Mobile Networking

Mohammad Hossein Manshaei

manshaei@gmail.com

1393

Mobile IP

MOBILE NETWORK LAYER

Content

- Mobile Network Layer: Problems and Concerns
- Entities and Terminology in Mobile IP
- Mobile Indirect Routing
- Mobile IP
  - Agent Advertisement
  - Registration
  - Tunneling and Encapsulation
  - Optimization: Direct Routing and Handoff
  - Reverse Tunneling
  - IPv6

What is Mobility?

- spectrum of mobility, from the *network* perspective:

No Mobility **High Mobility**

mobile wireless user, using same access point

mobile user, connecting/ disconnecting from network using DHCP.

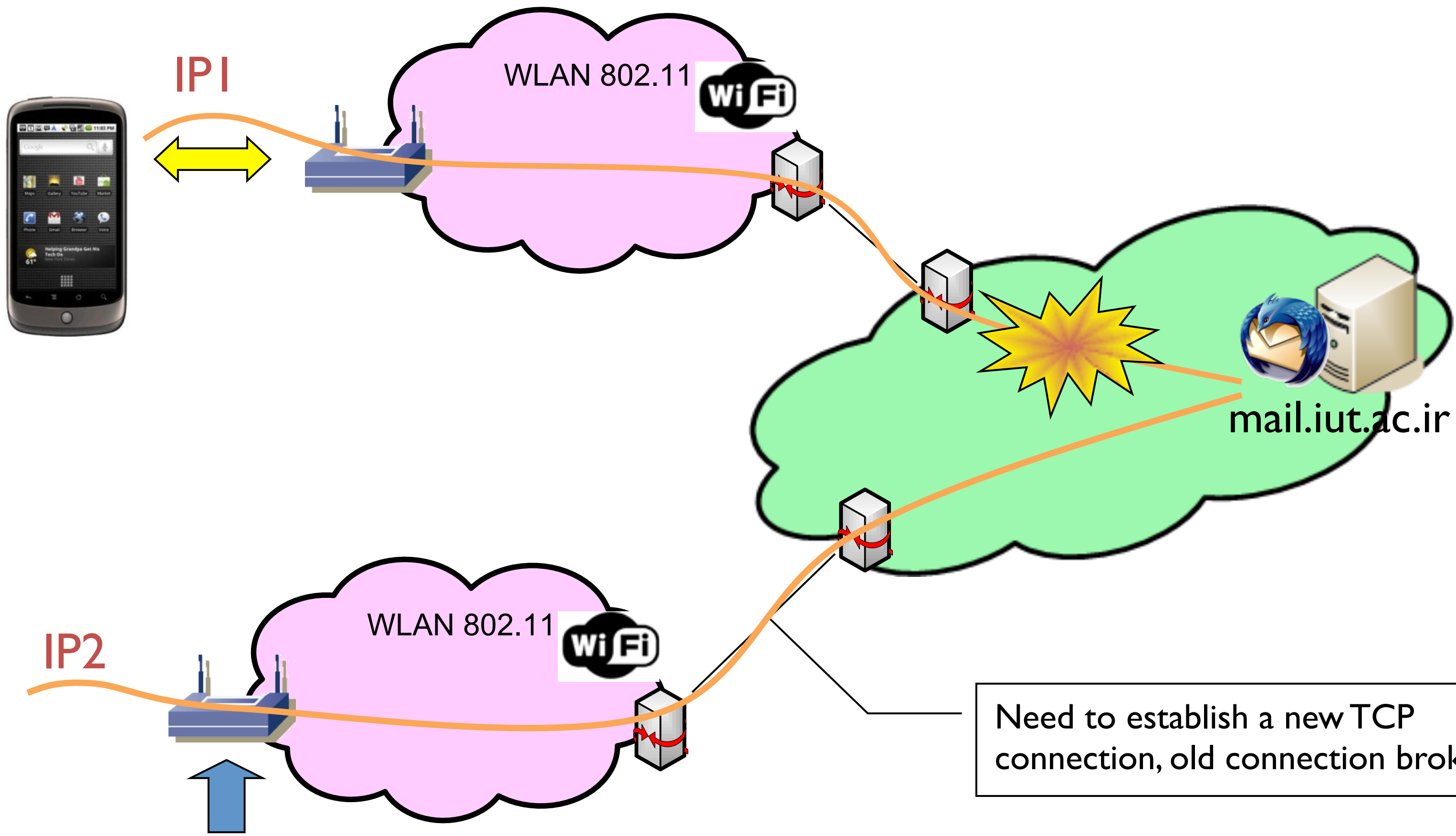
mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)

Enablers of IP mobility

- Mobile end systems
  - Laptops
  - PDAs
  - Smart-phones
  - …

- Wireless technologies
  - Wireless LANs (IEEE 802.11)
  - Bluetooth (www.bluetooth.com)
- Improved batteries (longer lifetime)

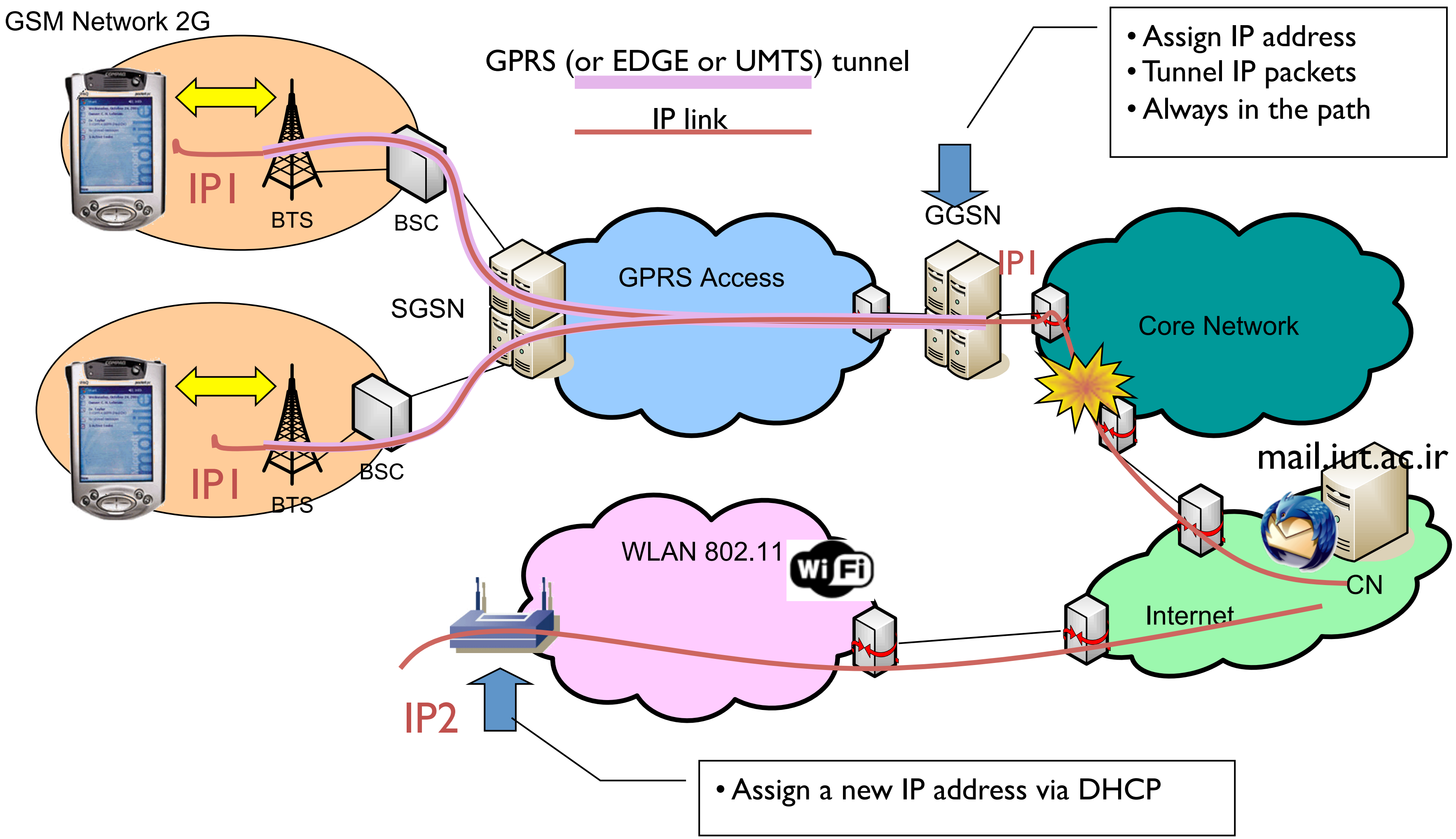
Problem with IP mobility



Need to establish a new TCP connection, old connection broken

Assign a new IP address via DHCP

IP mobility and cellular networks



Possible solution:
http://www.smart-wi-fi.com

TCP/IP was not designed for mobility

- Change of IP address means disconnection of the application
- TCP interprets dropped packets (channel errors, disconnections) as congestion
- Limitations due to a **fundamental design problem**

The IP address (network layer) has a dual role

- **Network locator (topological point of attachment) for routing purposes**
- **Host identifier (unique for a host and TCP/IP stack)**

Routing in the Internet

- Routing is based on the destination IP address
  - Network prefix (e.g. 129.13.42) determines physical subnet

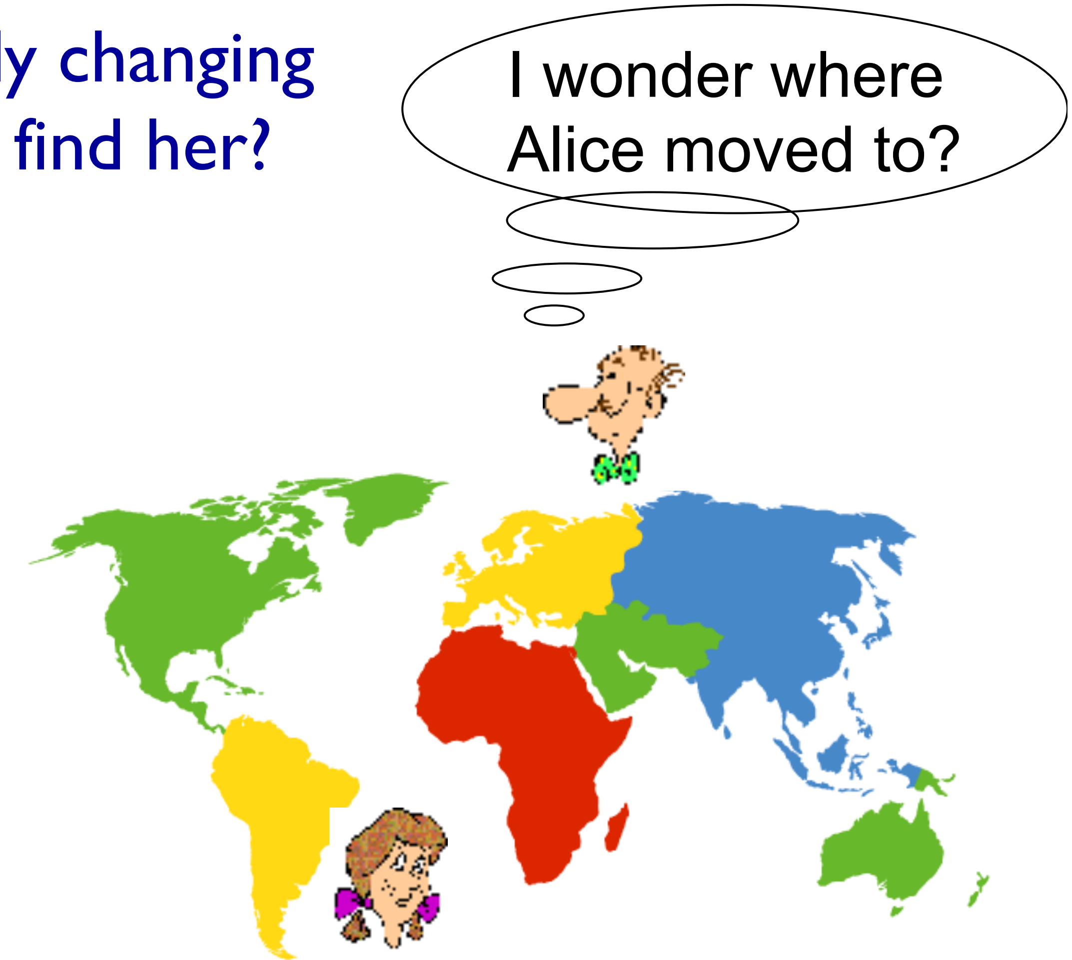
- Change of physical subnet implies change of IP address (standard IP)
  - The new IP address needs to be **topologically correct** (belong to the new subnet) to be routable

- Changing the IP address according to the current location
  - DHCP provides plug-and-play address update
  - Number of drawbacks:
    - Almost impossible to locate a mobile system; long delays for DNS updates
    - TCP connections break
    - Security problems

How do *you* contact a mobile friend:

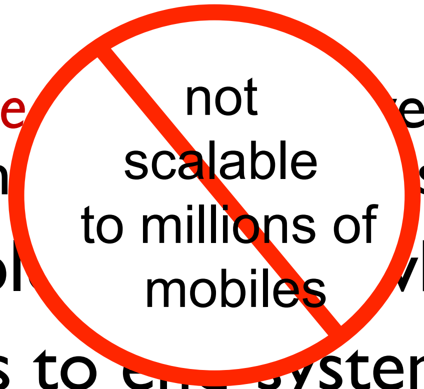
Consider friend frequently changing addresses, how do you find her?

- search all phone books?
- call her parents?
- expect her to let you know where he/she is?



Mobility: Approaches

- *Let routing handle* ... ertise permanent address of mobile-nodes-in ... sual routing table exchange.
  - routing tabl ... where each mobile located
  - no changes to ... systems



- *Let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Requirements to Mobile IP

- **Transparency**
  - Mobile end-systems (hosts) keep their IP address
  - Maintain communication in spite of link breakage
  - Enable change of point of connection to the fixed network
- **Compatibility**
  - Support the same Layer 2 protocols as IP
  - No changes to current end-systems and routers
  - 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 may be over a low-bandwidth radio link)
  - World-wide support of a large number of mobile systems

Two main solutions

1. **Mobile IP**
   - Support mobility transparently to TCP and applications
   - Rely on existing protocols

2. **Host Identity Protocol (HIP)**
   - A *new layer* between IP and transport layers
   - Architectural change to TCP/IP structure

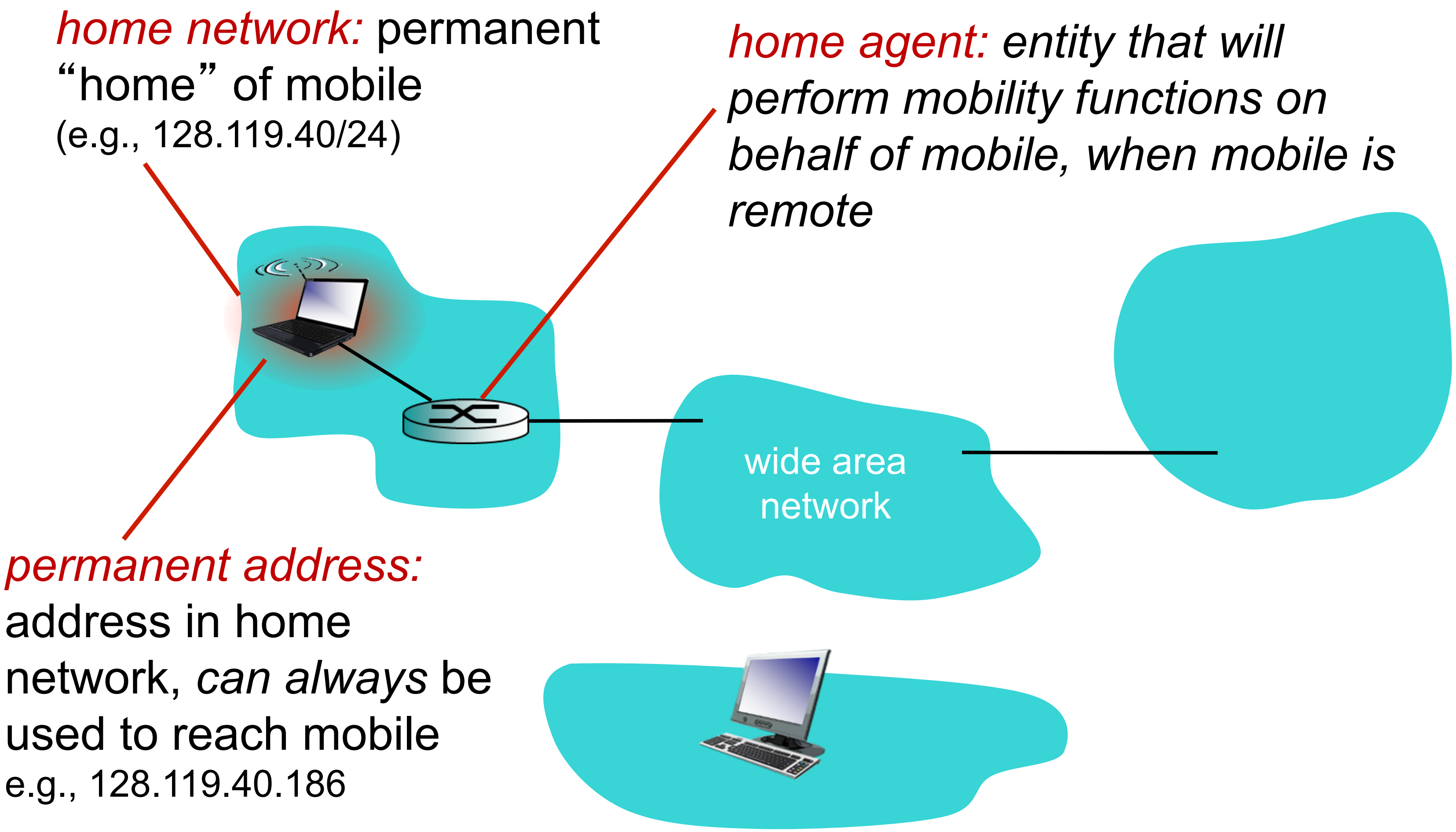
Content

- Mobile Network Layer: Problems and Concerns
- Entities and Terminology in Mobile IP
- Mobile Indirect Routing
- Mobile IP
  – Agent Advertisement
  – Registration
  – Tunneling and Encapsulation
  – Optimization: Direct Routing and Handoff
  – Reverse Tunneling
- IPv6

Terminology

- **Mobile Node (MN)**
  - Entity (node) that can change its point of connection to the network without changing its IP address
- **Home Agent (HA)**
  - Entity in the home network of the MN, typically a router
  - Registers the MN location, encapsulates and tunnels IP packets to the COA
- **Foreign Agent (FA)**
  - System in the current foreign network of the MN, typically a router
  - Decapsulates and forwards the tunneled packets to the MN
- **Care-of Address (COA)**
  - Address of the current tunnel end-point for the MN
    - ➔Foreign Agent COA or
    - ➔Co-located COA (no FA, MN performs decapsulation)
  - Actual location of the MN from an IP point of view
  - Co-located COA typically acquired via DHCP
- **Correspondent Node (CN)**
  - Communication partner

Mobility: Entities and Terminology

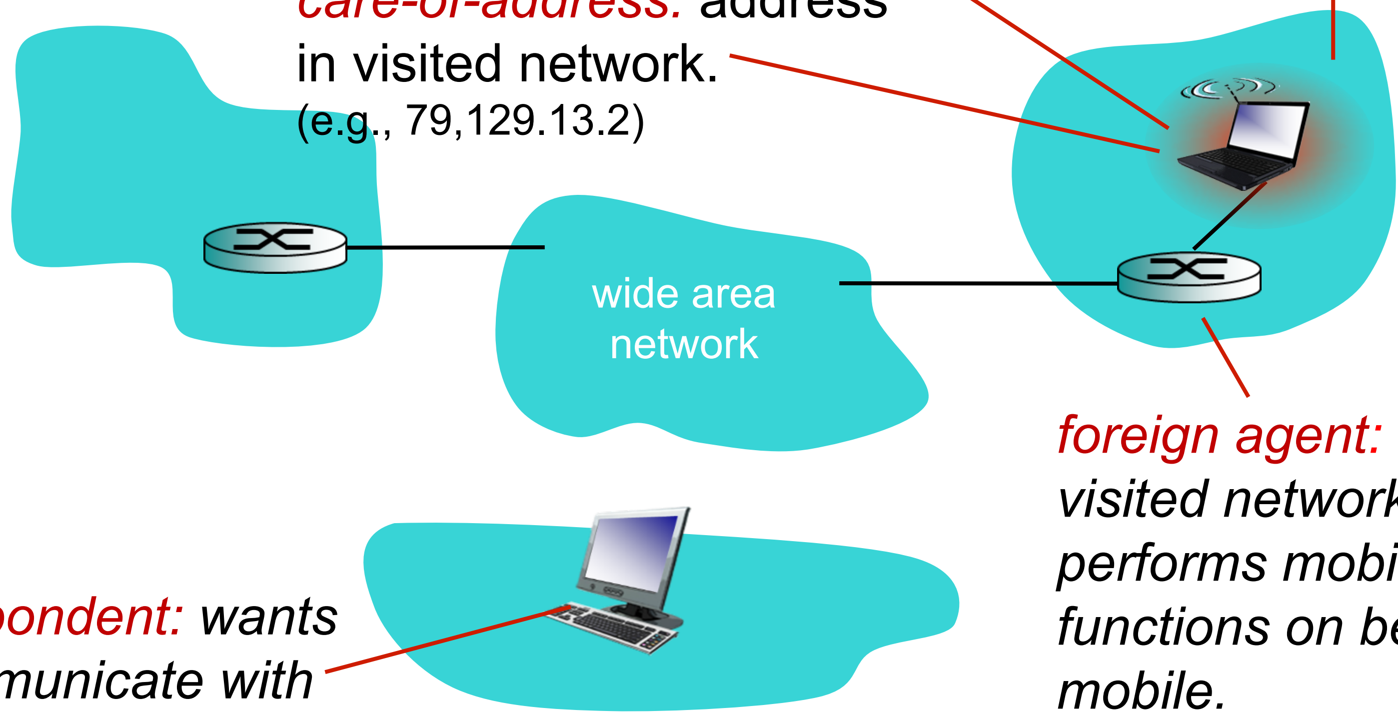


Mobility: Entities and Terminology

permanent address: remains constant (e.g., 128.119.40.186)

visited network: network in which mobile currently resides (e.g., 79.129.13/24)

care-of-address: address in visited network. (e.g., 79,129.13.2)



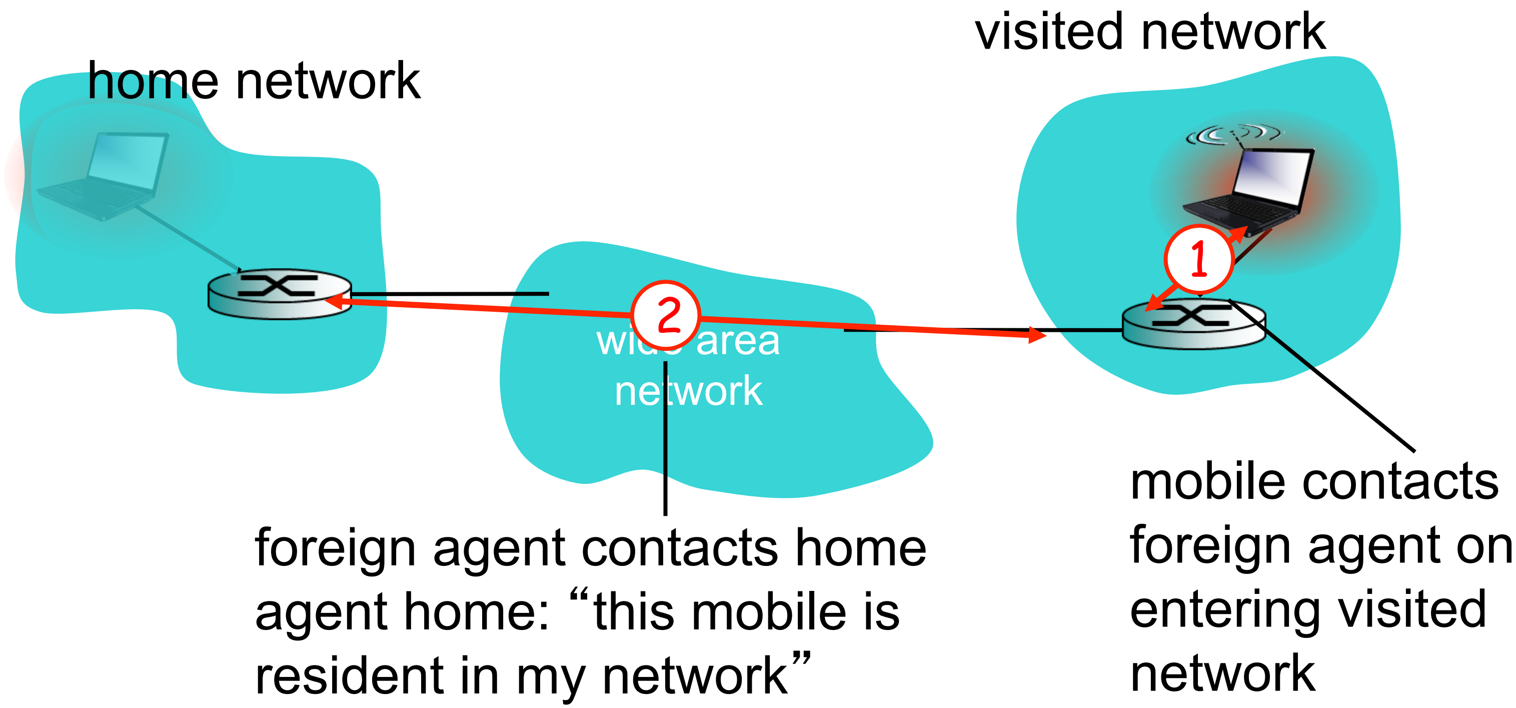
foreign agent: entity in visited network that performs mobility functions on behalf of mobile.

correspondent: wants to communicate with mobile

Content

- Mobile Network Layer: Problems and Concerns
- Entities and Terminology in Mobile IP
- Mobile Indirect Routing
- Mobile IP
  - Agent Advertisement
  - Registration
  - Tunneling and Encapsulation
  - Optimization: Direct Routing and Handoff
  - Reverse Tunneling
- IPv6

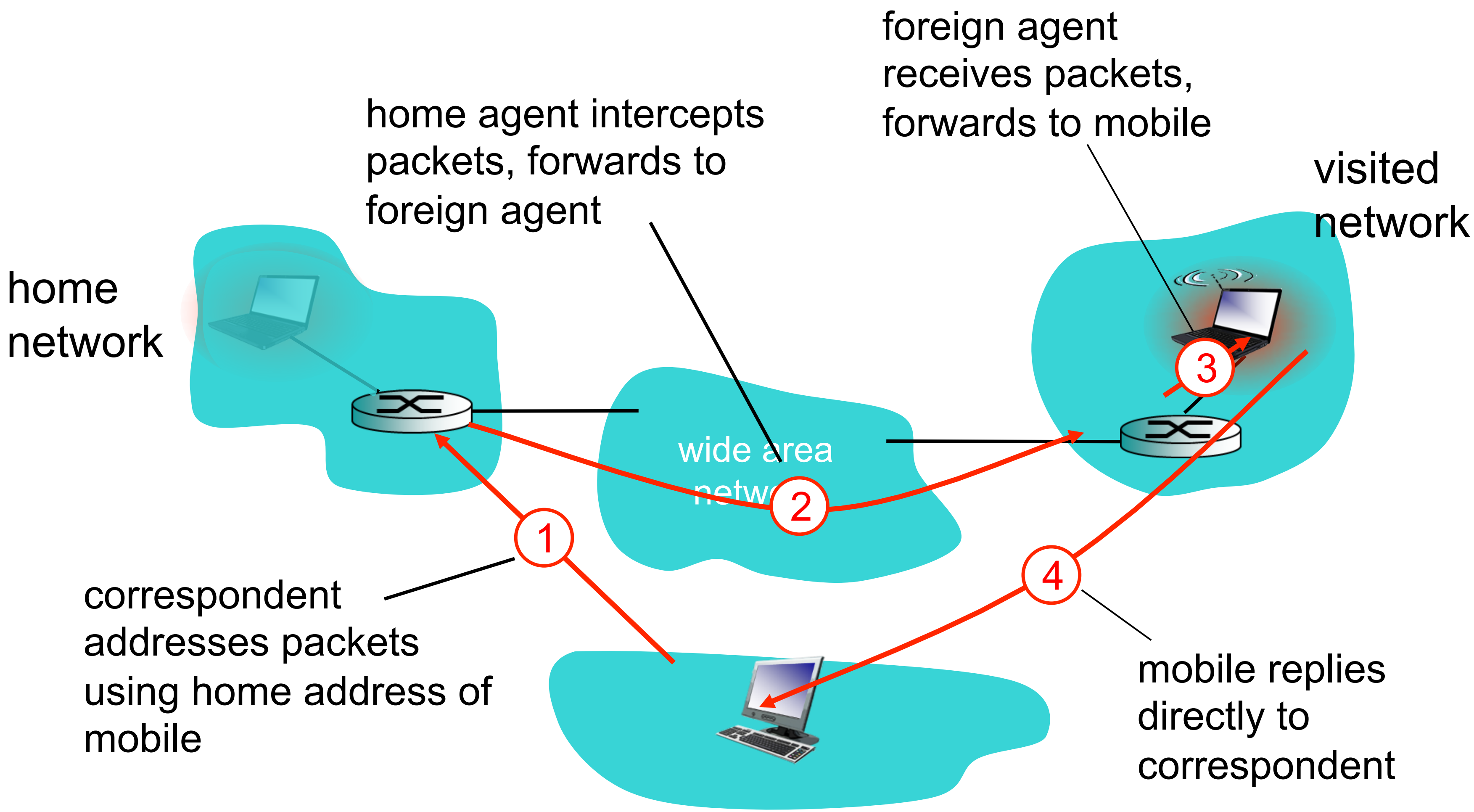
Mobility: Registration



end result:

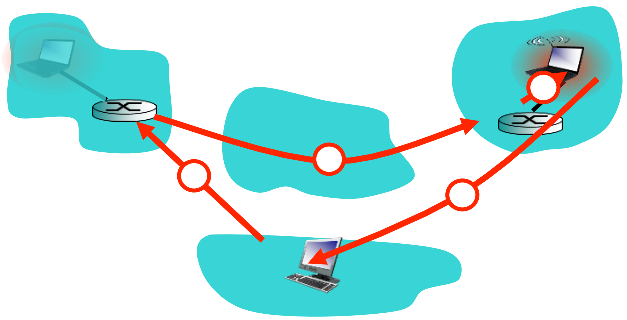
- foreign agent knows about mobile
- home agent knows location of mobile

Mobility via Indirect Routing

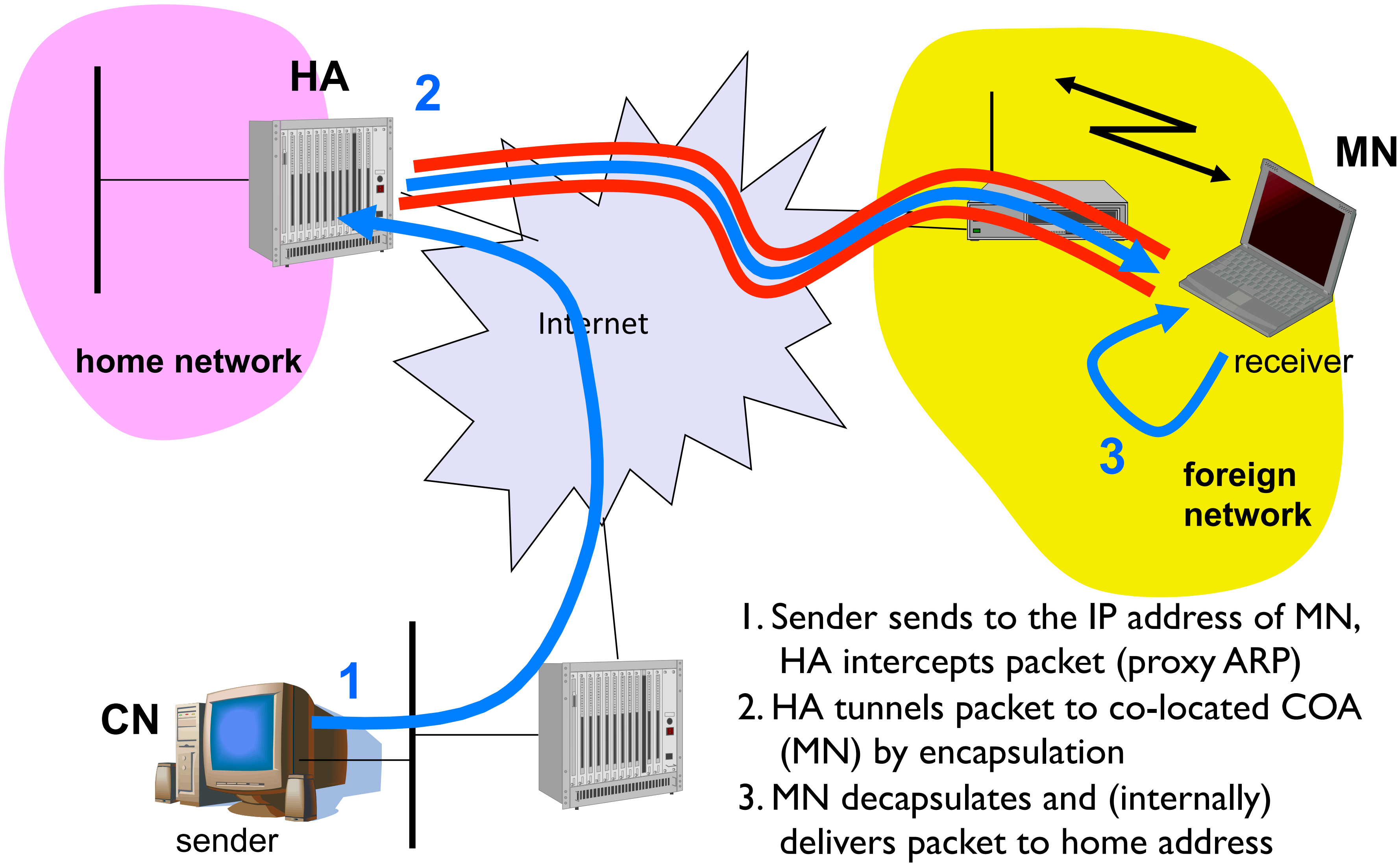


Indirect Routing: Comments

- Mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- Foreign agent functions may be done by mobile itself
- Triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network

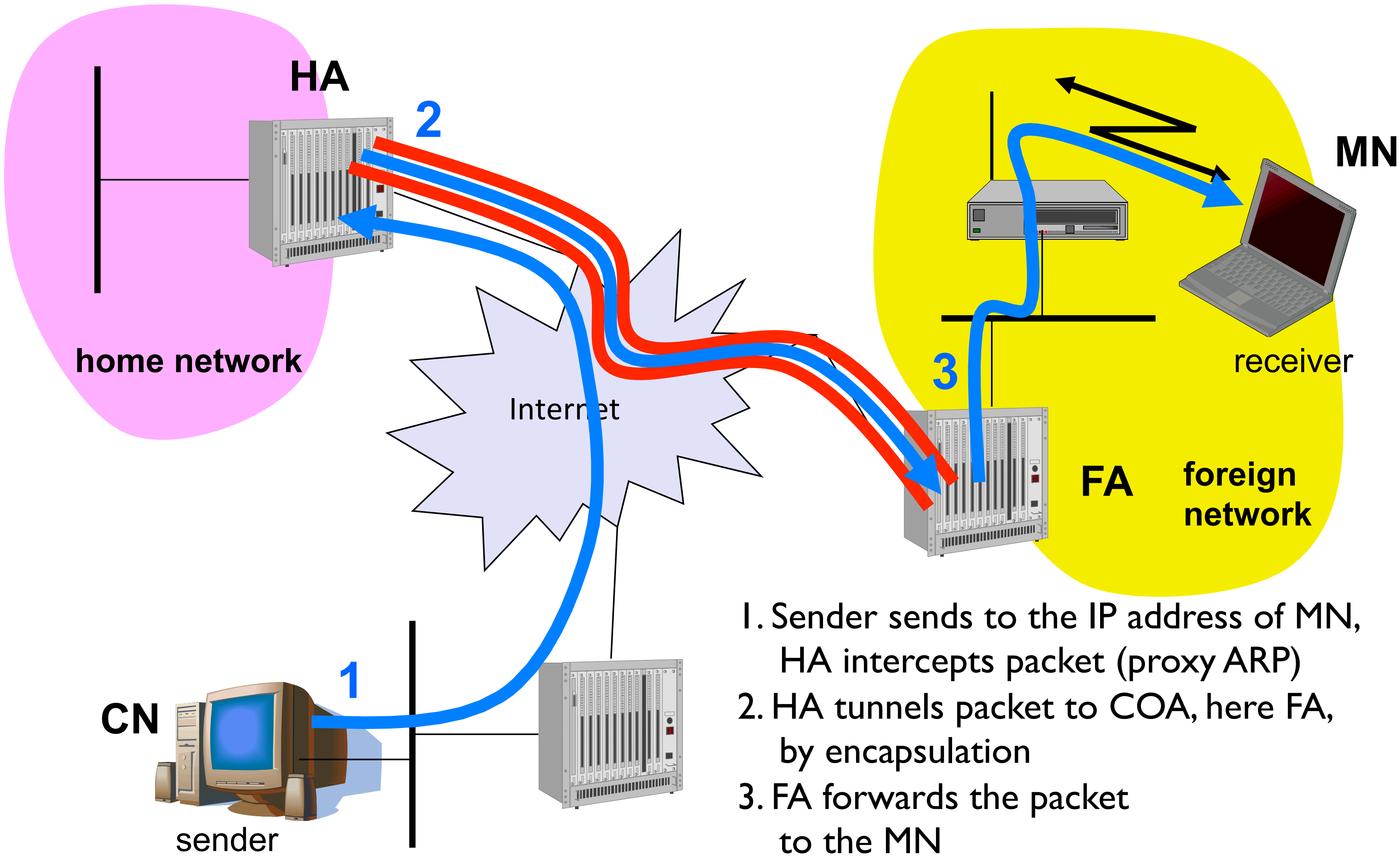


Data Transfer with Co-located COA



1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to co-located COA (MN) by encapsulation
3. MN decapsulates and (internally) delivers packet to home address

Data transfer to the Mobile Node:



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

Indirect Routing: Moving Between Networks

- Suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- Mobility, changing foreign networks transparent: *on going connections can be maintained!*

Content

- Mobile Network Layer: Problems and Concerns
- Entities and Terminology in Mobile IP
- Mobile Indirect Routing
- Mobile IP
  - Agent Advertisement
  - Registration
  - Tunneling and Encapsulation
  - Optimization: Direct Routing and Handoff
  - Reverse Tunneling
  - IPv6

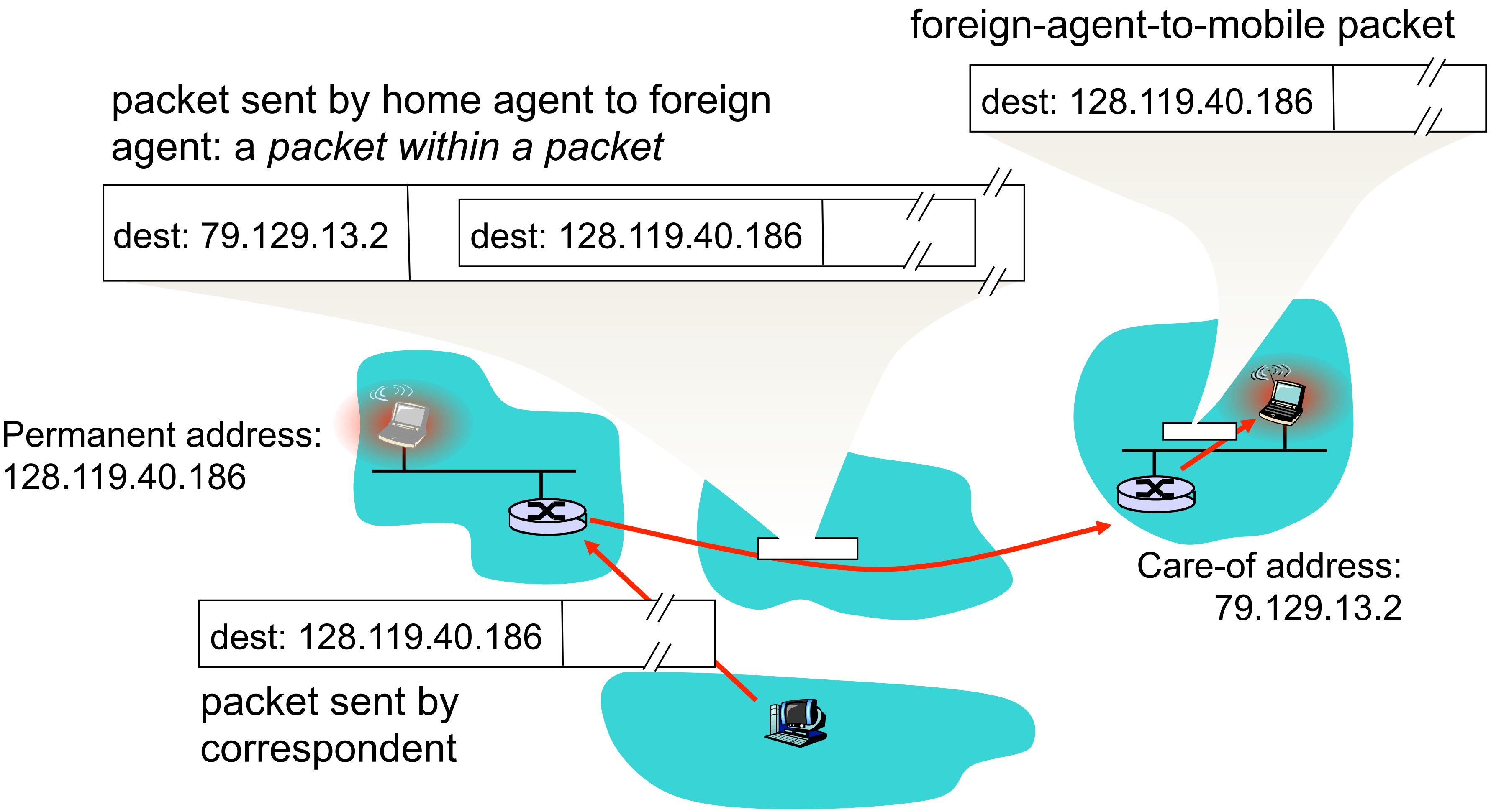
Mobile IP

- RFC 3344 and 5944 for IPv4
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- Three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

Mobile IP

- **Agent Discovery**
  - ✧MN discovers its location (home network, foreign network)
  - ✧MN learns a COA
- **Registration**
  - ✧MN securely signals the COA to the HA (via the FA)
- **Tunneling**
  - ✧HA encapsulates IP packets from CN and sends them to the COA
  - ✧FA (or MN) decapsulates these packets and sends them to the MN

Mobile IP: indirect routing



Agent Discovery

- **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
- **Agent Solicitation**
  - MN can request an Agent Advertisement message with a Agent Solicatation message

    ➔Helps decrease disconnection time
- Simple extension of ICMP Router Discovery (ICMP: Internet Control Message Protocol)

- Other mechanisms can be used to discover the network and the COA (e.g. DHCP)

Agent Advertisement

RFC 1256

0 7	8 15	16 23	24 31
Type = 9	Code = 0	checksum	
#addresses	addr. size	lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			

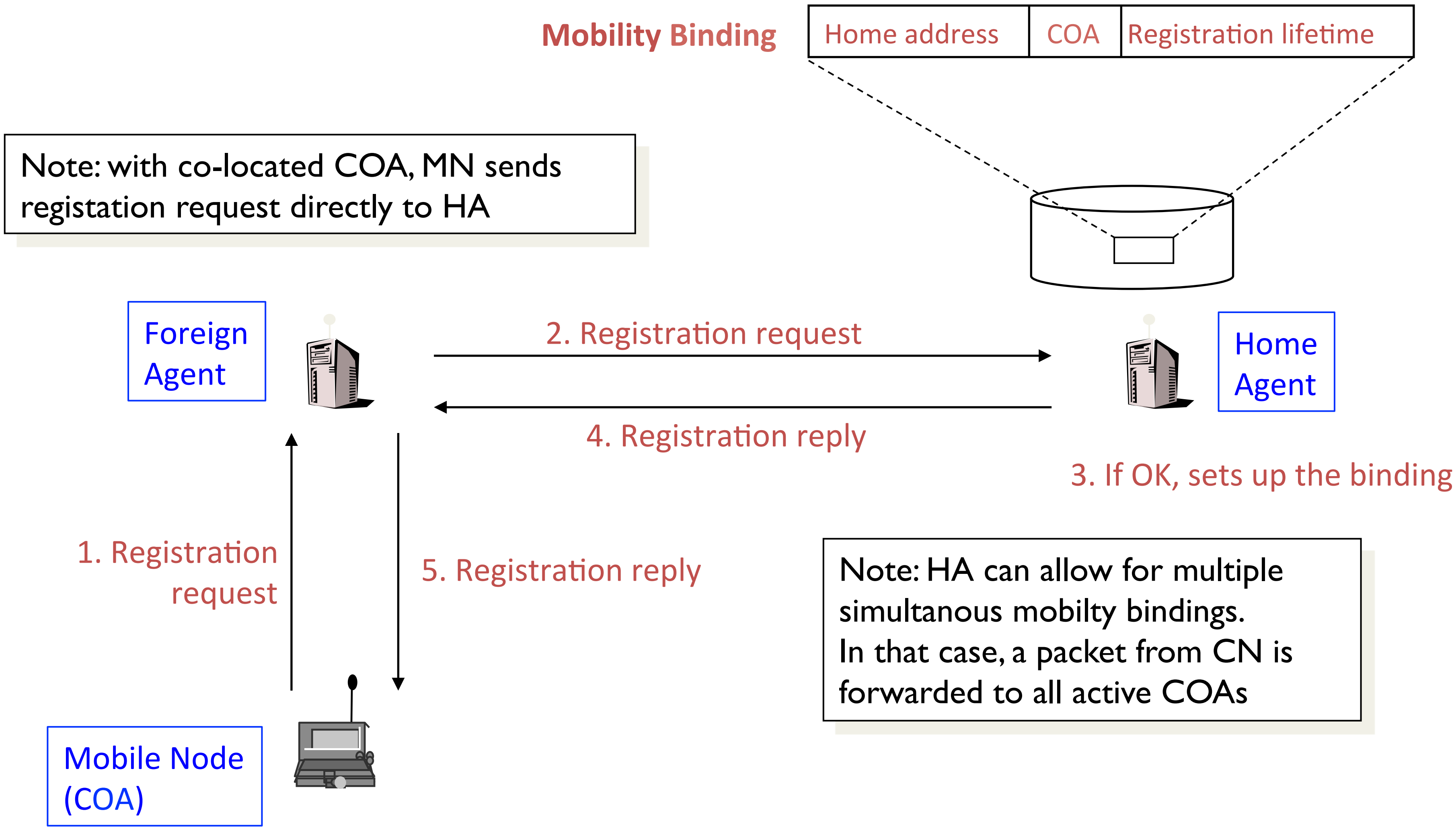
. . .

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 (even for co-located)
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE (Generic Routing Encapsulation)
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Registration



Mobile IP Registration Request

UDP message

0 7	8 15	16 23	24 31
type = 1	S B D M G r T x	lifetime	
home address			
home agent			
COA			
identification			
extensions . . .			

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

identification:
generated by MN, used for matching requests with replies and preventing replay attacks (must contain a timestamp and/or a nonce)

extensions:
mobile-home authentication extension (mandatory)
mobile-foreign authentication extension (optional)
foreign-home authentication extension (optional)

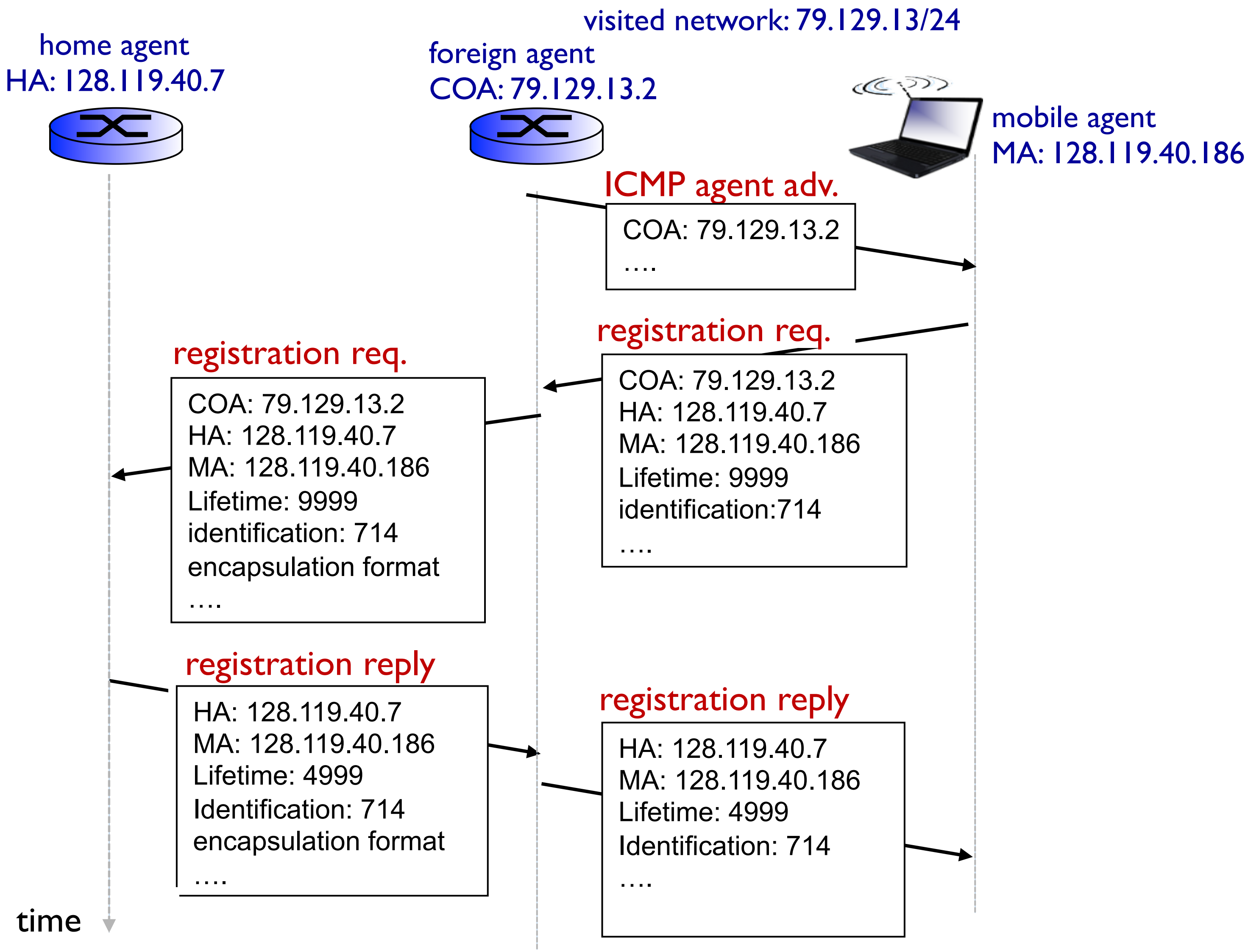
Mobile IP registration reply

UDP message

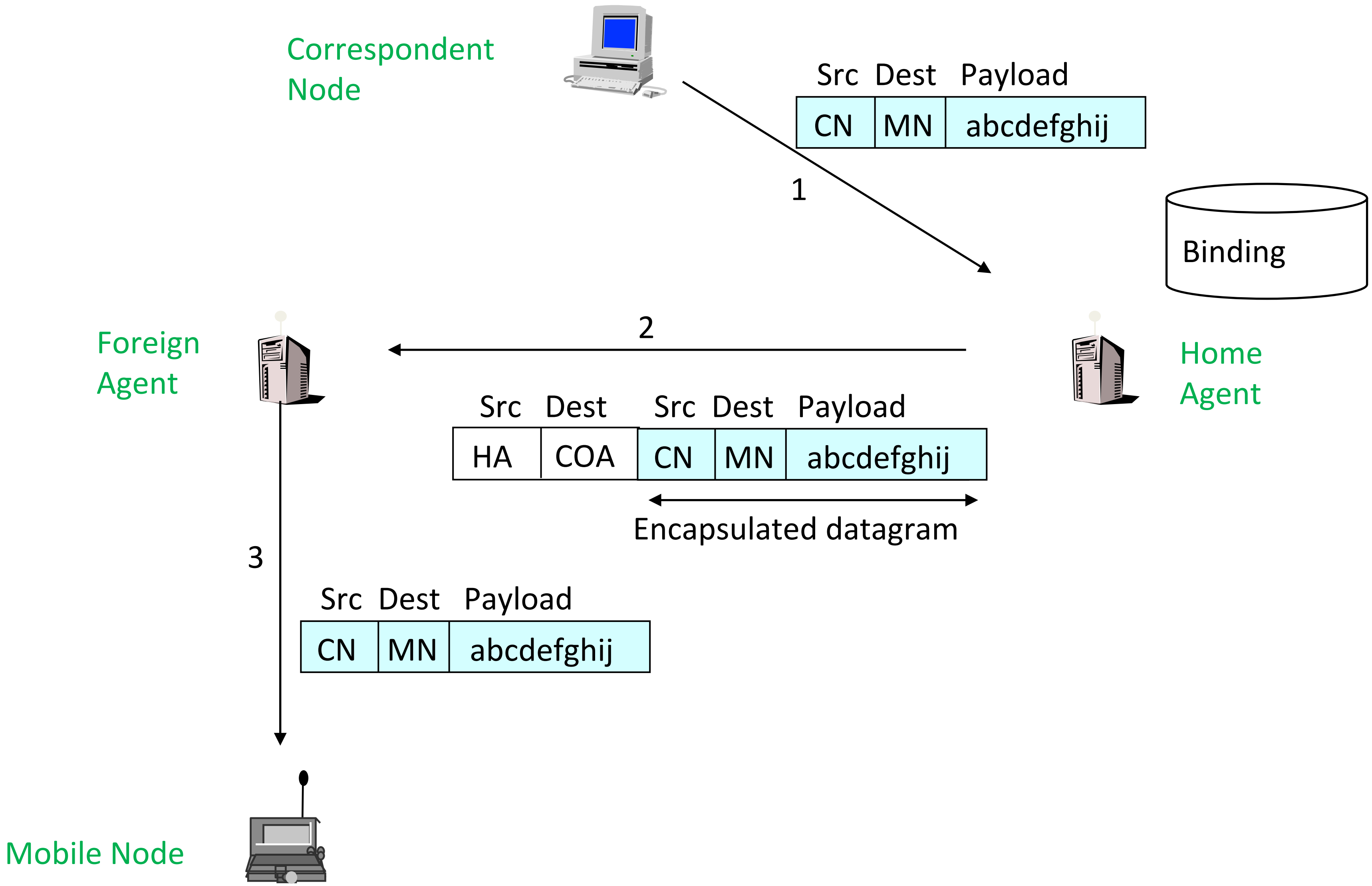
0 7	8 15	16 31
type = 3	code	lifetime
home address		
home agent		
identification		
extensions . . .		

Registration	Code	Explanation
successful	0	registration accepted
	1	registration accepted, but simultaneous mobility bindings unsupported
denied by FA	65	administratively prohibited
	66	insufficient resources
	67	mobile node failed authentication
	68	home agent failed authentication
	69	requested lifetime too long
denied by HA	129	administratively prohibited
	130	insufficient resources
	131	mobile node failed authentication
	132	foreign agent failed authentication
	133	registration identification mismatch
	135	too many simultaneous mobility bindings

Mobile IP: Registration Example



Tunneling



Correspondent
Node
Src Dest Payload
CN MN abcdefghij
1
Binding
2
Foreign
Agent
Home
Agent
Src Dest Src Dest Payload
HA COA CN MN abcdefghij
Encapsulated datagram
3
Src Dest Payload
CN MN abcdefghij
Mobile Node

IP-in-IP Encapsulation

- IP-in-IP-encapsulation
- (RFC 2003, updated by RFCs 3168, 4301, 6040)

<table>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>IP-in-IP</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of HA</td></tr>
<tr><td colspan="5">Care-of address COA</td></tr>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of CN</td></tr>
<tr><td colspan="5">IP address of MN</td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

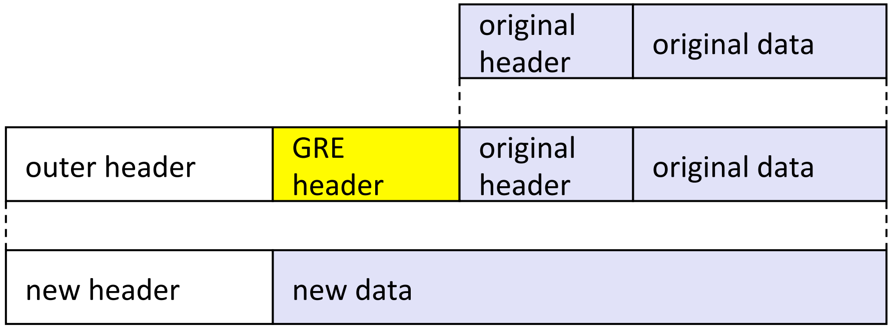
IHL: Internet Header Length
TTL: Time To Live
DS: Differentiated Service
TOS: Type of Service

Minimal Encapsulation

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

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

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								

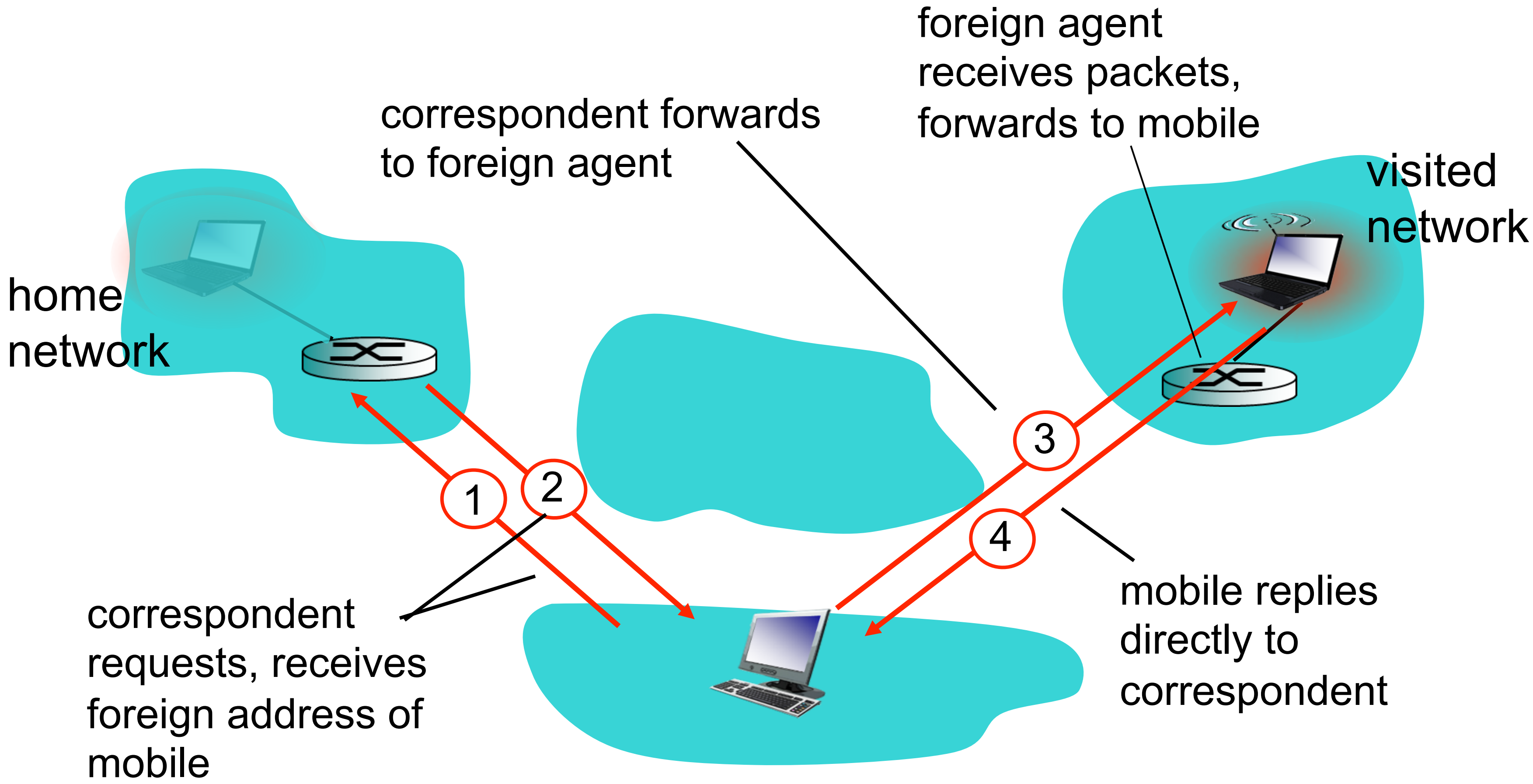
RFC 2784 (updated by 2890)

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

Route Optimization in Mobile IP

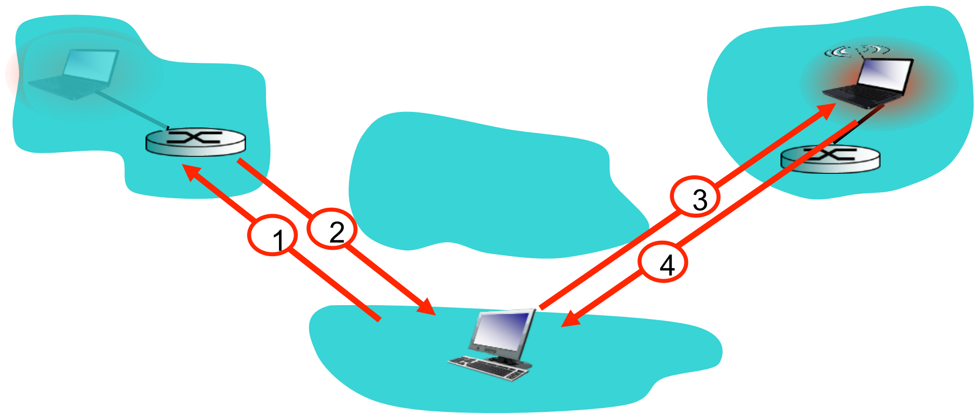
- **Route optimization**
  - HA provides the CN with the current location of MN (FA)
  - CN sends tunneled traffic directly to FA
- **Optimization of FA handover**
  - Packets on-the-fly during FA change can be lost
  - New FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
    - ➔This information also enables the old FA to release resources for the MN

Mobility via Direct Routing



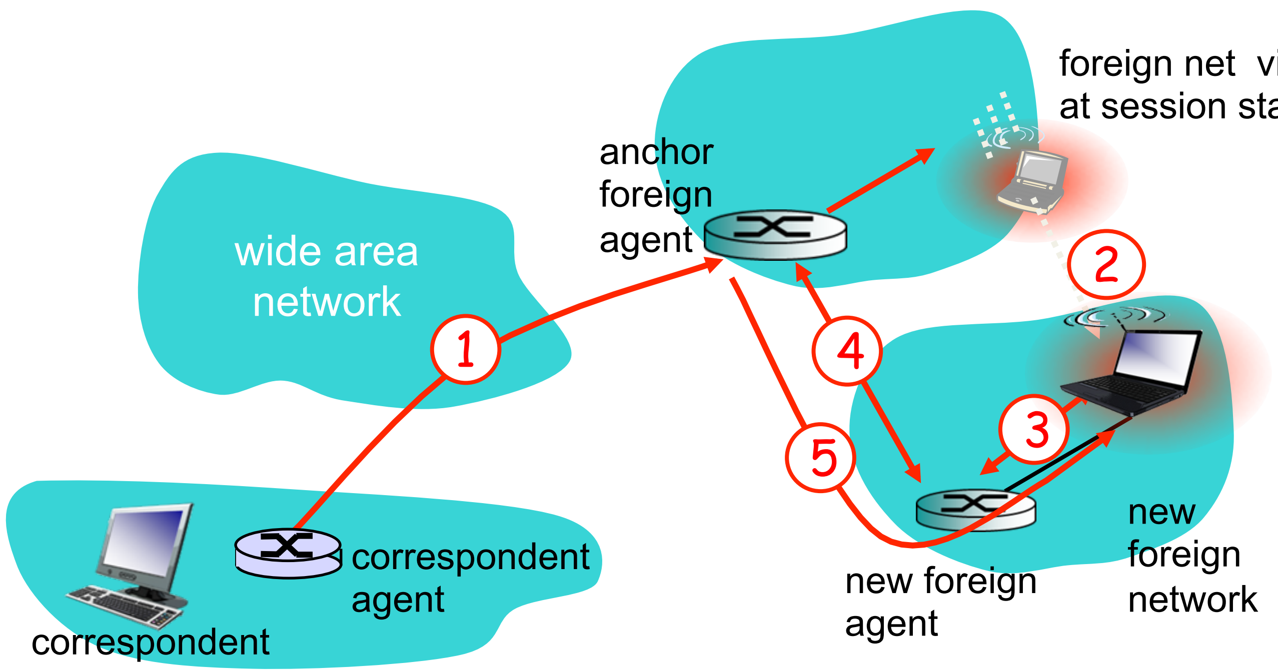
Mobility via Direct Routing: Comments

- Overcome triangle routing problem
- *Non-transparent to correspondent:* correspondent must get care-of-address from home agent
  – what if mobile changes visited network?

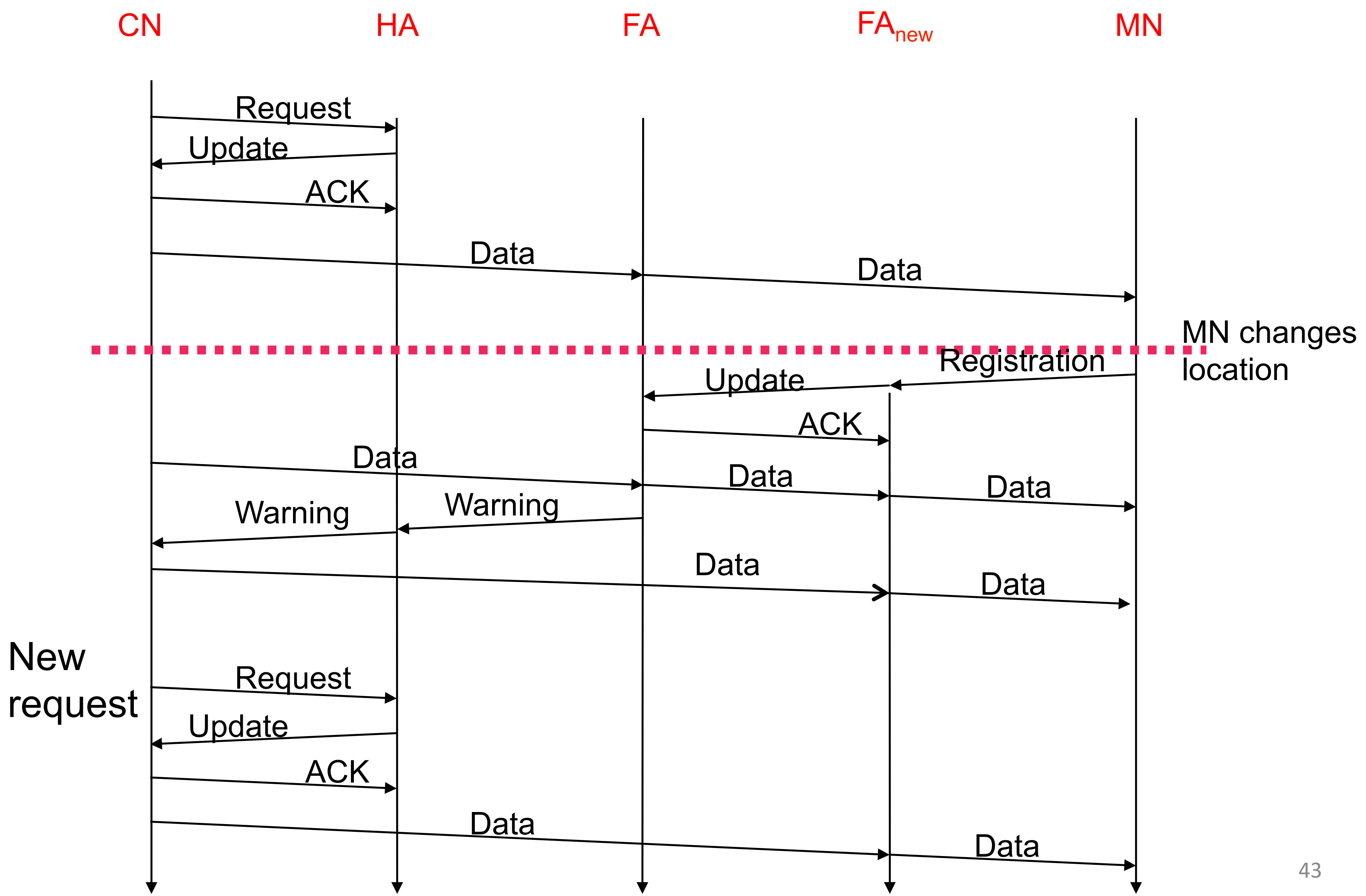


Accommodating Mobility with Direct Routing

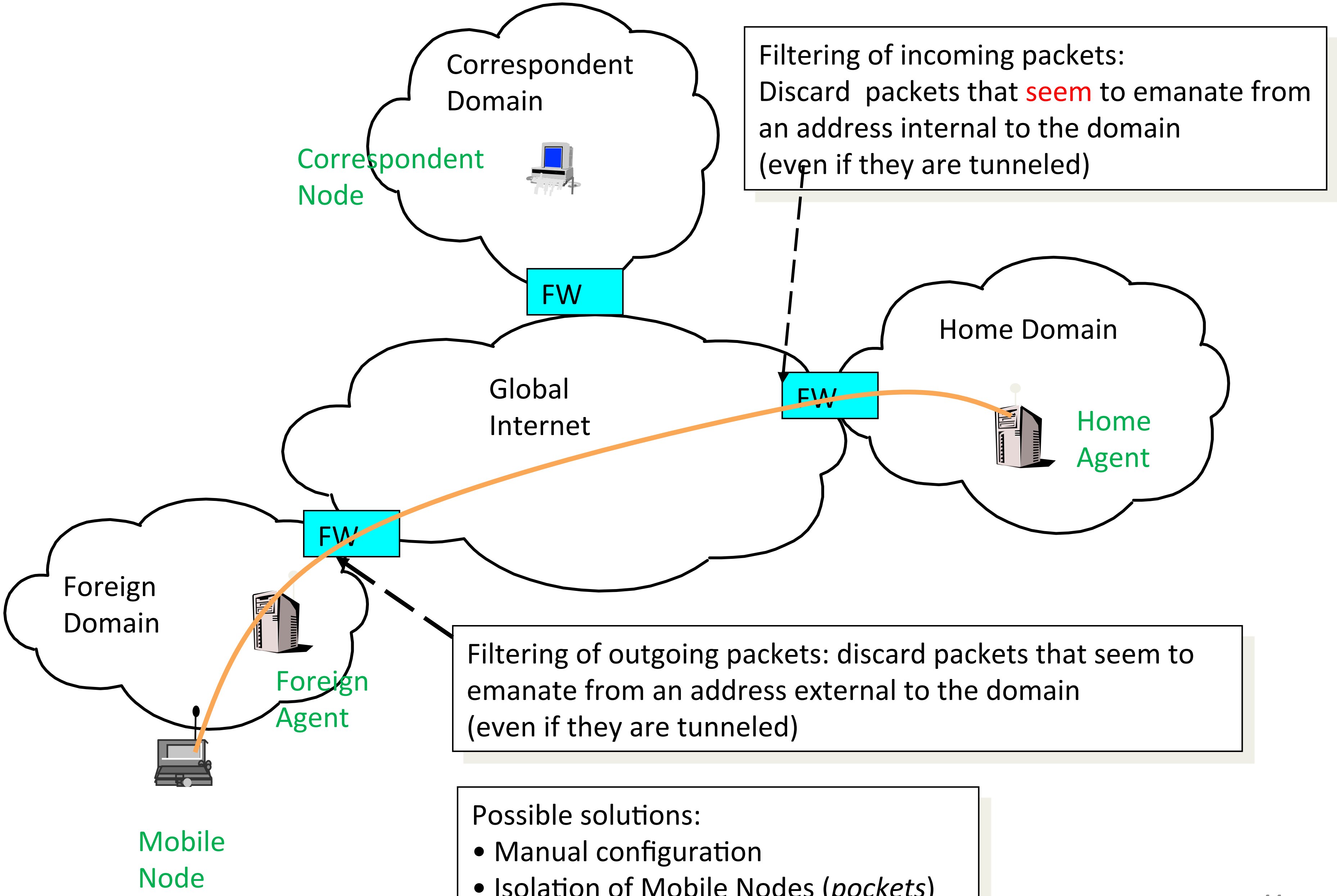
- **Anchor foreign agent**: FA in first visited network
- Data always routed first to anchor FA
- When mobile moves: new FA arranges to have data forwarded from old FA (chaining)



Route and FA Handover Optimizations



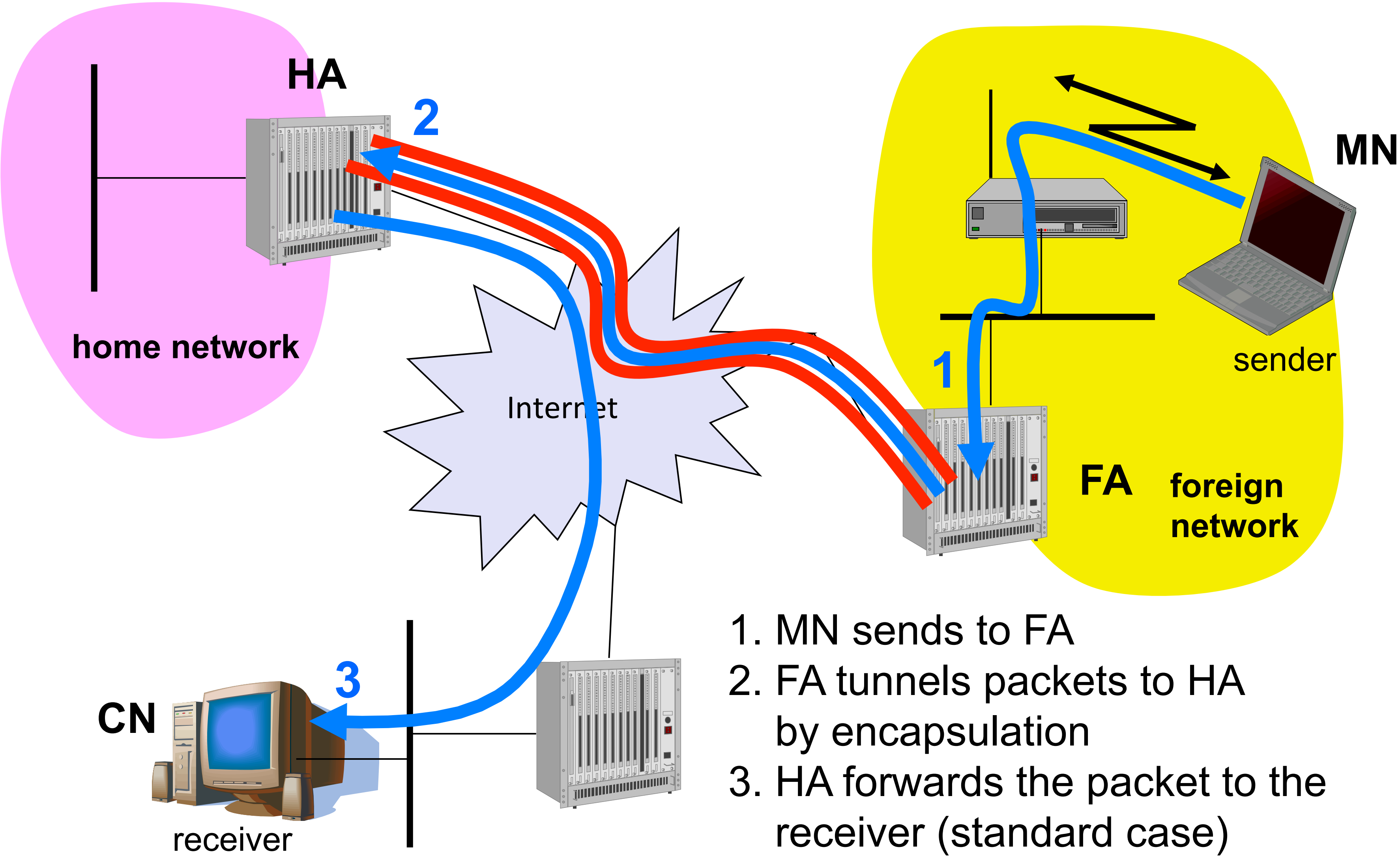
Firewalls



Possible solutions:

- Manual configuration
- Isolation of Mobile Nodes (*pockets*)

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)

Mobile IP with reverse tunneling

- **Reverse tunneling solves ingress filtering problem**
  - A packet from the MN encapsulated by the FA is now topological correct
  - Can cope with mobile routers
  - Protects MN location privacy
  - Multicast and TTL problems solved
- **Reverse tunneling does not solve**
  - Optimization of data paths
    - ➔Double triangular routing
  - Problems with *firewalls*
    - ➔The reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)

Mobile IPv6

- Mobile IPv6 introduces several modifications based on new IPv6 functionality and experiences with Mobile IPv4
  - No FA, COA is always co-located
  - Two modes of operation:
    - ➔Bidirectional tunnel (between HA and COA)
    - ➔Route optimization (MN informs CN about the COA)
  - Security integrated with IPsec (mandatory support in IPv6)
  - "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