Introduction to IPv6

(Chapter 4 in Huitema)

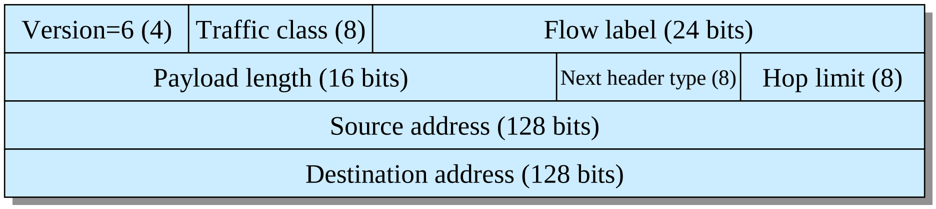
IPv6 addresses

- 128 bits long
- Written as eight 16-bit hexadecimal integers separated with colons
  - E.g. 1080:0000:0000:0000:0000:0008:200C:417A
    = 1080::8:800:200C:417A
- Types
  - Unicast
    - Defines one interface within their scope of validity
  - Multicast
    - Delivers packets to all members of a group
  - Anycast
    - Delivers packets to the *nearest* member of a group

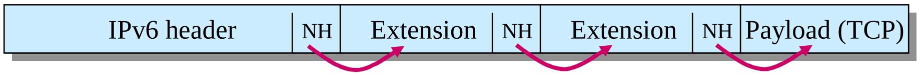
Special IPv6 addresses

- Unspecified = 0:0:0:0:0:0:0:0 = ::
  - Only as source address
- Loopback = 0:0:0:0:0:0:0:1 = ::1
  - For sending datagrams to itself
- IPv4 addresses prepended with zeroes
  - 0:0:0:0:0:0:AABB:CCDD = ::a.b.c.d
- Site-local addresses
  - FEC0:0000:0000:subnet:station (subnet 16 bits, station 64 bits)
- Link-local addresses (not relayed by router)
  - FEB0:0000:0000:0000:station

IPv6 header



- Differences between v4 and v6
  - No checksum (performed by lower layers)
  - No fragmentation (path MTU discovery instead, min. 1280 bytes)
  - No options (fixed length header, options in linked extension headers instead)
- Extension headers replace options



Source routing is implemented with the routing header

- Routing header:

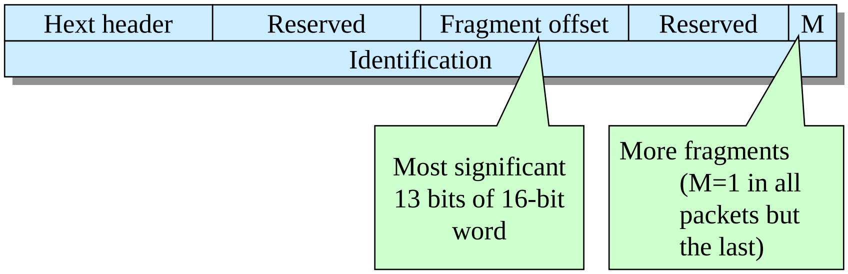
Next header	Header ext. length	Routing type = 0	Segments left
Reserved			
IPv6 address 1			
IPv6 address 2			
. . .			
IPv6 address N			

- Only the router whose address is destination address in IPv6 header examines this extension ⇒ better performance
- Forwarder
  - Swaps the next address in the list and the destination address of the header
  - Decrements the number of segments left

Can be replaced by IP-in-IP

Only the sender can fragment packets

- No fragmentation in routers
  - Packets larger than the next hop’s MTU are rejected, and ICMP message sent back
- Large packets (e.g. in UDP) must be fragmented by the sender
- Fragment header:



Hext header	Reserved	Fragment offset	Reserved	M
Identification				

Most significant 13 bits of 16-bit word

More fragments (M=1 in all packets but the last)

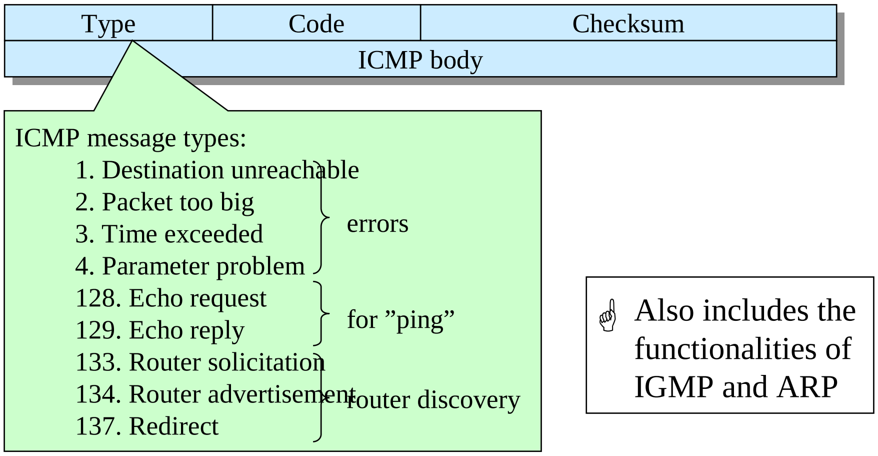
Other extensions

- Authentication Header (AH) for authentication
- Encrypted Security Payload (ESP) for authentication + encryption
- Destination options header is only examined by the destination
  - Contains one or several options
  - Also defines handling for unrecognized parameters
    - Ignore / discard silently / discard and send ICMP message
- Hop-by-hop options header is examined by each router
  - Similar format and coding as destination options header
  - E.g. jumbo payload

- Processing order is important
  - IPv6 → Hop-by-hop options → Destination options (for endpoint of tunnel) → Routing → Fragment → Authentication → Destination options (for destination) → Upper layers (TCP/UDP)

Internet Control Message Protocol Version 6

ICMPv6 header:



Type	Code	Checksum
ICMP body		

ICMP message types:

1. Destination unreachable
2. Packet too big
3. Time exceeded
4. Parameter problem

errors

128. Echo request
129. Echo reply

for ”ping”

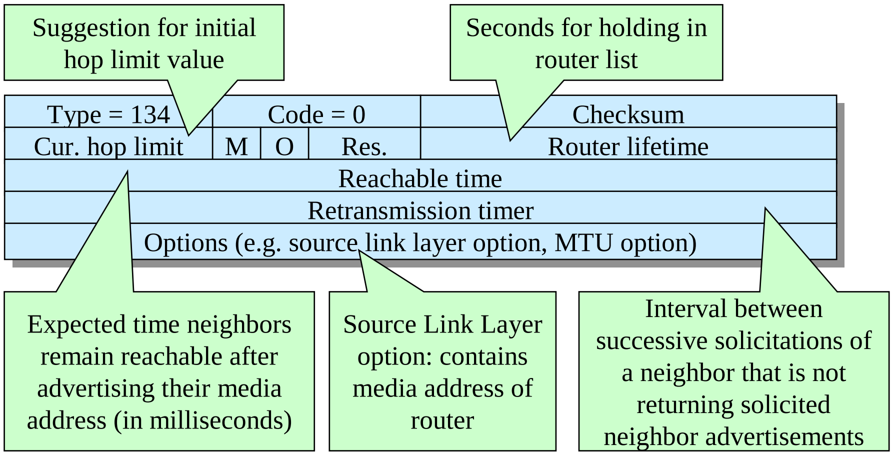
133. Router solicitation
134. Router advertisement
137. Redirect

router discovery

☝ Also includes the functionalities of IGMP and ARP

Router advertisements are sent by routers

- For building a local list of routers on the same network



Suggestion for initial hop limit value

Seconds for holding in router list

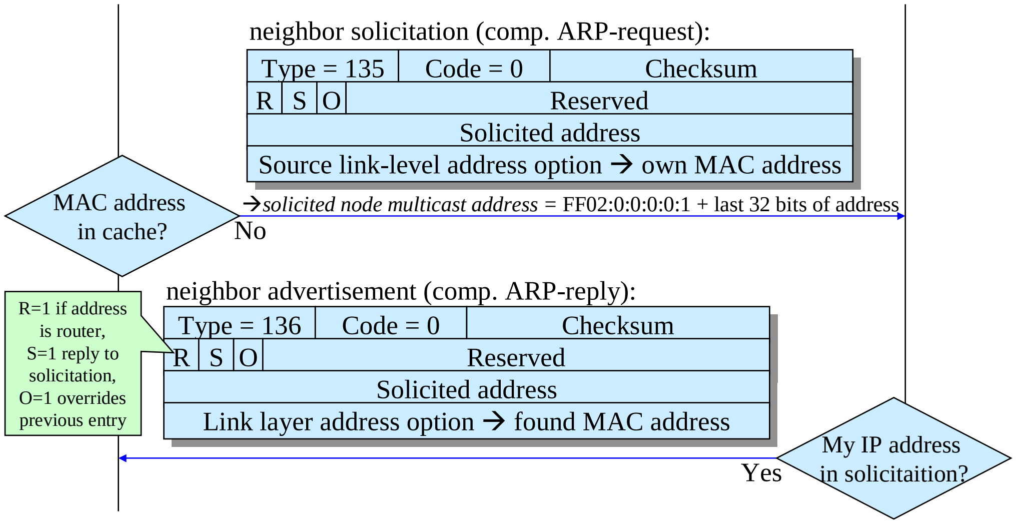
Type = 134	Code = 0			Checksum
Cur. hop limit	M	O	Res.	Router lifetime
Reachable time				
Retransmission timer				
Options (e.g. source link layer option, MTU option)				

Expected time neighbors remain reachable after advertising their media address (in milliseconds)

Source Link Layer option: contains media address of router

Interval between successive solicitations of a neighbor that is not returning solicited neighbor advertisements

Neighbor discovery finds the MAC address corresponding to the IP address of the next hop



neighbor solicitation (comp. ARP-request):

Type = 135			Code = 0	Checksum
R	S	O	Reserved	
Solicited address				
Source link-level address option → own MAC address				

MAC address in cache?

→*solicited node multicast address* = FF02:0:0:0:0:1 + last 32 bits of address

No

neighbor advertisement (comp. ARP-reply):

Type = 136			Code = 0	Checksum
R	S	O	Reserved	
Solicited address				
Link layer address option → found MAC address				

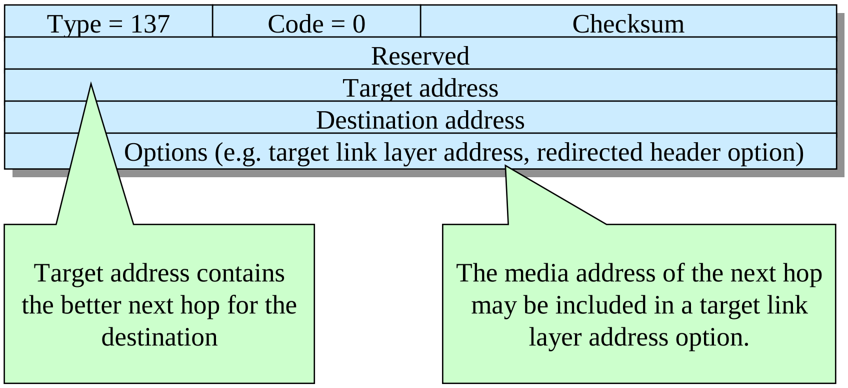
R=1 if address is router, S=1 reply to solicitation, O=1 overrides previous entry

Yes

My IP address in solicitaition?

Redirect works like in IPv4 but may include the media address of the next hop

- Redirect message:



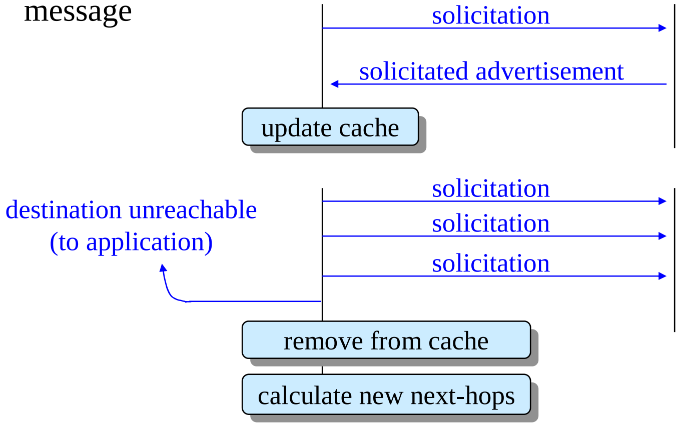
Type = 137	Code = 0	Checksum
Reserved		
Target address		
Destination address		
Options (e.g. target link layer address, redirected header option)		

Target address contains the better next hop for the destination

The media address of the next hop may be included in a target link layer address option.

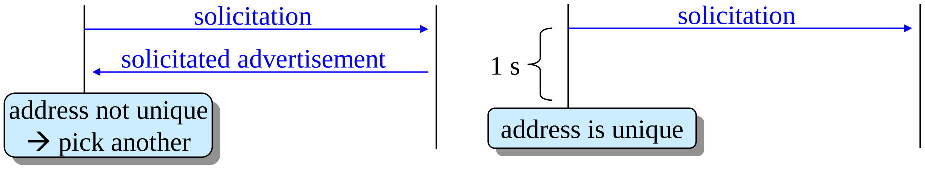
The sender needs feedback from the destination so that it does not send to a ”black hole”

- If the sender does not get feedback (e.g. TCP acks) within 30 seconds, it checks the existence of the receiver with a solicitation message



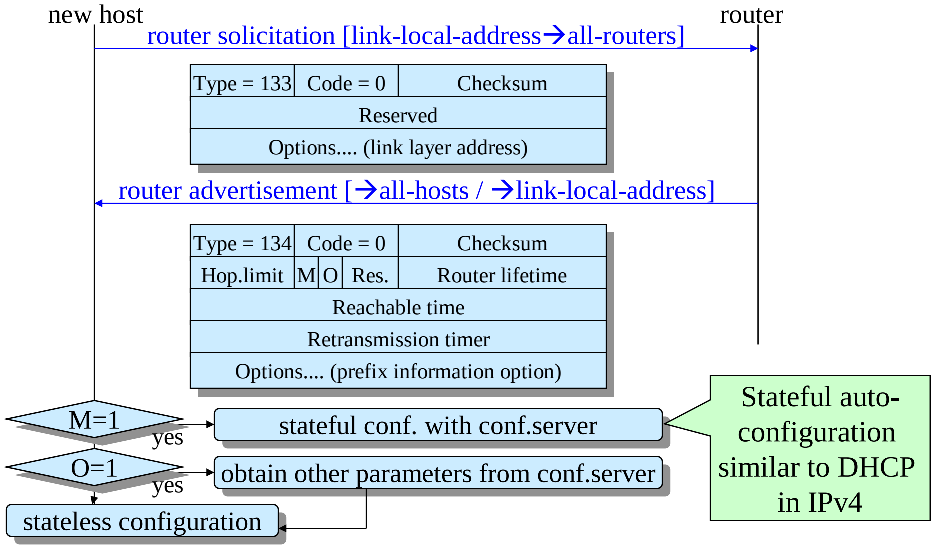
Before obtaining an address with autoconfiguration, the host uses a link local address

- FEB0:0000:0000:0000 + EUI-64 identifier
- The 64-bit EUI-64 identifier is generated from the 48-bit Ethernet address
- The host must check that the link local address is unique
  - In principle, addresses generated with the EUI-64 identifier should be unique, but...



- Lost messages ⇒ retry several times

Autoconfiguration can be stateful or stateless


new host
router
router solicitation [link-local-address→all-routers]
router advertisement [→all-hosts / →link-local-address]
M=1
yes
stateful conf. with conf.server
O=1
yes
obtain other parameters from conf.server
stateless configuration
Stateful auto-configuration similar to DHCP in IPv4

Type = 133	Code = 0	Checksum
Reserved		
Options.... (link layer address)		

Type = 134	Code = 0			Checksum
Hop.limit	M	O	Res.	Router lifetime
Reachable time				
Retransmission timer				
Options.... (prefix information option)				

Stateless autoconfiguration

<table>
<tr><td>Type = 134</td><td colspan="3">Code = 0</td><td>Checksum</td></tr>
<tr><td>Hop.limit</td><td>M</td><td>O</td><td>Res.</td><td>Router lifetime</td></tr>
<tr><td colspan="5">Reachable time</td></tr>
<tr><td colspan="5">Retransmission timer</td></tr>
<tr><td colspan="5">Options.... (<b>prefix information option</b>)</td></tr>
</table>

Contains list of prefixes with parameters

- on-link bit → the prefix is specific to the local link
- autonomous-bit → host can construct address by replacing the last bits of the prefix with EUI-64 identifier

Properties

- simple, no servers required
- inefficient: 64 bits used for one local network
- no access control

Mobile IP

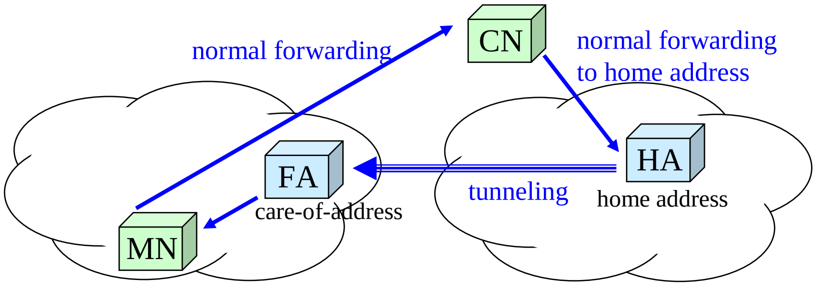
(Chapter 13 in Huitema)

Different types of mobility

- Computers transported and connected from different locations
  - Access through modem/ISDN/WLAN/…
  - Dynamic configuration
  - ⇒ new IP address
  - ⇒ TCP connection cut off
- Mobile computers, which stay connected during movements
  - Radio, infrared
  - ⇒ same IP address
- Mobile networks, e.g. in cars, planes, trains, ships
  - Recursive mobility (mobile host in mobile network)

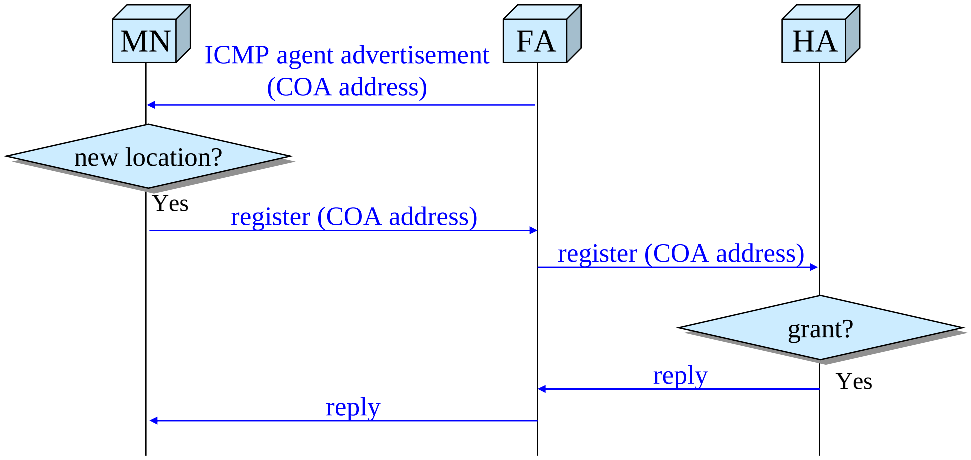
The traffic to a mobile node is tunneled from the home agent to the foreign agent

- ***Mobile Node*** (***MN***) – Node, who has a *home address* in the home network, and obtains a *care-of-address* (COA) in the visited foreign network
- ***Home Agent*** (***HA***) – Belongs to the home network and serves the home address
- ***Foreign Agent*** (***FA***) – Serves the visiting mobile node
- ***Corresponding Node*** (***CN***) – A node exchanging data with the mobile node



Home agents and foreign agents may be routers

When a host discovers that the location has changed, it must register the new COA with the HA

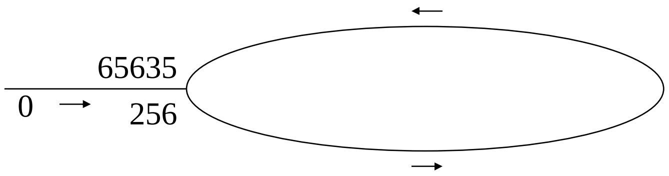


A lost request is resent by MN
FA never repeats the request.

Discovery of a Home Agent or Foreign Agent using periodical ICMP messages

- Agent advertisements are extensions to ICMP router advertisements
- The agent advertisements contain
  - Sequence number
  - Life-time of registration
  - Flags
    - Registration required
    - Foreign agent or home agent
    - Supporting Minimal encapsulation (RFC-2003)
    - Supporting Generic Routing Encapsulation (GRE) (RFC-1701)
    - Header compression used
  - List of care-of-addresses
  - Length of prefixes

The sequence numbers in the agent advertisement are similar to ”lollipop” sequence numbers in OSPF



- If one of the number is < 256
  - The higher number is ”higher”
- If both numbers are ≥ 256
  - If (b-a) < (65635-256)/2 then b is ”higher”
- If the received is ”lower” than the previous, then the server has been restarted

  ⇒ Register again

Alternative discovery mechanisms

- Periodic broadcast of ICMP messages wastes transmission capacity, especially on wireless LANs
  - Cannot be frequent
- The MN can detect changed location through media-level information
  - e.g. analyzing power of different basestations
- Instead of waiting, the MN can solicit the information
  - Similar to ICMP router solicitation
  - TTL = 1
  - Agent replies with agent advertisement

Registration request

- Registration request message contains
  - Message type = 1 (request)
  - Flags
    - FA co-located with MN
    - preferred encapsulation
  - Requested lifetime
    - 0 = cancel the previous
  - Home address of MN
  - HA address
  - COA address
  - 64-bit request identification
  - Extensions
    - E.g. authentication

Registration reply

- Registration reply message contains
  - Message type = 3 (reply)
  - Reply code (granted or denied)
    - Who denied (FA or HA)
    - Why denied
  - Accepted lifetime
    - Same as or smaller than requested lifetime
  - Home address of MN
  - HA address
  - 64-bit request identification
    - Same as in request
  - Extensions
    - E.g. authentication

Security issues (1)

- Attack types
  - Attacker pretends to be a FA to capture traffic
  - Attacker replays old registration messages
- Authentication extension proves the origin of the message and that the contents has not been changed
  - Security parameter index (SPI) together with HA, COA, or NM identifies security context
  - Shared secret, signature algorithm (e.g. keyed MD5) parameters of security context
  - Data and secret key → authentication field
  - MN to HA authentication mandatory
  - FA to HA and MN to FA authentications optional

Security issues (2)

- Attack types
  - Attacker pretends to be a FA to capture traffic
  - Attacker replays old registration messages
- Two requests must not contain the same identification
  - NTP timestamps (64-bit)
    - Only requests with higher timestamps are accepted
    - The timestamps must be close to the current time
  - Random numbers used only once (nonce)

Encapsulation

- Basic encapsulation, RFC-2003

Source=HA, Dest=COA,
Protocol=IP in IP=4
	Source=CN, Dest=MN,
	Protocol=TCP
		TCP header
		+ data

New IP header	Original IP packet	

- Minimal encapsulation, RFC-2004

Source=HA, Dest=COA,
Protocol=Min.encaps=55
	Compressed header	TCP header
		+ data

New IP header	Original IP packet	

Compressed header: Protocol type of encaps. packet (e.g. TCP), Destination address of encaps. packet, Optional source address of encaps. packet, Header checksum

- Generic Routing Encapsulation (GRE), RFC-1701

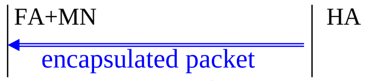
Source=HA, Dest=COA,
Protocol=GRE=24
	Encapsulation
	parameters
		Source=CN, Dest=MN,
		Protocol=TCP
			TCP header
			+ data

New IP header	GRE header	Original IP packet	

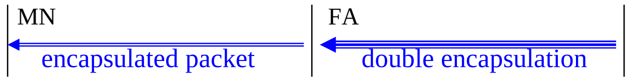
Parameters: Protocol type (similar to the one in Ethernet packet), optional checksum, optional sequence number, optional authentication key, (source) routing field, flags (which options are present)

Broadcast and multicast should only be received by the MN, not the network of MN

- Easy if FA is co-located with MN



- Double encapsulation of broadcast/multicast traffic



Source=HA, Dest=COA,
Protocol=IP in IP
	Source=HA, Dest=MN,
	Protocol=IP in IP
		Source=CN, Dest=bc,
		Protocol=UDP
			UDP header
			+ data

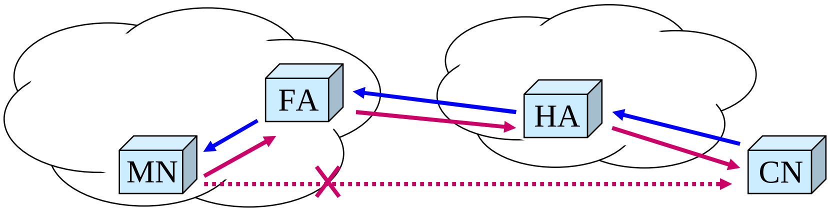
New IP header	Double encapsulation	Original broadcast packet	

- Joining multicast groups: ICMP messages are tunneled MN→HA
- More efficient: MN can subscribe to groups on the foreign network

Source address filtering is a problem in Mobile IP (1)

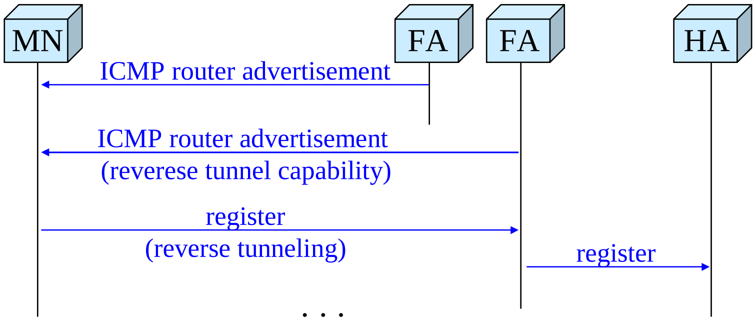
- Why source address filtering?
  - Address spoofing hides identity of attacker, helps targeting third parties' replies, helps gaining privileges
- Source address filtering is performed in firewalls, between ISP and customer, at peering points between provides, etc.

⇒ Packets sent by MN must be tunneled through the HA



Source address filtering is a problem in Mobile IP (2)

- FAs capable of tunneling packets back to HA, advertise it with a flag in agent advertisement message
- The MN requests reverse tunneling


MN
FA
FA
HA
ICMP router advertisement
ICMP router advertisement
(reverese tunnel capability)
register
(reverse tunneling)
register
. . .

Considerations

- Path MN→CN is shorter than the path CN→MN
  - Asymmetry
- If the MN moves relatively fast, it must choose a new FA often
  - ⇒ Many registration messages to HA

Mobile IPv6

(Chapter 13 in Huitema)

Mobility in IPv6

- Discovery performed with IPv6 neighbor discovery and address configuration mechanisms
- Security ⇒ MN can notify their COA to the CN in addition to the HA
- Efficient encapsulation with the source routing header

Discovery

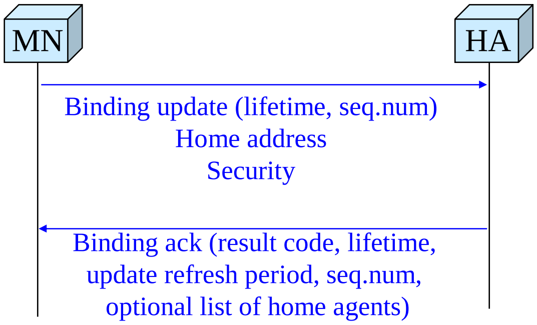
- The MN and FA are usually colocated ⇒ No separate FA
- Hosts listen to router advertisements to the learn prefixes of the link
  - Hosts can detect that they are visiting a foreign network
- COA obtained with address configuration procedures
- Routers willing to act as home agents indicate it in the router advertisement

Binding updates (1)

- Binding performed using *destination options*
  - Binding update – informs about the new COA
  - Binding ack – acknowledges the COA
  - Binding request – To request information about the current COA
  - Home address – Identifies the home address of the MN
- Authentication with the *security option*

Binding updates (2)

- COA transmitted in source address of IPv6 header
- Home address in the *Home Address option*



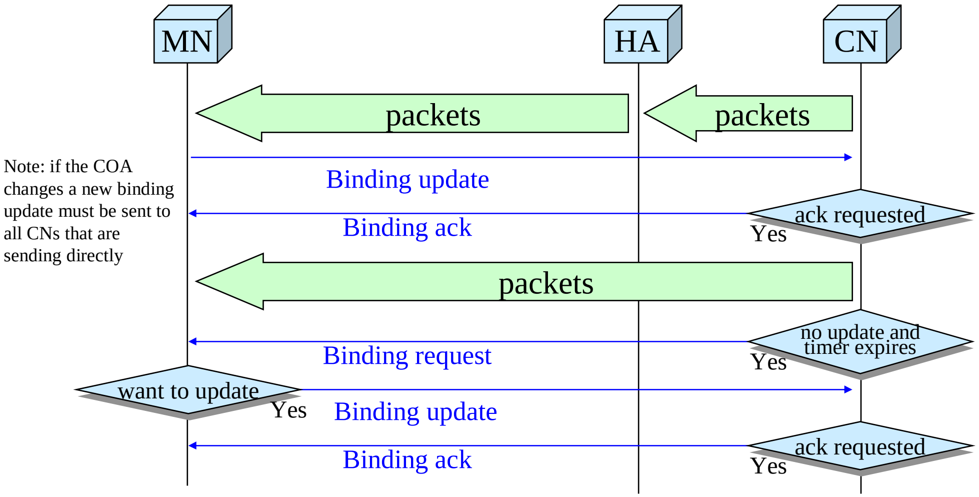
Binding update (lifetime, seq.num)
Home address
Security

Binding ack (result code, lifetime,
update refresh period, seq.num,
optional list of home agents)

Source address filtering is not a problem in IPv6

- The mobile node does not put its home address in the IPv6 header. Instead, the home address is sent in the Home Address option. The IPv6 header contains the COA.
- Mandatory requirement.

The MN can send a binding update to the CN to optimize the route



MN

HA

CN

packets

packets

Binding update

ack requested

Yes

Binding ack

packets

no update and timer expires

Yes

Binding request

want to update

Yes

Binding update

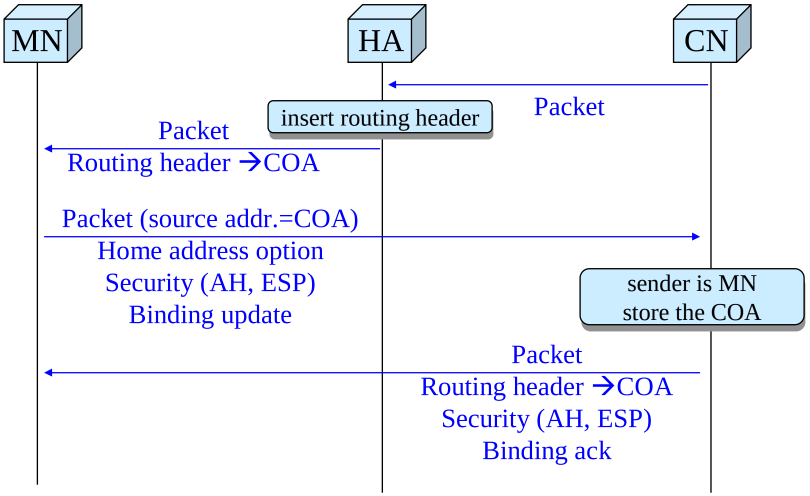
ack requested

Yes

Binding ack

Note: if the COA changes a new binding update must be sent to all CNs that are sending directly

IPv6 uses the routing header instead of encapsulation


MN
HA
CN
Packet
insert routing header
Packet
Routing header →COA
Packet (source addr.=COA)
Home address option
Security (AH, ESP)
Binding update
sender is MN
store the COA
Packet
Routing header →COA
Security (AH, ESP)
Binding ack