IP Mobility

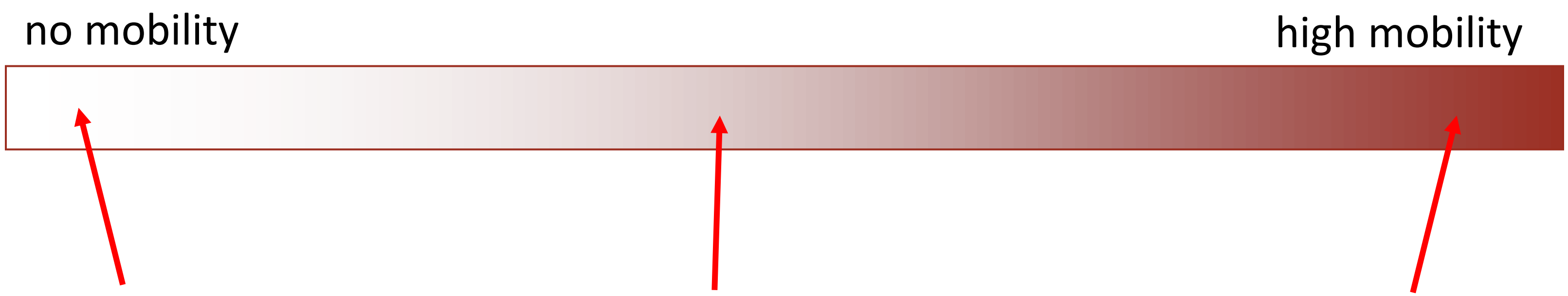
Tópicos Avançados em Redes
2023/2024

References

- Some slides are based on slides from the book “Computer Networking: A Top Down Approach 5th edition”. Jim Kurose, Keith Ross Addison-Wesley, April 2009

What is mobility?

- mobile ≠ wireless
- spectrum of mobility, from the *network* perspective:



no mobility

high mobility

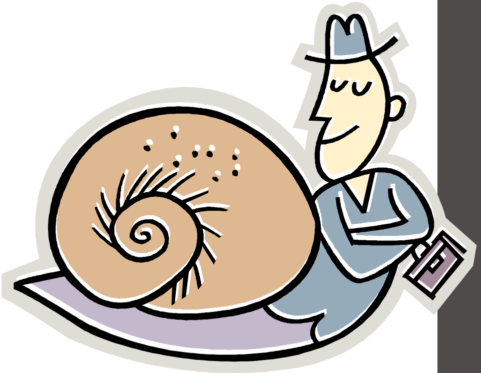
wireless user, using same access point

mobile user, connecting/ disconnecting from network using DHCP

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

Mobile IP – Motivation

- Traditional Routing
  - Based on destination IP address
  - Address prefix determined by physical network
- Mobility implies
  - Changing address (new prefix)
    - Dropping TCP connections
    - DNS updates (delayed propagation due to caching)
    - Security problems
  - Changing routing tables to deliver packets to new location
    - Not scalable
      - Increase in # of mobile terminals
      - Frequent changes of network
    - Security problems
      - Ensuring the right connection endpoint



Mobility: approaches

- Let routing han rs advertise permanent ad le-nodes-in-residence via able exchange.
  - routing tables each mobile located
  - no changes to en

not scalable to millions of mobiles

- Let end-systems handle it:
  - indirect routing: packets for the mobile node forwarded to its current location by an agent in its home network (home agent)
  - direct routing: correspondent learns foreign address of mobile node, then sends packets directly to its current location

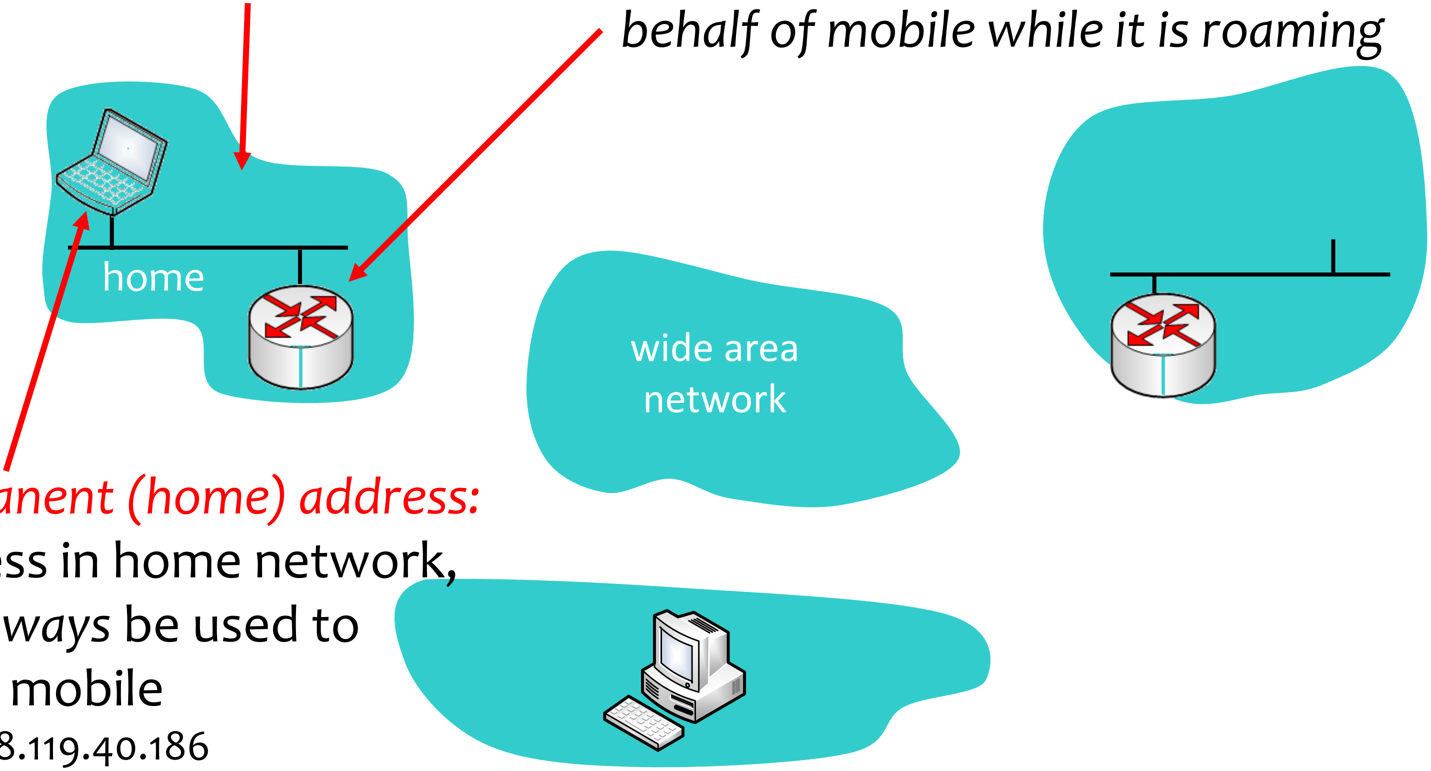
Mobile IP – Motivation

- A solution requires:
  - Keeping the same address, to support Hand-Over
  - Support for the same level 2 protocols as regular IP
  - Authentication of registration messages
- RFC 5944 – IP Mobility Support for IPv4, Revised
- RFC 6275 – Mobility Support in IPv6

Mobility: terminology

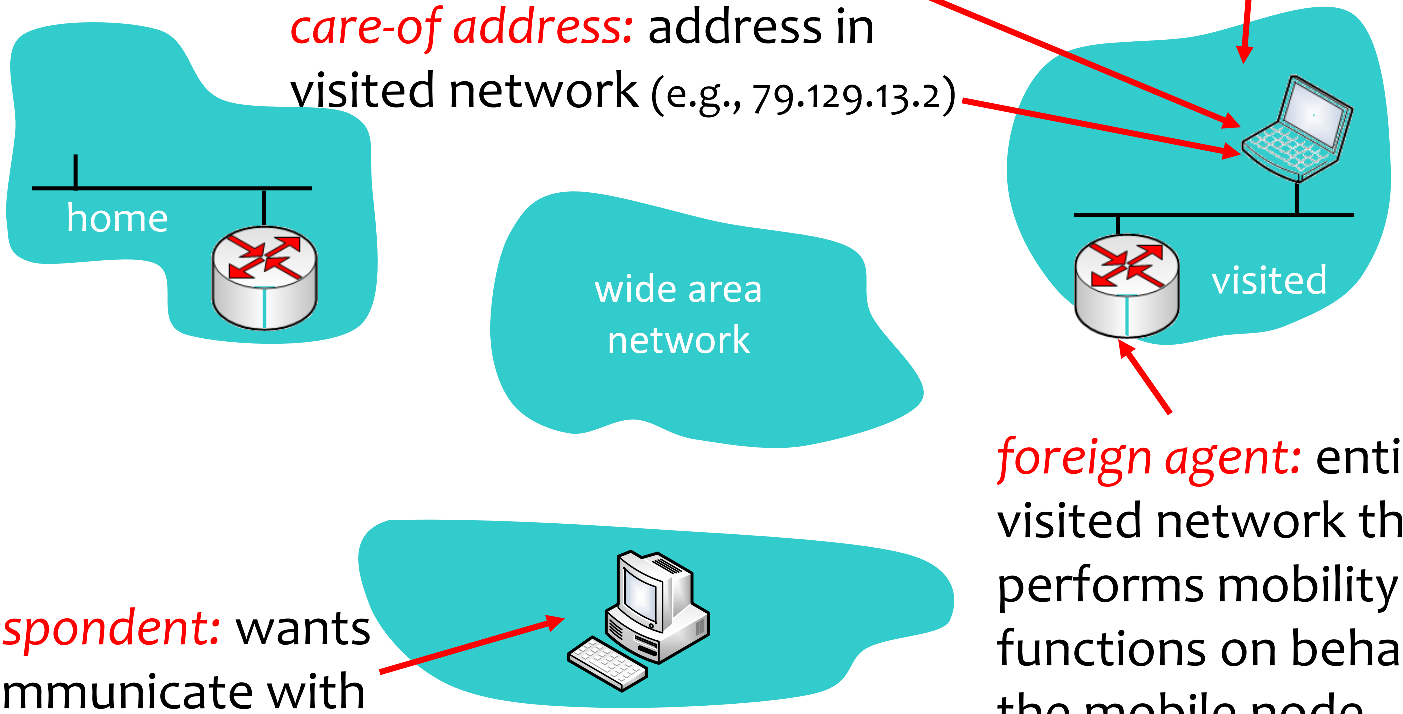
home network: permanent “home” of mobile (e.g., 128.119.40.0/24)

home agent: entity that will perform mobility functions on behalf of mobile while it is roaming



permanent (home) address: address in home network, can *always* be used to reach mobile e.g., 128.119.40.186

Mobility: more terminology



visited network: network in which the mobile node currently is (e.g., 79.129.13.0/24)

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

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 the mobile node

correspondent: wants to communicate with the mobile node

Mobile IP – Concepts

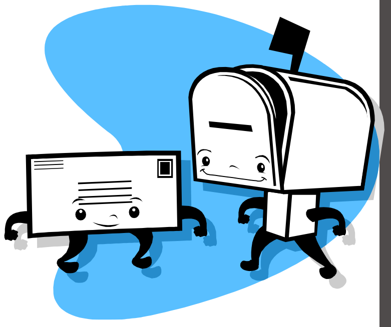
- Mobile Node (MN)
  - The moving node, changes access network
- Home Agent (HA)
  - Node on the home network, usually a router
  - Registers MN location and uses tunneling to send the MN's packets to the visited network
- Foreign Agent (FA)
  - Node on the visited network, usually a router
  - Routes packets from the tunnel to the MN
  - Usually is the MN's default router

Mobile IP – Concepts II

- Care-of Address (CoA)
  - Used to reach the MN at its current (foreign) location
  - Tunnel’s endpoint address (on the FA or MN)
  - Represents the real location of the MN (in terms of IP)
- Correspondent Node (CN)
  - Terminal with which the MN has a connection established
  - Does not need to understand Mobile IP
    - Such need would require changes to all terminals (including servers) on the Internet ➔ infeasible

Mobile IP – Overview

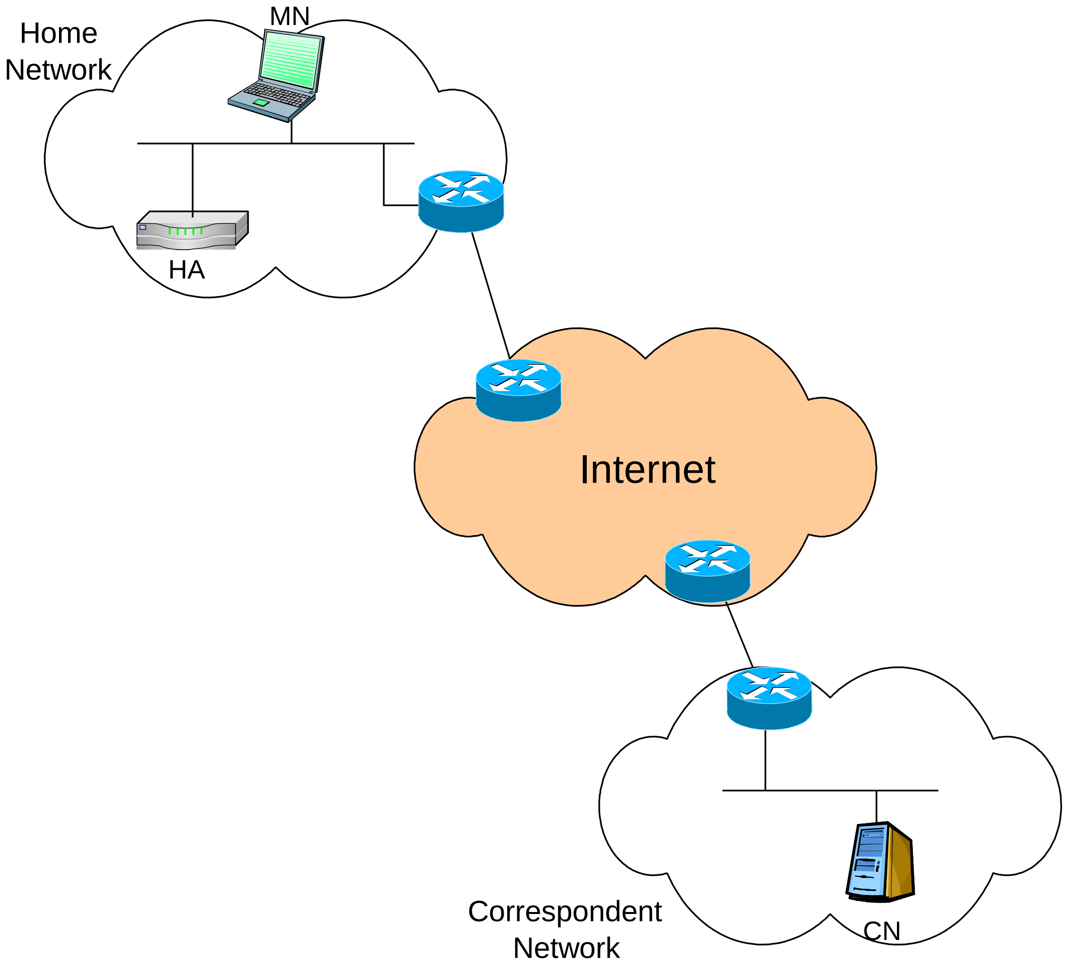
- Two levels of addressing
  - Home Address
    - MN's permanent address
      - MN's address on its home network
    - Used by other nodes to contact MN
    - Used as source address on MN's outgoing connections
  - Care-of Address
    - Address on the visited network



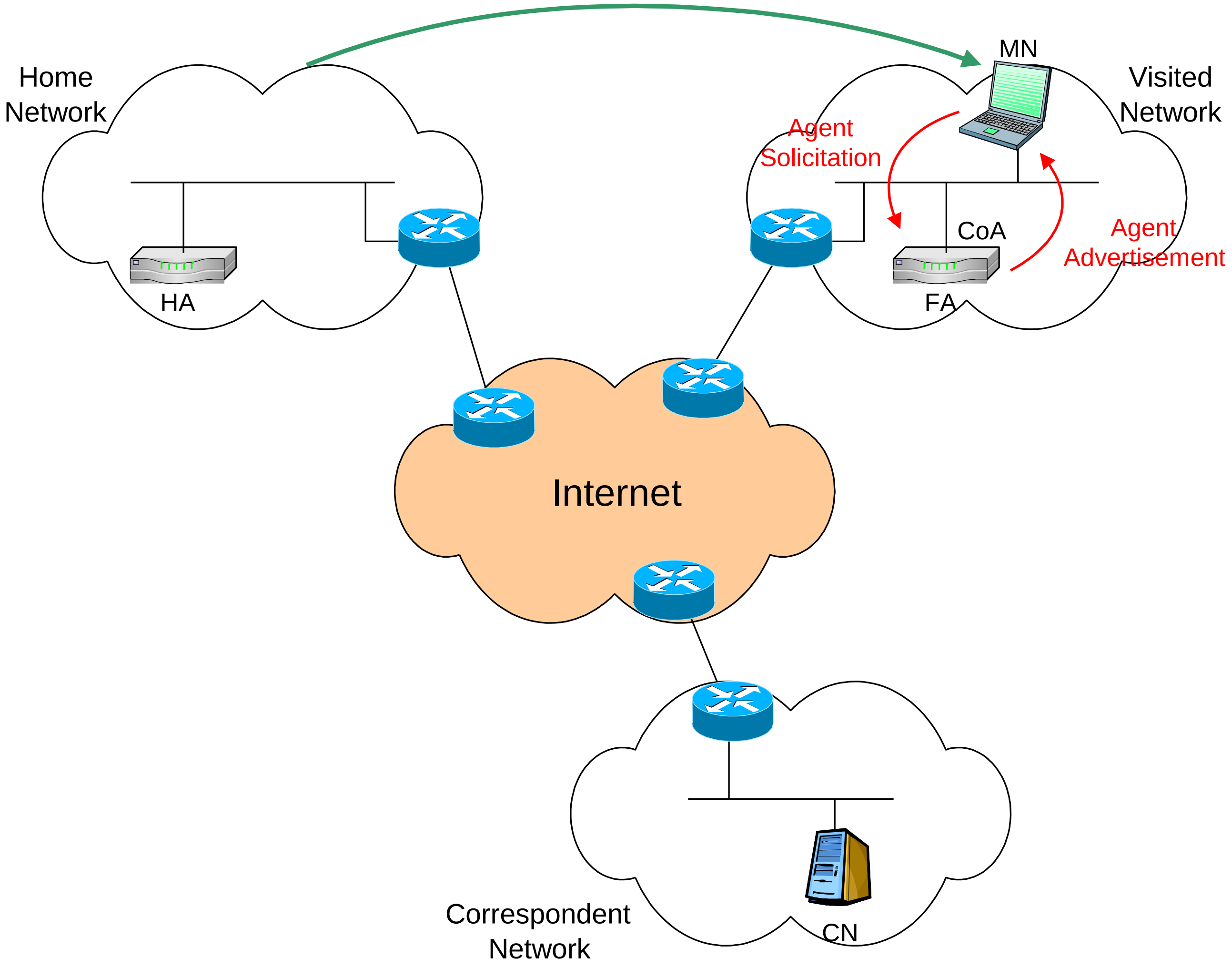
Mobile IP – Functions

- Home Agent
  - Keeps information about CoA of MN
  - Forwards to the CoA (through a tunnel) packets destined for the home address
- Foreign Agent
  - Provides the CoA to the MN
  - Terminates the tunnel from the HA
  - Default router for the MN's packets

MN at home network

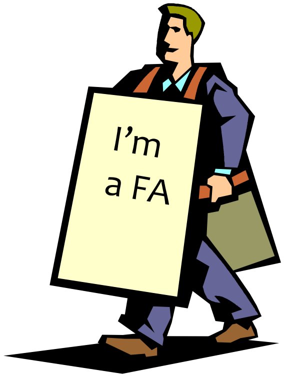


MN moving to foreign network



Mobile IP

- Agent Advertisement
  - HA and FA send periodic advertisements
  - Can be solicited explicitly by MN
  - Extension of Router Advertisement message (RFC1256)
  - These advertisements enable the MN to know whether it is on its home network
- Registration
  - MN informs HA of its CoA (through the FA)
  - HA acknowledges registration (through the FA)
  - Has a lifetime
  - Must be protected by authentication



ICMP Router Advertisement Message

- Sent periodically by router

<table>
<tr><td>Type</td><td>Code</td><td>Checksum</td></tr>
<tr><td>Num Addrs</td><td>Addr Entry Size</td><td>Lifetime</td></tr>
<tr><td colspan="3">Router Address (i)</td></tr>
<tr><td colspan="3">Preference Level (i)</td></tr>
<tr><td colspan="3">…</td></tr>
</table>

Type (8 bits) = 9 Code (8 bits) = 0 Checksum (16 bits)

Num Addrs (8 bits) = Number of routers

Addr Entry Size (8bits) = Number of 32 bit words for each address

Lifetime (16 bits) = Validity time of advertisement (seconds)

Router Address (i = 1..Num Addrs) = IP router's ith address

Preference Level (i = 1..Num Addrs) = Preference level of address i

From RFC1256

Mobility Agent Advertisement Extension

<table>
<tr><td>Type</td><td>Length</td><td colspan="12">Sequence Number</td></tr>
<tr><td colspan="2">Registration Lifetime</td><td>R</td><td>B</td><td>H</td><td>F</td><td>M</td><td>G</td><td>r</td><td>T</td><td>U</td><td>X</td><td>i</td><td>Reserved</td></tr>
<tr><td colspan="14">Zero or more Care-of Addresses</td></tr>
</table>

Type (8 bits) = 16 Length (8 bits) = 6+4*N (N = Nr of CoA)

Sequence Number (16 bits) = Advertisements sent since agent started

Registration Lifetime (16 bits) = registration request longest lifetime

R = Registration required, even if using co-located CoA

B = Busy, no more registrations from MNs

H = Agent is HA on link

F = Agent is FA on link

M = Supports tunnelled datagrams with minimum encapsulation

G = Supports tunnelled datagrams with GRE encapsulation

r = Sent as zero; ignored on reception

T = Foreign agent supports reverse tunnelling

U = Mobility agent supports UDP Tunnelling

X = Mobility agent supports Registration Revocation

I = Foreign agent supports Regional Registration.

From RFC5944#2.1

Mobility Agent Advertisement Extension

- Sent by a mobility agent (HA or FA)
- Sent with the Router Advertisement, after the regular fields

ICMP Router Solicitation Message

- Explicit request by MN (Mobile IP Agent Solicitation)
- Routers respond directly (unicast) to MN
- TTL=1 => answering router must be one hop away

Type	Code	Checksum
Reserved		

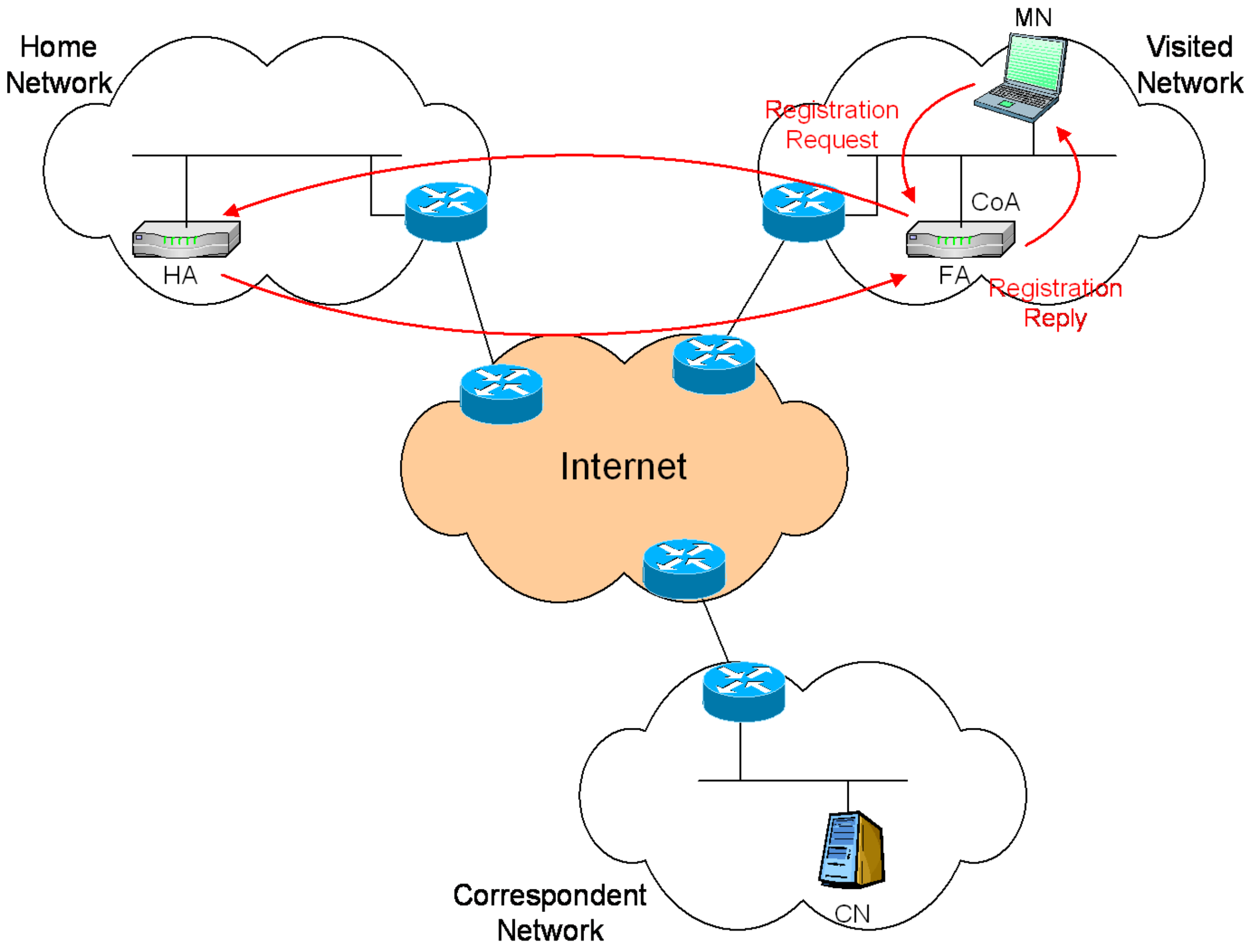
Type (8 bits) = 10 Code (8 bits) = 0 Checksum (16 bits)

Reserved (32 bits) = 0 (Ignored on reception)

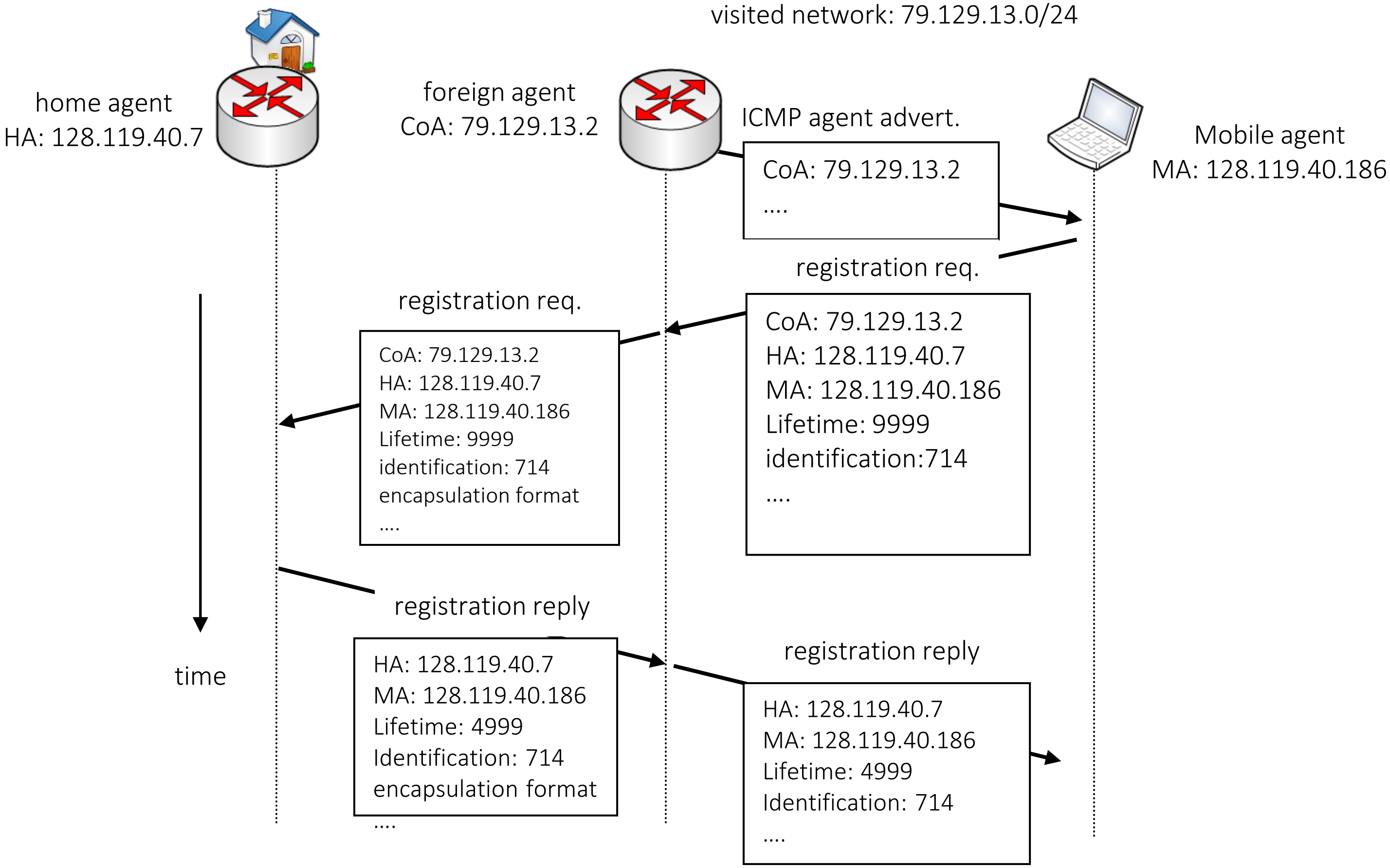
(TTL on IP header = 1)

From RCF1256

Registering (external FA)



Mobile IP: registration example



visited network: 79.129.13.0/24

home agent
HA: 128.119.40.7

foreign agent
CoA: 79.129.13.2

Mobile agent
MA: 128.119.40.186

ICMP agent advert.

CoA: 79.129.13.2
....

registration req.

CoA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification:714
....

registration req.

CoA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification: 714
encapsulation format
....

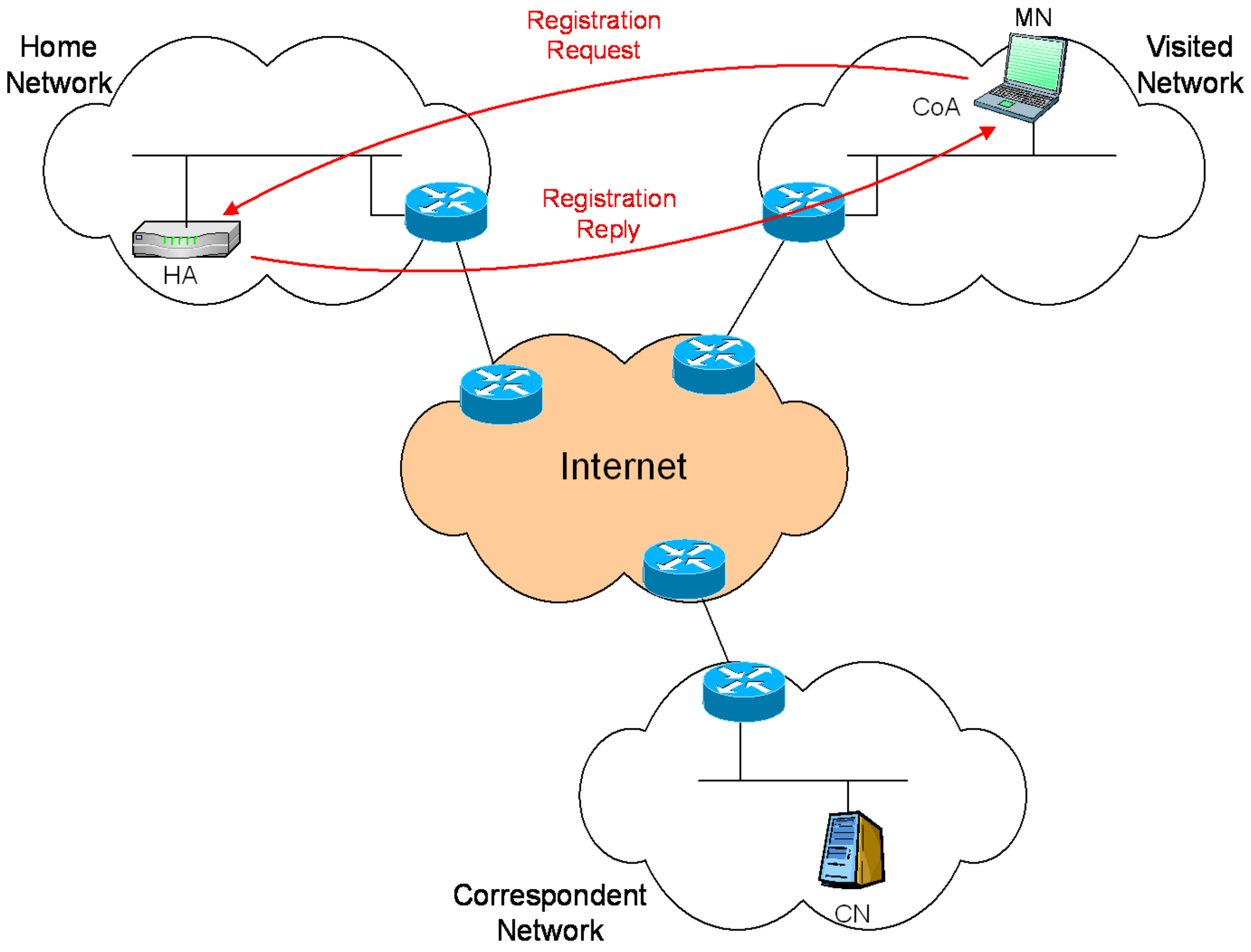
registration reply

HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply

HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
....

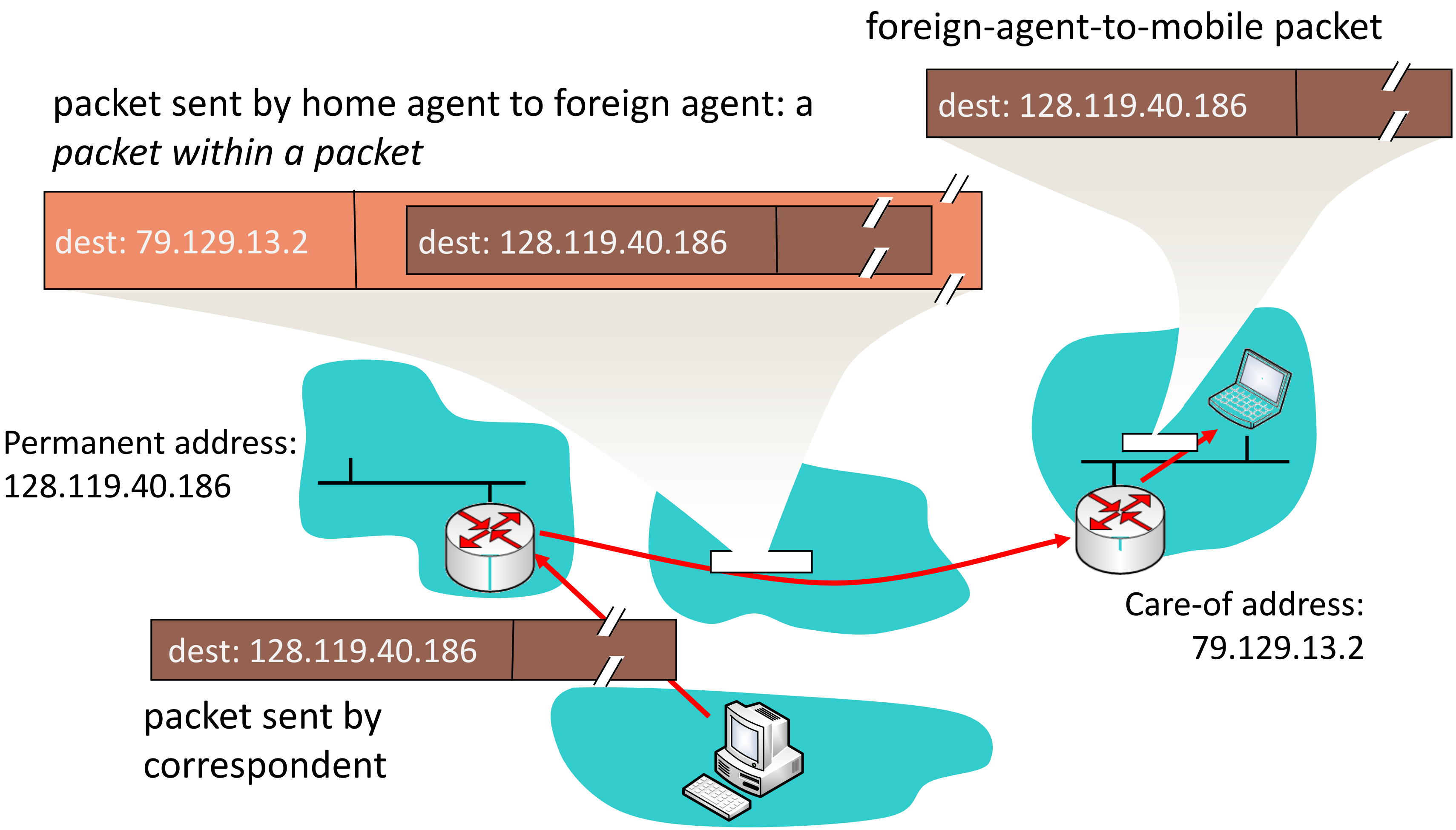
Registering (internal FA)



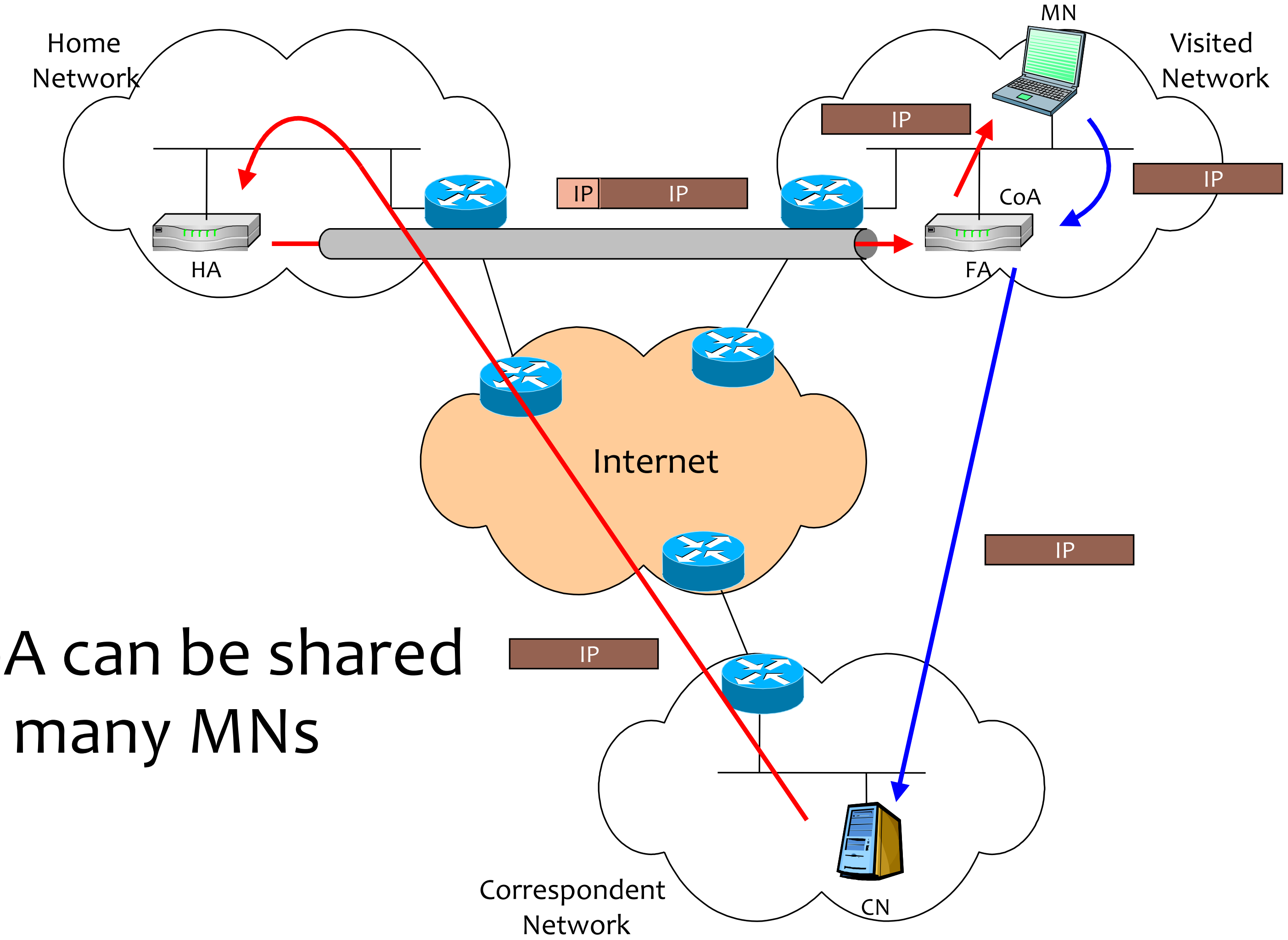
HA registration

- Can be done with or without FA
  - Needs to be through FA if
    - FA supplies CoA (in the advertisement message)
    - FA Advertisement has the R bit set
  - Directly to HA if
    - MN is on home network
    - CoA co-located (CoA obtained through DHCP)
- Re-registration
  - About 3 min. before expiration of lifetime
  - Retransmitted if no answer (> 1 seg.)
- Registration removal
  - Through a registration with lifetime set to zero

Mobile IP: indirect routing

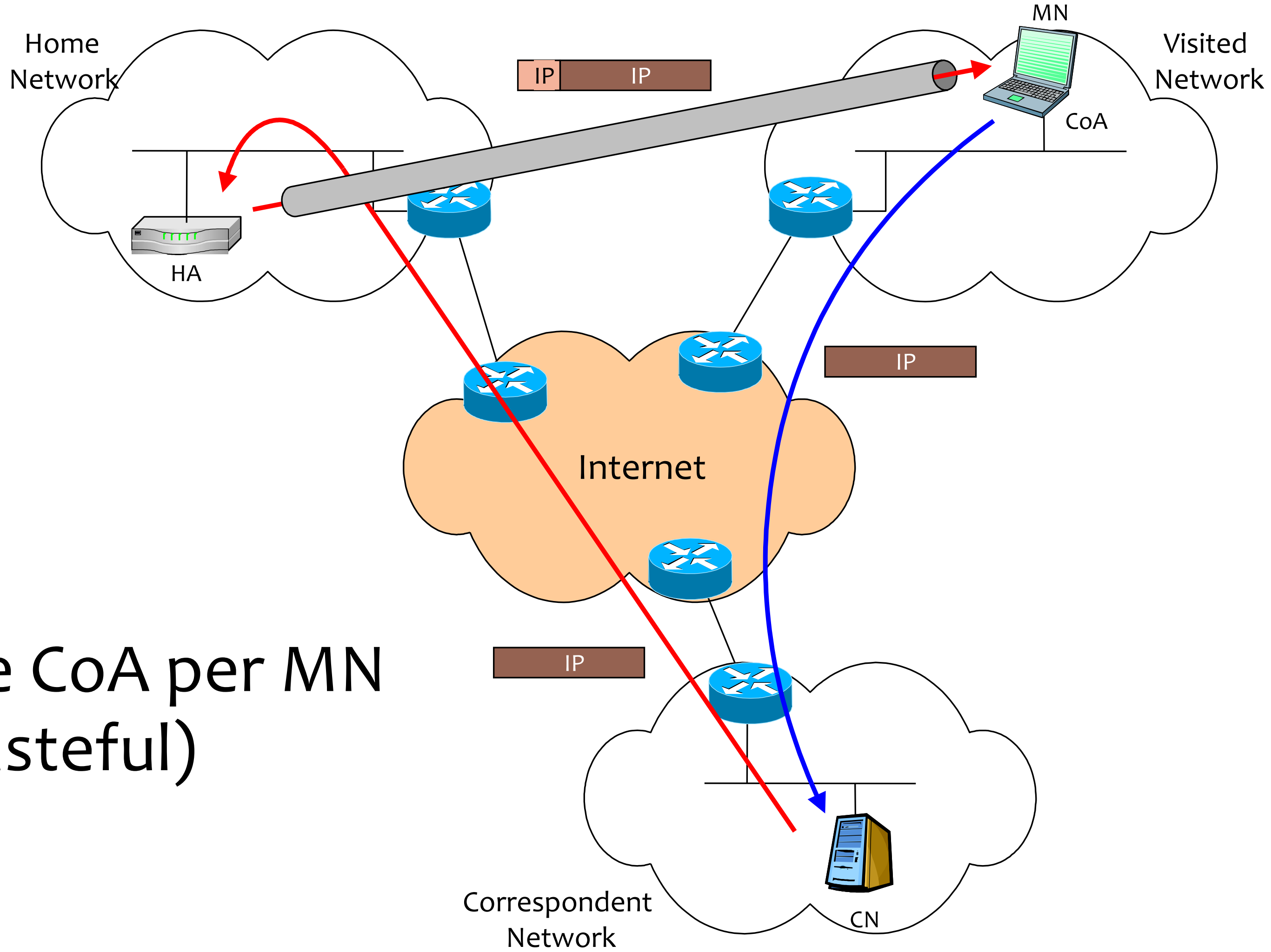


Tunnels (external FA)



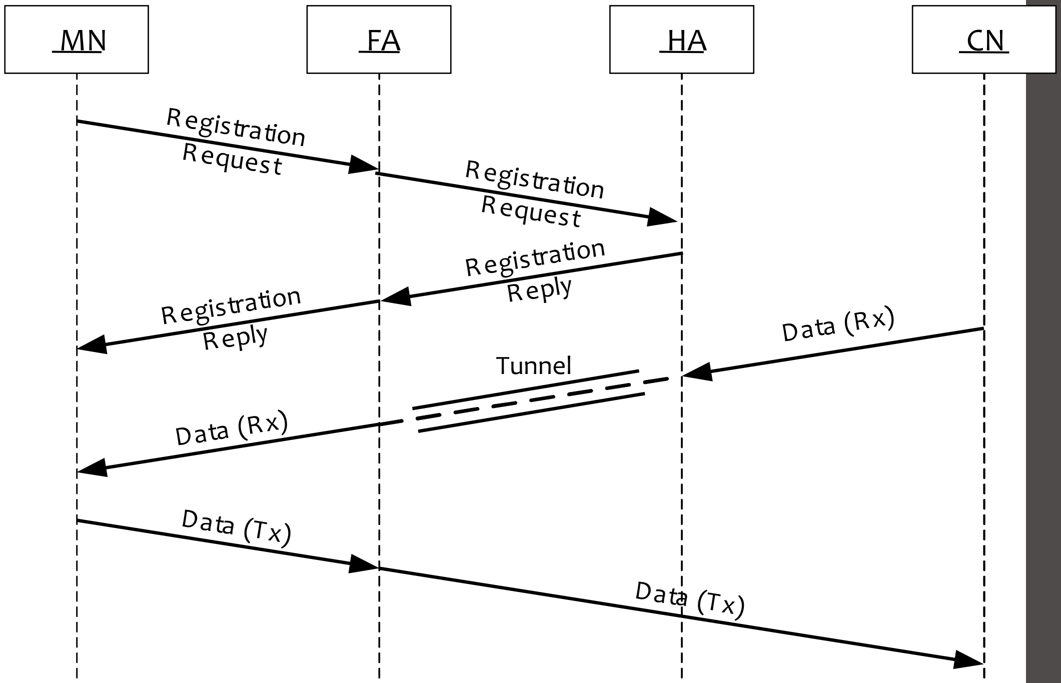
CoA can be shared by many MNs

Tunnels (internal FA)



One CoA per MN (wasteful)

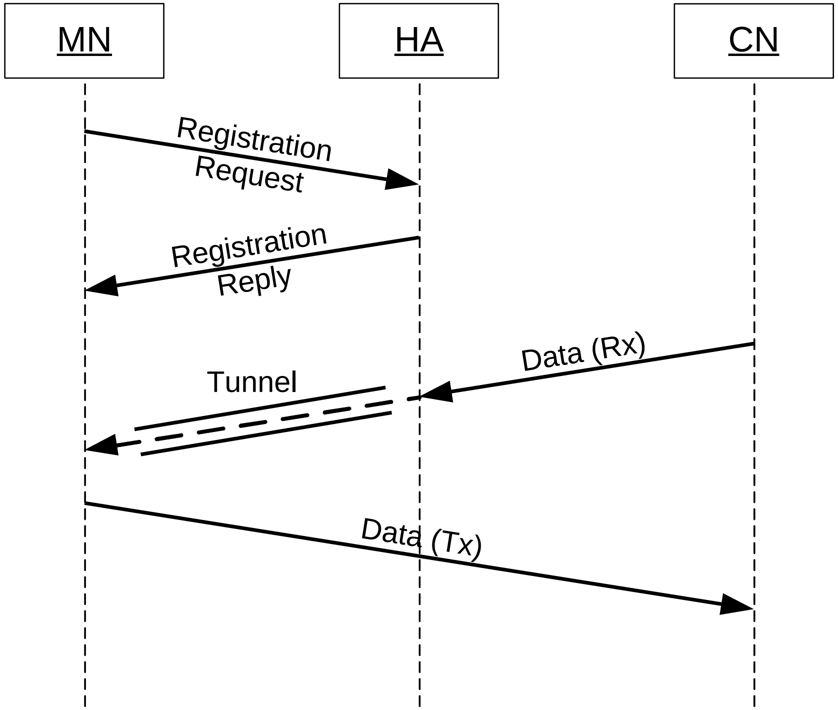
Messages (external FA)



- Two phases
  - Registration
  - Communication
- MN talks with FA
- FA is usually the MN's default router
  - MN may use a different router among those indicated in the Agent Advertisement
- Communication between FA and MN "normal"

Messages (internal FA)

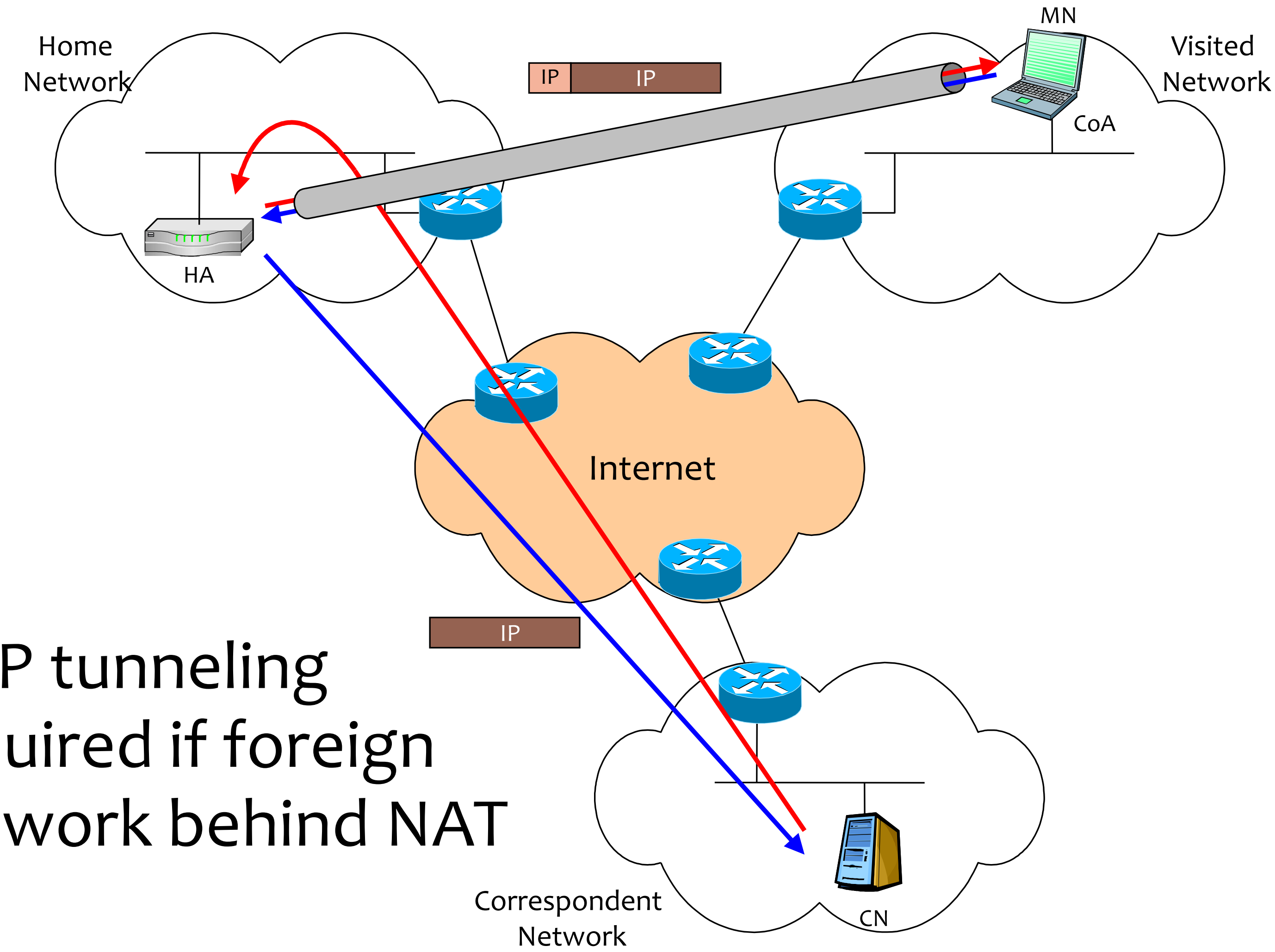
- Two phases
  - Registration
  - Communication
- FA is internal to MN
  - Co-located CoA tunnel
  - Terminated at MN
  - Communication from MN



Triangular Routing: Problem & Solution

- Triangular routing
  - CN –> MN packets go through HA
  - MN –> CN packets go directly
- Problem: ingress filtering (reverse path filtering)
  - Firewalls only allow topologically correct addresses
  - If source address not related with entry itf ➔ drop packet
- Solution
  - Tunneling also for packets from MN (extension)
  - Bit T on Mobility Agent Advertisement Extension, indicating support for reverse Tunnel.
  - RFC 3024 - Reverse Tunneling for Mobile IP, revised

Reverse Tunneling



UDP tunneling required if foreign network behind NAT

ARP, Proxy ARP, and Gratuitous ARP

- RFC5944-Section4.6
- Proxy ARP: sent by HA on behalf of MN
  - Allows nodes on the home network to communicate with the MN when it is abroad
- Gratuitous ARP: sent to update caches
  - Used by HA when MN moves to and from foreign network
  - Also by MN when returning home
- When abroad, MN should not send ARP requests or replies nor send gratuitous ARP for home address
  - It may reply only to ARP requests from the FA

MIPv6

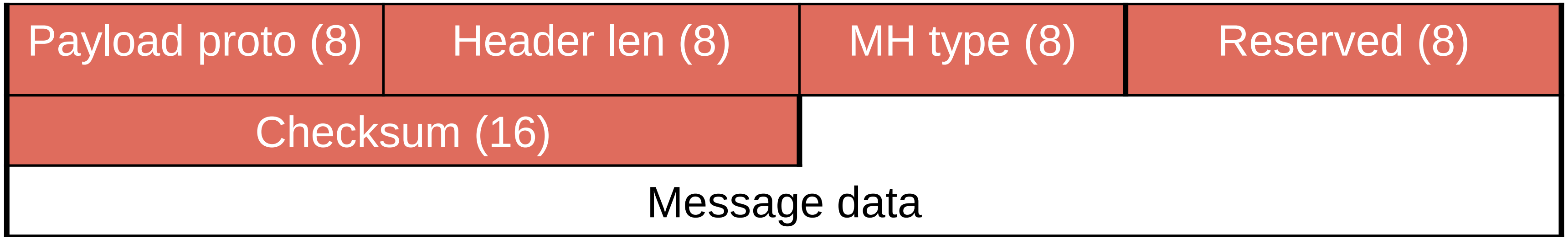
RFC6275

MIPv6

- Adds a new Mobility header to IPv6
  - For several messages, including binding updates
- New Destination Option header
  - Home address
- New ICMPv6 messages
  - For home agent address discovery
- Security built into the protocol from scratch
- Avoids triangular routing
  - Reverse tunnelling or optimized routing

Mobility Header

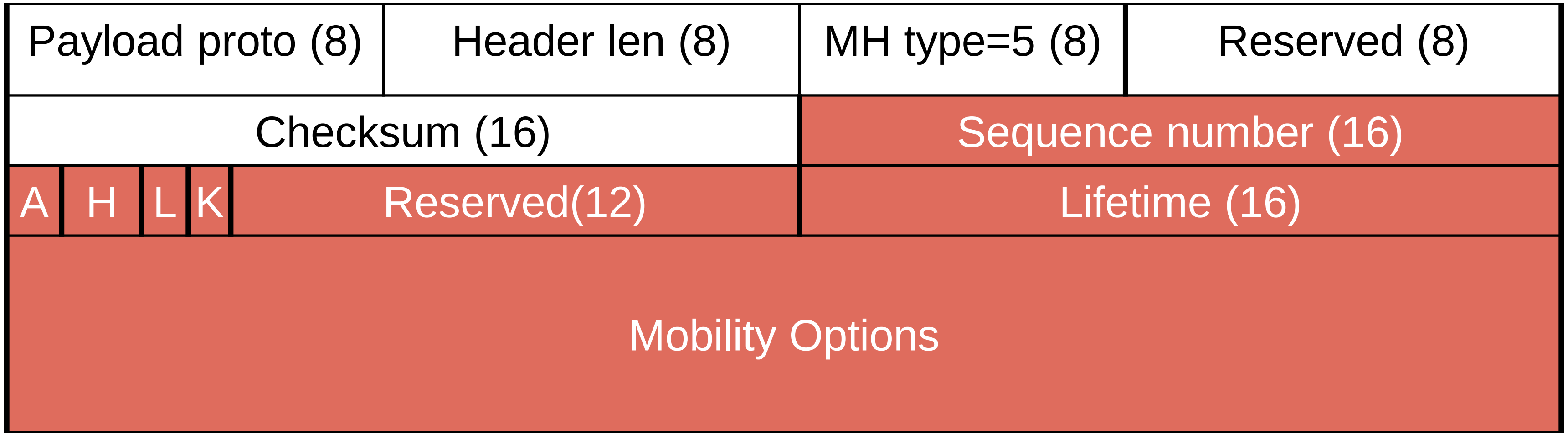
- Used to send mobility messages
- Next-header for this is 135
- Payload Proto: same as IPv6 next header
- MH type: identifies the specific message



Payload proto (8)	Header len (8)	MH type (8)	Reserved (8)
Checksum (16)			
Message data			

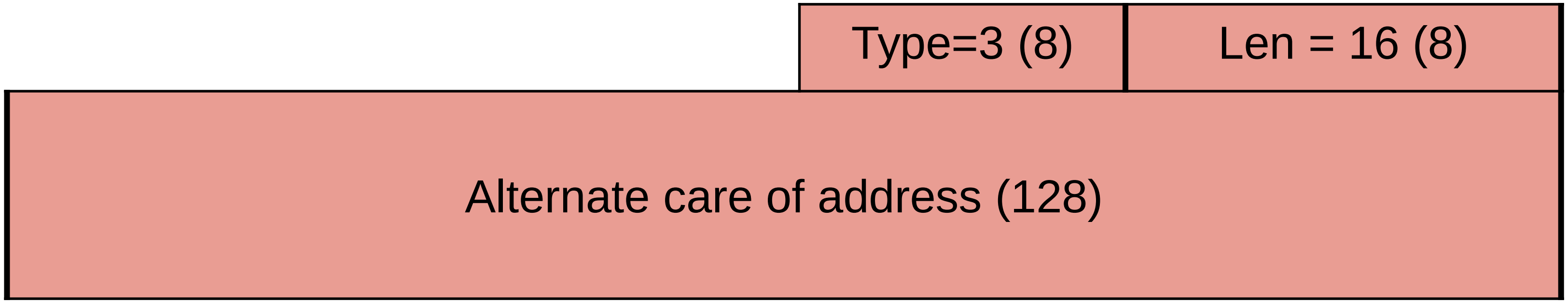
Binding update (BU)

- Used to notify HA (or other nodes) of current CoA
- Mobility Header type = 5
- Sequence number: used to match BU with Ack
- Lifetime: time to expiration of the BU (in 4 sec units)
  - A lifetime of 0 means deletion of entry



<table>
<tr><td colspan="4">Payload proto (8)</td><td colspan="2">Header len (8)</td><td>MH type=5 (8)</td><td>Reserved (8)</td></tr>
<tr><td colspan="6">Checksum (16)</td><td colspan="2">Sequence number (16)</td></tr>
<tr><td>A</td><td>H</td><td>L</td><td>K</td><td colspan="2">Reserved(12)</td><td colspan="2">Lifetime (16)</td></tr>
<tr><td colspan="8">Mobility Options</td></tr>
</table>

BU – Mobility Option for CoA



Type=3 (8)

Len = 16 (8)

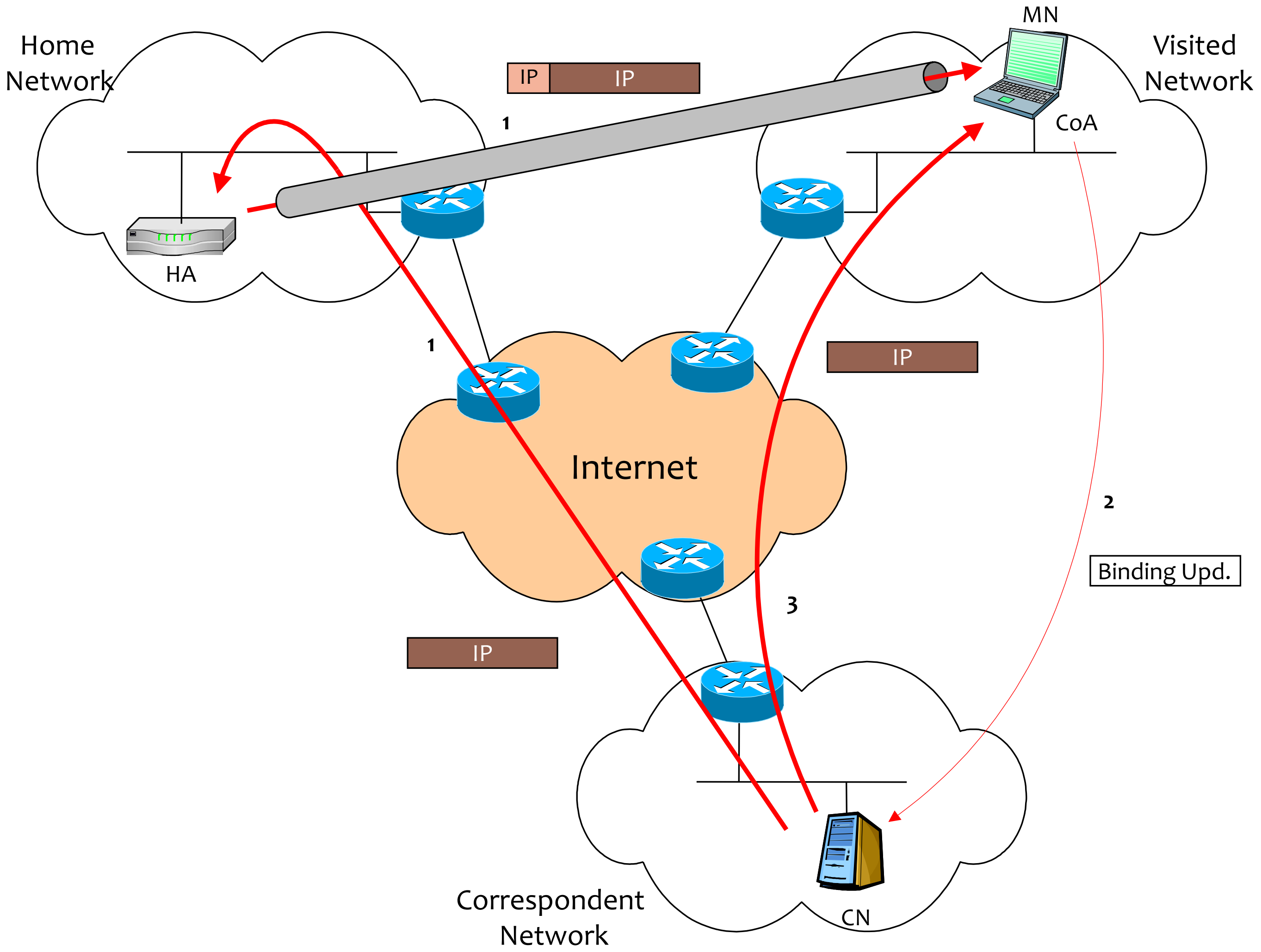
Alternate care of address (128)

- Not mandatory
- CoA determined
  - From the Alternate CoA Mobility Option, if present
  - Else from the Source Address of the IPv6 header

Optimization: Binding Update to CN

- Requires support in CN
- Binding Cache
  - Located at the CN
  - Has CoAs of MNs
- Packets are sent directly to the MN
  - HA no longer part of the path
- If CoA is unknown (not in Binding Cache), packets will go through the HA
- Cache updated by Binding Updates
  - With a lifetime

Optimization: Binding Update to CN



Cache entries at CN or HA

- Lifetime: remaining time for the cache entry
- Sequence no: max no received in previous BUs

Home address	Care-of-address	Seq. no	Lifetime	Flags
1ee3:44bb:34:24:3:1:2:1	34ef:35e:3:4:3:a3:45:42	23	2078	A/H
1ee3:44bb:34:24:d:c:d:a	4ff2:345:3:4:5:a:4:4	230	320	A/K

Binding acknowledgement

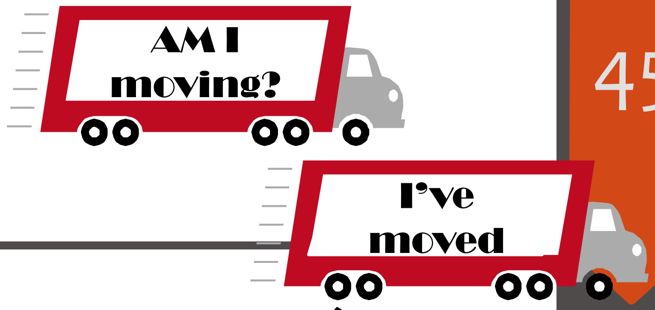
- MH type = 6
- Includes status field
  - < 128: BU accepted
  - ≥ 128: BU rejected
- Lifetime
- Sequence number: copied from BU

<table>
<tr><td>Payload proto (8)</td><td>Header len (8)</td><td>MH type=6 (8)</td><td colspan="2">Reserved (8)</td></tr>
<tr><td colspan="2">Checksum (16)</td><td>Status (8)</td><td>K</td><td>Reserved (7)</td></tr>
<tr><td colspan="2">Sequence number (16)</td><td colspan="3">Lifetime (16)</td></tr>
<tr><td colspan="5">Mobility Options</td></tr>
</table>

Binding acknowledgement options

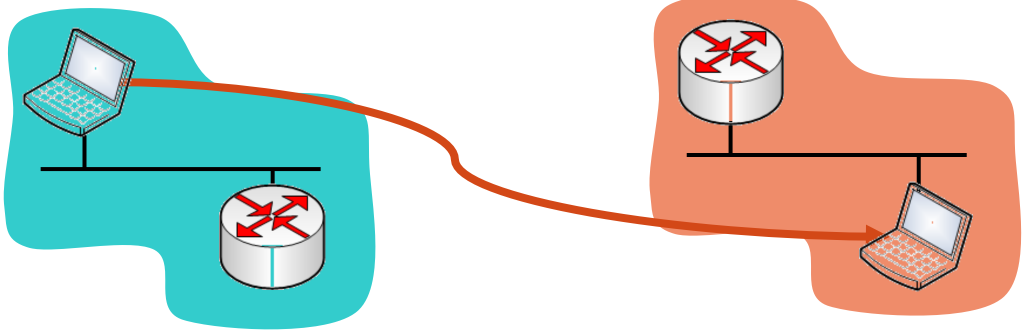
- Type-Length-Value (TLV) encoded
  - Similarly to BU options
- Options
  - Authorization data
  - Refresh advice

Movement detection



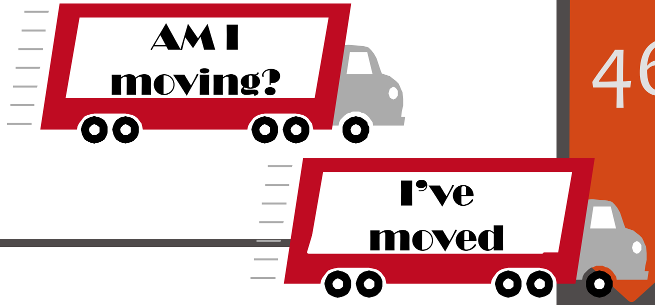
- New prefix appears on link (Router Advert.)
- Unreachability of old router can be detected using NUD
    - Send Router Solicitation to obtain new prefix faster

Prefix: 34ef:35e:3:4::

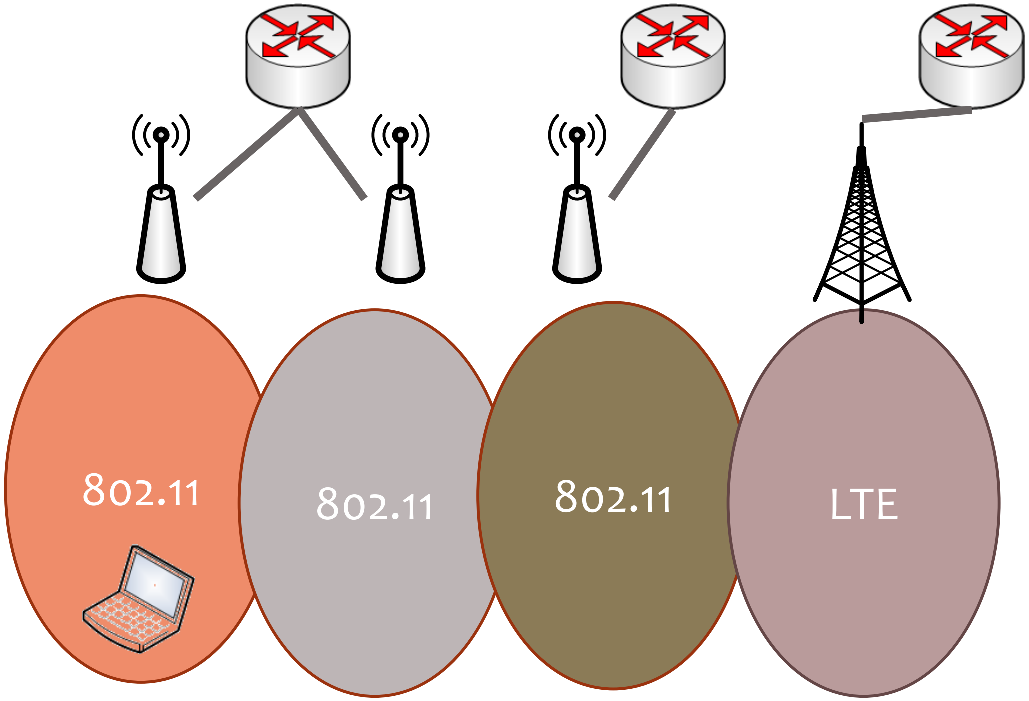


Prefix: 4ff2:345:3:4::

Movement detection II



- Detection through Router Adv. / NUD can be slow
- If possible, get notified of link change from lower layers



Back home

- BU with 0 lifetime
- Problem with source address of packet:
  - If at home use Home Address… But HA “uses” Home address…
    - DAD would fail for mobile node
  - =>Do not use DAD for the home address configuration
- Must use neighbour solicitation to know HA's link-layer address
- RFC6275#11.5.5

Back home – HA link-layer address

- MN sends Neighbor Solicitation
  - Source IP: unspecified address (::)
  - Dst IP: Solicited-Node multicast address (of the MN's home address)
  - Target: MN's home address
- HA sends Neighbor Advertisement to multicast address
  - Source IP: address assigned to the interface where advertisement is sent
  - Dst IP: all-nodes multicast address
  - Target: MN's home address
- MN knows HA link layer address from the advertisement
  - Can now send the BU

Route optimization

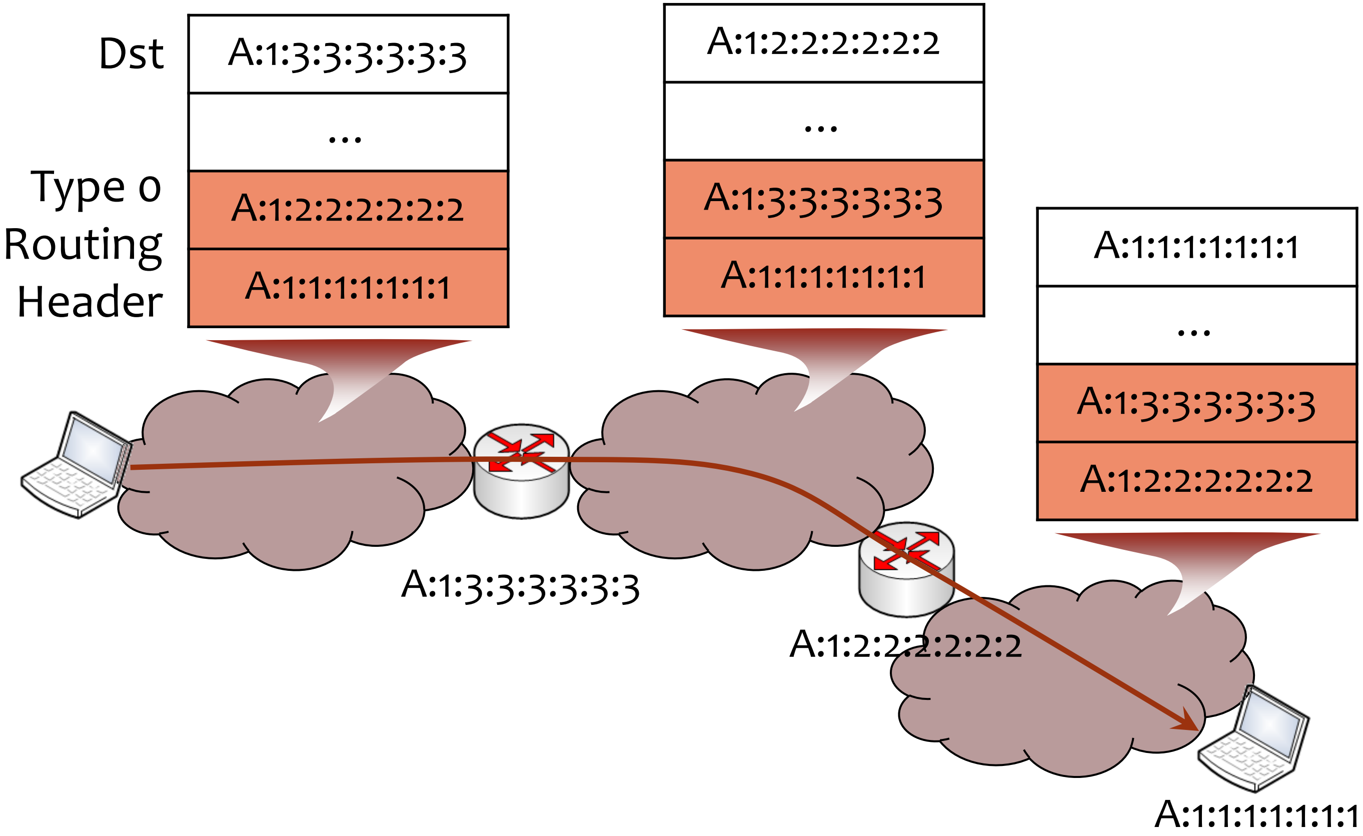
- MN sends BU to CN
- CN keeps a binding cache, similarly to the HA
- CN can use CoA of MN as destination address
- MN can use the CoA as source address
  - Without suspicion of forgery
- Q: How to ensure authenticity of BU?
  - Security Association established on the fly using the Return Routability procedure (more on this later…)

Remember IPv6 Routing header?

- IPv6 routing header was used for loose source routing
  - Now deprecated for security reasons
- Addresses are the next destination(s) of the packet
- Segments Left: route segments remaining

Next Header(8)	Header ext Len(8)	Routing Type (8)	Segments left (8)
Address [1] (128)			
Address [2] (128)			
…			

Source routing in IPv6 (deprecated)

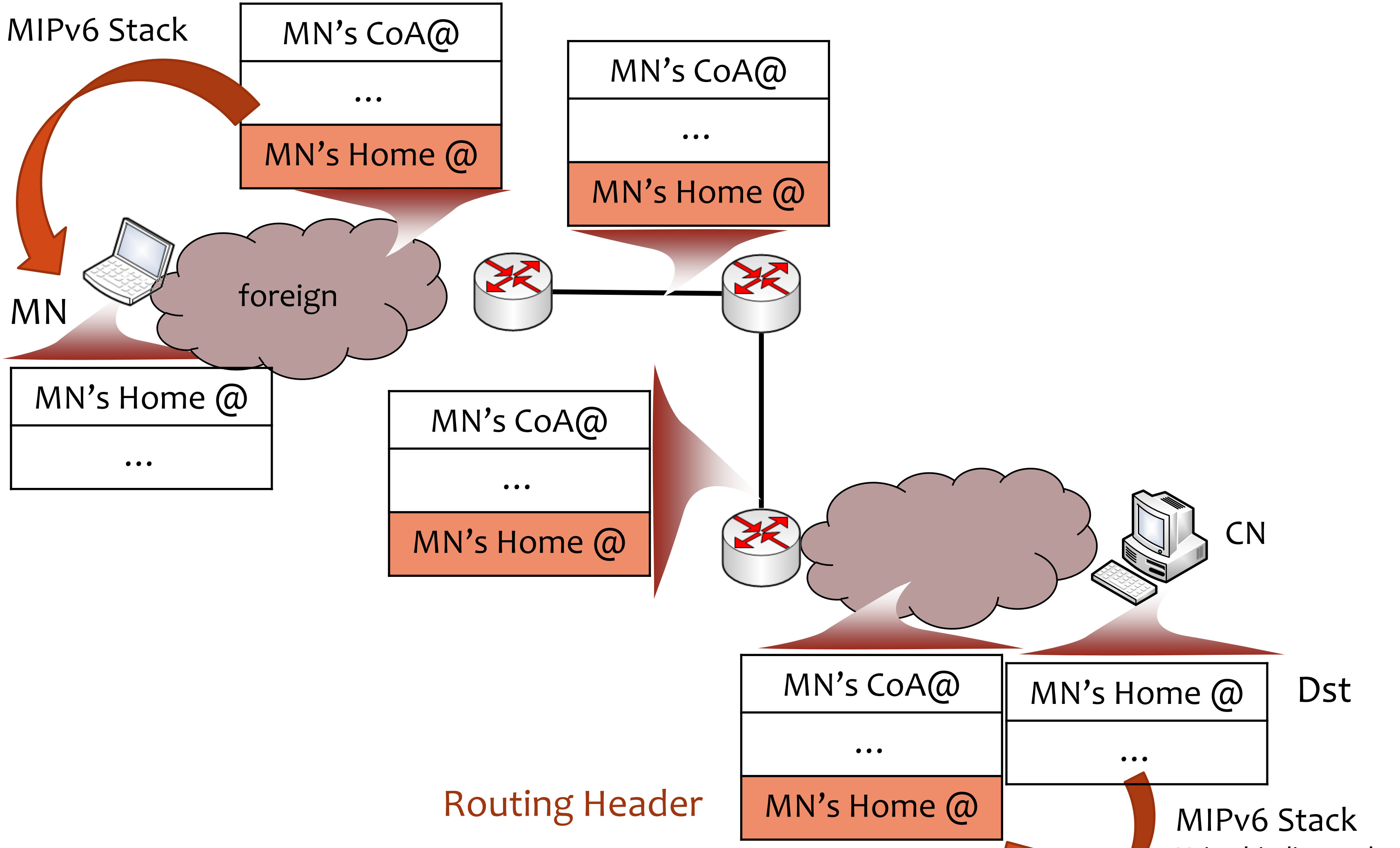


Source is always the same: original sender

Route optimization: CN → MN

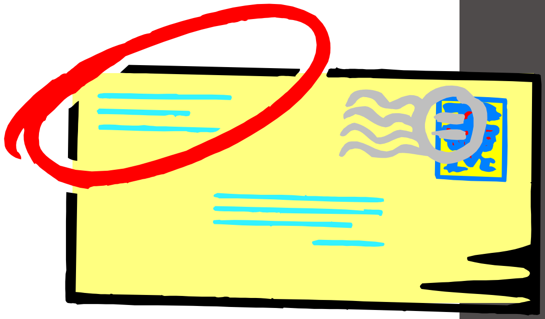
- CN sends packets to the CoA
- Adds a Routing header with Home Address
  - Type 2 routing header (not deprecated)
    - A type 2 RH carries a single address, therefore is safe
- MN replaces CoA in dst address with Home Address

Route optimization: CN → MN



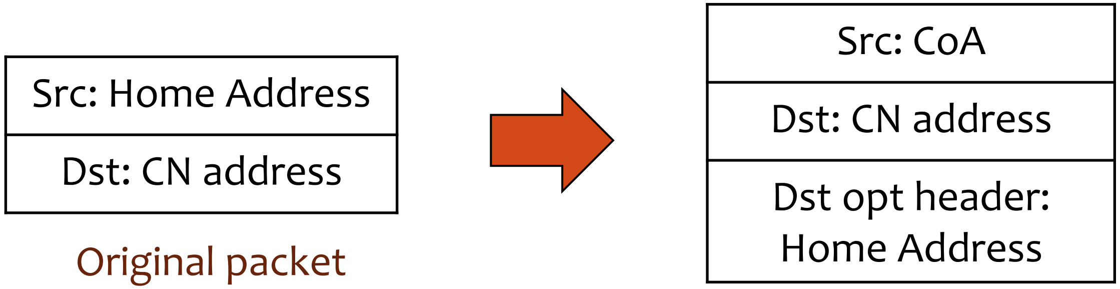
Route optimization: MN → CN

- Problem with *source address*
  - HA is topologically incorrect
- MN sends packets with
  - CoA as Src address
  - Home Address option containing the HA
    - Carried in an IPv6 Destination Option extension header
    - Processed at the CN



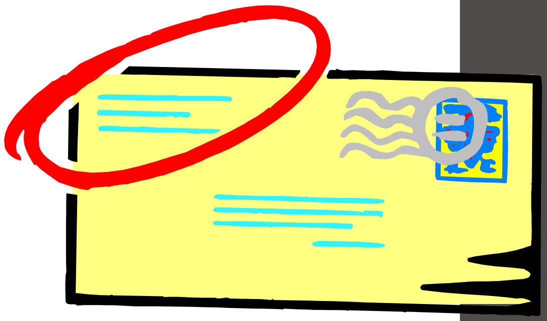
Route optimization: MN → CN

- MN adds the destination Home Address option to every packet that has the Home Address as source address



Original packet from application

Packet actually sent, with Home Address destination option



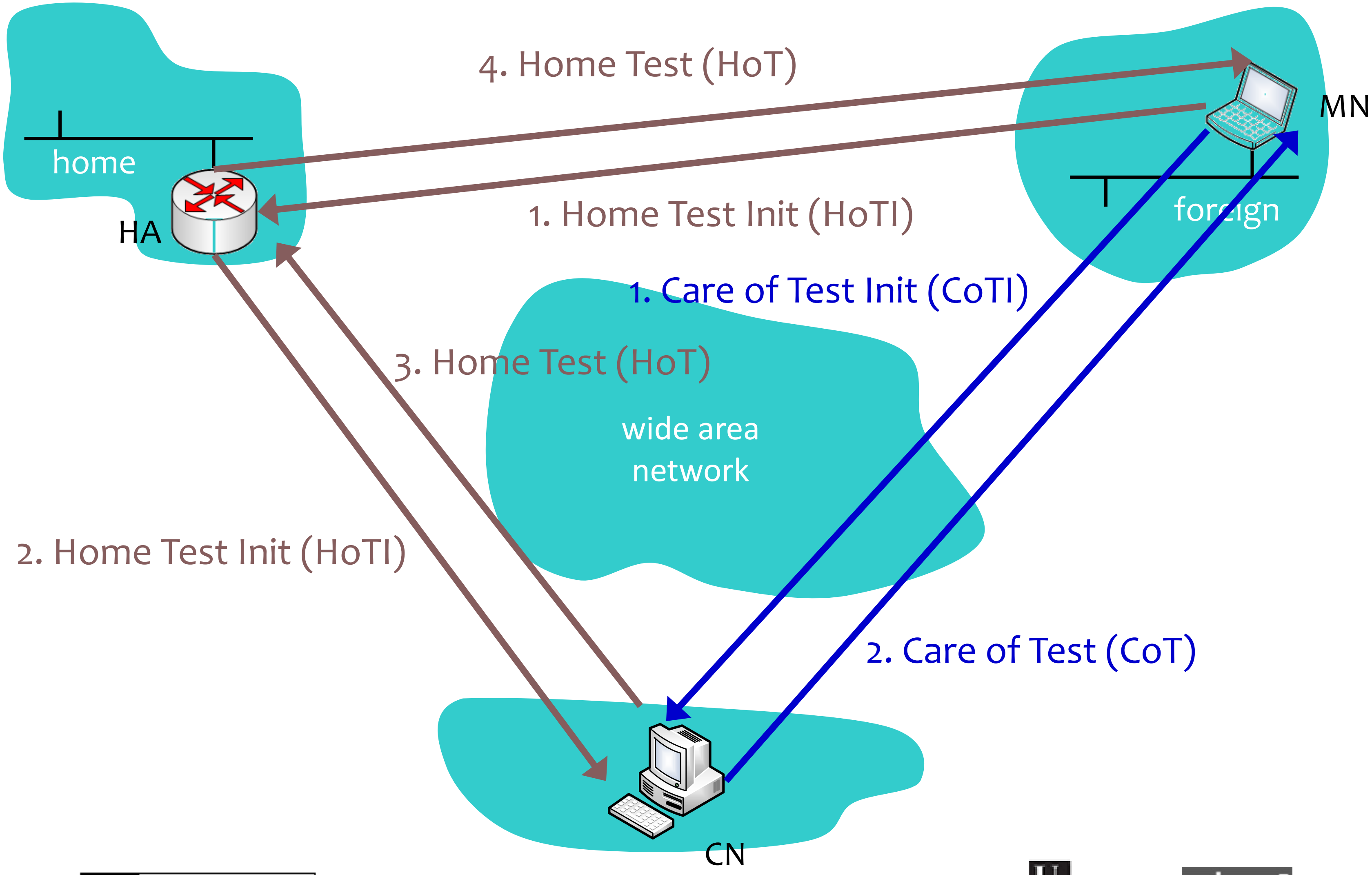
Some notes

- Should use CoA directly for short lived connections
  - E.g., it is faster (RTT) to query local DNS directly instead of going through HA
  - Need to decide when to do so…
- Dynamic Home Agent Address Discovery (DHAAD)
  - Home Agent option added to Router Advertisement
    - Allows home agents to discover each other
  - ICMPv6 messages for discovering list of Home Agents
    - Home Agent Address Discovery Request sent to the *home agents* anycast address on the home link
    - The HAAD Response contains a list of Home Agents on that link
    - Note that the home link prefix must still be configured by other means…
- Discovering Home Address dynamically
  - Could resort to DNS

Security RFC6275#5

- BU to HA
  - Uses IPsec security association (SA) between HA and MN
  - MUST support and SHOULD use Encapsulating Security Payload (ESP) in transport mode
  - SAs have policies for receiving only for specific home address
    - Prevent a MN from sending BU on behalf of another MN
- BU to CN
  - Cannot have a preconfigured SA with every possible CN!
  - Use the *return routability procedure*
    - MN proves that it is reachable both through the HA and the CoA
    - Limits attack possibilities
  - Key is derived in this procedure

Security: Return routability



Security tokens used

- HoTI
  - Home init cookie
- CoTI
  - Care-of init cookie
- HoT
  - home init cookie
  - home keygen token
  - home nonce index
- CoT
  - care-of init cookie
  - care-of keygen token
  - care-of nonce index

Use of nonces to protect against Binding Update replay attacks

Security generation

- home keygen token :=
  - First (64, HMAC_SHA1 (Kcn, (home address | home nonce | 0)))
- care-of keygen token :=
  - First (64, HMAC_SHA1 (Kcn, (care-of address | care-of nonce | 1)))
- Kcn: key on CN (not shared)
- Key on MN derived from material
  - Kbm = SHA-1 (home keygen token | care-of keygen token)
  - For revocation is only SHA-1 (home keygen token)

Security: BU to CN

- BU contains
  - Home address (in Home Address destination option if different from the Source Address)
  - Sequence number (in the Binding Update message header)
  - Home nonce index (in the Nonce Indices option)
  - Care-of nonce index (in the Nonce Indices option)
  - First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BU)))
- This information can reassure the CN that the BU is legit

Improvements

- Mobile IPv6 Fast Handovers (RFC5568)
- Hierarchical Mobile IPv6 (RFC5380)
- Mobile IPv6 Fast Handovers for 3G CDMA Networks (RFC5271)
- Mobile IPv6 Fast Handovers for 802.11 Networks (RFC4260)
- Enhanced Route Optimization for Mobile IPv6 (RFC4866)
- …

The end

References

- Hesham Soliman “Mobile IPv6: Mobility In A Wireless Internet”, Addison-Wessley, 2004, ISBN: 0201788977

Acronyms

- BU – Binding Update
- CoA – Care-of Address
- CN – Correspondent Node
- FA – Foreign Agent
- HA – Home Agent
- HO – HandOver
- MN – Mobile Node