Mobile Internet Protocol v6

MIPv6

A brief introduction

Holger.Zuleger@hznet.de

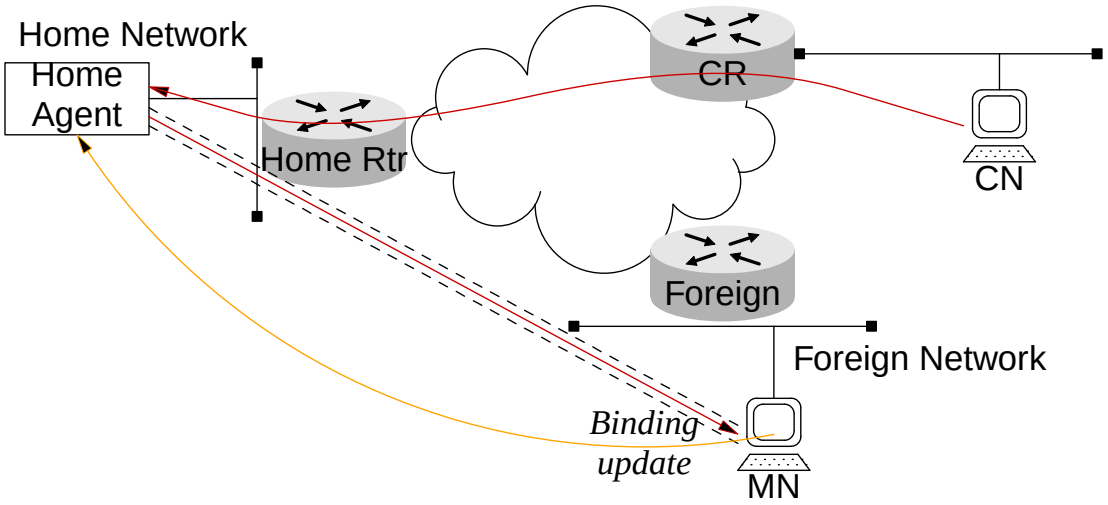
MIPv6

- Defined by
  - RFC3775: Mobility Support in IPv6 (June 2004)
  - RFC3776: Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents
- Goals of IPv6 mobility
  - Always on IP connectivity
  - Roaming between different L2 technologies
    WLAN, WiMAX, UMTS, fixed
  - Roaming between different (sub)networks
    Huge WLAN deployments use often different L3 subnets
  - Application continuity (Session persistence)
  - Static IP addresses for mobile nodes
  - Mobile devices may act as servers

Terminology

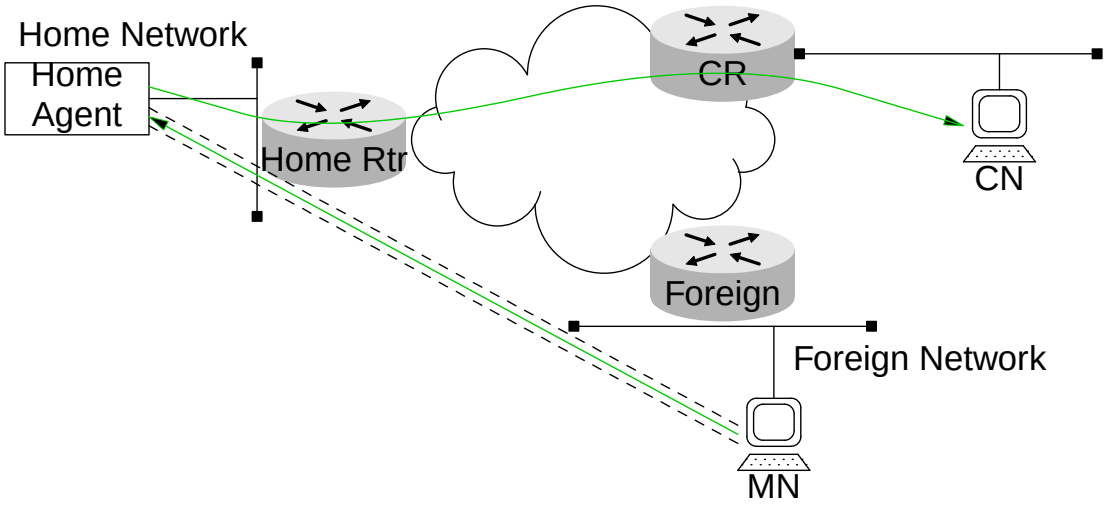
- Home Address (HoA)
  A (static) IP address out of the mobile nodes home network
- Mobile Node (MN)
  Could change its point of attachment while still being reachable via HoA
- Care of Address (CoA)
  The physical IP address of a MN while visiting a foreign network
- Home Agent (HA)
  A router on the home network which represents the MN while it's not attached to the home network
- Binding
  Association of the home address with the Care-of address of a MN
- Correspondent Node (CN)
  A peer node with which a MN is communicating.
  The CN may be either mobile or stationary

Bidirectional Tunnel Mode (1)



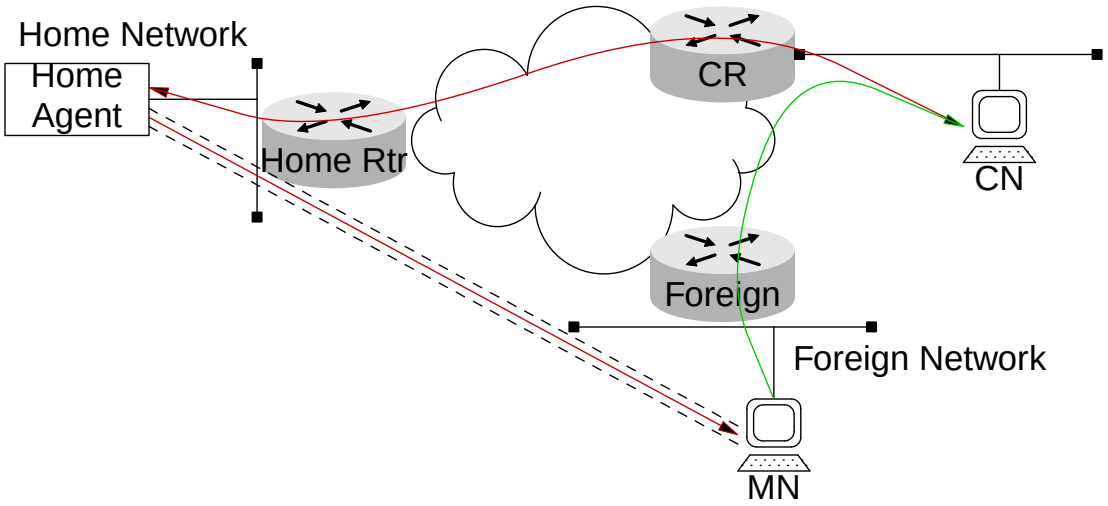
- MN connects to foreign network and gets a CoA
- MN sends binding update to HA
  Should be secured by IPsec ESP in transport mode
- HA uses proxy neighbor discovery (IPv6 equivalent of proxy ARP) to represent the MN in the home network
- Every traffic destined to the MN will be encapsulated in a IPv6-in-IPv6 Tunnel and send to the CoA of the MN

Bidirectional Tunnel Mode (2)



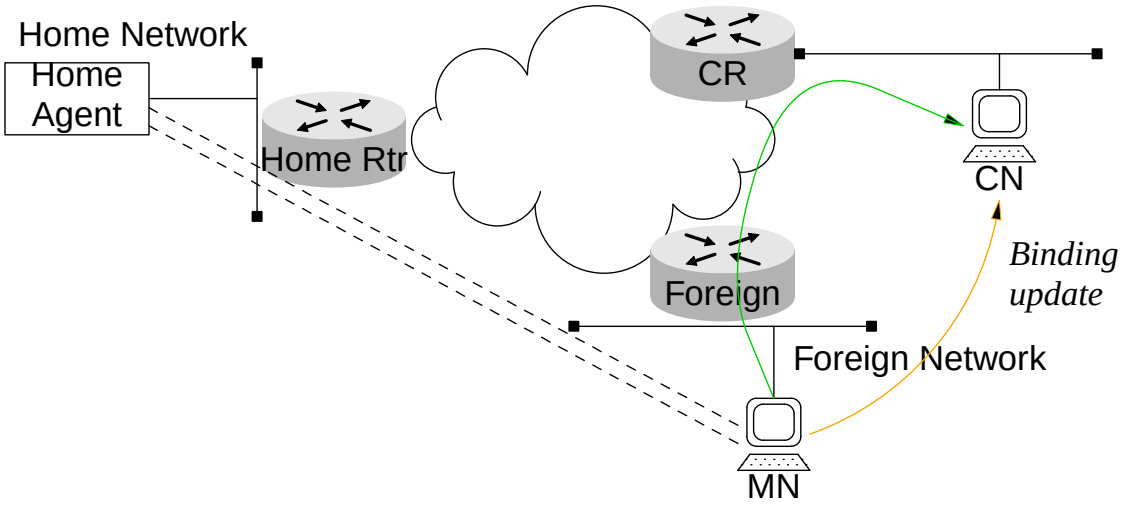
- Traffic from the MN uses the same tunnel in reverse mode
- Results in suboptimal routing
  Especially if both peers are far away from the home network
- Only HA and MN have to do some special packet handling
  MIPv6 is completely transparent for CN

Triangle Routing ?



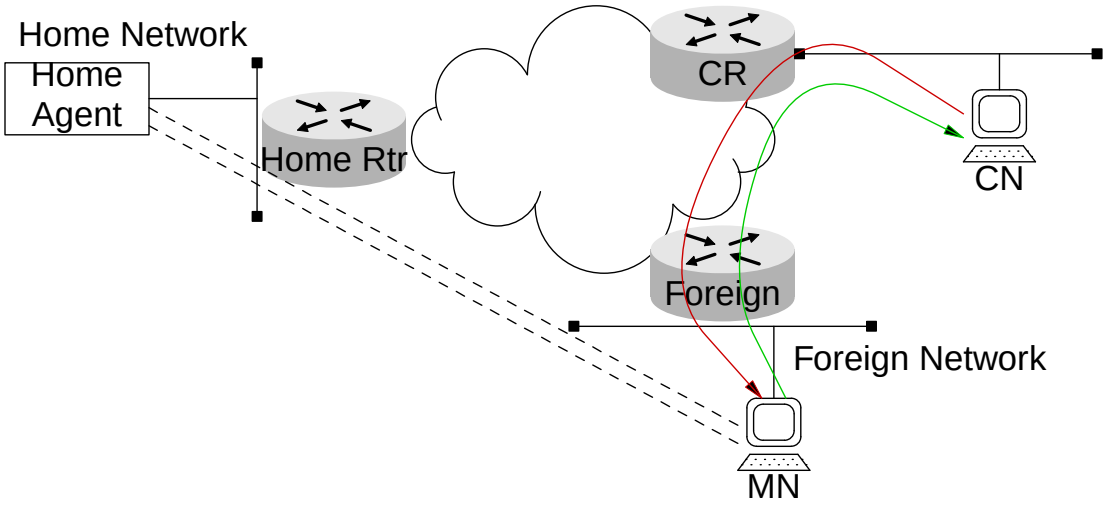
- Traffic from MN will be send directly to CN
- MIPv4 Solution
- Problem: Outgoing traffic can’t use the HoA as source address
  Anti spoofing ACLs at the foreign network usually prevent this
- Suboptimal routing anyway
- MIPv6 Solution: Route Optimization

Route optimization (1)



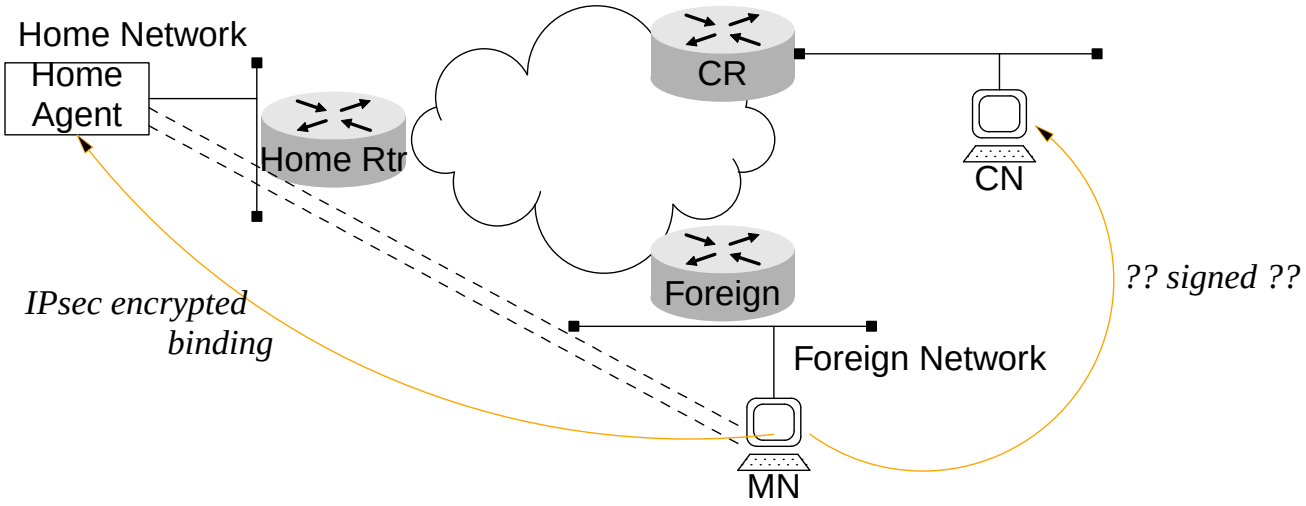
- MN sends binding update to correspondent node
- MN sends traffic to CN with CoA as source address
  This is to bypass the anti spoofing ACLs at the foreign network
- Packet contains an HoA destination option
- CN replaces the source address with the home address before passing the packet to upper layer protocols

Route optimization (2)



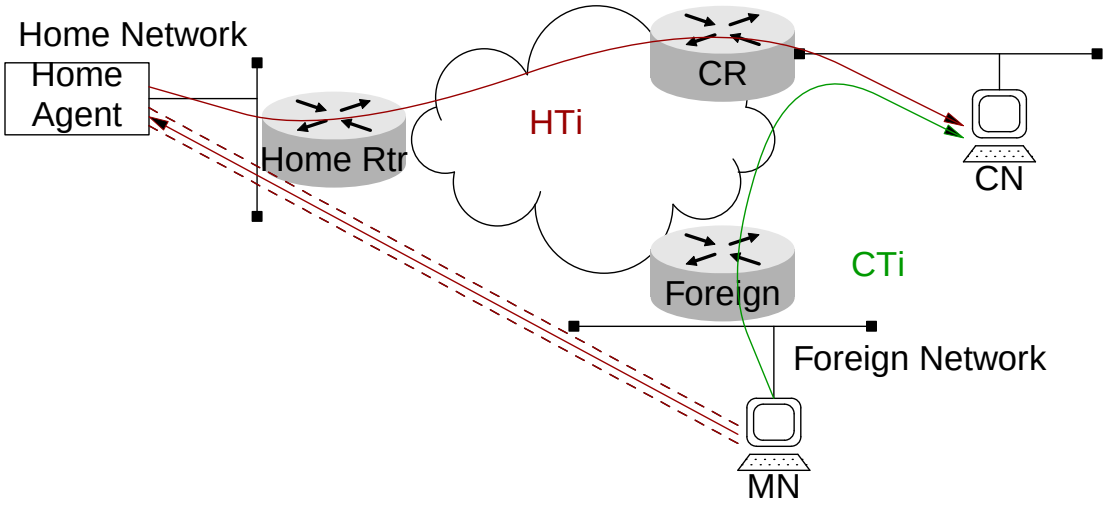
- CN sends traffic to MN with CoA as destination address
- Packet contains a special Routing Header with HoA as second hop
- MN removes the routing header and „forwards“ the packet to the next hop specified by the routing header
- Upper layer protocol is only aware of HoA
- But: Binding update **must** be secured in some way

Secure Binding



- Trust relationship between MN and HA
  IPsec with ESP in transport mode must be used for binding update message
- No trust relation between MN and CN
  Return Routeability mechanism is used to proof the reachability of MN

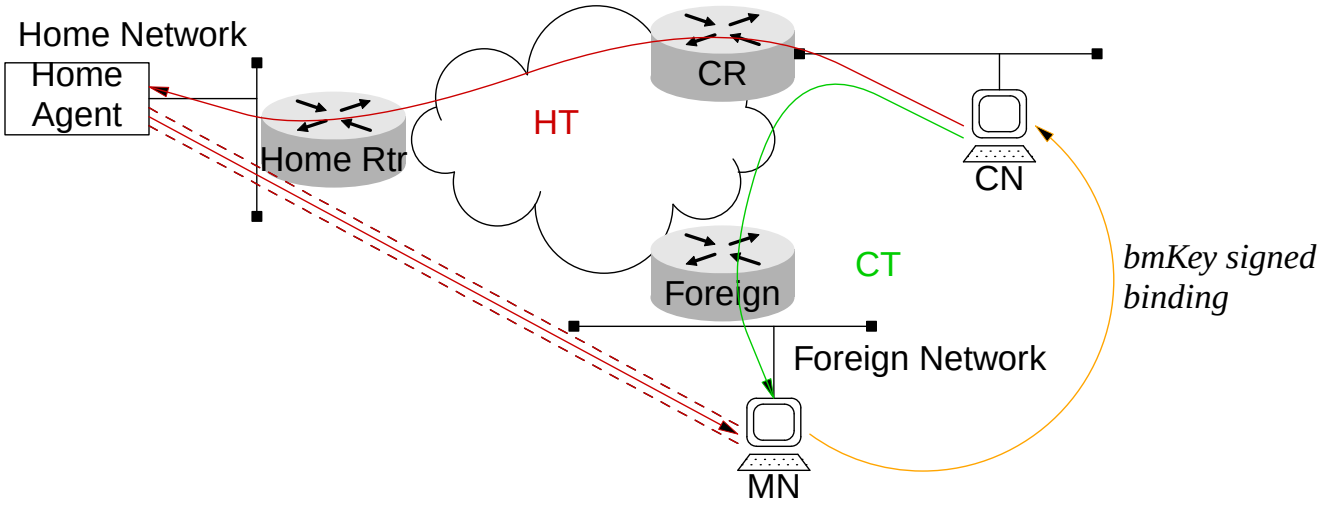
Return Routeability Procedure (1)



- MN sends two messages with a cookie to CN
  - Home Test init (HTi) is send via HA
    (traffic to HA must be encrypted)
  - Care-of Test init (CTi) is send to CN directly
- CN uses pre-generated key and nonce to build two keygen tokens
  (Key: random number of 20 octets; Nonce: random octet string of any length)

```
home keygentok    := FIRST (64, HMAC_SHA1 (key, (HoA | nonce | "0")))
care-of keygentok := FIRST (64, HMAC_SHA1 (key, (CoA | nonce | "1")))
```

Return Routeability Procedure (2)



- CN sends keygen tokens and cookies back to MN
  Home Test (HT) and Care-of Test (CT) messages
- MN builds binding message key

  `bmKey := SHA (home keygen token | care-of keygen token)`
- MN sends binding update message signed with bmKey
- CN can prove that the MN is reachable via both paths

What next?

- Bootstrapping MIPv6
  No static configuration of HA address and HoA on mobile nodes
- Network mobility (NEMO) (Instead of node mobility)
  IETF working group with focus on mobile networks (e.g. prefix delegation)
- Mobile adhoc networks (MANET)
  Interworking of Mobile Ad-hoc networks and Mobile IPv6 Networks
  - Mobile node roaming in between MIPv6 and MANET
  - MANET roaming as a MIPv6 client
- Signaling and Handoff Optimization (mipshop)
  - Fast Handovers for Mobile IPv6 (FMIPv6, RFC4068)
    See also www.fimpv6.org and www.rz.fhtw-berlin.de/projekte/mipv6
  - Hierachical MIPv6 mobility management (HMIPv6, RFC4140)
- Cryptographically generated (IPv6) addresses (RFC 3972)
  MN can prove that it owns its HoA by including its public key in the binding update and by signing the resulting message (No PKI needed)

Summary

- No foreign agent required
- Scalable solution if CN supports MIPv6
  Microsoft Windows 2003 and XP, {Free|Open|Net}BSD, Linux (with MIPL patch)
- Home network router can also act as Home Agent
  Cisco IOS 12.3(14)T, 12.4(2)T, but RFC3776 is not supported :-(
- Redundant HA with dynamic discovery (IPv6 anycast address)
- MIPv6 support the use of End-to-End IPsec (transport or tunnel mode)
- Some open security issues (CGA prevents this)
  Attacker which is able to capture all RR packets could send bindings on behalf of the MN
- Handover time must be improved
  - MIPv6: Handover latency = 2 seconds; packet loss = rate x latency
  - FMIPv6: Handover latency = Wlan handover latency; packet loss = 0
- MIPv6 requires (naturally) a IPv6 network :-(
  But think about 6to4 as a care of address... ;-)

References

Tutorial: IPv6 mobility and security
Wolfgang Fritsche, IABG, German IPv6 Summit, Bad Godesberg 2004

Mobile IPv6 White Paper
Wolfgang Fritsche, Florian Heissenhuber IABG, August 2000

Mobility Support in IPv6
RFC3775, June 2004

Using IPsec to Protect MIPv6 Signaling between Mobile Nodes and Home Agents
RFC3776, June 2004

Analysis of the handover in a WLAN MIPv6 scenario
Albert Cabellos Aparicio, Global IPv6 Summit, Barcelona 2005

Deliverable4.1.4: Final Mobile IPv6 Support Guide
6net − Large-Scale International IPv6 Pilot Network, Februar 2005

Technical Report: Mobility over IPv6 Networks
Euro6IX, March 2003

RFC3972, RFC4048, RFC4140, ...

Questions ?

http://www.hznet.de/ipv6/mipv6-intro.pdf

Questions ?

http://www.hznet.de/ipv6/mipv6-intro.pdf

Thank you very much
for your attention!

CONTENTS

..... 1
MIPv6 2
Terminology 3
Bidirectional Tunnel Mode (1) 4
Bidirectional Tunnel Mode (2) 5
Triangle Routing ? 6
Route optimization (1) 7
Route optimization (2) 8
Secure Binding 9
Return Routeability Procedure (1) 10
Return Routeability Procedure (2) 11
What next? 12
Summary 13
References 14
..... 15