodes can use a single FA COA
  - a **colocated COA** is a COA acquired by the mobile node as a local IP address through some external means, which the mobile node then associates with its own network - the address may be dynamic, e.g., DHCP
    - only a single mobile can use this address

More Mobile IP Mechanisms

- Agent Discovery
  - Advertisement
  - Solicitation
- Registration
- Tunneling datagrams

Agent Discovery:

Advertisement (Network initiated) and Solicitation (Mobile Initiated)



Overview: Advertisement and Registration

- 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

hard ↑ soft state

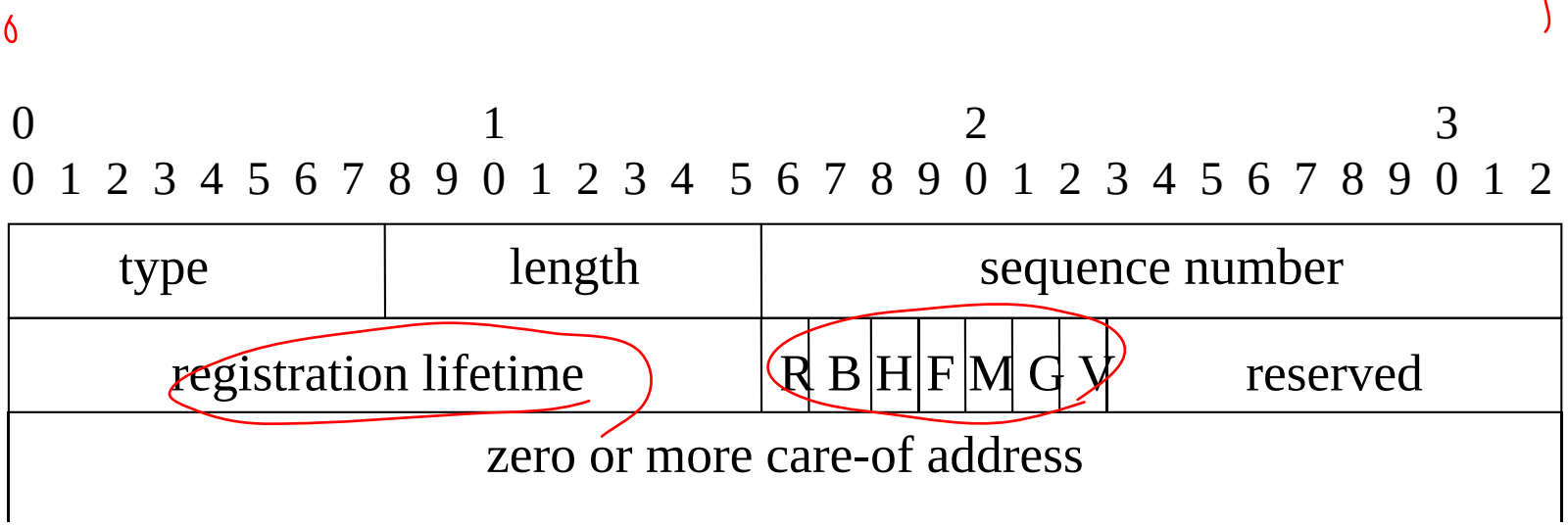
Advertisement

- Agent discovery is the method by which a mobile host
  - determines whether it is currently connected to its home network or a foreign network; and
  - detects when it has moved from one network to another
- Agent solicitation and discovery mechanisms
- Router discovery protocol
- Agent advertisement
- Agent solicitation
- Agent discovery by mobile nodes

Agent Advertisement

- An agent advertisement is an ICMP router advertisement that has been extended to also carry mobility advertisements extensions
  - A mobility agent transmits agent advertisements to advertise its service on a link
  - Mobile hosts use these advertisements to determine their current point of attachment to the Internet

Agent Advertisement Extension



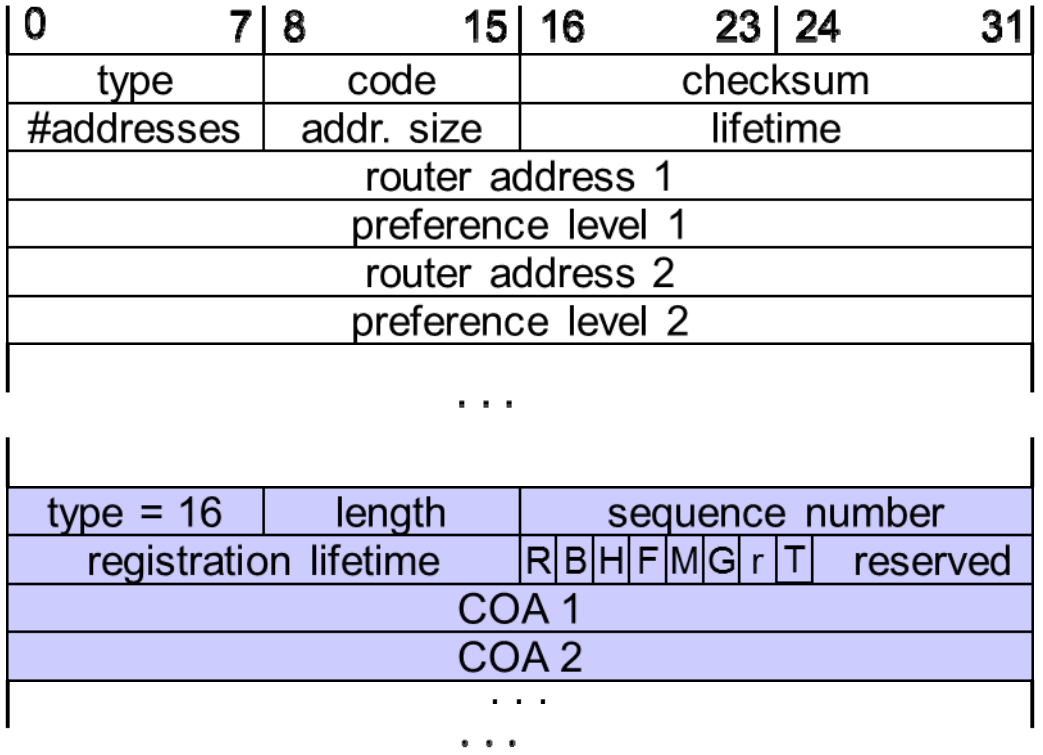
Important Fields

- R (registration required)
  - registration with the FA is required rather than collocated care-of address
- B (busy)
  - if this bit is set the FA will not accept any registrations from additional mobile hosts
- H (home agent)
  - if this bit is set the agent offers home agent services on the link which the advertisement is sent

Important Fields

- F (foreign agent)
  - this agent offers service as a foreign agent on the link on which the advertisement if sent
- M (minimal encapsulation)
- G (generic record encapsulation)
- V (VJ header compression)
- care-of addresses (COA)
  - the advertised FA care-of address provided by the FA. Must include at least one COA if the F bit is set. More than one COA can be advertised

Agent advertisement

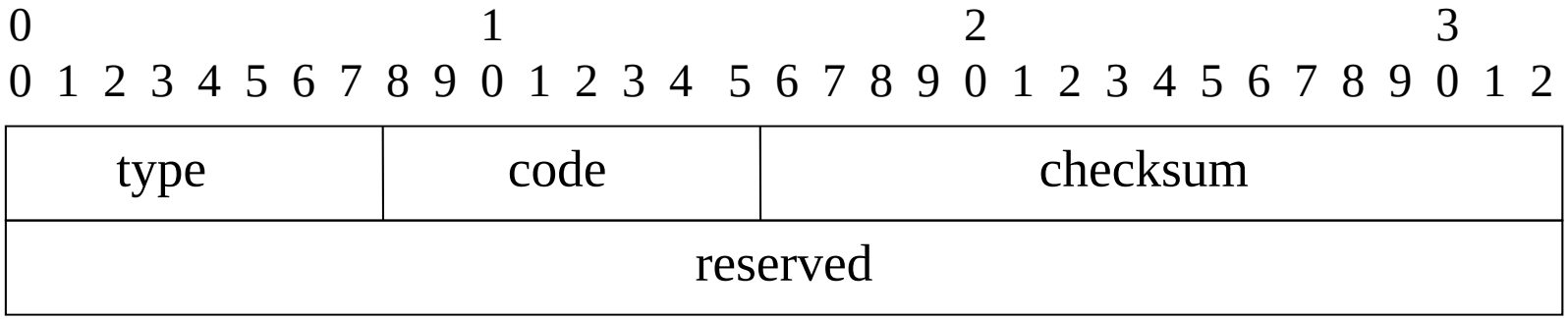


type = 16
length = 6 + 4 * #COAs
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Agent Solicitation

time-to-live

- The format of the agent solicitation is the same as the ICMP router solicitation. Agent solicitation do, however, always set the TTL to one.
- Advertisements only need to be sent when the site policy requires registration with the agent (R-bit is set) or as a response to a specific agent solicitation



Mobile Agent Operations

- A mobility agent should limit the rate of sending agent advertisements.
  - recommended maximal rate = 1/second.
- A FA must accept router solicitations even when the IP source address appears to reside on a different subnet

- A mobility agent "may" be configured to send agent advertisements only in response to an agent solicitation

Agent Discovery by Mobile Nodes

- Agent solicitations should only be sent in the absence of agent advertisements and when the care-of address can not be determined through a link-layer protocol or other means

- Operational differences to the router solicitation
  - mobile nodes may solicit more often than once every three seconds
  - mobile node that is currently not connected to any FA may solicit more times than currently configured.

Limiting Signaling Overhead

- MN should limit the rate at which its sends solicitations.
  - 3 initial solicitations at the max rate(1/second) while searching for an agent.
  - Subsequent solicitations are required to be sent using a binary exponential backoff mechanism up to a maximal interval (one minute).

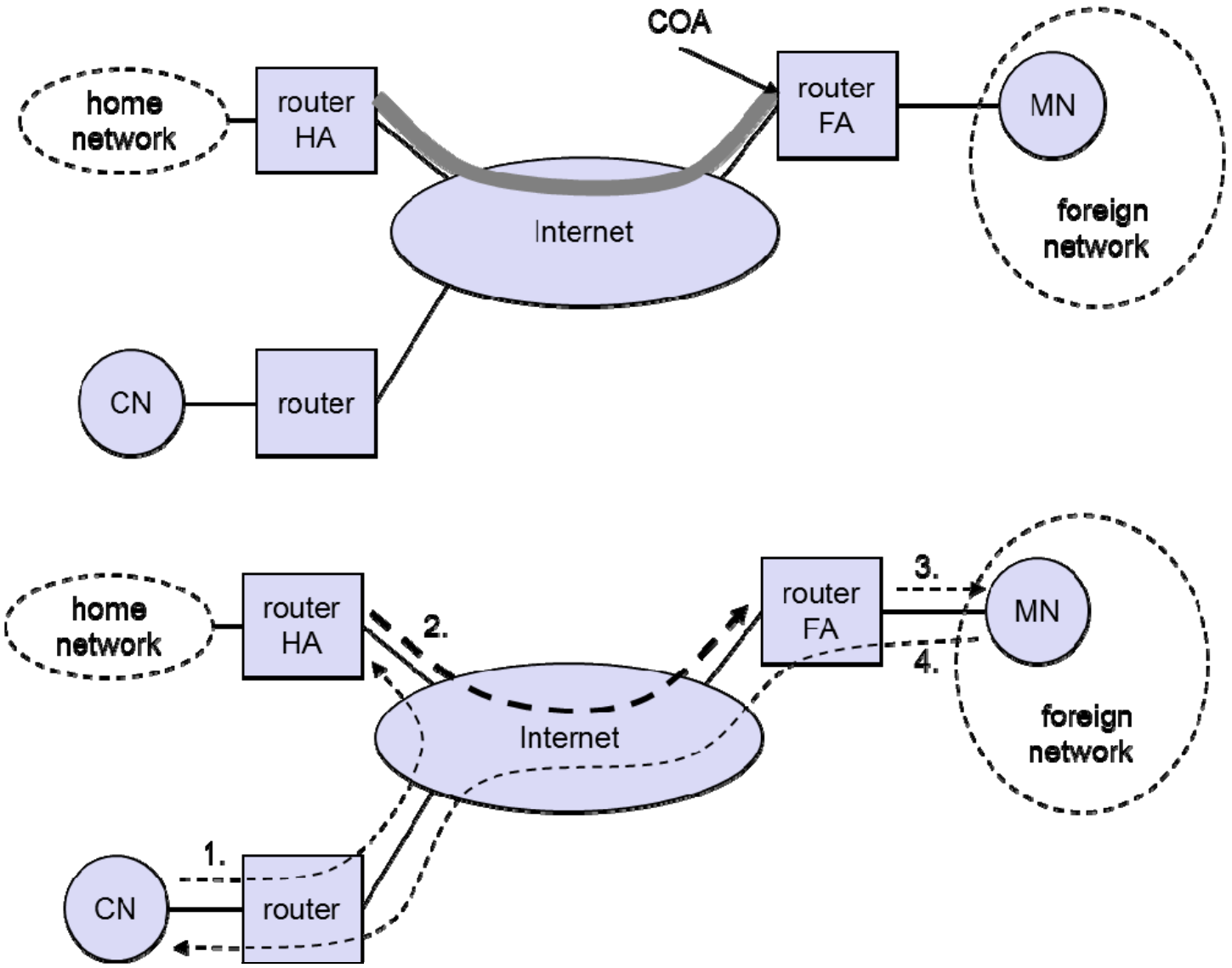
- While searching for an agent the mobile node is not allowed to increase the rate at which it sends solicitations unless it knows it has moved to a new link

Agent Discovery

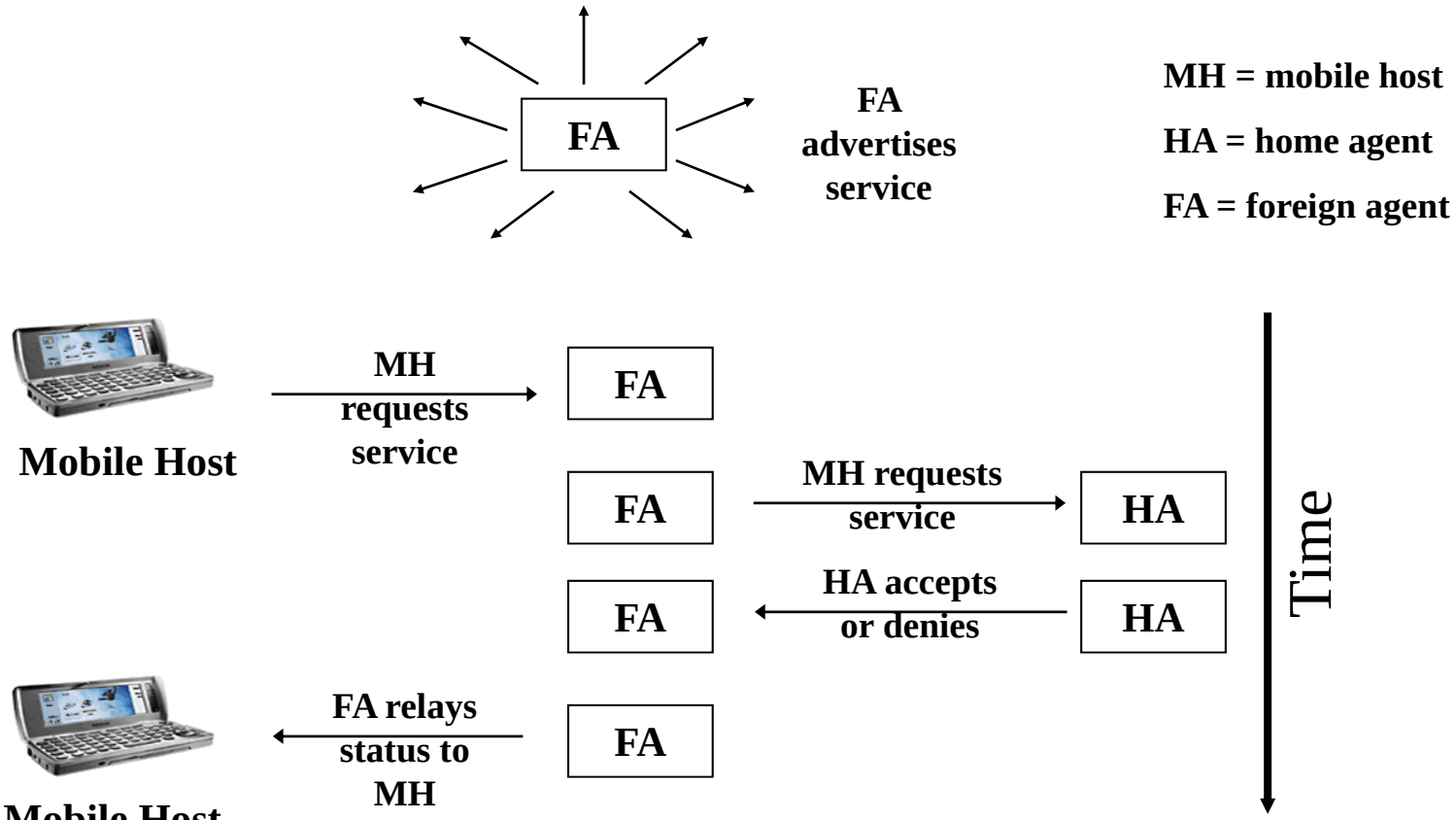
- Mobile nodes process agent advertisements to discover a care-of address and FA. This is to for the registration phase
- Foreign networks can enforce visiting policy.
  - E.g Set R bit in agent advertisements
    - Force mobile nodes to register with FA(when when the mobile might be able to acquire its own COA.)
- Detect returning to home network
  - MN receives an agent advertisement from its own home agent

Registration

Review


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

Mobile IP Registration



Operations

- Request forwarding services when visiting a foreign network
- Inform their home agent of their current care-of address
- Renew a binding that is due to expire
- Deregister when they return home

Movement Detection

- Important issue for handoff performance
- How does the mobile device know its moved to a new cell?
  - Handoff initiation (criteria and procedures)
- When the mobile node determines that it has moved it should register with a suitable care-of address (COA) on the new foreign network
- Limitations: can't register more than once per-second on average
  - Mobile IP is designed to support mobility with handoff rate less than once per second
- Mobile IP supports three types of movement detection schemes
  - Room for improvement → research in fast handoff

Movement detection methods

- Lazy Cell Switching
- Prefix Matching
- Eagar Cell Switching

Movement detection → handoff in network layer

Lazy Cell Switching

- Lazy Cell Switching
  - MH waits to hear new agent advertisement based on the lifetime timeout. If it receives one then it knows its still taking to the current BS
  - If advertisements are missed then it attempts to register with a possibly new cell using agent solicitation.
  - MHs typically try to receive two or more advertisements before expiring any advertisement before attempting to find a new foreign agent (FA)

Prefix Matching

- MH uses the "prefix extension" to determine whether a newly received agent advertisement is from the same subnet
  - If the prefix is different it knows its connected to a new cell and registers

- Downside: the prefix-extension in agent advertisements is optional

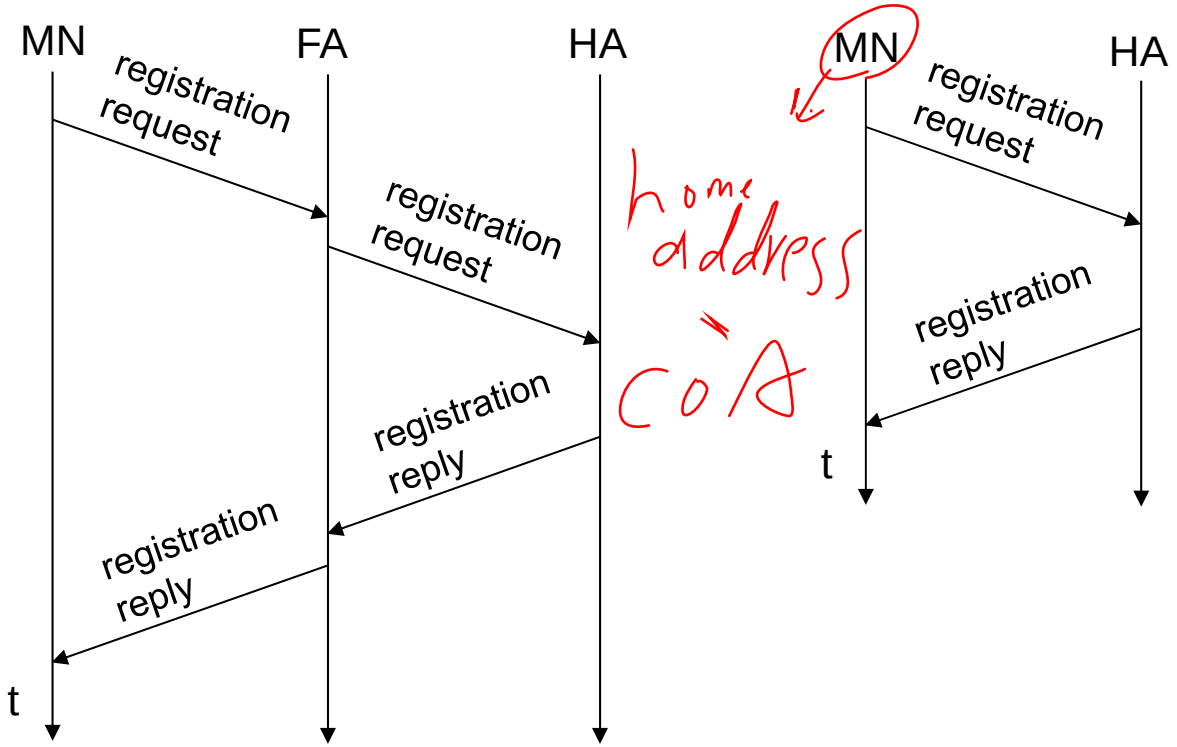
Eagar Cell Switching

- Based on the mobile host hearing beacons from multiple FAs simultaneously. Also make some assumptions about mobility patterns which may not hold – traveling in a straight line.
  - Maintains list of FAs and their COAs; and the current FA/COA
  - Once the current FA is no longer available (e.g., because the mobile has moved) then it selects a new one form this list
- Faster than Lazy Cell Switching but makes a number of assumptions

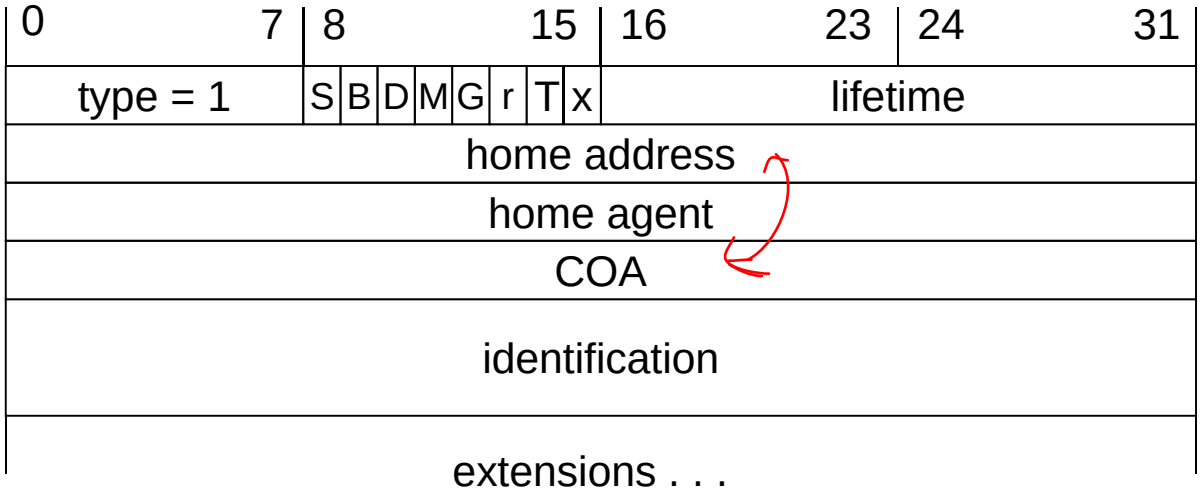
Registration

- Registration messages exchange the mobile node's current binding information among a mobile node (possibly a FA) and its home network
- Registration creates or modifies a mobility binding at the home agent, associating the mobile node's home address with its COA for a certain length of time called the registration lifetime

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

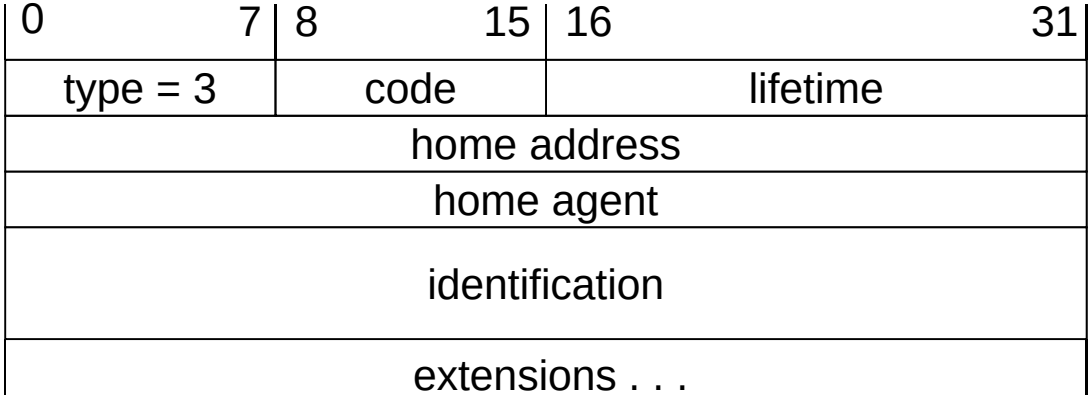
Registration Request Fields

- Lifetime
  - the number of seconds remaining before the registration is considered expired
- Home address
- Home agent
- COA
    - The IP address for the end of the tunnel
- Identification
  - 64 bits used to match reg. Request and replay pairs and to solve the playback problem

Registration Reply

- The HA can update some of the information in the registration request
  - Registration Request
  - Registration Reply
- Home agent can reduce the lifetime value

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

HA Registration State

- The home agent is required to be configured with the home address and mobility security association of each of its authorized mobile nodes
- When a registration request is accepted the HA creates or modifies the entry for the mobile in its mobility binding list
  - mobile nodes COA
  - Identification field from the registration reply
  - remaining lifetime of the registration
- The HA also maintains security associations with various FAs

Registration Denied by the HA

- Insufficient resources
- mobile node failed authentication
- FA failed authentication
- Registration ID mismatch
- Too many simultaneous bindings

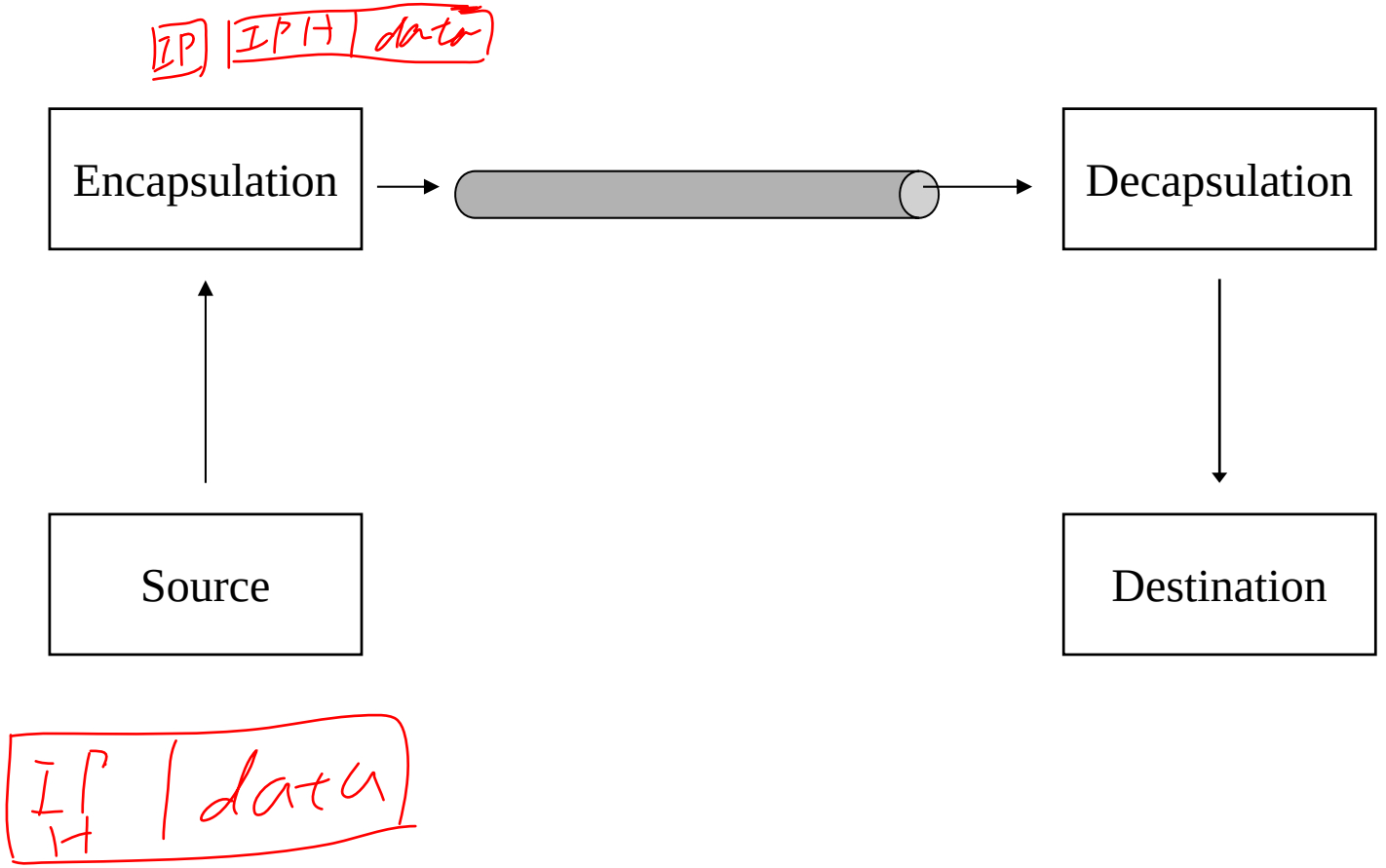
FA Registration State

- Link layer source address of the mobile node
- IP source address (the mobile node's home address)
- IP destination address
- UDP source port
- Home agent address
- Identification field
- Request registration lifetime
- Remaining lifetime of the pending or current registration

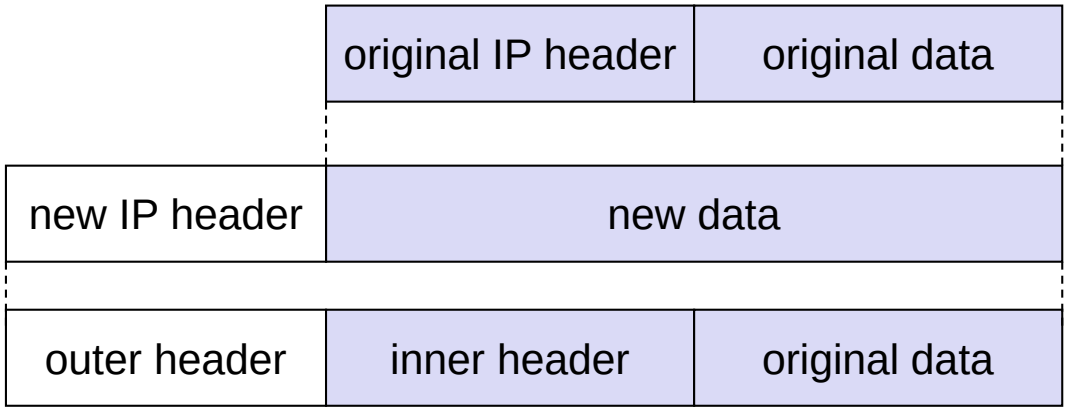
Tunneling

What is Tunneling ?

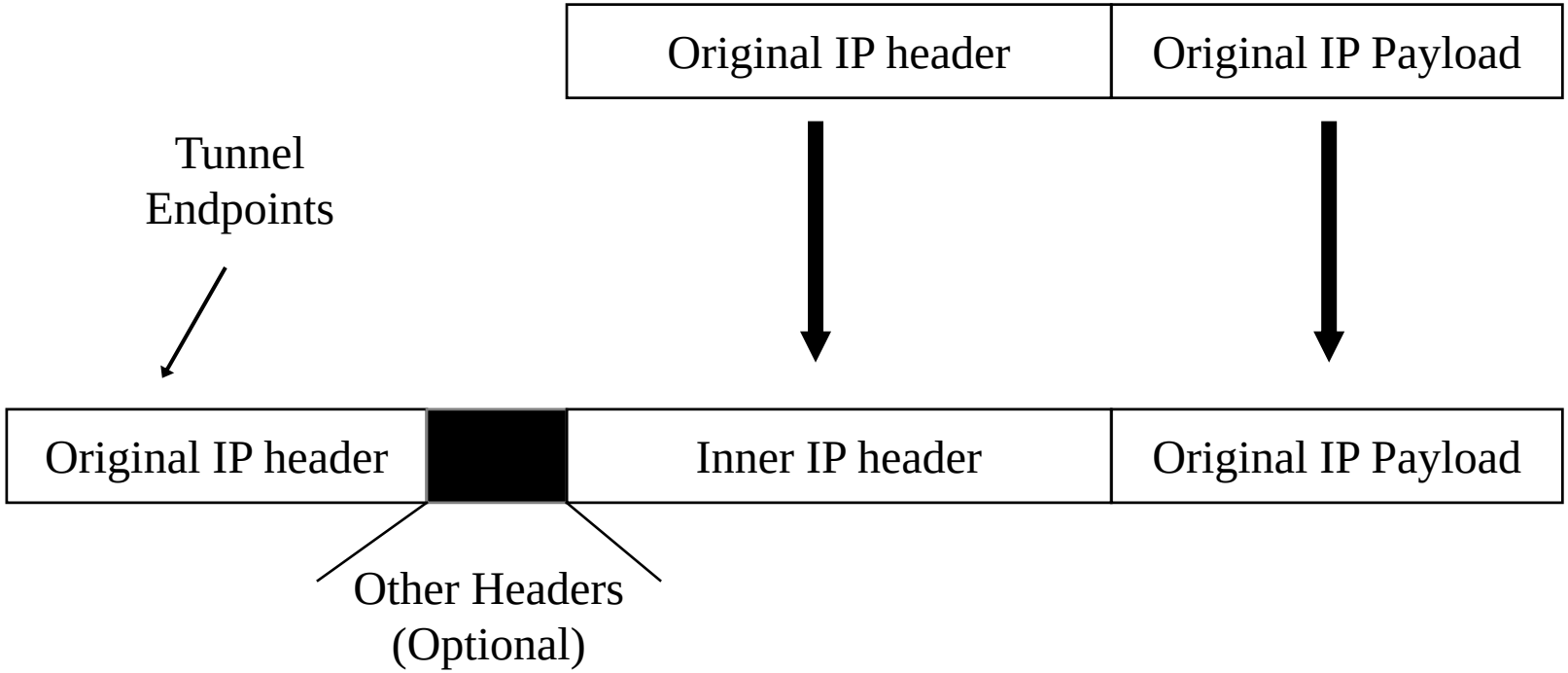
Forwarding data packets through tunnel



Encapsulation

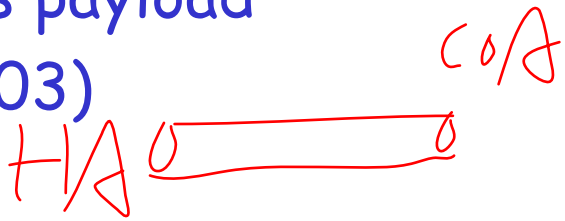


(1) IP-in-IP Encapsulation



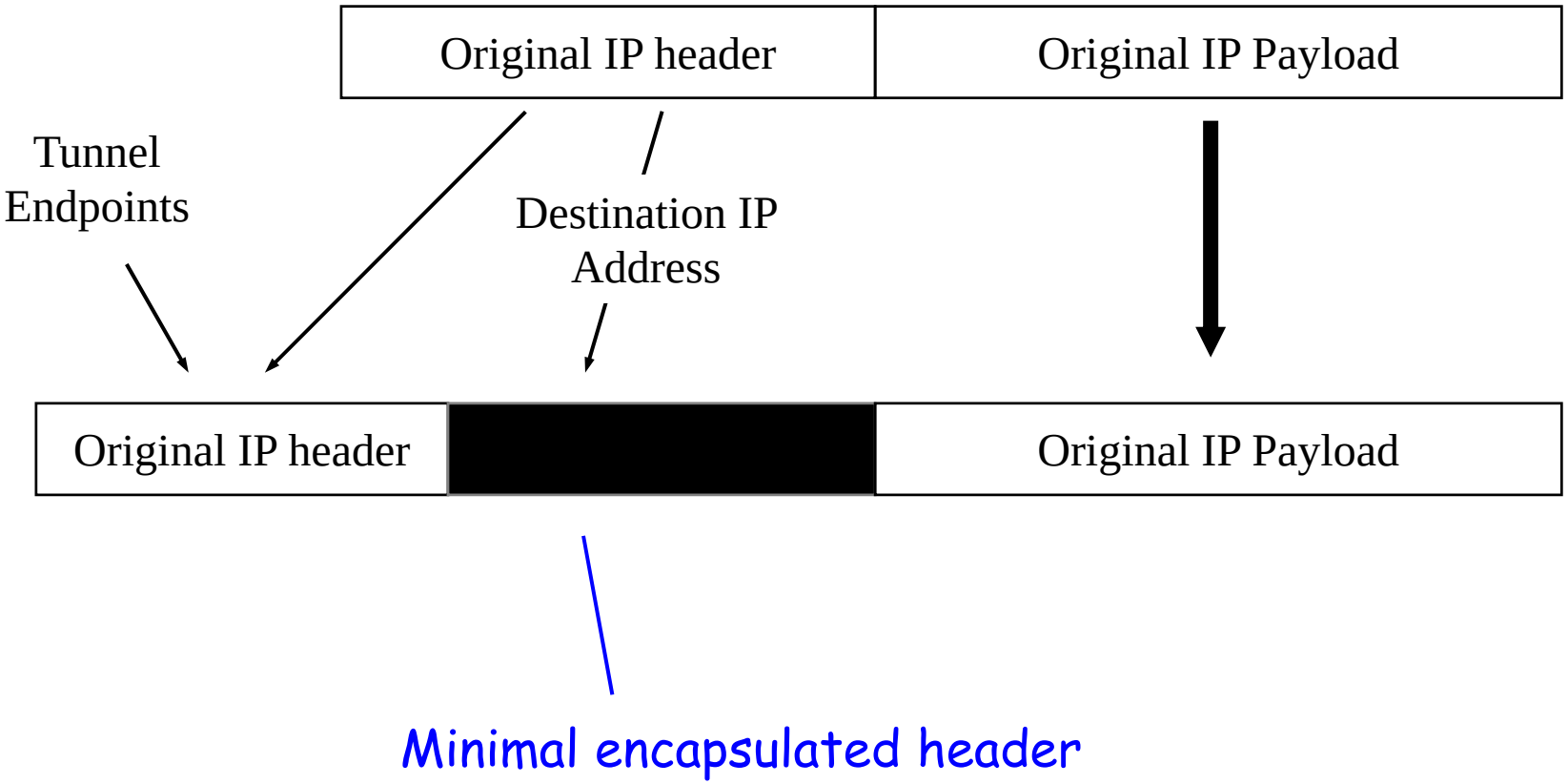
IP-in-IP Encapsulation Message Fromat

- Encapsulation of one packet into another as payload
- IP-in-IP-encapsulation (mandatory, RFC 2003)
  - tunnel between HA and COA



ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		*IP-in-IP*	IP checksum	
IP address of HA				
Care-of address COA				
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				

(2) Minimal Encapsulation



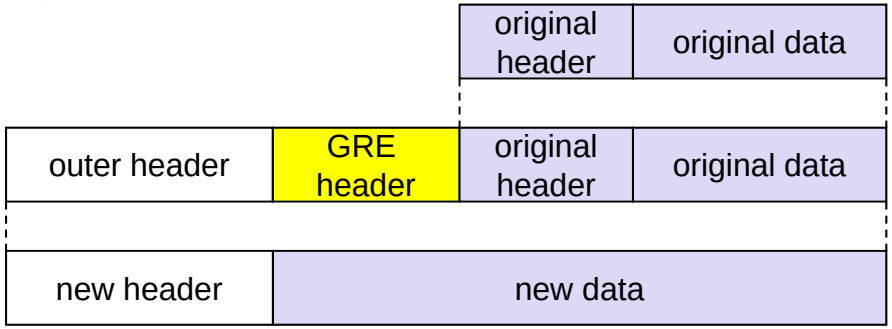
Minimal Encapsulation Message Formats

- Minimal encapsulation (optional)
  - avoids repetition of identical fields
    - Using IP-in-IP encapsulation requires unnecessary duplication of several IP header fields.
  - only applicable for unfragmented packets, no space left for fragment identification

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

(3) Generic Routing Encapsulation

- GRE could be applied to encapsulate more generic packet besides IP packets (e.g. IP, frame relay, transport ethernet bridging, Novell IPX).



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

C	reserved0	ver.	protocol
checksum (optional)			reserved1 (=0)

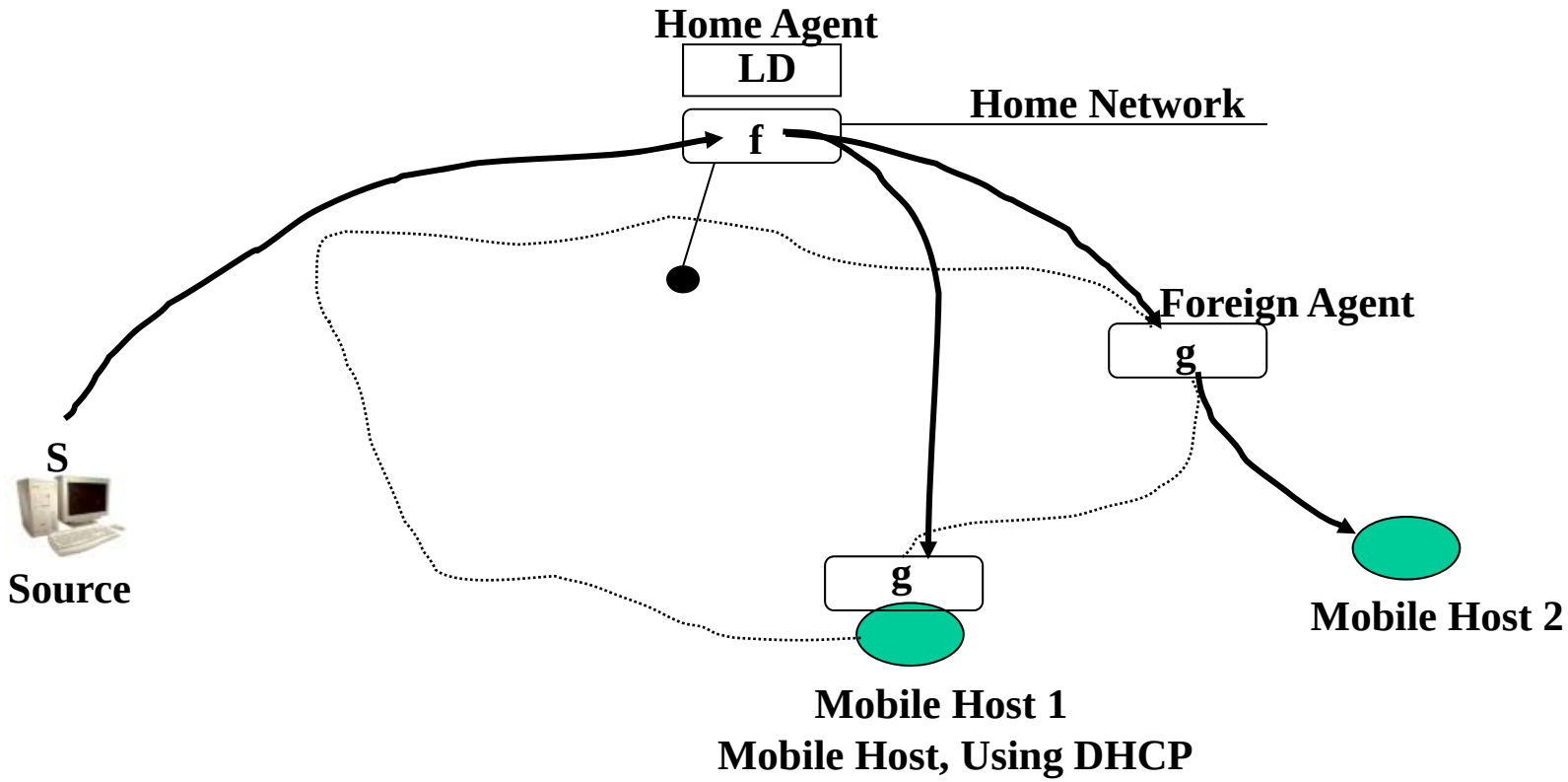
Tunnel Management

- Tunnel soft state
  - MTU size
  - TTL
  - Ability to reach the end of the tunnel
- ICMP errors
  - datagram too big
  - time exceeded
  - destination unreachable
  - source quench

Other Mobile IP schemes

Reference: IETF Mobile IP

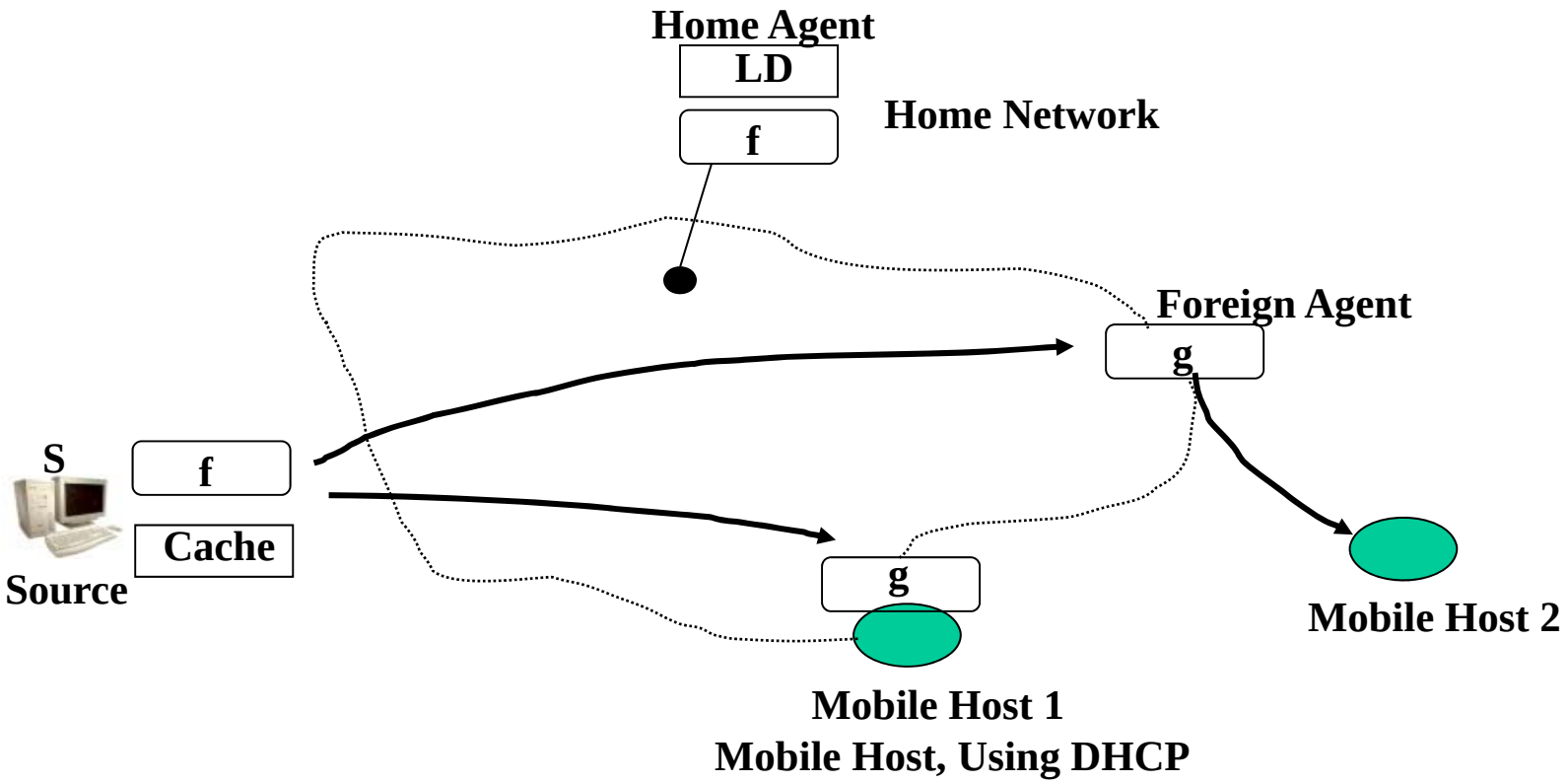
- Basic Mobile IPv4



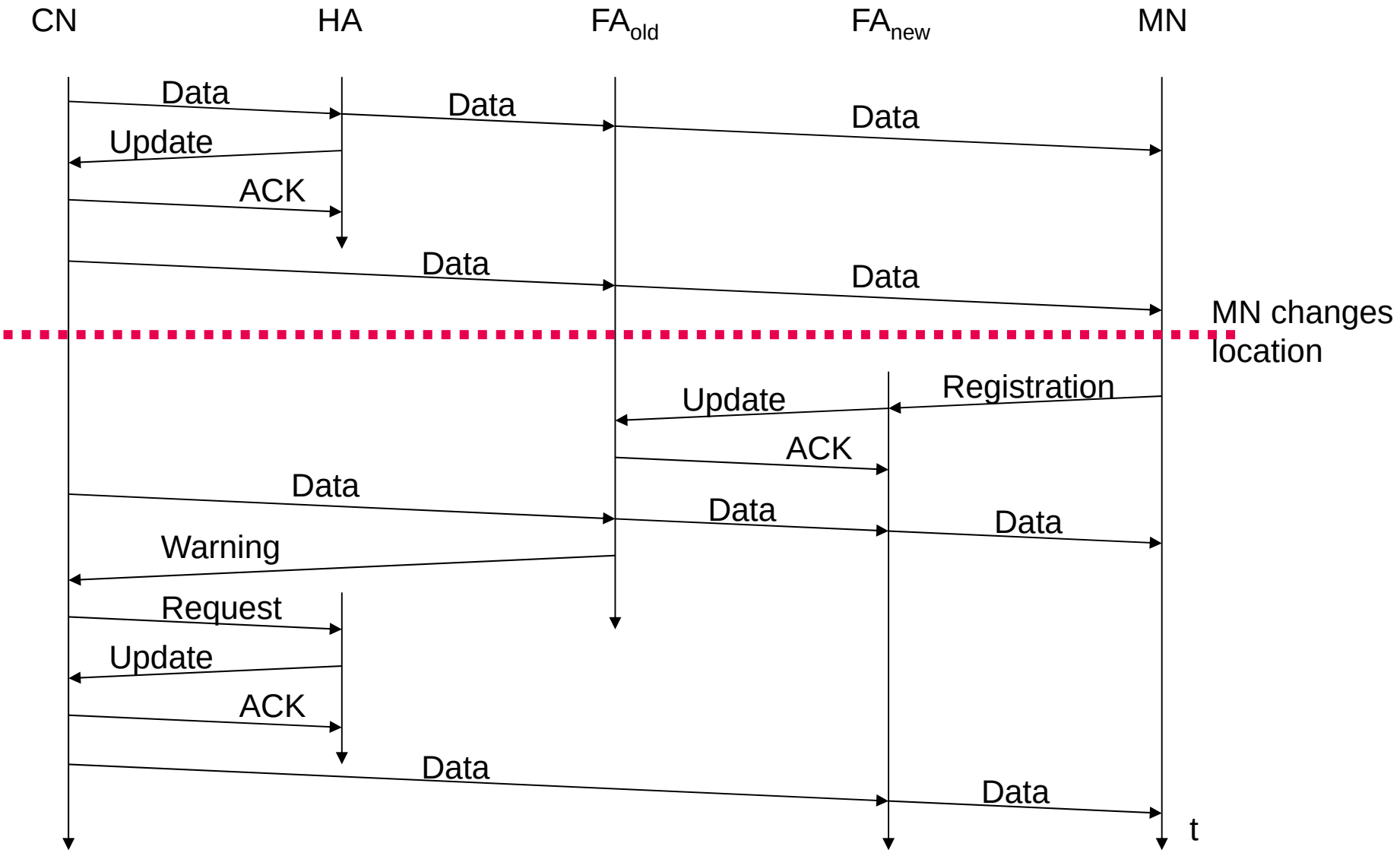
Optimization of packet forwarding

- 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

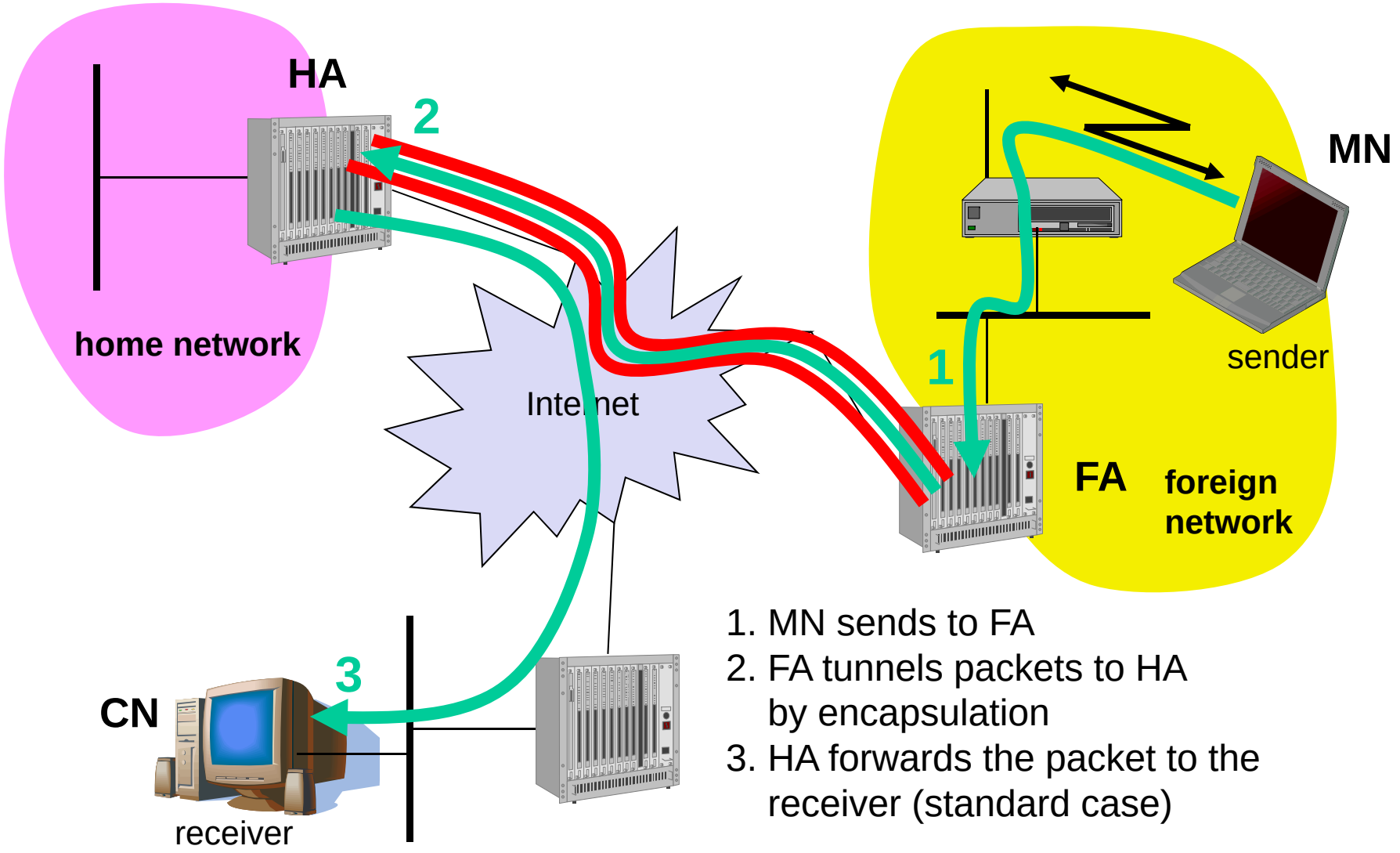
Mobile IP with Route Optimization



Change of FA (with Route Optimization)



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)

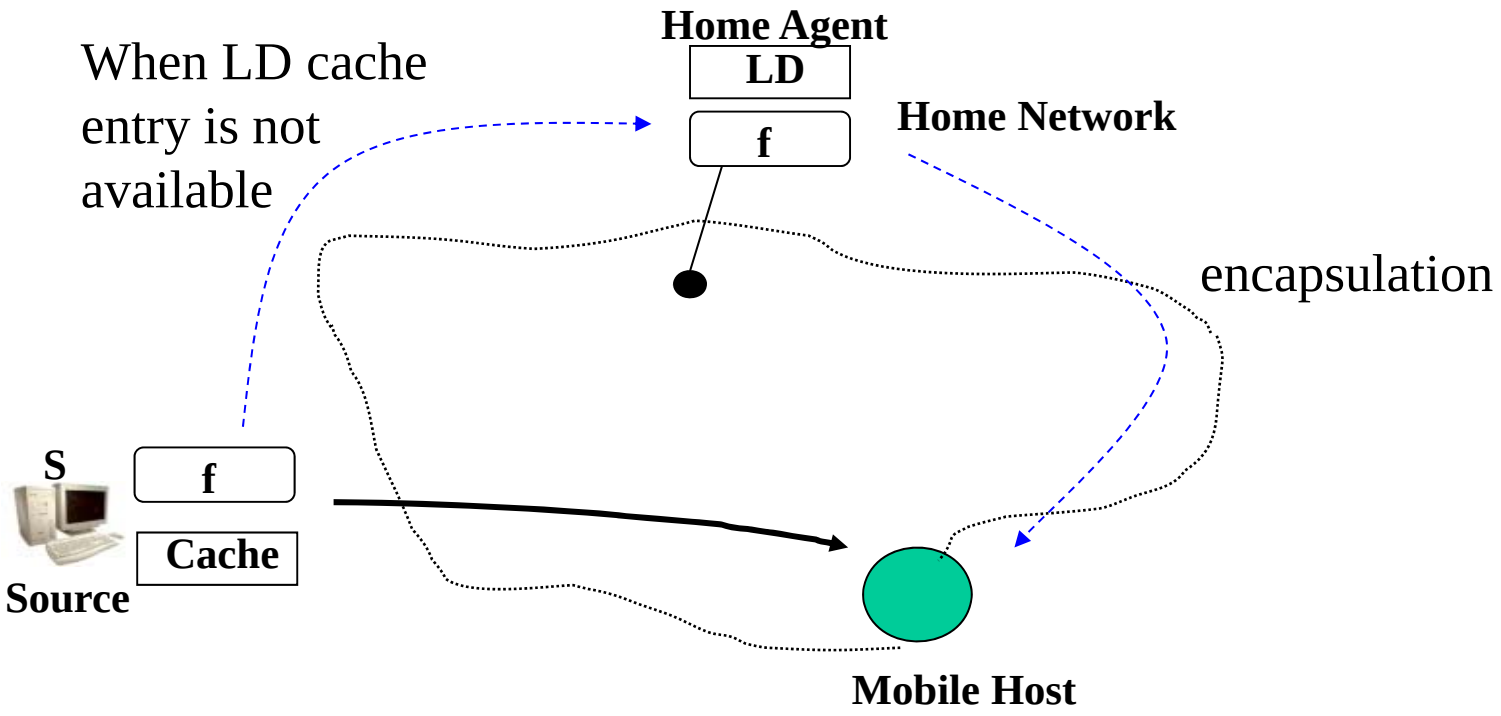
Mobile IP with reverse tunneling

- 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

Mobile IP and IPv6

- 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 autoconfiguration
  - 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)
  - „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

Mobile IPv6


When LD cache entry is not available
Home Agent
LD
f
Home Network
encapsulation
S
f
Cache
Source
Mobile Host

Summary: Mobile IP

- Basic data forwarding
  - FA mode
  - Co-located mode
- Agent discovery
- Registration
- Tunneling