IPv6 Workshop

János Mohácsi
NIIF/HUNGARNET

Copy ... Rights

- This slide set is the ownership of the 6DISS project via its partners
- The Powerpoint version of this material may be reused and modified only with written authorization
- Using part of this material must mention 6DISS courtesy
- PDF files are available from www.6diss.org
- Looking for a contact ?
- Mail to : martin.potts@martel-consulting.ch
- Or bernard.tuy@renater.fr

Contributions

- Main authors
  - Jean-Marc Barozet, Cisco, France
  - Faycal Hadj, Cisco, France
  - Patrick Grossetete, Cisco, France
  - Gunter Van de Velde, Cisco, Belgium
  - Bernard Tuy, Renater, France
  - Laurent Toutain, ENST-Bretagne – IRISA, France
- Contributors
  - Octavio Medina, ENST-Bretagne, France
  - Mohsen Souissi, AFNIC, France
  - Vincent Levigneron, AFNIC, France
  - Thomas Noel, LSIIT, France
  - Alain Durand, Sun Microsystems, USA
  - Alain Baudot, France Telecom R&D, France
  - Bill Manning, ISI, USA
  - David Kessens, Qwest, USA
  - Pierre-Emmanuel Goiffon, Renater, France
  - Jérôme Durand, Renater, France

IPv6 Mobility

Mobility Overview

- ***Mobility*** is much wider than ***"nomadism"***
- Keep the same IP address regardless of the network the equipment is connected to:
  - reachability
  - configuration
  - real mobility
- Difficult to optimize with IPv4 (RFC 3344 PS)
- Use new facility of IPv6: MIPv6

IPv6 Mobility (MIPv6)

- IPv6 mobility relies on:
  - New IPv6 features
  - The opportunity to deploy a new version of IP
- Goals:
  - Offer the direct communication between the mobile node and its correspondents
  - Reduce the number of actors (Foreign Agent (IPv4) no longer used)
- MIPv6: RFC 3776

General Considerations

- A globally unique IPv6 address is assigned to every ***Mobile Node*** (**MN**): ***Home Address*** (**HA**)
- This address enables the MN identification by its ***Correspondent Nodes*** (**CN**)
- A MN must be able to communicate with non mobile nodes
- Communications (keep layer 4 connections) have to be maintained while the MN is moving and connecting to foreign (visited) networks

Main features/requirements of MIPv6

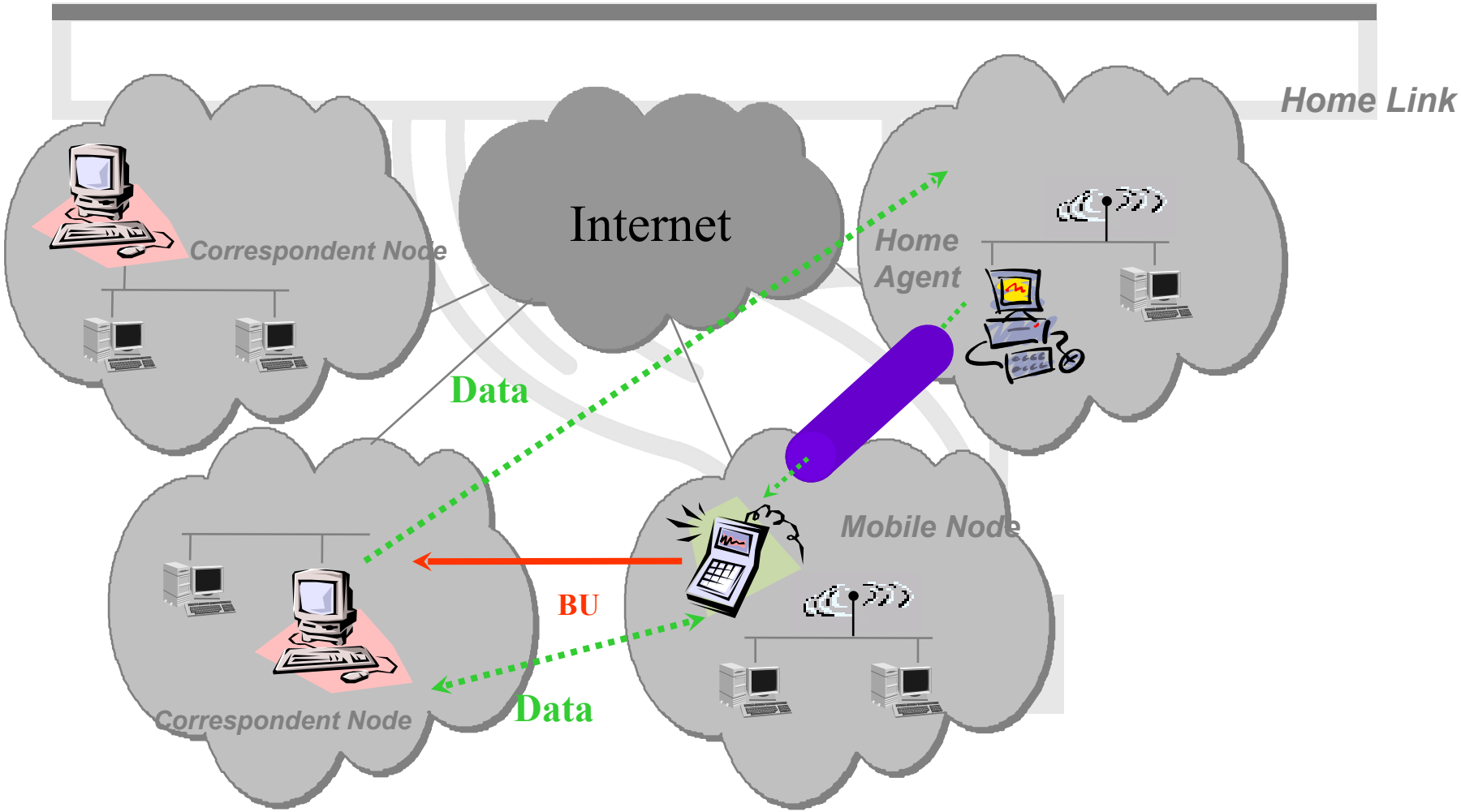
- CN can:
  - Put/get a Binding Update (BU) in/from their Binding Cache
  - Learn the position of a mobile node by processing BU options
  - Perform direct packet routing toward the MN (Routing Header)

- The MN's Home Agent must:
  - Be a router in the MN's home network
  - Intercept packets which arrive at the MN's home network and whose destination address is its HA
  - Tunnel (IPv6 encapsulation) those packets directly to the MN
  - Do reverse tunneling (MN → CN)

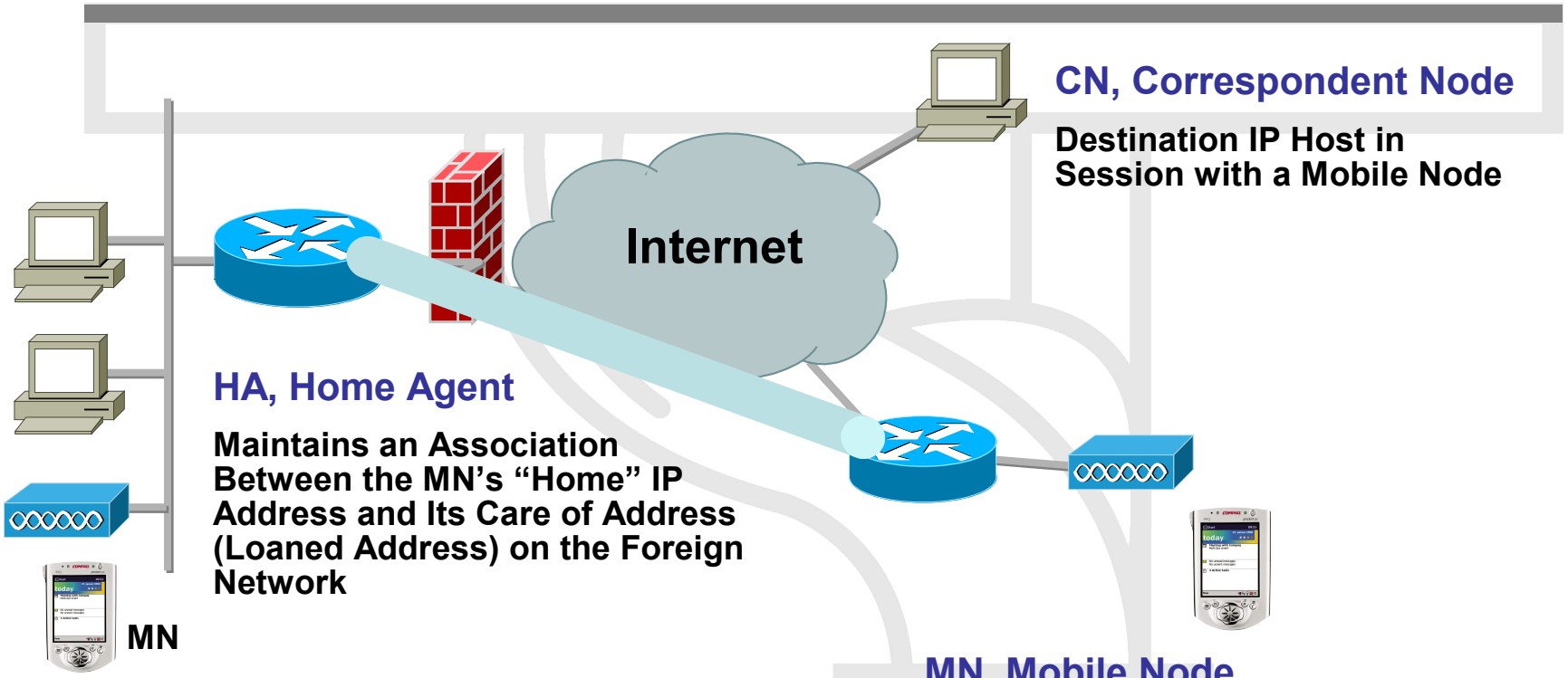
Mobile Node Addressing

- A MN is always reachable on its Home Address
- While connecting to foreign networks, a MN always obtains a temporary address, “the Care-of Address” (CoA) by auto-configuration:
  - It receives Router Advertisements providing it with the prefix(es) of the visited network
  - It appends that (those) prefix(es) to its Interface-ID
- Movement detection is also performed by Neighbor Discovery mechanisms

MIPv6: IETF Model



Mobile IPv6: Key Components



CN, Correspondent Node

Destination IP Host in Session with a Mobile Node

HA, Home Agent

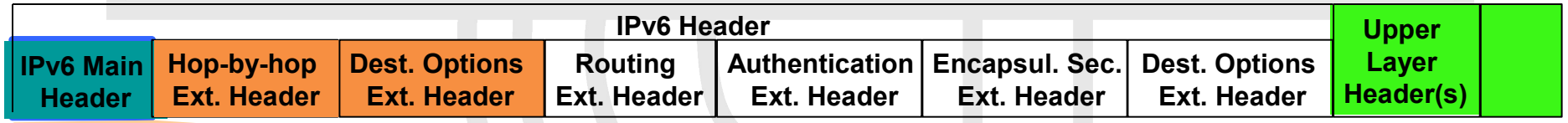
Maintains an Association Between the MN's "Home" IP Address and Its Care of Address (Loaned Address) on the Foreign Network

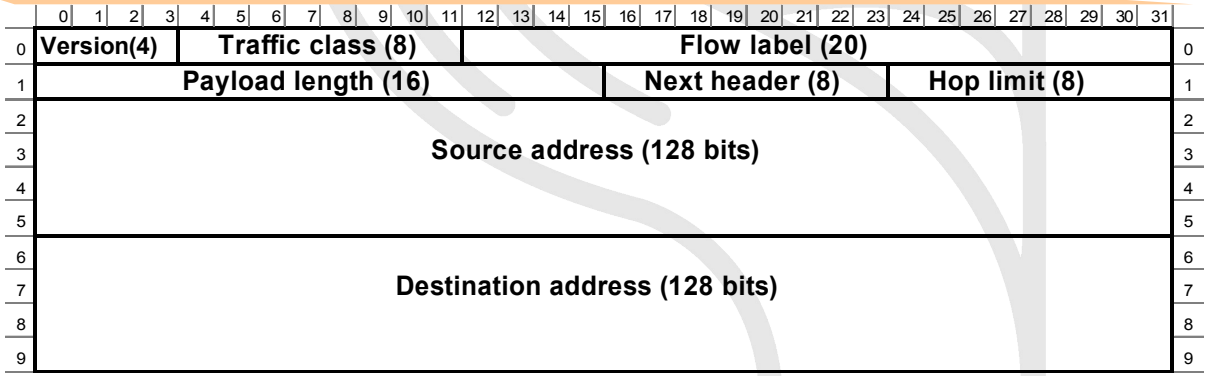
MN, Mobile Node

An IP Host that Maintains Network Connectivity Using Its "Home" IP Address, Regardless of which Link (or Network) It Is Connected to

Mobile IPv6 – a native extension of IPv6

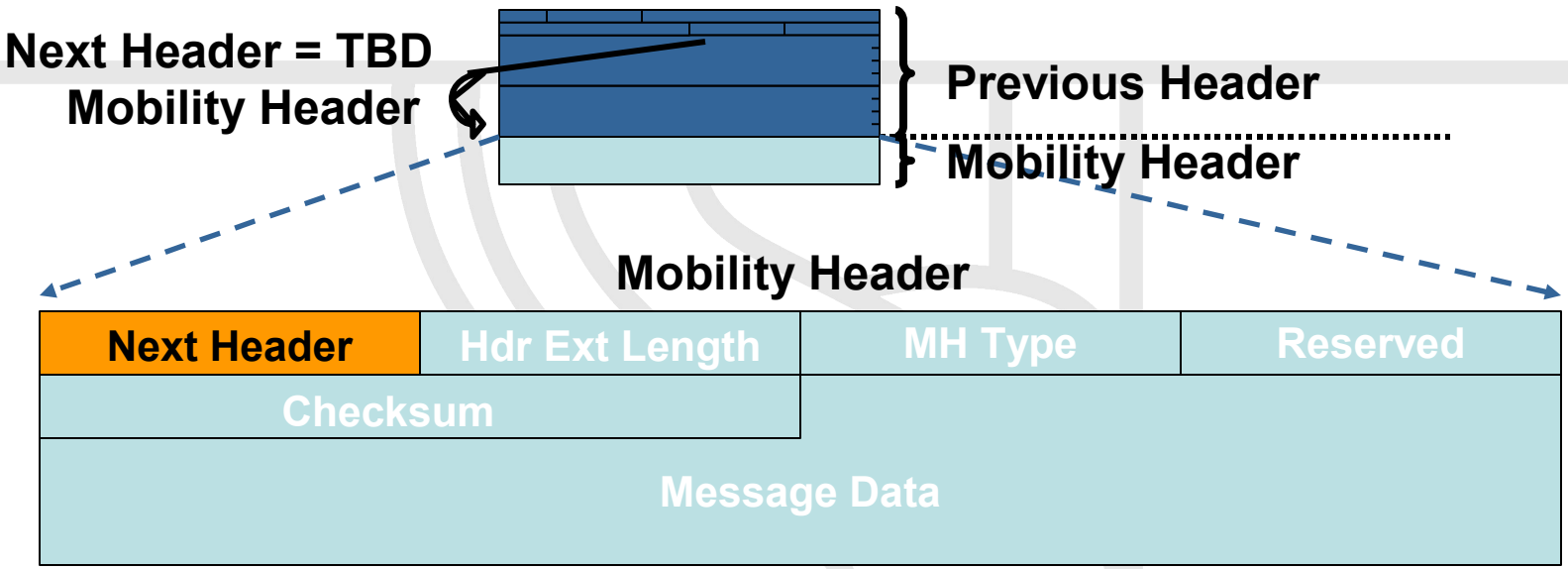
Un-fragmented Packet Example:





- Take benefit of the IPv6 packet structure as defined in RFC 2460
- Create new extension header – Mobility header
- Add new Routing Header Type
- Add new Destination option

IPv6 Protocol Extension: Mobility Header

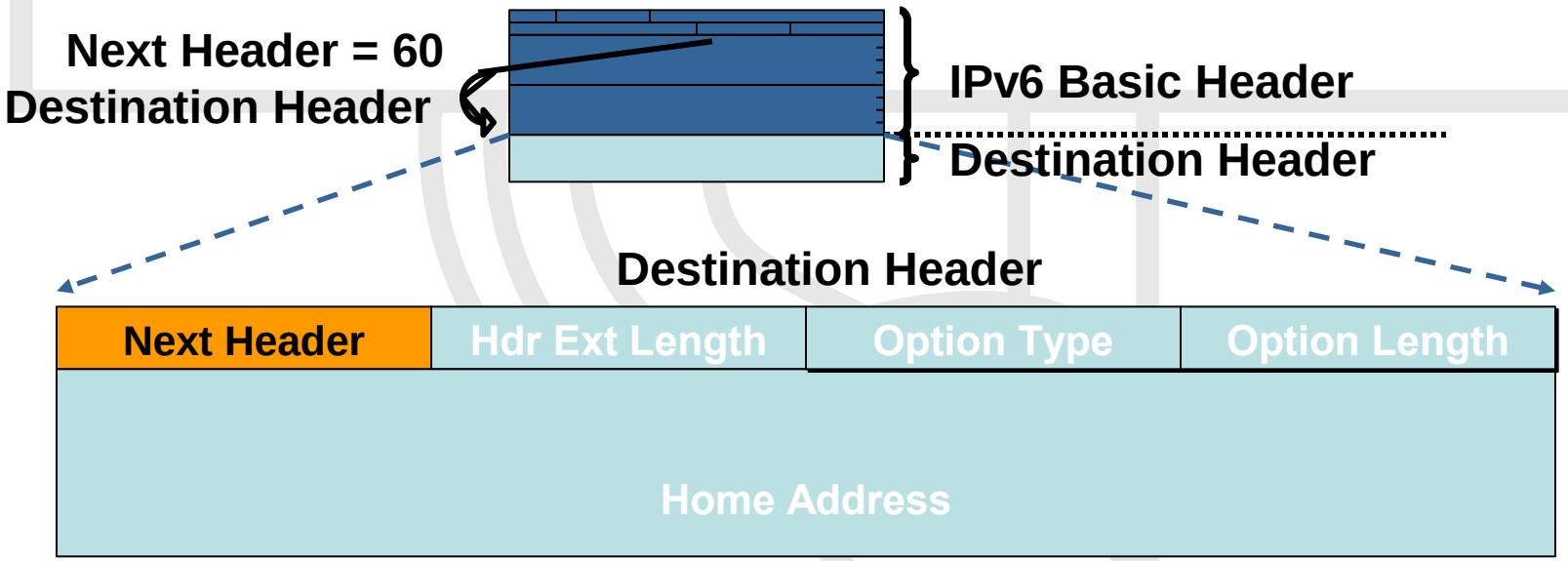


- New extension header to be used by MN, HA and CN in all messaging related to the creation and management of binding
- IPv6 option header may allow piggybacking of these messages
  - Another advantage over IPv4

Mobility Header

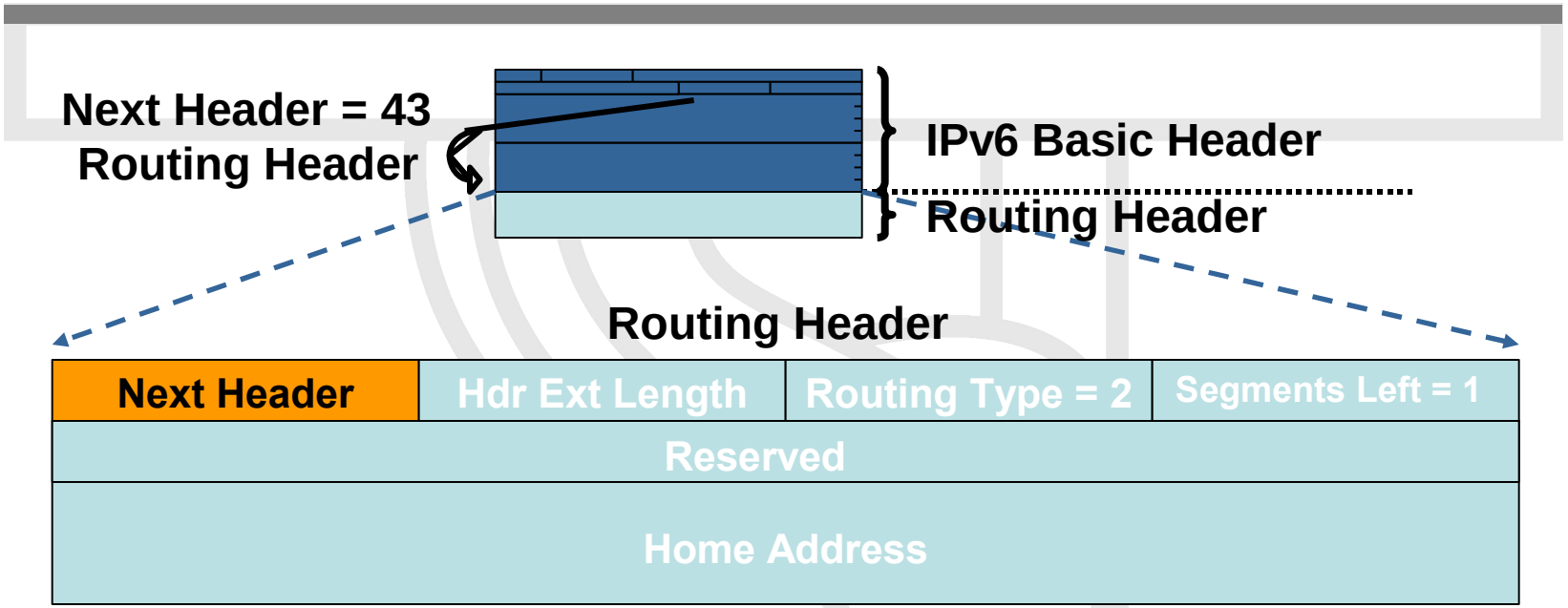
- Mobility header type
  - Binding Refresh Request Message
  - Home Test Init Message (HoTI)—Home Test Message (HoT)
  - Care-of Test Init Message (CoTI)—Care-of Test Message (CoT)
  - Binding Update Message (BU)—Binding Acknowledgement Message (BA)
  - Binding Error Message (BE)
- Message data field contains mobility options
  - Binding refresh advice
  - Alternate Care-of Address
  - Nonce Indices
  - Binding authorization data
- Triangular routing does not require all these message, only BU, BA and BE

New Option in Destination Option Header



- The home address option is carried by the destination option extension header
- It is used in a packet sent by a MN while away from home, to inform the recipient of the MN's home address
  - HAO is not a security risk, if mobile is unknown, hosts send a parameter problem; otherwise contents are verified
- Have to use CoA as source due to RPF

Type 2 Routing Header

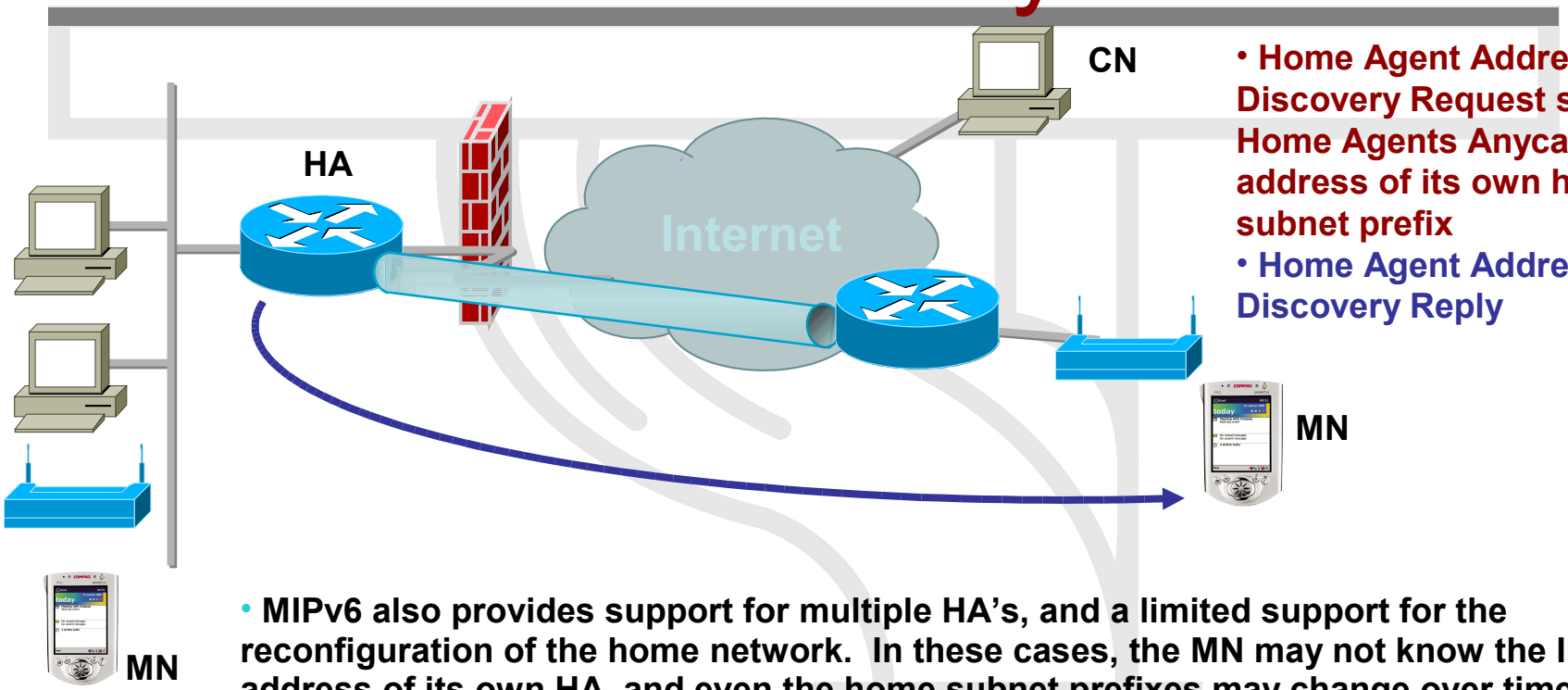


- MIPv6 defines a new routing header variant to allow the packet to be routed directly from a CN to a MN CoA
- MN CoA is inserted into the IPv6 destination address field; once the packet arrives at the care-of address, the MN retrieves its home address from the routing header, and this is used as the final destination address for the packet
- The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to mobile IPv6

MIPv6 – 4 new ICMPv6 Messages

- Use of ICMPv6 and Neighbor Discovery makes MIPv6 independent from the data link layer technology
- Two for use in the dynamic home agent address discovery (DHAAD) mechanism
  - –Home Agent Address Discovery Request – use of Home Agents Anycast address of its own home subnet prefix
  - –Home Agent Address Discovery Reply
- Two for renumbering and mobile configuration mechanisms.
  - – Mobile Prefix Solicitation
  - – Mobile Prefix Advertisement

Dynamic Home Agent Address Discovery



- Home Agent Address Discovery Request sent to Home Agents Anycast address of its own home subnet prefix
- Home Agent Address Discovery Reply

- MIPv6 also provides support for multiple HA's, and a limited support for the reconfiguration of the home network. In these cases, the MN may not know the IP address of its own HA, and even the home subnet prefixes may change over time.
- A mechanism, known as "dynamic home agent address discovery (DHAAD)" allows a MN to dynamically discover the IP address of a HA on its home link, even when the MN is away from home.
- MN can also learn new information about home subnet prefixes through the "mobile prefix discovery" mechanism.

Modifications to Neighbor Discovery

- Modified Router Advertisement Message Format
  - –Single flag bit indicating HA service
- Modified Prefix Information Option Format
  - –To allow a router to advertise its global address
- New Advertisement Interval Option Format
- New Home Agent Information Option Format
- Changes to Sending Router Advertisements
  - –To provide timely movement detection for mobile nodes

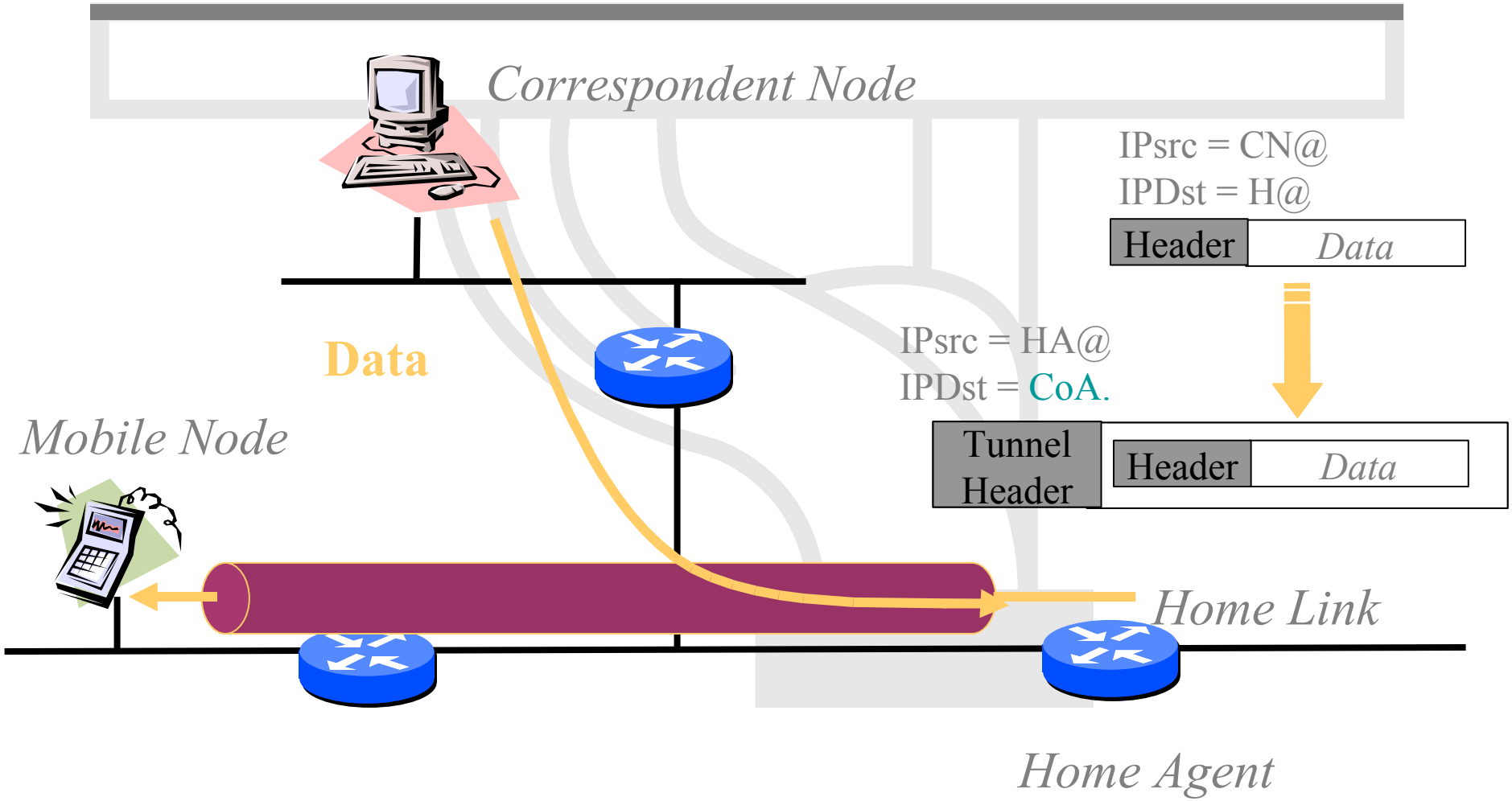
Binding Cache Management

- Every time the MN connects to a foreign network, it sends a Binding Update (BU):
  - Every BU carries a TTL
  - A MN caches the list of CNs to which it sent a BU
  - The MN may have multiple CoAs, the one sent in the BU to the HA is called the ***primary CoA***

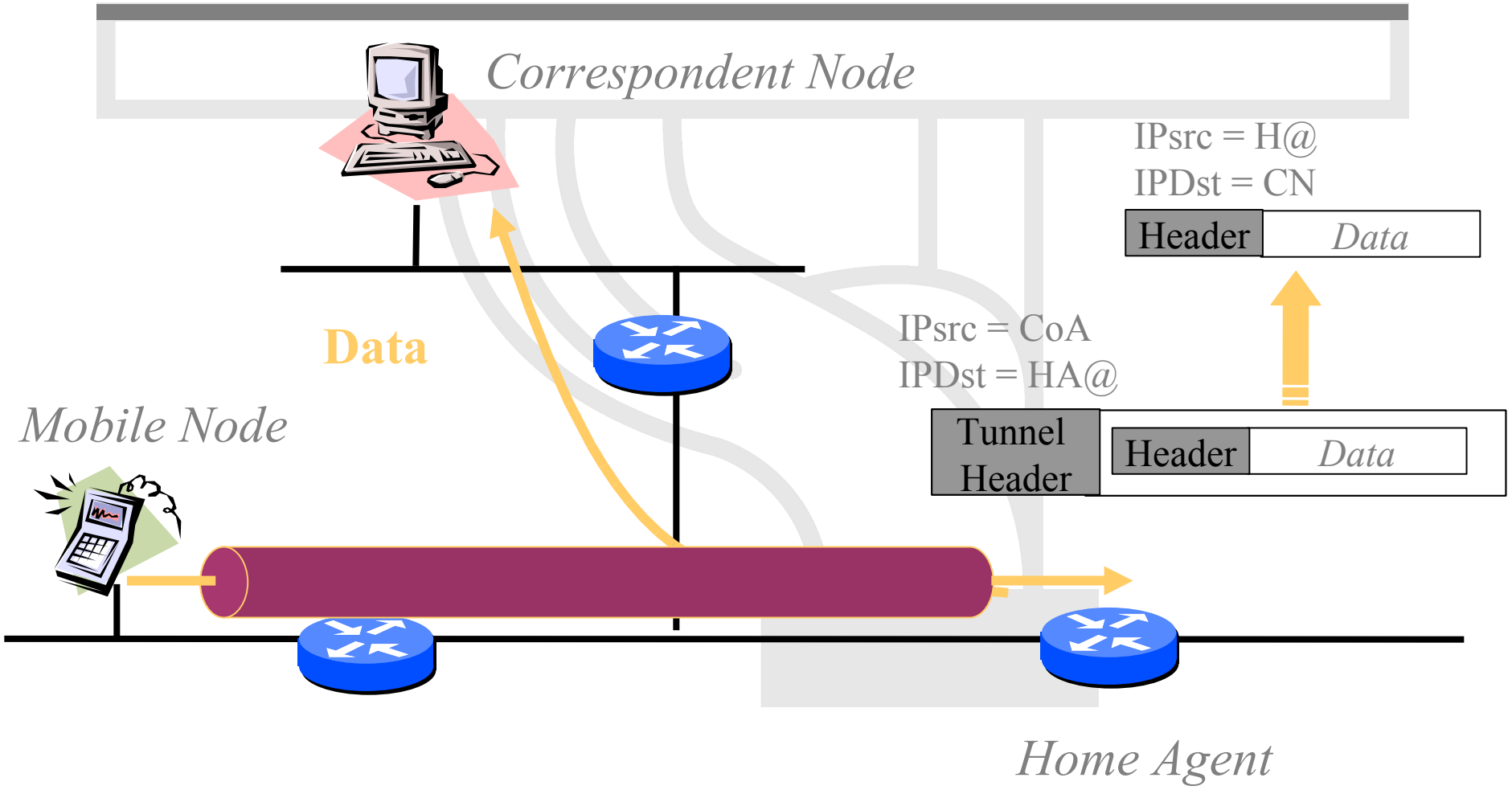
Communication with a Mobile Node

- 2 methods:
  - Bi-directional Tunneling
    - No mobility requirements on CNs
    - No visibility of MNs for CNs
    - Network load increased
    - HA role much reinforced
  - Direct Routing
    - Much more complex mechanism
    - HA role much alleviated

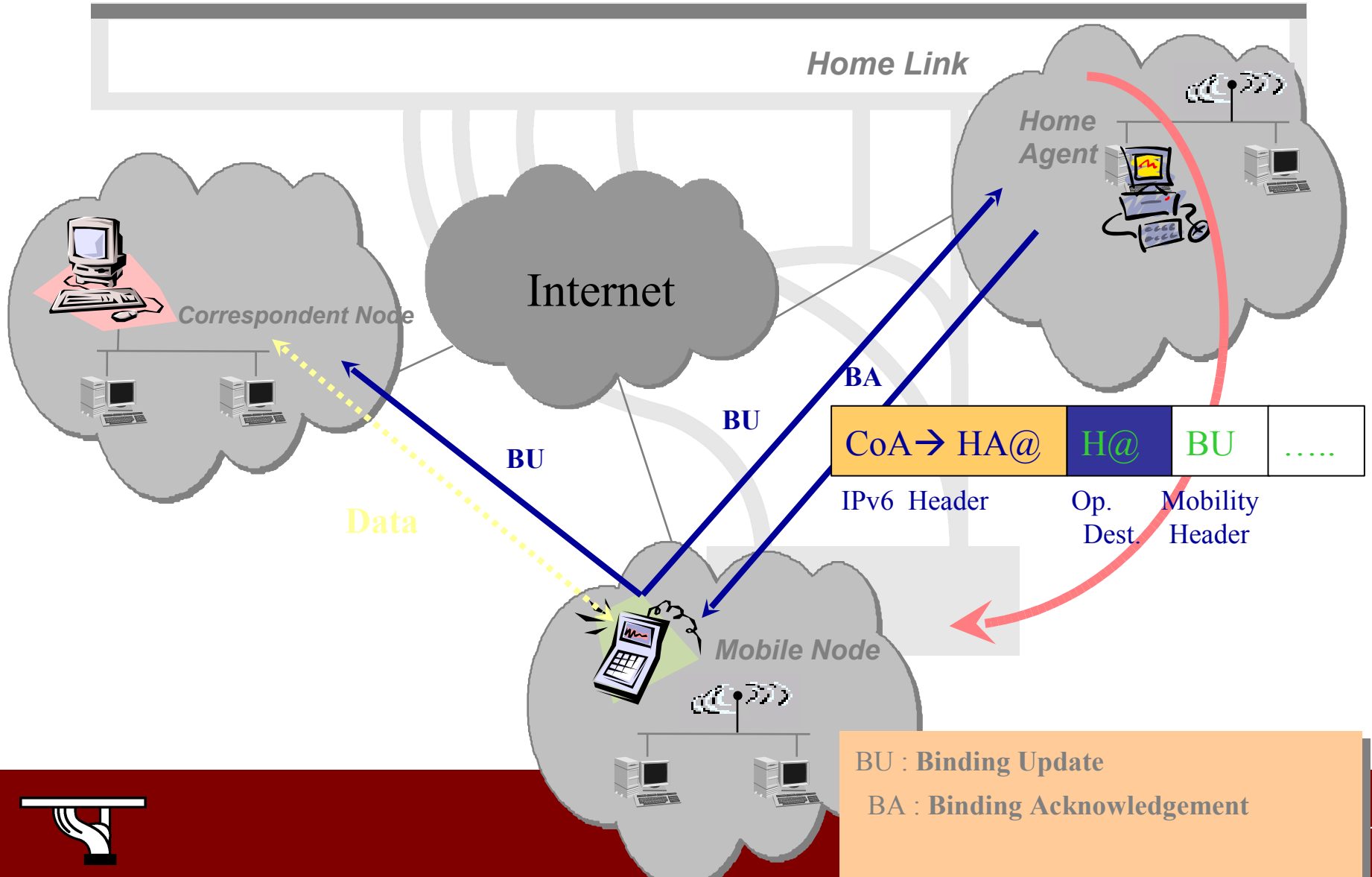
Bi-directional Tunneling



Bi-directional Tunneling (2)



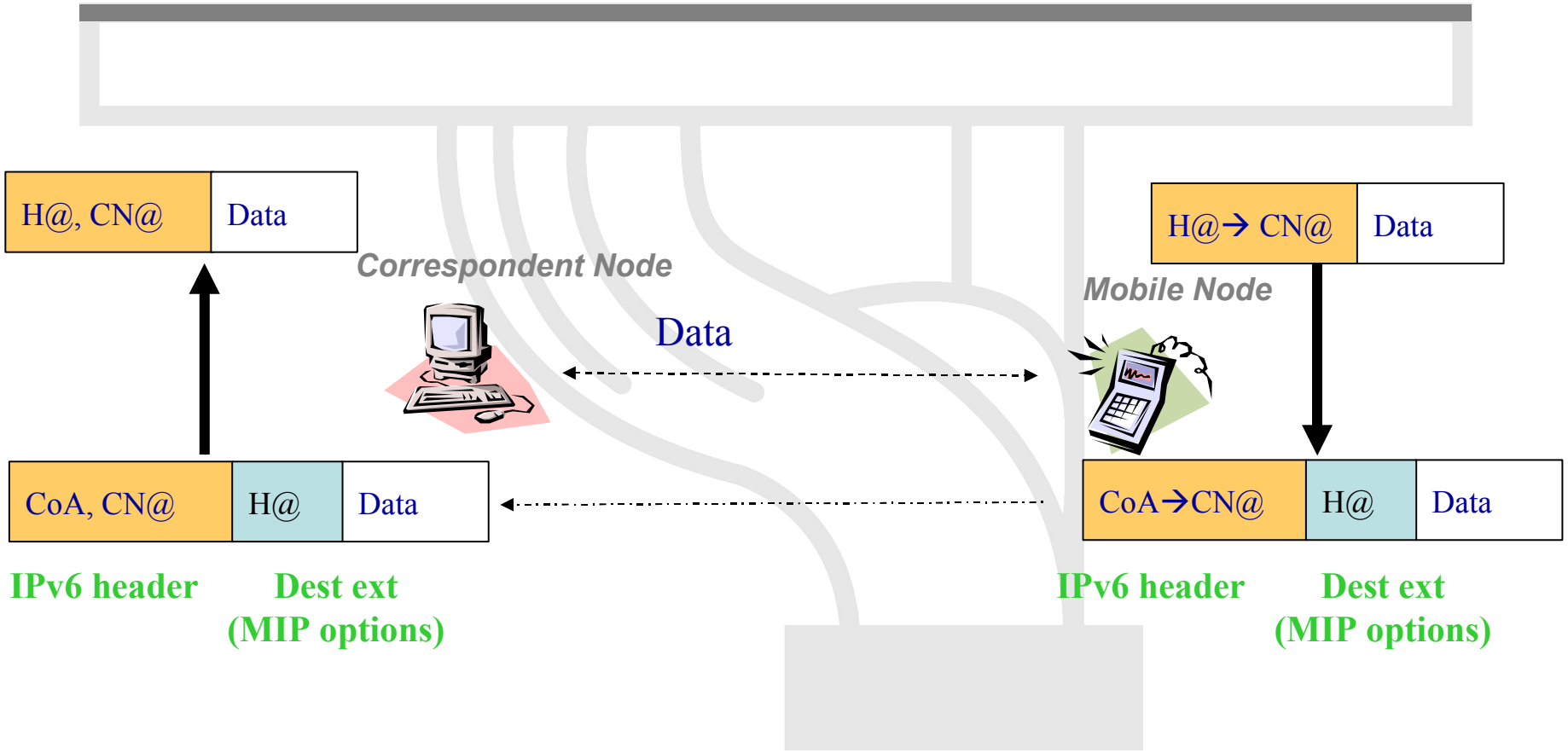
Direct Routing



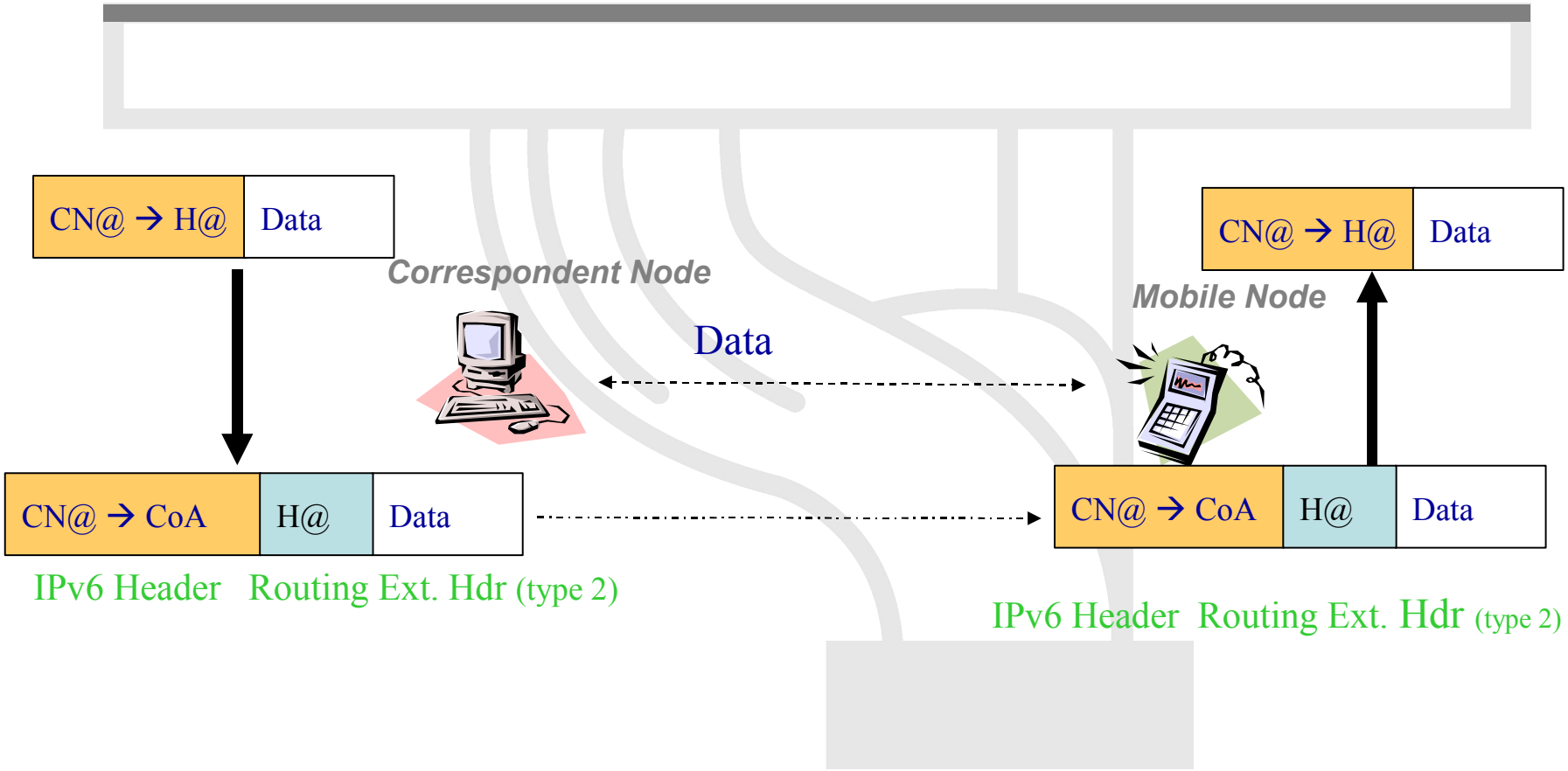
BU : **Binding Update**

BA : **Binding Acknowledgement**

Direct Routing: MN → CN



Direct Routing: CN → MN



Binding Update Authentication

- BU information needs protection and authentication
  - Sender authentication
  - Data integrity protection
  - Replay protection
- Authentication Data sub-option used to carry necessary data authentication
- IPsec may be used to fulfill all these needs
  - MIPv6 is seen as a good opportunity to boost IPsec (and IPv6) deployment

Mobility Features For IPv6 Hosts

- For MNs
  - To perform IPv6 packet encapsulation/decapsulation
  - To send BUs and receive BAs (process the Mobility Header)
  - To keep track of BUs sent
- For CNs
  - To be able to process the Mobility Header (Binding Update, Binding Acknowledge)
  - To use the Routing Header (type 2)
  - Maintain a Binding Cache

Mobility Features For IPv6 Routers

- At least one IPv6 router on the Home Link of the MN must be able to act as a Home Agent

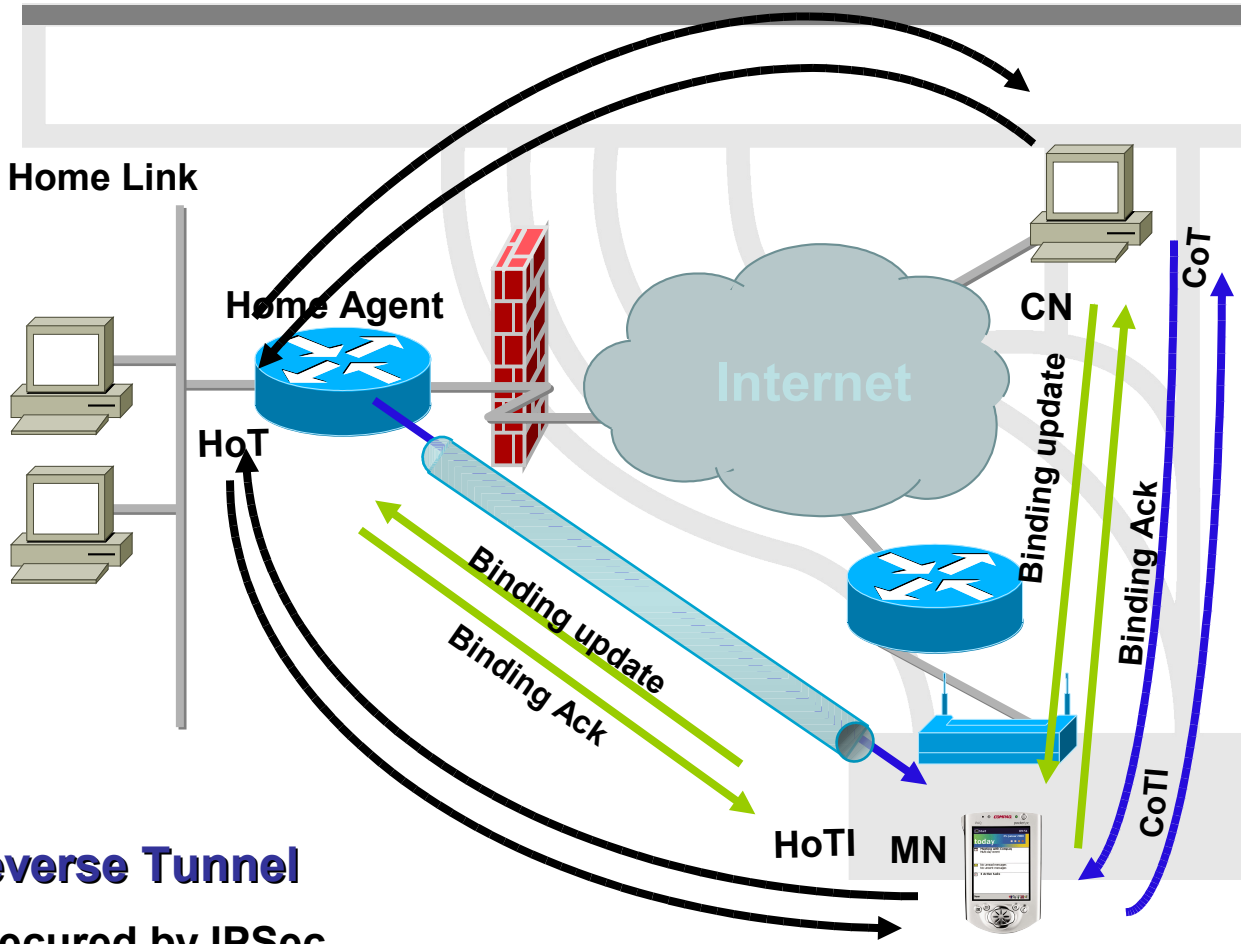
- A Home Agent must:
  - Maintain MN's binding information
  - Intercept packets for a MN in a Home Link it is responsible for
  - Encapsulate/decapsulate (tunnel) these packets and forward them to the CoA of the MN

MOBILE IPv6 SECURITY OVERVIEW

Mobile IPv6 Security Overview

- MIPv6 RFC 3775/3776 provides a number of security features.
- Protection of Binding Updates both to home agents and correspondent nodes
  - –Use of IPSec extension headers, or by the use of the Binding Authorization Data option. This option employs a binding management key, Kbm, which can be established through the return routability procedure.
- Protection of mobile prefix discovery
  - –Through the use of IPSec extension headers.
- Protection of the mechanisms that MIPv6 uses for transporting data packets.
  - –Mechanisms related to transporting payload packets - such as the Home Address destination option and type 2 routing header - have been specified in a manner which restricts their use in attacks.

Security Threats and Solutions



Correspondent Node

Arbitrary: No preexisting Security Association

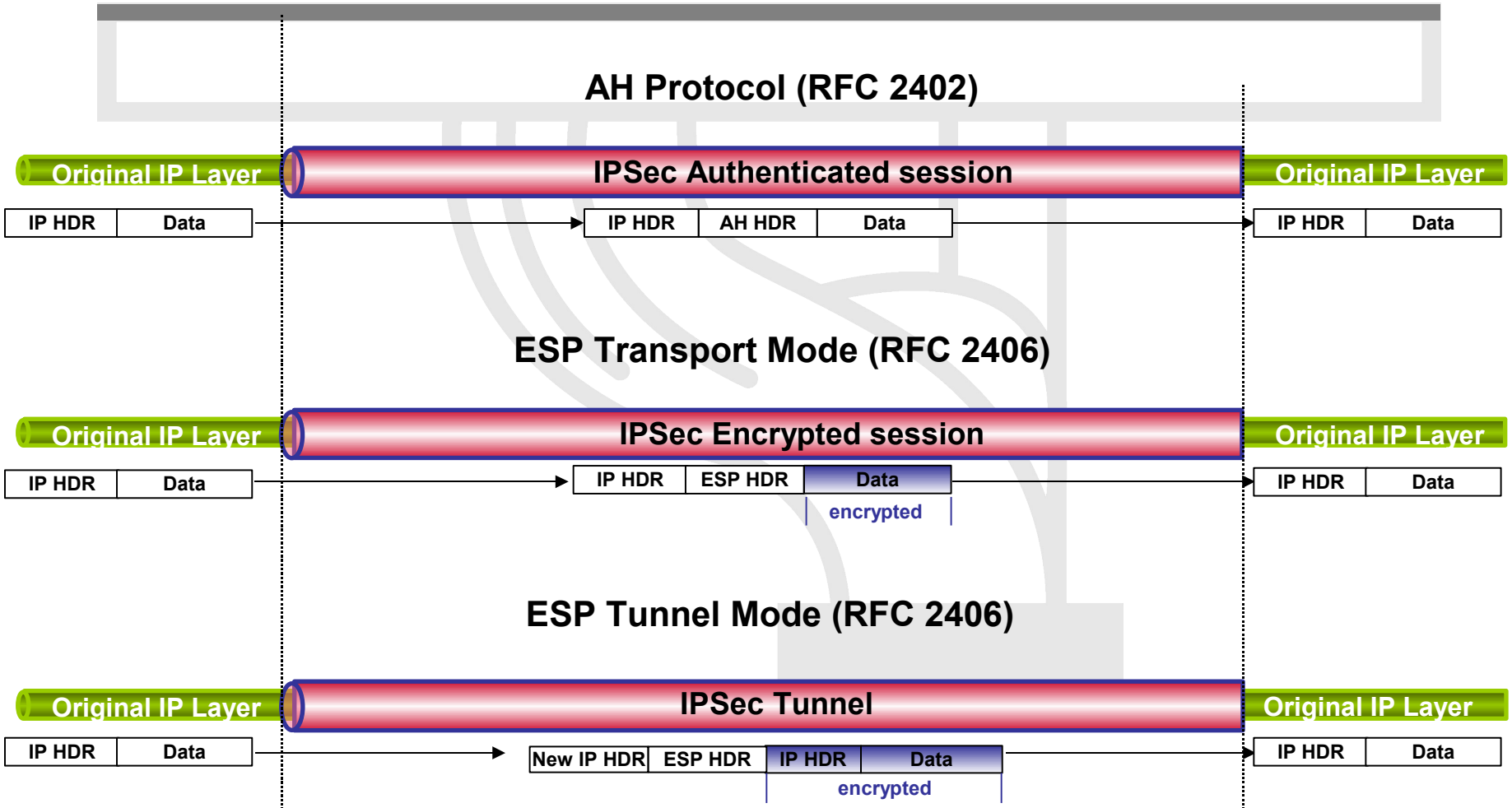
Return Routability test

- **Verifies the collocation of the CoA and the Home Address**
- **Assumes better Security Association between HA and MN**
- **Scalable and stateless**

Reverse Tunnel

- **Secured by IPSec**
- **Requires a preexisting Security Association**

IPSec Technology Primer



Binding Updates Protection

- BU/BA to Home Agents MUST be secured through IPSec
  - –ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.
  - –ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.
  - –ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.
  - –ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.
  - –If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Mobile Prefix Discovery

- Mobile Node and the Home Agent SHOULD use an IPSec security association to protect the integrity and authenticity of the Mobile Prefix Solicitations and Advertisements.
  - –Both the MNs and the HAs MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode with a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection

Payload Packets

- Payload packets exchanged with MN can be follow the same protection policy as other IPv6 hosts
- Specific security measures are defined to protect the specificity of MIPv6
  - –Home Address destination option
  - –Routing header
  - –Tunneling headers
- Home Address Destination Option can only be used when a CN already has a Binding Cache entry for the given home address.
- Tunnels protection between a MN and HA
  - –MN verifies that the outer IP address corresponds to its HA.
  - –HA verifies that the outer IP address corresponds to the current location of the MN (Binding Updates sent to the home agents are secure).
  - –HA identifies the MN through the source address of the inner packet. (home address of the MN)
- For traffic tunneled via the HA, additional IPSec ESP encapsulation MAY be supported

Mobile IPv6 Terms

- Binding management key (Kbm)
  - –A binding management key (Kbm) is a key used for authorizing a binding cache management message (e.g., BU or BA). Return routability provides a way to create a binding management key.
- Cookie
  - –A cookie is a random number used by a mobile nodes to prevent spoofing by a bogus correspondent node in the return routability procedure.
- Keygen Token
  - –A keygen token is a number supplied by a correspondent node in the return routability procedure to enable the mobile node to compute the necessary binding management key for authorizing a Binding Update.
- Nonce
  - –Nonces are random numbers used internally by the correspondent node in the creation of keygen tokens related to the return routability procedure. The nonces are not specific to a mobile node, and are kept secret within the correspondent node.

MOBILE IPv6 @ CISCO

Mobile IPv6 @ Cisco

- Home Agent
  - In Field Trial since CY01
  - RFC3775 Compliant
  - Available from Cisco IOS 12.3(14)T, 12.4 & 12.4T
  - Enhanced ACL – routing type filtering capability – future feature of 12.4T
  - Securing MIPv6 is future deliverable on 12.4T
- Mobile IPv6 is part of the planned IPv6 rollouts
  - http://www.cisco.com/warp/public/732/Tech/ipv6/ipv6_learnabo
  - http://www.cisco.com/warp/public/732/Tech/ipv6/

Mobile IPv6 @ Cisco

Microsoft
Mobile IPv6 Client

1.1.1.7

Other client sources:
- **Elmic Systems**
- **Lancaster Univ.**
- **Rice University**

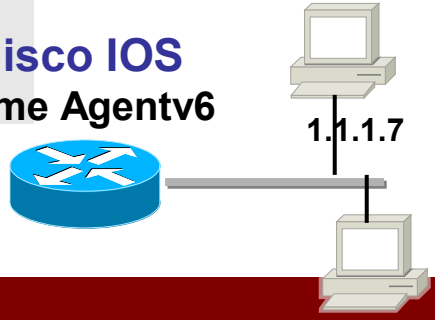
Cisco IOS
Home Agentv6

1.1.1.7

Mobile Networksv6 (NEMO) – in development

Cisco IOS
Mobile Networksv6

Cisco IOS
Home Agentv6



1.1.1.7

1.1.1.7

Cisco IOS MIPv6 Implementation

- Supported on Cisco 1800, 2600XM, 2691, 2800, 3640, 3660, 3700, 3800 and 7200 series
  - –Cisco IOS 12.3(14)T
  - –Planned on MWAM 3.0
- TAHI
  - –few aspects from TAHI testing bring resolved
  - –Dynamic HA Address Discovery, Mobile Prefix Discovery
- Future authentication mechanisms
  - –MD5 Lightweight authentication
  - – Cisco authored a draft to IETF
  - –IPSec support planned in a future stage
- CEF support on the roadmap
- Track NEMO working group
  - –Develop a plan to bring Mobile Networksv6 to market

CLI for MIPv6 HA – Global commands

- Router# (config) ipv6 mobile mh-number <0-255>
  - –Changes the number used in the MIPv6 MH. Default is 62
- Router# (config) ipv6 mobile binding maximum <integer>
  - –Specifies the maximum number of registration bindings which may be maintained concurrently. By default, binding maximum is unset indicating unlimited. If the configured number of home agent registrations is reached or exceeded, subsequent registrations will be refused with the error "Insufficient resources". No existing bindings will discarded until their lifetime has expired, even if binding maximum is set to a value below the current number of such bindings.
- Router# (config) ipv6 mobile binding refresh <seconds>
  - –Default is 5 minutes (300 seconds).

CLI for MIPv6 HA – Interface subcommands

- Router# (config-if) ipv6 mobile home-agent { create | run }
  - –Enables home agent operation on the interface. By default, home agent operation is disabled.
  - –create is used to initialize the home agent feature on the interface, but does not start operation. Interface level parameters may be configured before operation is commenced.
  - –run causes home agent operation to commence on the interface. Interface level parameters may be configured whilst the home agent is in operation.
- Router# (config-if) ipv6 mobile home-agent access <acl>
  - –Configures a binding update filter using an ACL. When an ACL is configured, all received binding updates are filtered. This feature may be used to deny home agent services to mobile nodes that have roamed to particular sub-networks. When the filter blocks a binding update, a binding acknowledgement is returned with error status "Administratively prohibited". Default is no filter; all binding updates are accepted. Note that the filter is also applied to Home Agent Address Discovery messages. When blocked, these are silently discarded. In configuration of the ACL, the src is the CoA and the dst is the HoA.
- Router# (config-if) ipv6 mobile home-agent preference <integer>
  - –Specifies the value to be use for Preference in the Home Agent Information Option transmitted on the interface. A value in the range -32768 to +32767 may be specified. By default, a value for Preference of zero is assumed for home agent operation on this interface.

CLI for MIPv6 HA – Interface subcommands

- Router# (config-if) ipv6 nd ra-interval <integer> [msec]
  - –Specifies the interval between sending unsolicited multicast Router Advertisements on this interface. This command already exists, but the optional sufffix has been introduced to indicate that the interval has been specified in milliseconds, rather than the default of seconds. This allows specification of the new minimum value of 0.05 seconds. The interval should be set to a low value on interfaces providing service to visiting mobile nodes.
- Router# (config-if) ipv6 nd advertise-interval
  - –Specifies whether an Advertisement Interval option should be transmitted in Router Advertisements. This option may be used to indicate to a visiting mobile node how frequently it may expect to receive RAs. It may use this information in its movement detection algorithm.
- Router# (config-if) ipv6 nd prefix <prefix> | default [[<valid-lifetime> <preferred-lifetime>] | [at <valid-date> <preferred-date>] [off-link] [no-rtr-address] [no-autoconfig]]
  - –This command already exists and is modified to support the no-rtr-address option. By default all prefixes configured as addresses on the interface will be advertised in Router Advertisements. This command allows control over the individual parameters per prefix, including whether the prefix should be advertised or not. The "default" keyword can be used to set default parameters for all prefixes. A date can be set for prefix expiry. The valid and preferred lifetimes are counted down in real time. When the expiry date is reached the prefix will no longer be advertised.

CLI for MIPv6 HA – Show commands

- Router# show ipv6 interface <interface>
  - –Ouput extended to include home agent data where and when applicable.
- Router# show ipv6 mobile binding [home-address <prefix>] [care-of-address <prefix>] [interface <interface>]
  - –Displays details of all bindings which match all the search criteria. If no parameters are specified, all bindings are listed.
- Router# show ipv6 mobile globals
  - –Displays the values of all global configuration parameters associated with MIPv6, and lists the interfaces on which home agent functionality is currently operating.
- Router# show ipv6 mobile traffic
  - –Displays counters and other information associated with MIPv6.
- Router# show ipv6 mobile home-agents [<interface> [<prefix>]]
  - –Displays the Home Agents List for the specified interface or, if none is specified, displays the Home Agents List for each interface on which the router is acting as a home agent.

CLI for MIPv6 HA – Clear commands

- Router# clear ipv6 mobile binding [home-address <prefix>] [care-of-address <prefix>] [interface <interface>]
  - –Clears all bindings with the mobile nodes which match the search criteria. E.g.,
    - router# clear ipv6 mobile binding
    - Clear 27 bindings [confirm]
  - –Note that when this command is used to delete bindings, the mobile node will not be informed that its home agent is no longer acting on its behalf.
- Router# clear ipv6 mobile home-agent <interface>
  - –Clears the Home Agents List on the specified interface. It will be subsequently reconstructed from received Router Advertisements.
- Router# clear ipv6 mobile traffic
  - –Zeros counters associated with MIPv6.

CLI for MIPv6 HA – Debug commands

- Router# debug ipv6 nd
  - –output modified to include relevant home agent data.
- Router# debug ipv6 mobile {home-agent | registration | correspondent-node | forwarding}
  - –Best to turn all on currently.

Implementations and Interoperability

MIPv6 Implementation

- Mobile IPv6 implementations must be referred as
  - –Mobile Node (MN)
  - –Home Agent (HA)
  - –Correspondent Node (CN)
- MIPv6 draft ID is important for interoperability
  - –Draft ID not always backward compatible

Known Implementations

- 6Wind
- Cisco – HA
- Elmic systems now Treck Inc. www.treck.com
  - –http://www.elmic.com/pdf/MobileIPv6_data.pdf
- Ericsson
- HP – HP-UX (HA, CN) and Tru64 (HA, CN)
- Keio University (Wide) – HA, MN, CN and IPsec (no IKE)
- Microsoft Window XP and CE beta
- Mobile IP v4 and v6 implementation http://www.mip4.org/2004/implementations/

Known Implementations

- NEC – MN, HA, CN and IPsec
- Nokia – MN, HA, CN
- Samsung – MN, CN
- Siemens
- SUN – CN
- University of Helsinski (Linux) – MN, CN
  - http://www.mipl.mediapoli.com
- 6NET MIPv6 implementation survey
  - http://www.6net.org/publications/deliverables/D4.1.1.pdf

Interoperability

- Connecthaton
  - –http://www.connectathon.org/
- Test suites
  - –TAHI, UNH
- Previous testing required similar ID compliancy

CISCO Mobile Networks

Cisco IOS Mobile Networks Delivers....

- Always-on IP connectivity for entire LAN segments
- Subnets are mobile without devices on those subnets being aware
- Mobile Router (MR) is in effect a Mobile IP Client
- Unconstrained by location
- Transport independent
- Robust roaming connections
- Transparent to applications
- Transparent to end devices

Vertical Market Applications

Public Services
- Emergency services
- Police
- Fire Fighters

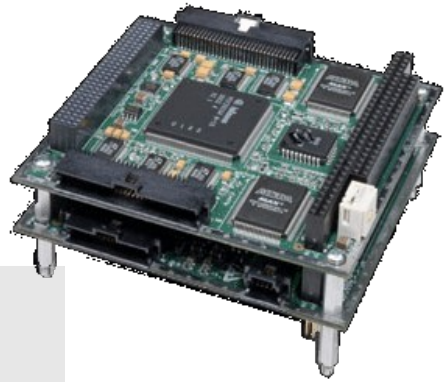
Armed Services
- Military: Army, Navy, Marines, NATO, UK DoD, etc.

Commercial Markets
- Package delivery fleets
- Trucking
- Rental fleets

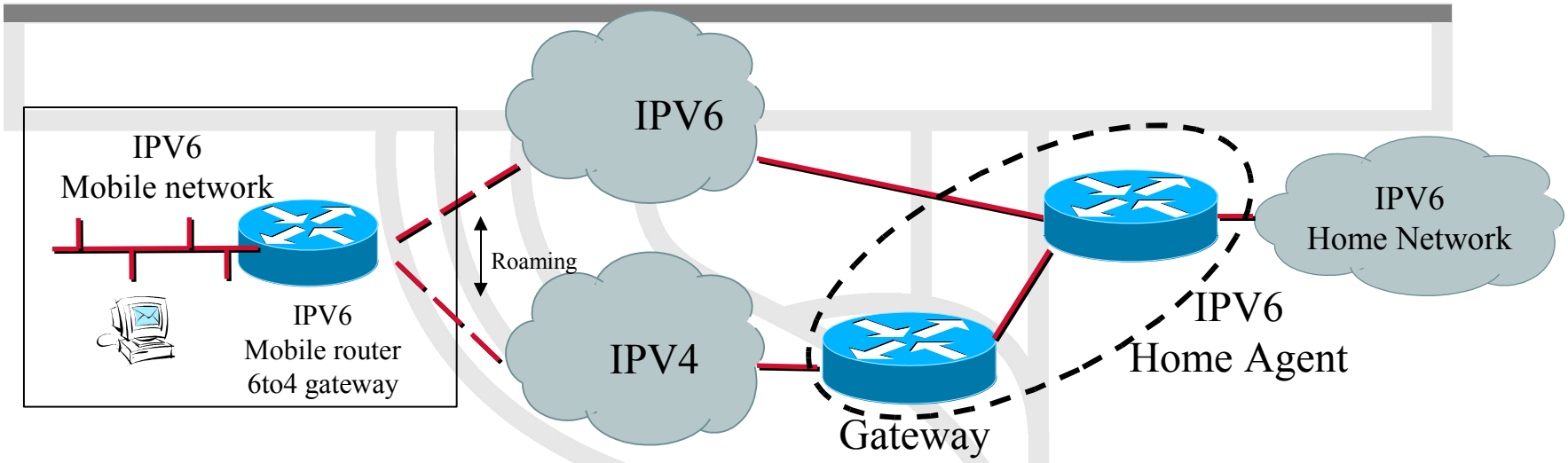
Consumer Automotive
- Telematics
- Infotainment
- Railroads

Cisco Mobile Networks

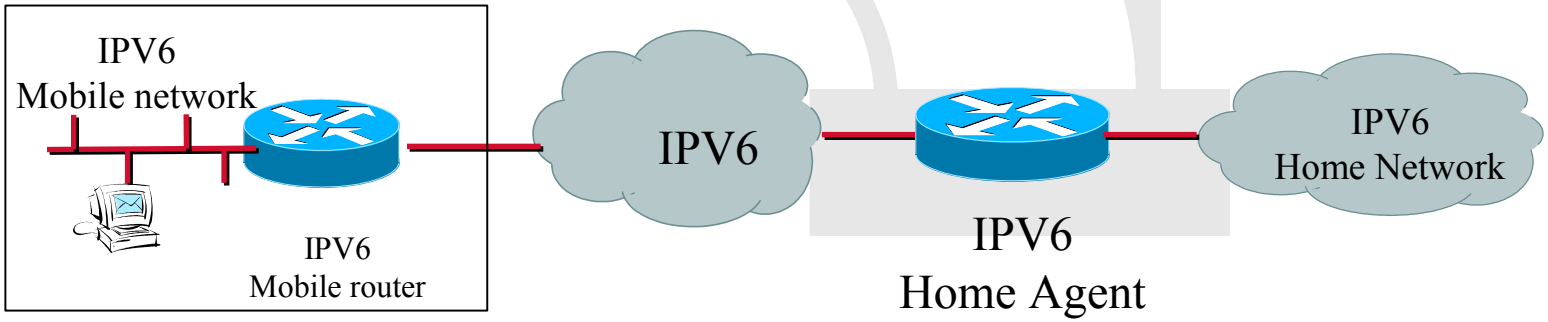
- Available Today on IPv4
- Mobile router feature set on 12.2(4)T and above
- Cisco 2600 to 7500
- Cisco MAR 3200
- Basic Mobile Router IPv6
  - –EFT available for trial now



Mobile Networks IPv6: Roaming Scheme



Mobile IPV6 router roaming into a V4 or V6 network



Ideal topology

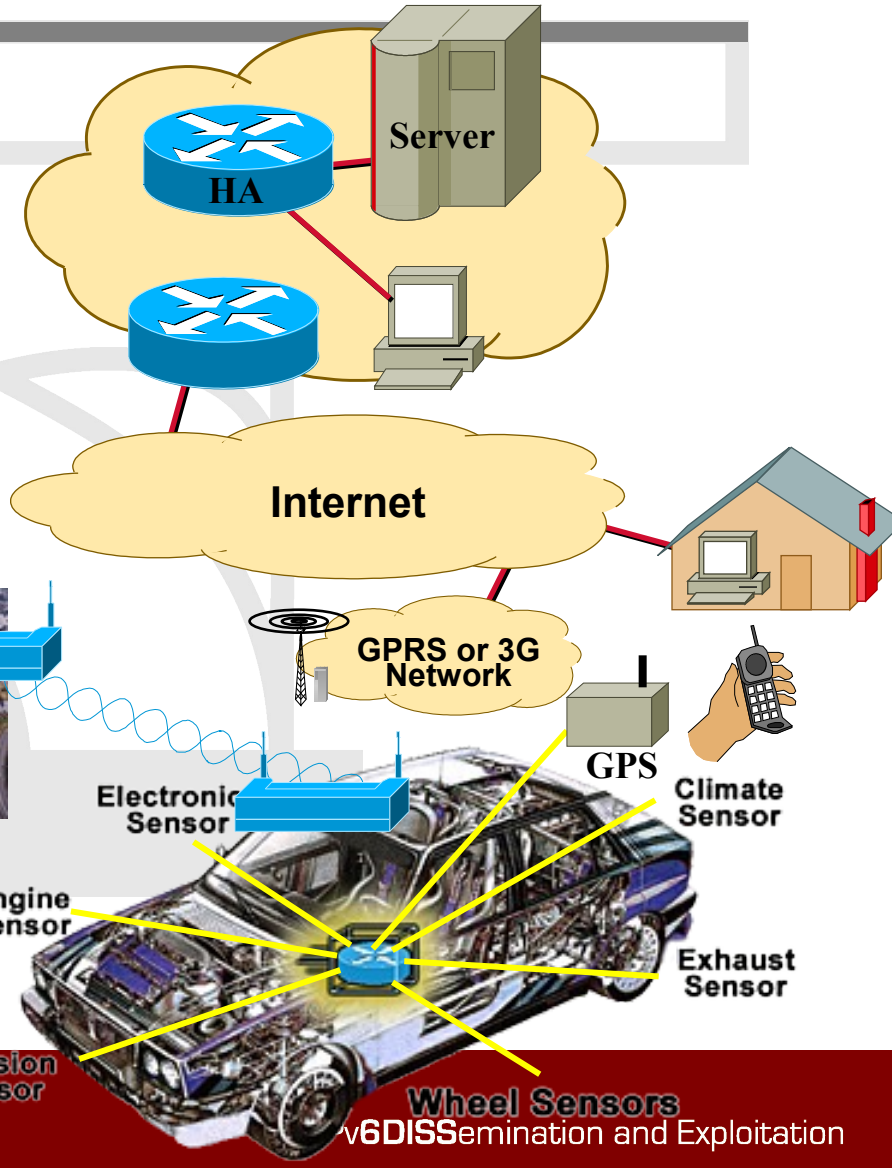
Networks in Motion

Telematics:

Industry related to using computers in concert with telecommunications systems. This includes Internet access, as well as all types of networks that rely on a telecommunications system to transport data.

"Telematics to Become $8 Billion Industry by 2005, According to New Study from Allied Business Intelligence"

http://www.telematicsupdate.com



References

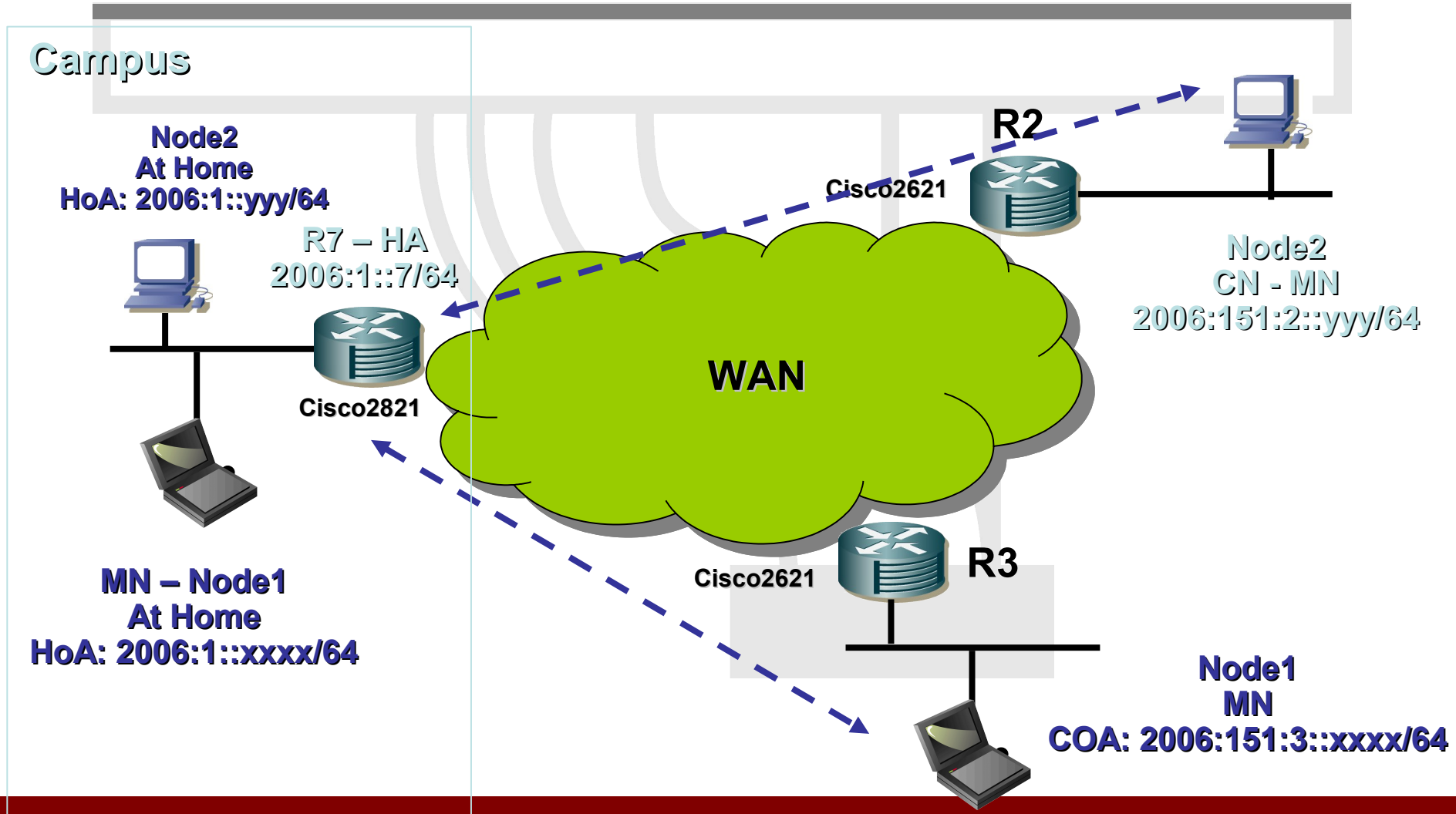
- IETF Working Group URL
  - http://www.ietf.org/html.charters/mip6-charter.html
- Mobile IP for IPv6
  - http://www.ietf.org/rfc/rfc3775.txt
- Fast Handover for MIPv6
  - http://www.ietf.org/internet-drafts/draft-ietf-mobileip-fast-mipv6-07.txt
- Using IPsec to protect MIPv6
  - http://www.ietf.org/rfc/rfc3776.txt
- Hierarchical MIPv6 mobility management
  - http://www.ietf.org/internet-drafts/draft-ietf-mobileip-hmipv6-08.txt
- Mobile IP implementations for v4 and v6
  - http://www.mip4.org/2004/implementations/

Mobile IPv6 Testbed

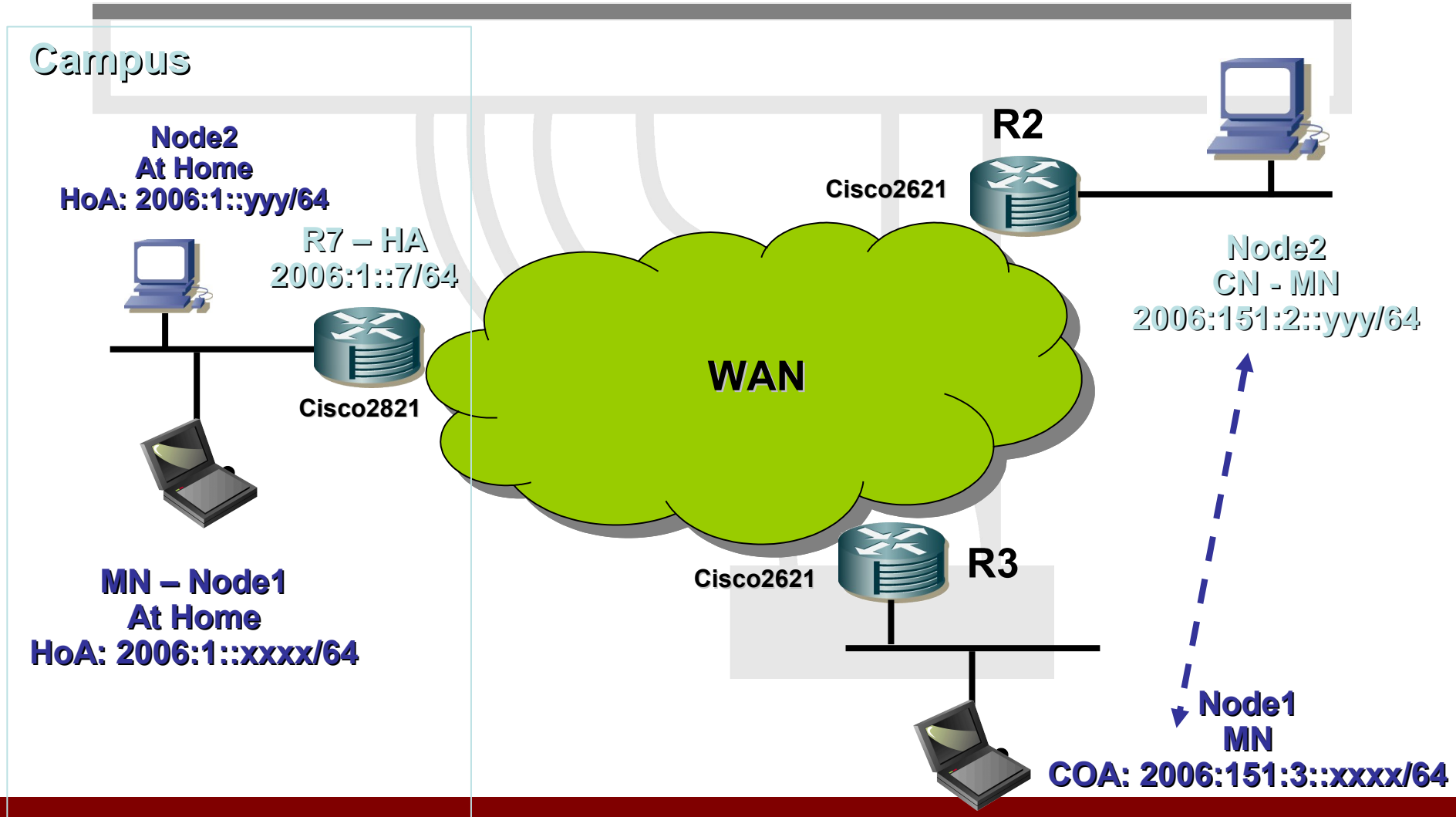
MIPv6 Devices

- Home Agent
  - Cisco 2821
  - IOS 12.3(14)T1
- Node1 (laptop): WinXP SP1 – MIPv6 Tech Preview
  - HoA: 2006:1::20D:60FF:FEFA:E15B
  - CoA: 2006:151:3:0:20D:60FF:FEFA:E15B
- Node2 (Server3): WinXP SP1 – MIPv6 Tech Preview
  - HoA: 2006:1::20C:29FF:FEB9:8D7C
  - CoA: 2006:151:2:0:20C:29FF:FEB9:8D7C

Topology – Without Optimized Routing



Topology – With Optimized Routing



HA – Configuration

```
ipv6 mobile home-agent
!
interface GigabitEthernet0/0
 description ==== Vers le Campus ===
 ip address 10.151.1.7 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2006:1::7/64
 ipv6 mobile home-agent preference 1
 ipv6 mobile home-agent
 ipv6 ospf 200 area 0
!
```

HA Display – No Mobile Node

```
R7#sh ipv6 mobile globals
Mobile IPv6 Global Settings:

  1 Home Agent service on following interfaces:
    GigabitEthernet0/0
  Bindings:
    Maximum number is unlimited.
    1 bindings are in use
    1 bindings peak
    Binding lifetime permitted is 262140 seconds
    Recommended refresh time is 300 seconds
R7#
```

```
R7#sh ipv6 mobile home-agents
Home Agent information for GigabitEthernet0/0
  Configured:
    FE80::20F:35FF:FE2D:38C9
    preference 1 lifetime 1800
      global address 2006:1::7/64
  No Discovered Home Agents

R7#
```

HA Display – Current Bindings

```
R7#sh ipv6 mobile binding
Mobile IPv6 Binding Cache Entries:

  2006:1::20C:29FF:FEB9:8D7C
    link local address FE80::20C:29FF:FEB9:8D7C
    via care-of address 2006:151:2:0:20C:29FF:FEB9:8D7C
    home-agent 2006:1::7
    state ACTIVE, sequence 4, flags AHLk
    lifetime: remaining 40 (secs), granted 60 (secs), requested 60 (secs)
    interface GigabitEthernet0/0
    17 tunneled, 17 reversed tunneled
  2006:1::20D:60FF:FEFA:E15B
    link local address FE80::20D:60FF:FEFA:E15B
    via care-of address 2006:151:3:0:20D:60FF:FEFA:E15B
    home-agent 2006:1::7
    state ACTIVE, sequence 29, flags AHLk
    lifetime: remaining 16 (secs), granted 60 (secs), requested 60 (secs)
    interface GigabitEthernet0/0
    18 tunneled, 29 reversed tunneled
Selection matched 2 bindings
R7#
```

Node2

Node1

HA – deb ipv6 mobile forwarding

Ping from Node1 (on R3) to R2 loop0

```
R7#
*Apr 20 16:46:24 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=80 ttl=61)
*Apr 20 16:46:24 UTC: MIPv6-Fwd: Tunneled packet
*Apr 20 16:46:24 UTC:            from 2006:151::2
*Apr 20 16:46:24 UTC:            to 2006:1::20D:60FF:FEFA:E15B
*Apr 20 16:46:24 UTC:            using COA 2006:151:3:0:20D:60FF:FEFA:E15B
*Apr 20 16:46:25 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=80 ttl=61)
*Apr 20 16:46:30 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=80 ttl=61)
*Apr 20 16:46:30 UTC: MIPv6-Fwd: Tunneled packet
*Apr 20 16:46:30 UTC:            from 2006:151::2
*Apr 20 16:46:30 UTC:            to 2006:1::20D:60FF:FEFA:E15B
*Apr 20 16:46:30 UTC:            using COA 2006:151:3:0:20D:60FF:FEFA:E15B
*Apr 20 16:46:31 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=80 ttl=61)
*Apr 20 16:46:45 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=80 ttl=61)
```

HA – deb ipv6 mobile forwarding

Ping from server2 to Node1 (on R3)

```
*Apr 20 17:08:35 UTC: MIPv6-Fwd: Tunneled packet
*Apr 20 17:08:35 UTC:            from 2006:1::202:55FF:FEB7:ACC3
*Apr 20 17:08:35 UTC:            to 2006:1::20D:60FF:FEFA:E15B
*Apr 20 17:08:35 UTC:            using COA 2006:151:3:0:20D:60FF:FEFA:E15B
*Apr 20 17:08:35 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=104 ttl=61)
*Apr 20 17:08:38 UTC: MIPv6-Fwd: Tunneled packet
*Apr 20 17:08:38 UTC:            from 2006:1::202:55FF:FEB7:ACC3
*Apr 20 17:08:38 UTC:            to 2006:1::20D:60FF:FEFA:E15B
*Apr 20 17:08:38 UTC:            using COA 2006:151:3:0:20D:60FF:FEFA:E15B
*Apr 20 17:08:38 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=104 ttl=61)
*Apr 20 17:08:41 UTC: MIPv6-Fwd: Tunneled packet
*Apr 20 17:08:41 UTC:            from 2006:1::202:55FF:FEB7:ACC3
*Apr 20 17:08:41 UTC:            to 2006:1::20D:60FF:FEFA:E15B
*Apr 20 17:08:41 UTC:            using COA 2006:151:3:0:20D:60FF:FEFA:E15B
*Apr 20 17:08:41 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=104 ttl=61)
```

HA - deb ipv6 mobile forwarding ping node1 to node2

```
*Apr 21 14:54:55 UTC: MIPv6-Fwd: Tunneled packet
*Apr 21 14:54:55 UTC:            from 2006:151:2:0:20C:29FF:FEB9:8D7C
*Apr 21 14:54:55 UTC:            to 2006:1::20D:60FF:FEFA:E15B
*Apr 21 14:54:55 UTC:            using COA 2006:151:3:0:20D:60FF:FEFA:E15B
*Apr 21 14:54:55 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=96 ttl=61)
*Apr 21 14:55:12 UTC: MIPv6-Fwd: Tunneled packet
*Apr 21 14:55:12 UTC:            from 2006:151:3:0:20D:60FF:FEFA:E15B
*Apr 21 14:55:12 UTC:            to 2006:1::20C:29FF:FEB9:8D7C
*Apr 21 14:55:12 UTC:            using COA 2006:151:2:0:20C:29FF:FEB9:8D7C
*Apr 21 14:55:12 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:3:0:20D:60FF:FEFA:E15B->2006:1::7 (len=56 ttl=61)
*Apr 21 14:55:12 UTC: MIPv6-Fwd: Tunneled packet
*Apr 21 14:55:12 UTC:            from 2006:1::20D:60FF:FEFA:E15B
*Apr 21 14:55:12 UTC:            to 2006:1::20C:29FF:FEB9:8D7C
*Apr 21 14:55:12 UTC:            using COA 2006:151:2:0:20C:29FF:FEB9:8D7C
*Apr 21 14:55:12 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:2:0:20C:29FF:FEB9:8D7C->2006:1::7 (len=64 ttl=61)
*Apr 21 14:55:12 UTC: MIPv6 tunnel: IPv6/IPv6 to decaps
2006:151:2:0:20C:29FF:FEB9:8D7C->2006:1::7 (len=64 ttl=61)
*Apr 21 14:55:12 UTC: MIPv6-Fwd: Tunneled packet
*Apr 21 14:55:12 UTC:            from 2006:1::20C:29FF:FEB9:8D7C
*Apr 21 14:55:12 UTC:            to 2006:1::20D:60FF:FEFA:E15B
*Apr 21 14:55:12 UTC:            using COA 2006:151:3:0:20D:60FF:FEFA:E15B
```

WinXP MIPv6 Commands

```
Disabling IPSec (Cisco doesn't support IPSec yet)
C:\> ipv6 gpu MIPv6Security off

Manual HA Configuration
C:\> ipv6 hau <HoA> <HA>

[Optional] Route Optimization off
C:\> ipv6 gpu MIPv6RouteOptimize no

Display MIPv6 Home Agent Configuration
C:\> ipv6 ha

Display MIPv6 Binding Updates
C:\> ipv6 bu

Display MIPv6 Binding Cache
C:\> ipv6 bc
```

Node1 : HA config & Parameters

```
F:\Documents and Settings\fefe>ipv6 ha
Home Address: 2006:1::20d:60ff:fefa:e15b
  Home Agent: 2006:1::7
  ESPTunnelSPI: 0
  ESPTunnelSPD: 0


F:\Documents and Settings\fefe>
```

Node1 : Binding update

```
F:\Documents and Settings\fefe>ipv6 bu
Home Address: 2006:1::20d:60ff:fefa:e15b
  Host: 2006:1::7
    CoA       : 6/2006:151:3:0:20d:60ff:fefa:e15b
    Expires   : 47s
    Comments  : HOME_AGENT
    RRState   : NO_RR ACTIVE


F:\Documents and Settings\fefe>
```

Node1: Ping to HoA of Node2 (2006:1::20c:29ff:feb9:8d7c)

```
F:\Documents and Settings\fefe>ping6 -t 2006:1::20c:29ff:feb9:8d7c

Envoi d'une requête 'Ping' 2006:1::20c:29ff:feb9:8d7c
à partir de 2006:1::20d:60ff:fefa:e15b avec 32 octets de données :

Réponse de 2006:1::20c:29ff:feb9:8d7c : octets = 32 temps=7 ms
Réponse de 2006:1::20c:29ff:feb9:8d7c : octets = 32 temps=7 ms

Statistiques de Ping pour 2006:1::20c:29ff:feb9:8d7c :
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (0% de perte),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, maximum = 7ms, moyenne = 7ms
Ctrl+C
^C
```

Node1: BU during ping to Node2

```
F:\Documents and Settings\fefe>ipv6 bu
Home Address: 2006:1::20d:60ff:fefa:e15b
  Host: 2006:1::20c:29ff:feb9:8d7c
    CoA       : 6/2006:151:3:0:20d:60ff:fefa:e15b
    Expires   : 27s
    BU_Rexmits    : 2
    RRState   : AWAIT_ACK SEND_BU

  Host: 2006:1::7
    CoA       : 6/2006:151:3:0:20d:60ff:fefa:e15b
    Expires   : 39s
    Comments  : HOME_AGENT
    RRState   : NO_RR ACTIVE
```

HoA Node2

HA

Node1: Binding Cache during ping to MN2

```
F:\Documents and Settings\fefe>ipv6 bc
home: 2006:1::20c:29ff:feb9:8d7c
 c/o: 2006:151:2:0:20c:29ff:feb9:8d7c
 seq: 50   Lifetime: 14s
 RRState : ACTIVE
```

HoA Node2

CoA Node2

Node1: CoA Care-of address

```
F:\Documents and Settings\fefe>ipv6 if 6
Interface 6: Ethernet: Connexion au réseau local
  Guid {7F0A41C9-F7DC-462D-9212-9EB81B88F96A}
  zones: link 6 site 2
  Firewall disabled
  uses Neighbor Discovery
  uses Router Discovery
  media reconnect flushes stale auto-configured state after 1500ms
  does not heuristically flush stale auto-configured state
  link-layer address: 00-0d-60-fa-e1-5b
    preferred global 2006:151:3:0:20d:60ff:fefa:e15b, life 2m52s/72s (public)
    preferred link-local fe80::20d:60ff:fefa:e15b, life infinite
    multicast interface-local ff01::1, 1 refs, not reportable
    multicast link-local ff02::1, 1 refs, not reportable
    multicast link-local ff02::1:fffa:e15b, 2 refs, last reporter
  link MTU 1500 (true link MTU 1500)
  current hop limit 64
  reachable time 43500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 1
```

Node1 : HoA home Link address

```
F:\Documents and Settings\fefe>ipv6 if 4
Interface 4: MIPv6 Pseudo-Interface
  Guid {BADE68B3-9FC9-5E9E-6285-D4F8E3E476DD}
  zones: link 4 site 3
  Firewall disabled
  does not use Neighbor Discovery
  does not use Router Discovery
  media reconnect flushes stale auto-configured state after 1500ms
  does not heuristically flush stale auto-configured state
    preferred global 2006:1::20d:60ff:fefa:e15b, life infinite (manual)
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 43000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
```

Node2 – IPv6 CoA Address

```
C:\JMB>ipv6 if 5
Interface 5: Ethernet: Connexion au reseau local
  Guid {CCBD611D-5624-4FB2-8496-EE8B99CE7B38}
  Firewall disabled
  uses Neighbor Discovery
  uses Router Discovery
  media reconnect flushes stale auto-configured state after 1500ms
  does not heuristically flush stale auto-configured state
  link-layer address: 00-0c-29-b9-8d-7c
    preferred global 2006:151:2:0:20c:29ff:feb9:8d7c, life 4m49s/89s (public)
    preferred link-local fe80::20c:29ff:feb9:8d7c, life infinite
    multicast interface-local ff01::1, 1 refs, not reportable
    multicast link-local ff02::1, 1 refs, not reportable
    multicast link-local ff02::1:ffb9:8d7c, 2 refs, last reporter
  link MTU 1500 (true link MTU 1500)
  current hop limit 64
  reachable time 16500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 1

C:\JMB>
```

Node2 – MIPv6 IPSec is ON by default

```
C:\JMB>ipv6 hau 2006:1::20c:29ff:feb9:8d7c 2006:1::7
Home address update error: 57
Note: Check that host is in mobile mode (ipv6 gpu MobilityMode [ MN | MN CN ]).
Note: SPI must indicate valid inbound ESP tunnel SPI used by HA for tunnelling to
MN.
Note: SPD must indicate valid IPSec SPD entry on MN for ESP tunnel from HA.

C:\JMB>
```

Disabling IPv6 IPSec

- Microsoft has provided a means of disabling the use of IPSec in the stack via the MIPv6Security global parameter.
- If security is disabled by the command:
  - ipv6 gpu MIPv6Security off
- Then no authentication is performed on home bindings, and (reverse) tunnelling is done without IPSec leaving the Return Routability protocol is vulnerable to monitoring on a mobile node's foreign network

Node2 – Disabling MIPv6 IPSec

```
C:\JMB>ipv6 gpu MIPv6Security off

C:\JMB>ipv6 gp
DefaultCurHopLimit = 128
UseAnonymousAddresses = no
MaxAnonDADAttempts = 5
MaxAnonLifetime = 7d/24h
AnonRegenerateTime = 5s
MaxAnonRandomTime = 10m
AnonRandomTime = 2m47s
NeighborCacheLimit = 256
RouteCacheLimit = 32
BindingCacheLimit = 32
ReassemblyLimit = 1568640
MIPv6Security = off
MIPv6Mode = MN CN
MIPv6RouteOptimize = yes
MIPv6KcnInterval = 30s
MIPv6KcnGenerations = 8
MIPv6HomeBindingLife = 60s
MIPv6RRBindingLife = 30s
MIPv6ErrorTimeout = 5s
MIPv6HomeAgentPreference = 1
MIPv6SendMobilePrefixAdvertisements = yes
MIPv6InitialBindackTimeoutFirstReg = 1500ms

C:\JMB>
```

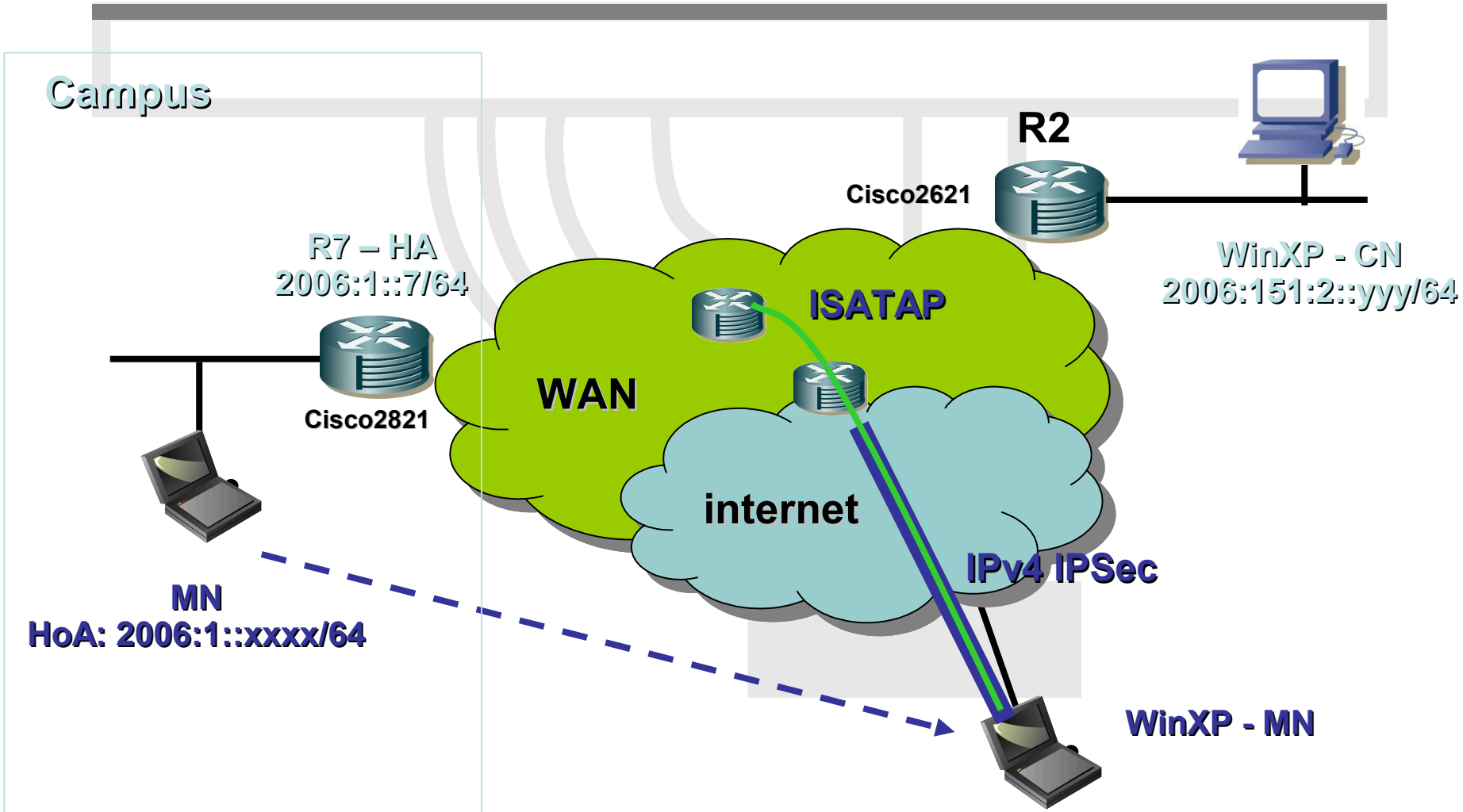
Node2 – HA Manual Configuration

```
C:\JMB>ipv6 hau 2006:1::20c:29ff:feb9:8d7c 2006:1::7
Note: Due to MIPv6 dependency on IPSec for
ESP tunnelling both IPSec and MIPv6 Home
Addresses must be reconfigured, in that order,
after every reboot.

C:\Documents and Settings\JMB>

C:\JMB>ipv6 ha
Home Address: 2006:1::20c:29ff:feb9:8d7c
  Home Agent: 2006:1::7
  ESPTunnelSPI: 0
  ESPTunnelSPD: 0


C:\JMB>
```

Node2 – Binding Updates

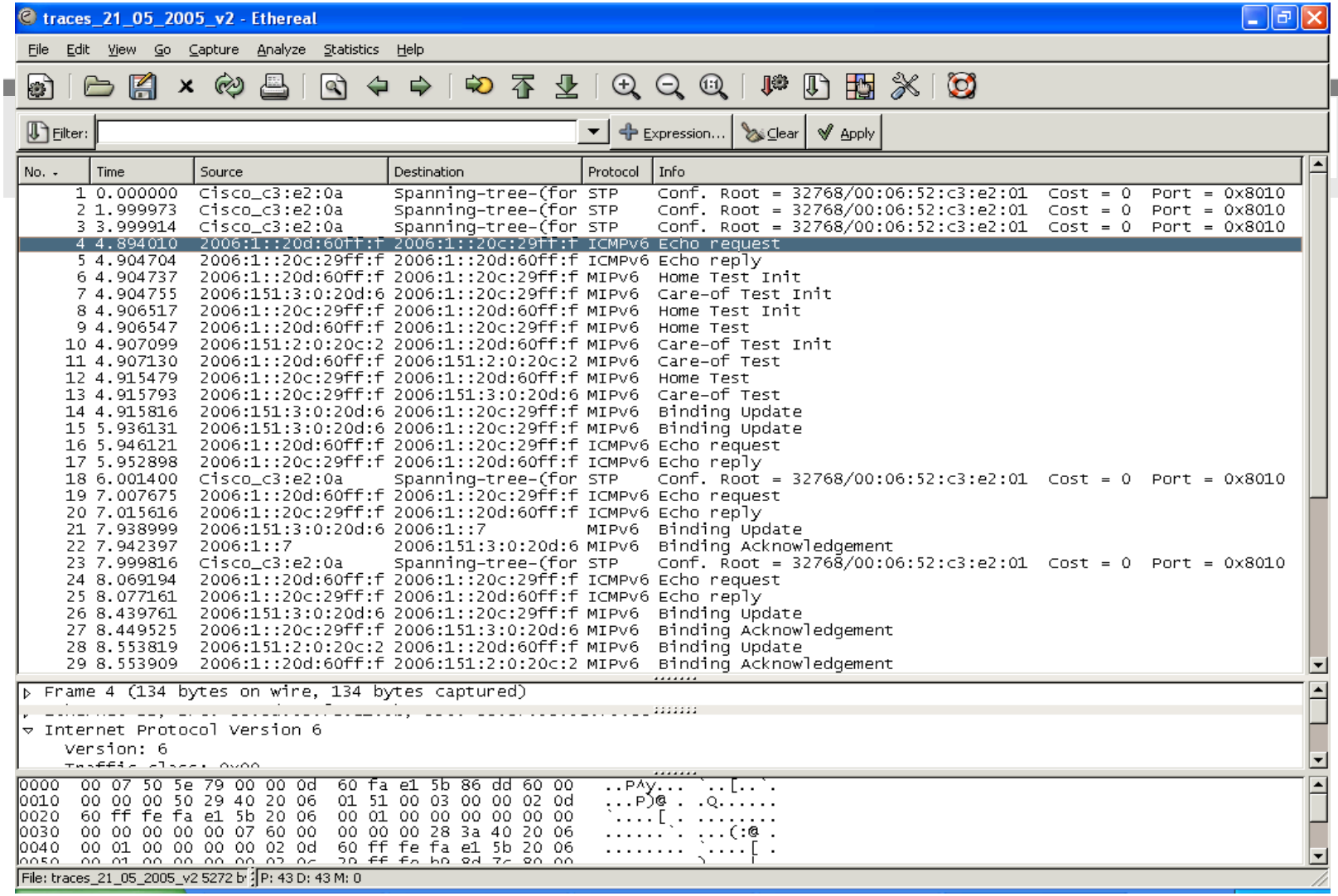
```
C:\>ipv6 bu
Home Address: 2006:1::20c:29ff:feb9:8d7c
  Host: 2006:1::20d:60ff:fefa:e15b
    CoA       : 5/2006:151:2:0:20c:29ff:feb9:8d7c
    Expires   : 3s
    RRState   : ACTIVE
    TunnelBypassIndex: 2

  Host: 2006:1::7
    CoA       : 5/2006:151:2:0:20c:29ff:feb9:8d7c
    Expires   : 57s
    Comments  : HOME_AGENT
    RRState   : NO_RR ACTIVE
C:\>
```

Topology – Internet Access

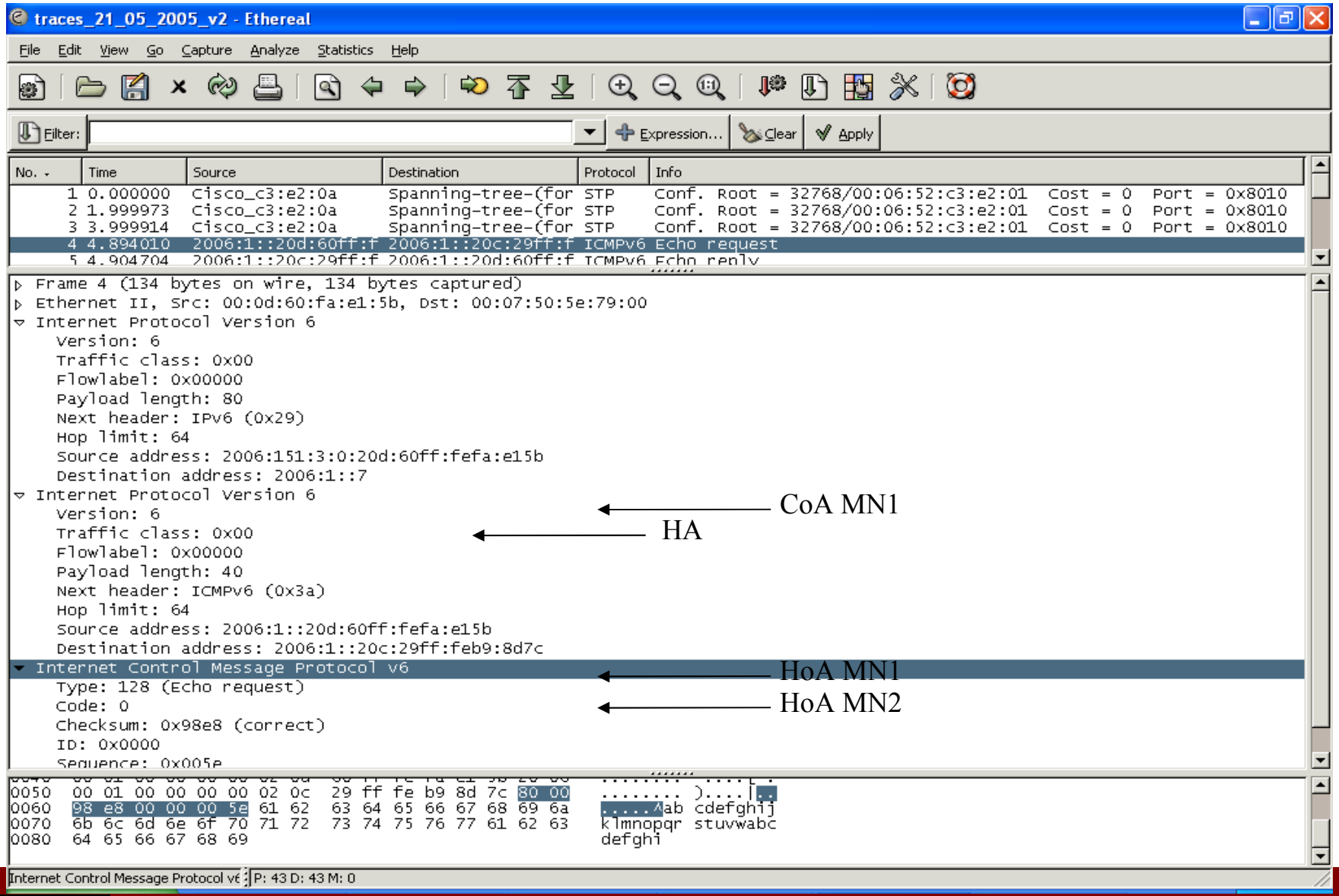


Mobile IPv6 Testbed Ethereal Traces

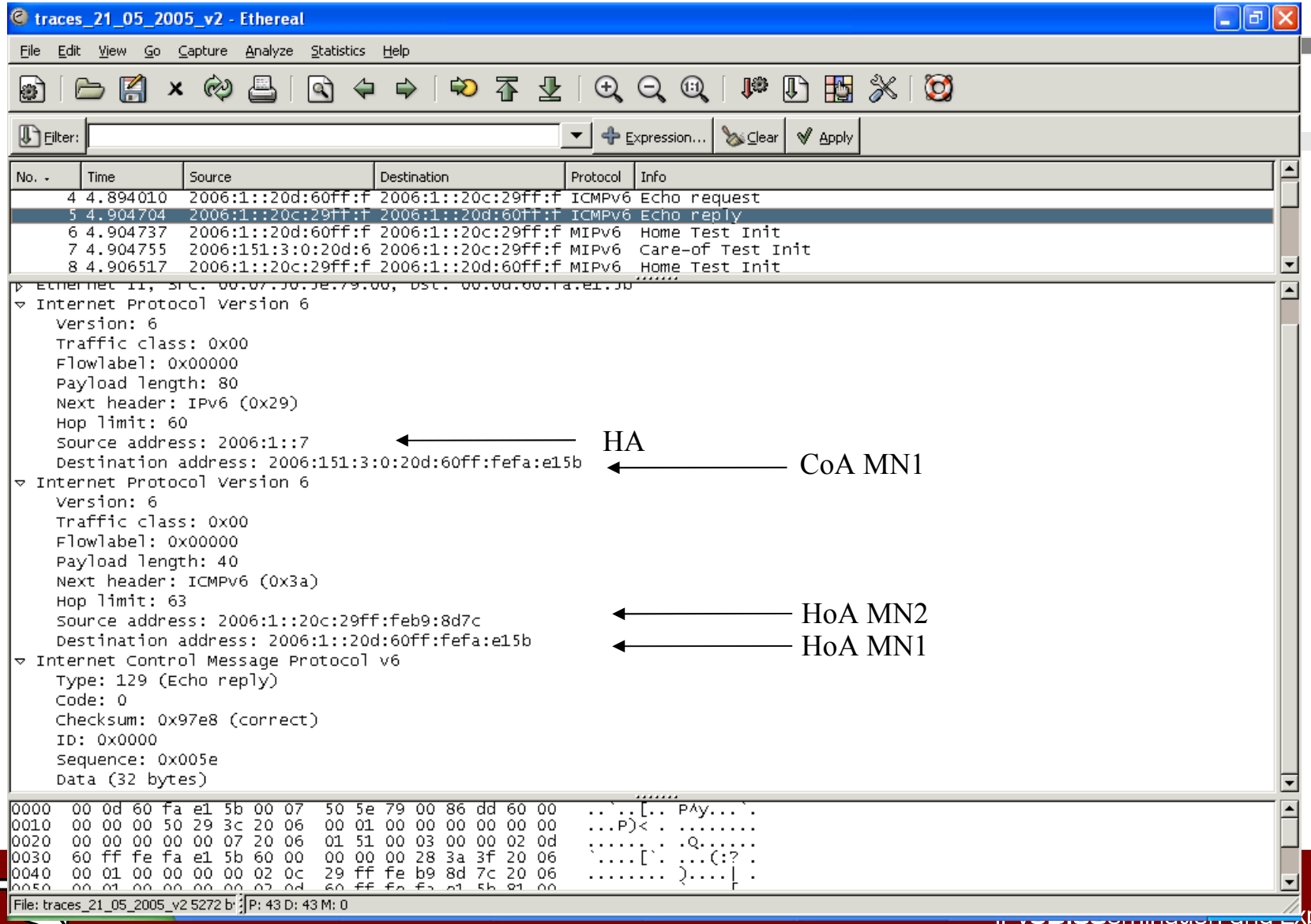
Traces after successful pings between MN1 & MN2



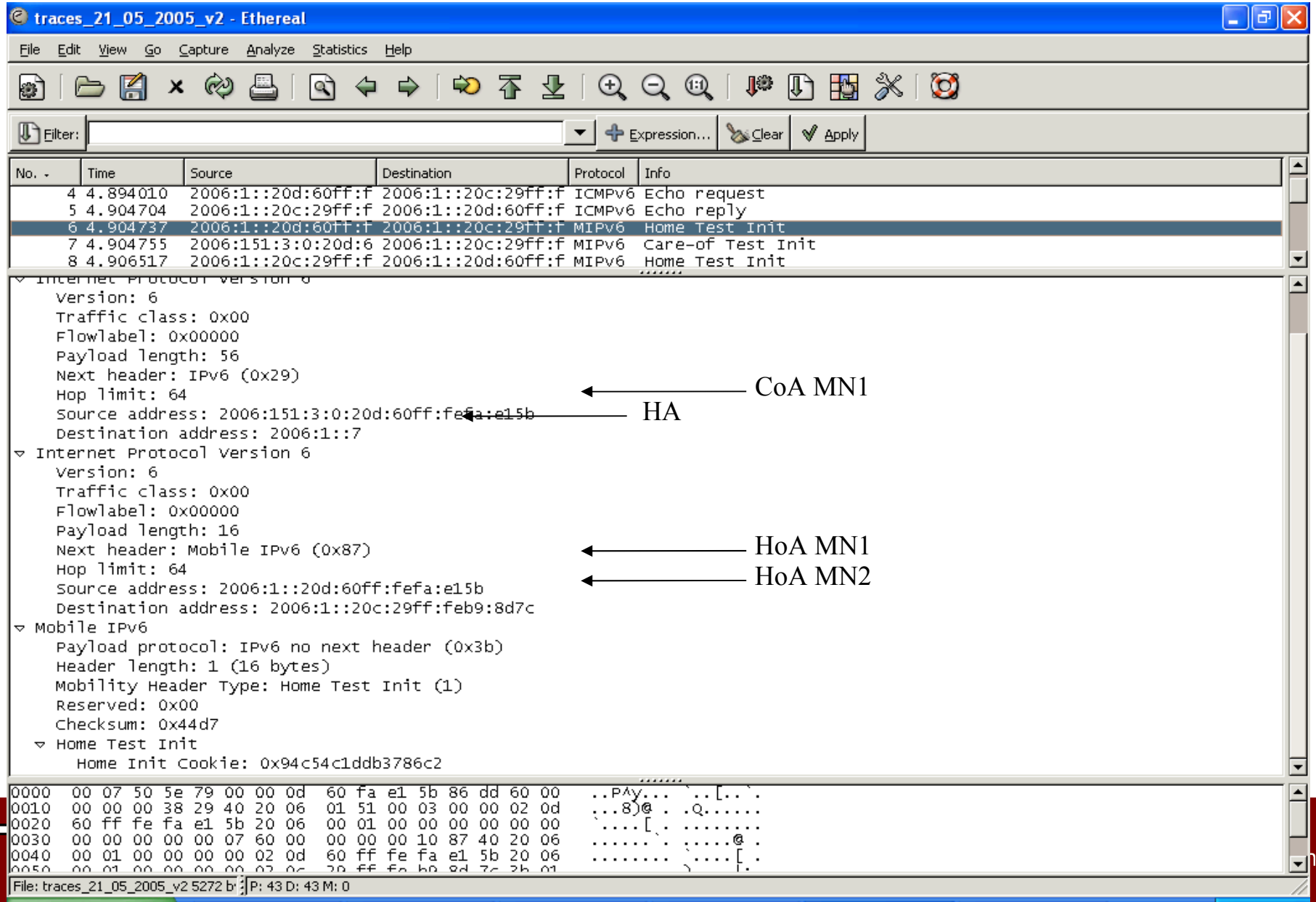
Ping without direct routing IPv6 tunnelised in IPv6)



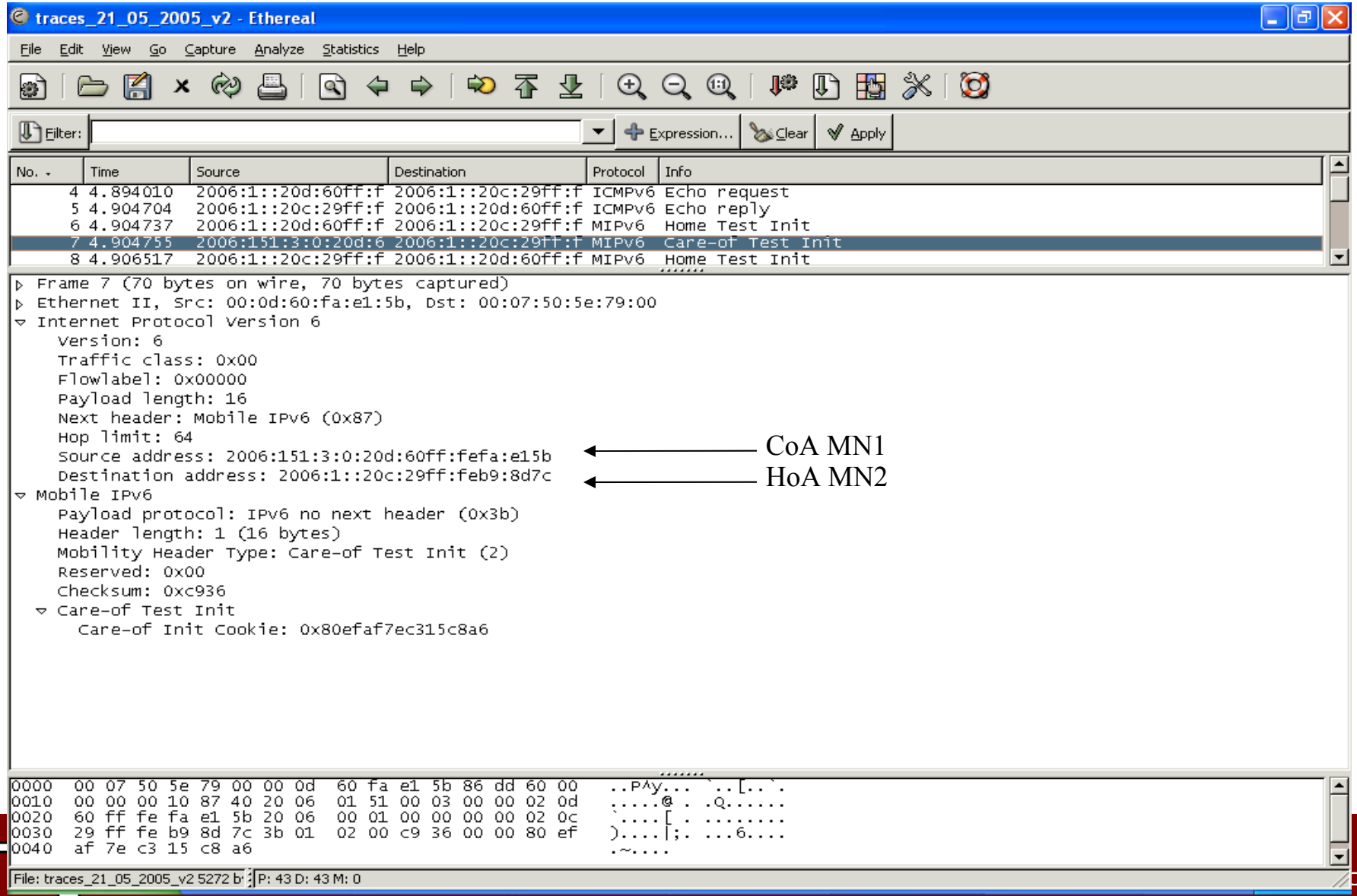
Echo reply w/o DR



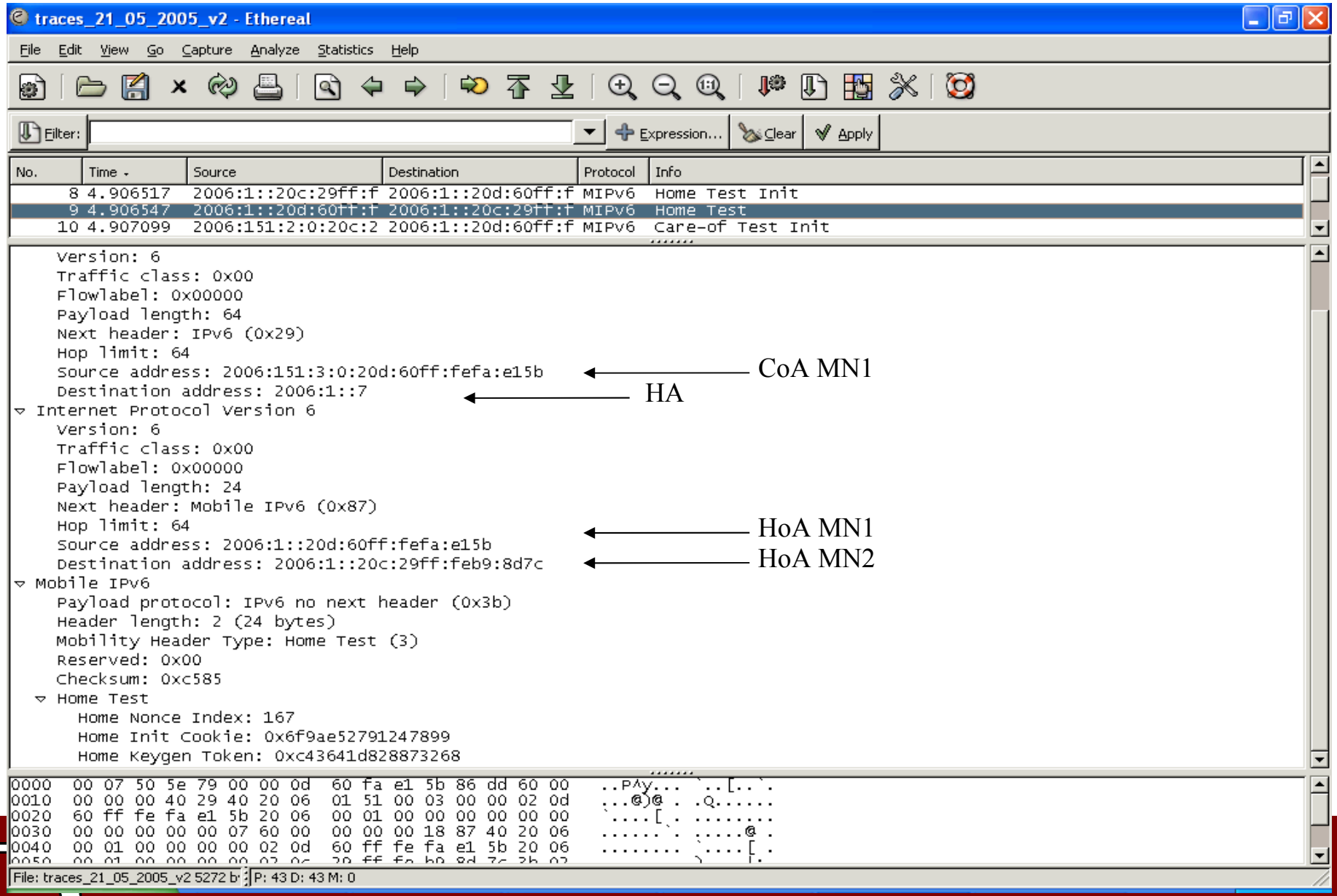
Home test init



Care-of test init



Home test



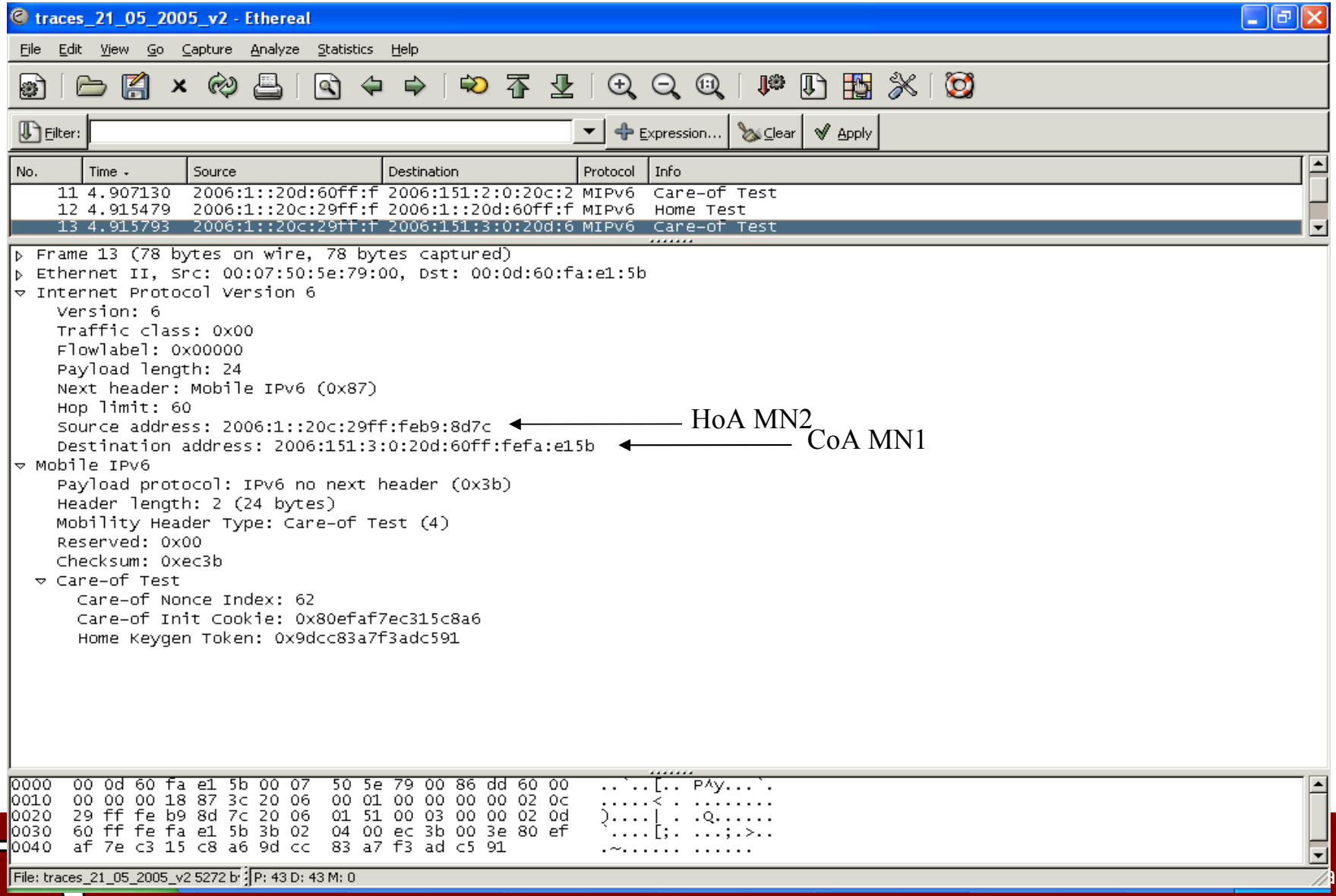
CoA MN1

HA

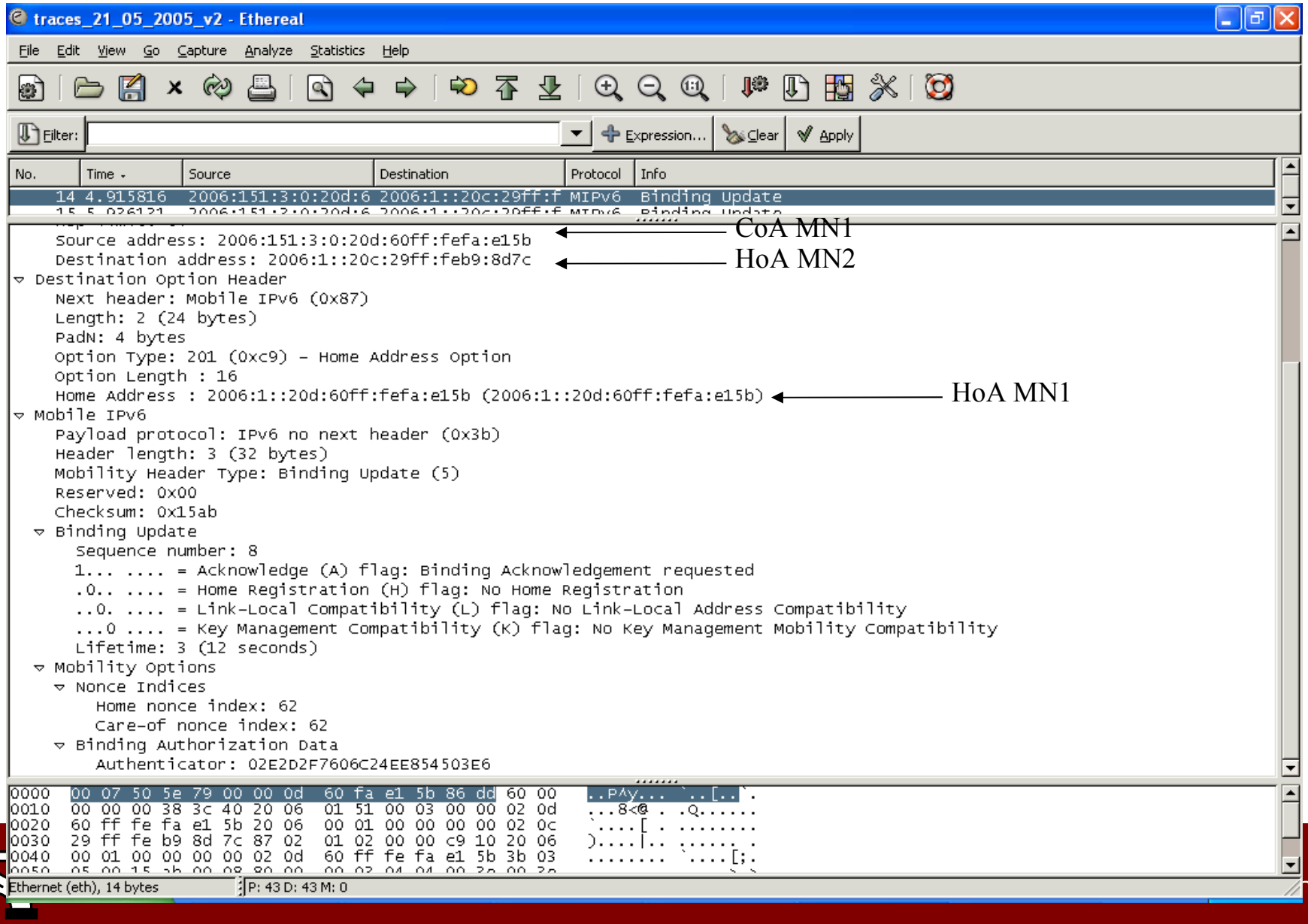
HoA MN1

HoA MN2

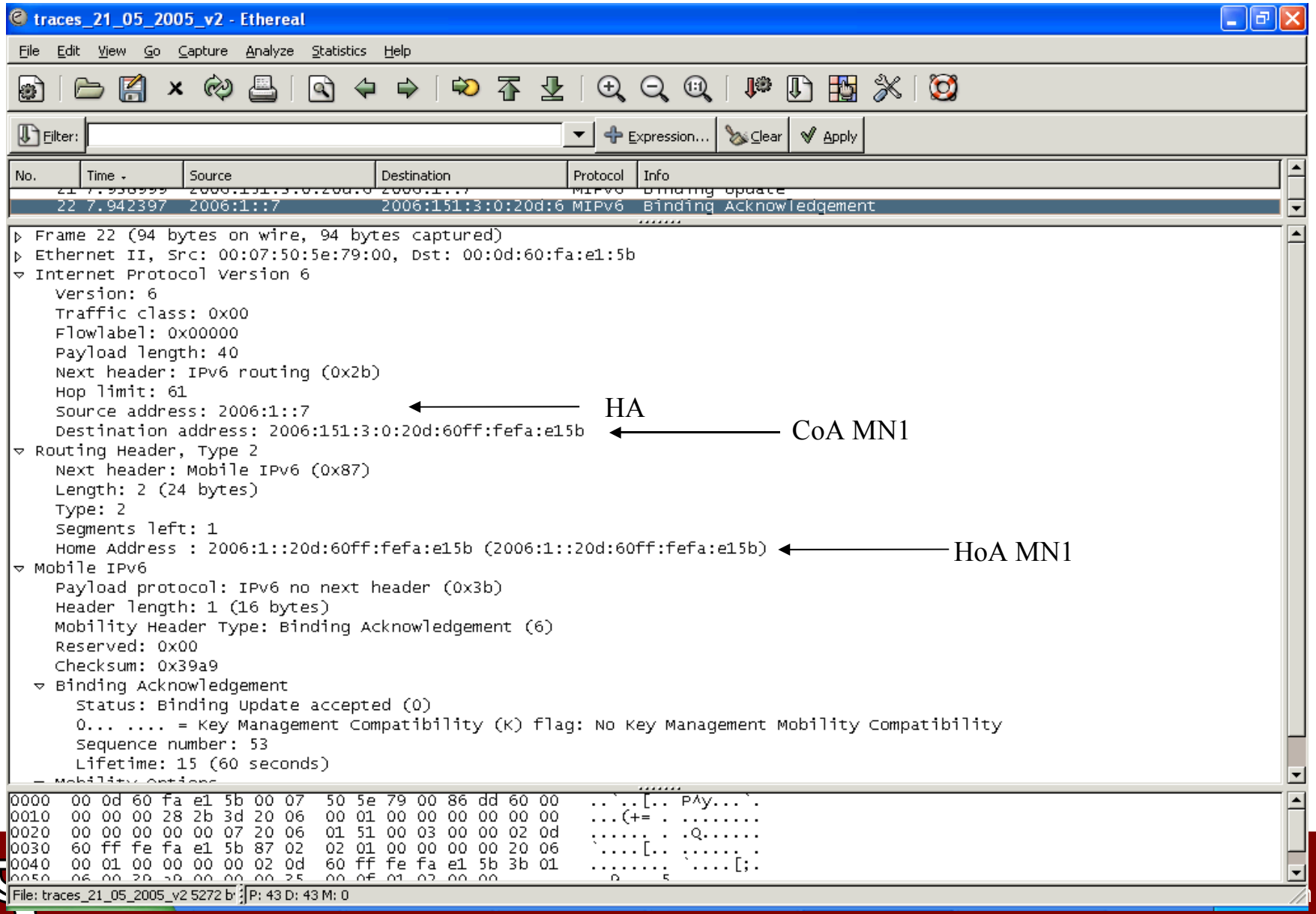
Care-of test


traces_21_05_2005_v2 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
11 4.907130 2006:1::20d:60ff:f 2006:151:2:0:20c:2 MIPv6 Care-of Test
12 4.915479 2006:1::20c:29ff:f 2006:1::20d:60ff:f MIPv6 Home Test
13 4.915793 2006:1::20c:29ff:f 2006:151:3:0:20d:6 MIPv6 Care-of Test
Frame 13 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: 00:07:50:5e:79:00, Dst: 00:0d:60:fa:e1:5b
Internet Protocol Version 6
Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 24
Next header: Mobile IPv6 (0x87)
Hop limit: 60
Source address: 2006:1::20c:29ff:feb9:8d7c
Destination address: 2006:151:3:0:20d:60ff:fefa:e15b
HoA MN2
CoA MN1
Mobile IPv6
Payload protocol: IPv6 no next header (0x3b)
Header length: 2 (24 bytes)
Mobility Header Type: Care-of Test (4)
Reserved: 0x00
Checksum: 0xec3b
Care-of Test
Care-of Nonce Index: 62
Care-of Init Cookie: 0x80efaf7ec315c8a6
Home Keygen Token: 0x9dcc83a7f3adc591
0000 00 0d 60 fa e1 5b 00 07 50 5e 79 00 86 dd 60 00
0010 00 00 00 18 87 3c 20 06 00 01 00 00 00 00 02 0c
0020 29 ff fe b9 8d 7c 20 06 01 51 00 03 00 00 02 0d
0030 60 ff fe fa e1 5b 3b 02 04 00 ec 3b 00 3e 80 ef
0040 af 7e c3 15 c8 a6 9d cc 83 a7 f3 ad c5 91
File: traces_21_05_2005_v2 5272 b
P: 43 D: 43 M: 0

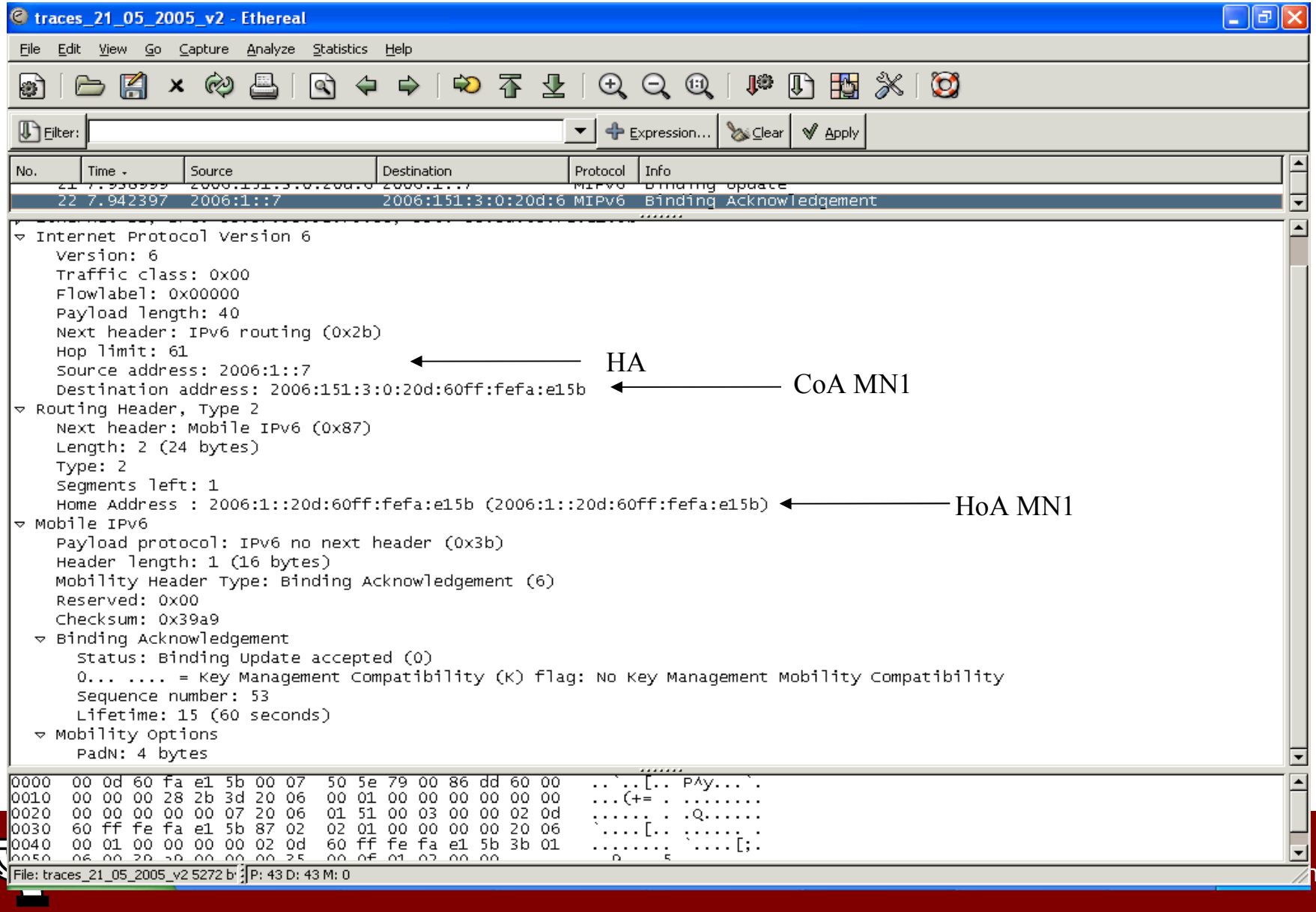
Binding update



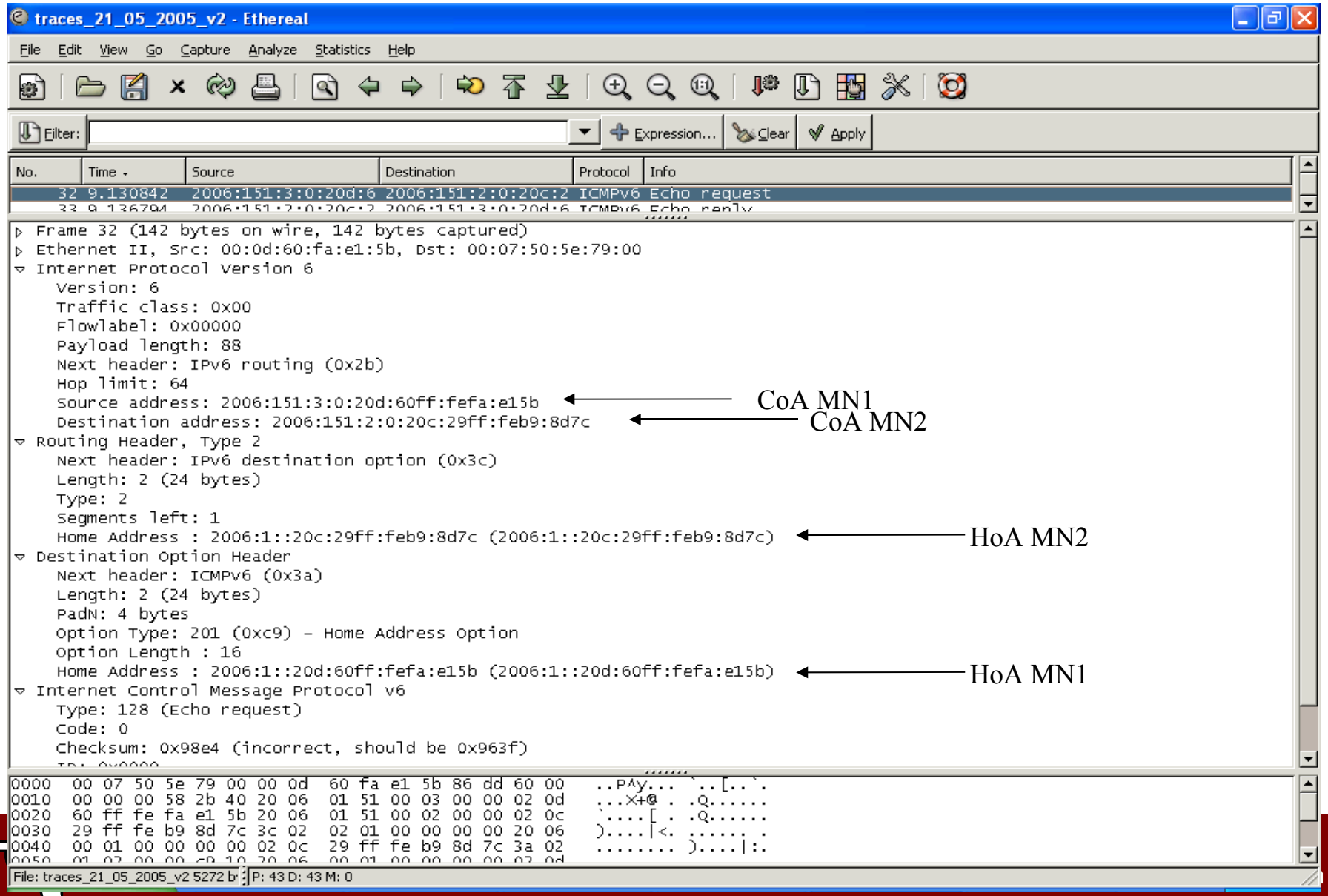
Binding acknowledgement ...



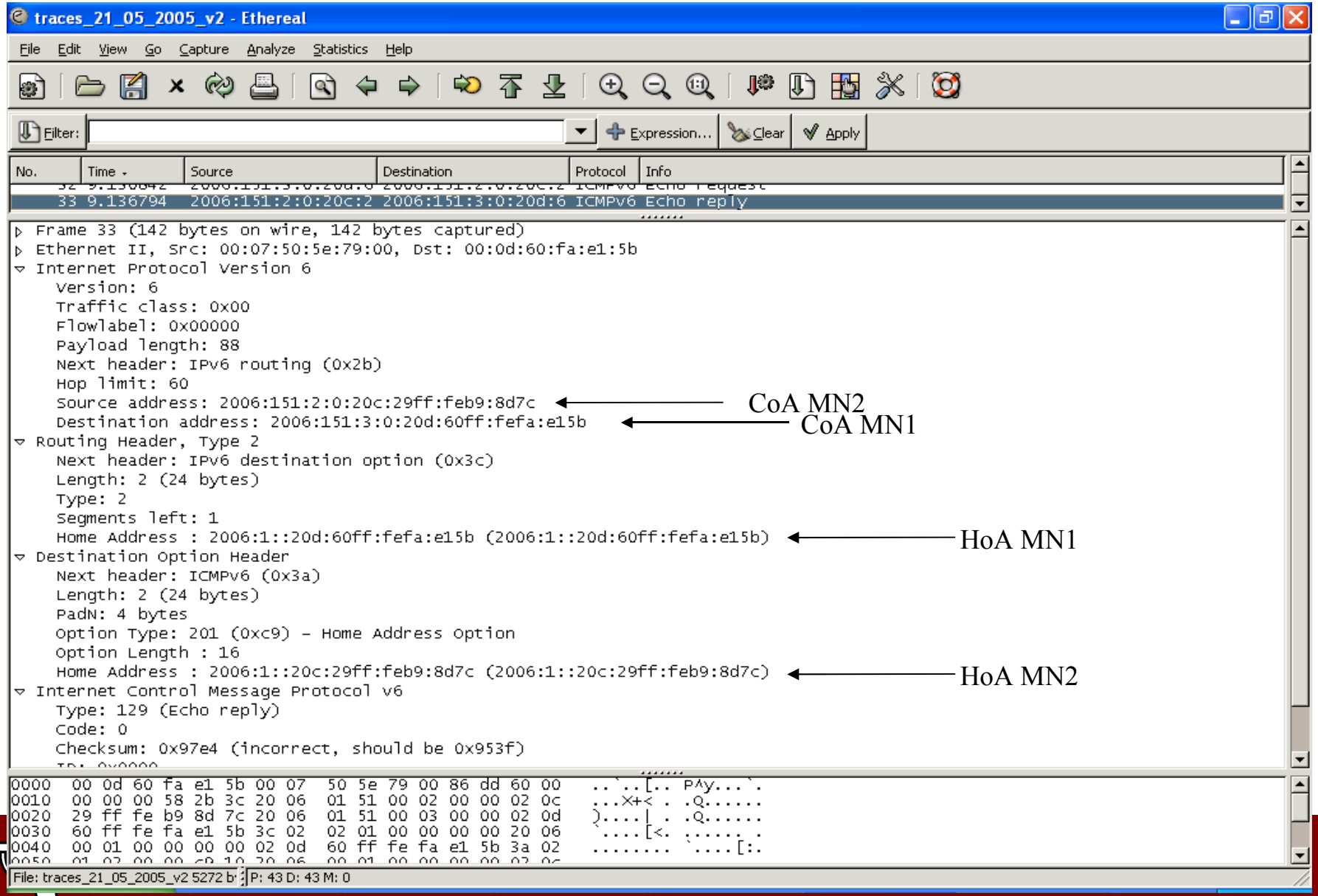
Binding acknowledgement



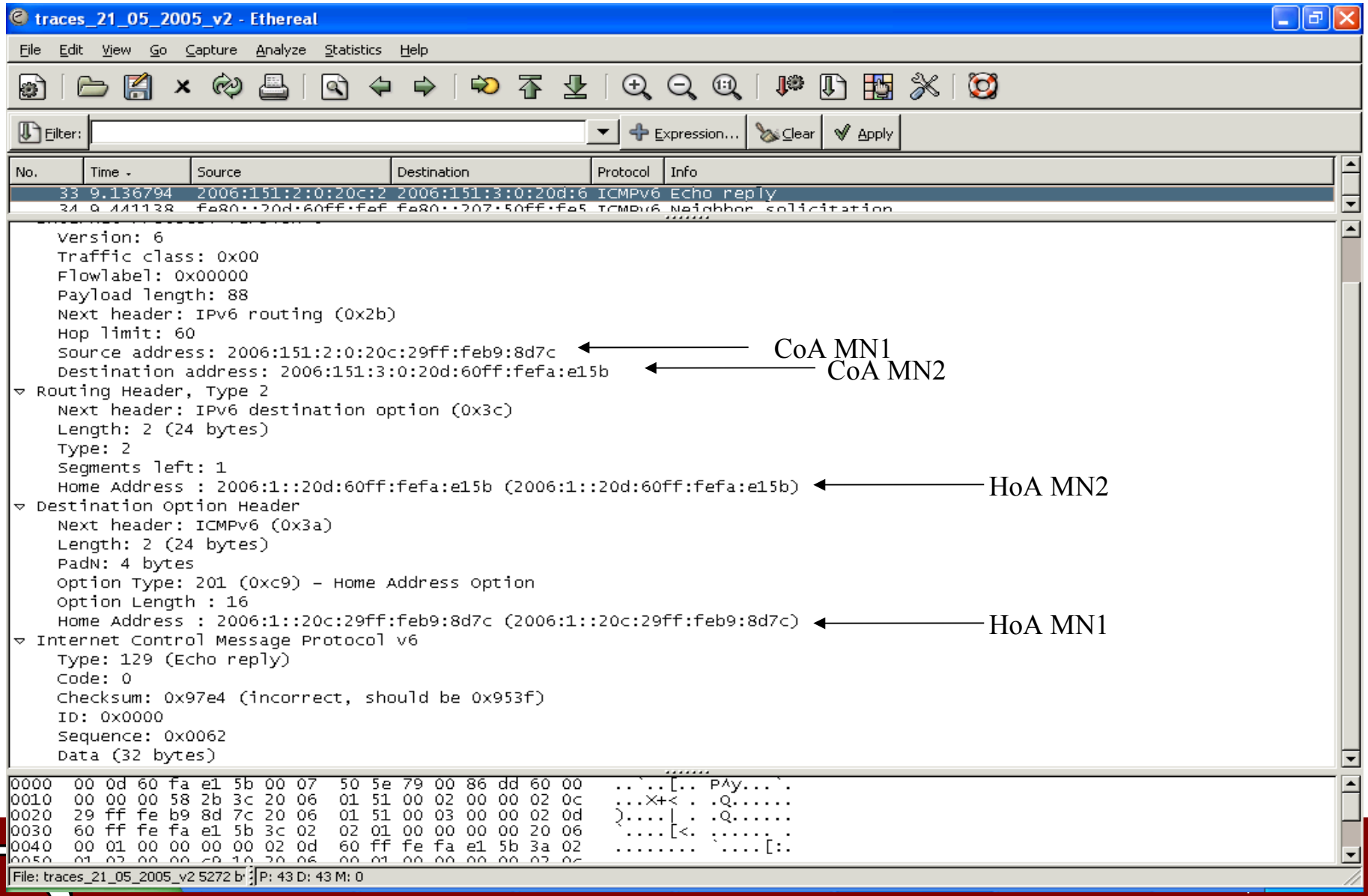
Ping with DR


traces_21_05_2005_v2 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
32 9.130842 2006:151:3:0:20d:6 2006:151:2:0:20c:2 ICMPv6 Echo request
Frame 32 (142 bytes on wire, 142 bytes captured)
Ethernet II, Src: 00:0d:60:fa:e1:5b, Dst: 00:07:50:5e:79:00
Internet Protocol Version 6
Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 88
Next header: IPv6 routing (0x2b)
Hop limit: 64
Source address: 2006:151:3:0:20d:60ff:fefa:e15b
Destination address: 2006:151:2:0:20c:29ff:feb9:8d7c
Routing Header, Type 2
Next header: IPv6 destination option (0x3c)
Length: 2 (24 bytes)
Type: 2
Segments left: 1
Home Address : 2006:1::20c:29ff:feb9:8d7c (2006:1::20c:29ff:feb9:8d7c)
Destination Option Header
Next header: ICMPv6 (0x3a)
Length: 2 (24 bytes)
PadN: 4 bytes
Option Type: 201 (0xc9) - Home Address Option
Option Length : 16
Home Address : 2006:1::20d:60ff:fefa:e15b (2006:1::20d:60ff:fefa:e15b)
Internet Control Message Protocol v6
Type: 128 (Echo request)
Code: 0
Checksum: 0x98e4 (incorrect, should be 0x963f)
0000 00 07 50 5e 79 00 00 0d 60 fa e1 5b 86 dd 60 00
0010 00 00 00 58 2b 40 20 06 01 51 00 03 00 00 02 0d
0020 60 ff fe fa e1 5b 20 06 01 51 00 02 00 00 02 0c
0030 29 ff fe b9 8d 7c 3c 02 02 01 00 00 00 00 20 06
0040 00 01 00 00 00 00 02 0c 29 ff fe b9 8d 7c 3a 02
File: traces_21_05_2005_v2 5272 b
P: 43 D: 43 M: 0
CoA MN1
CoA MN2
HoA MN2
HoA MN1

Icmp reply with DR...

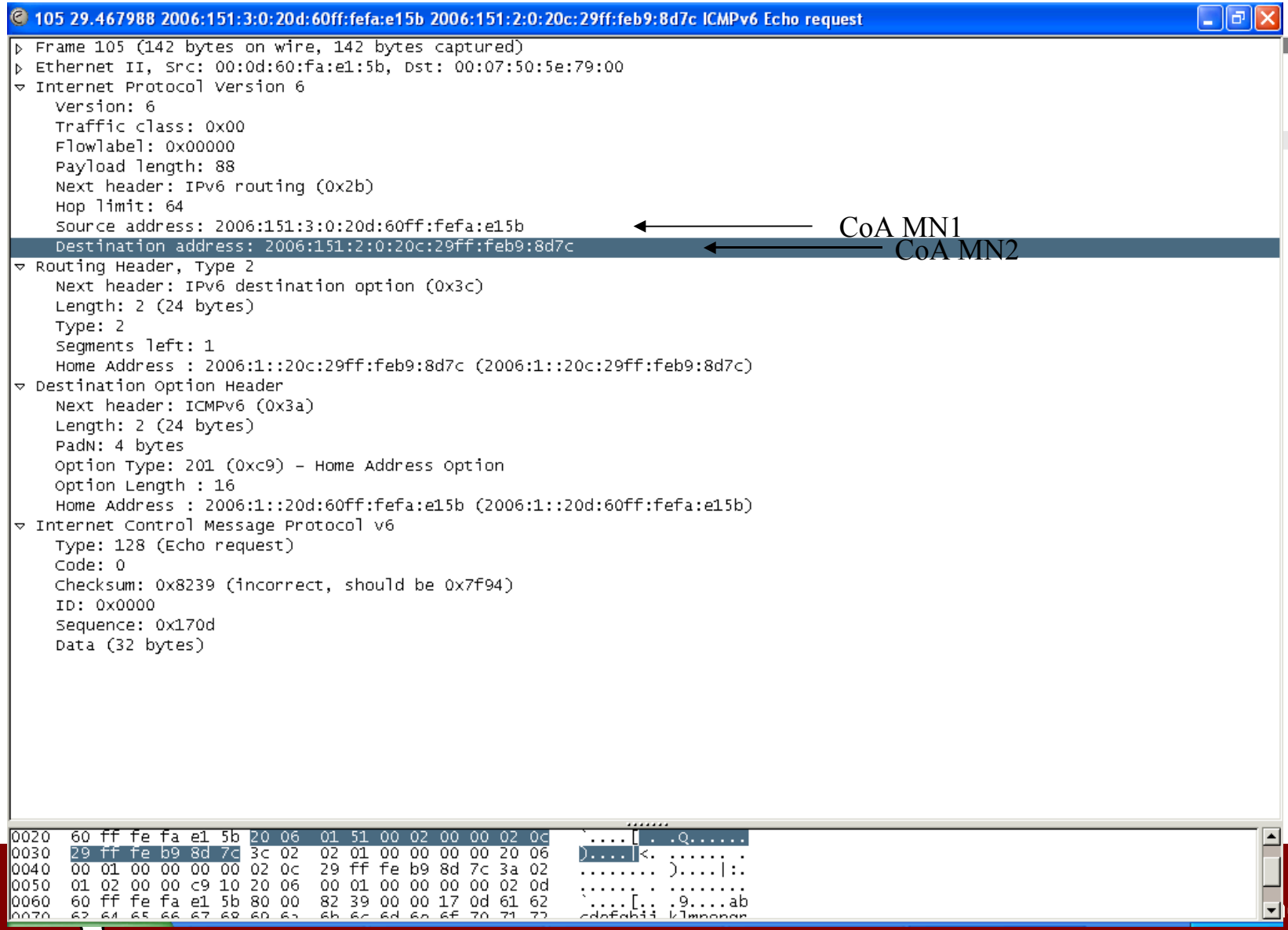


Icmp reply with DR

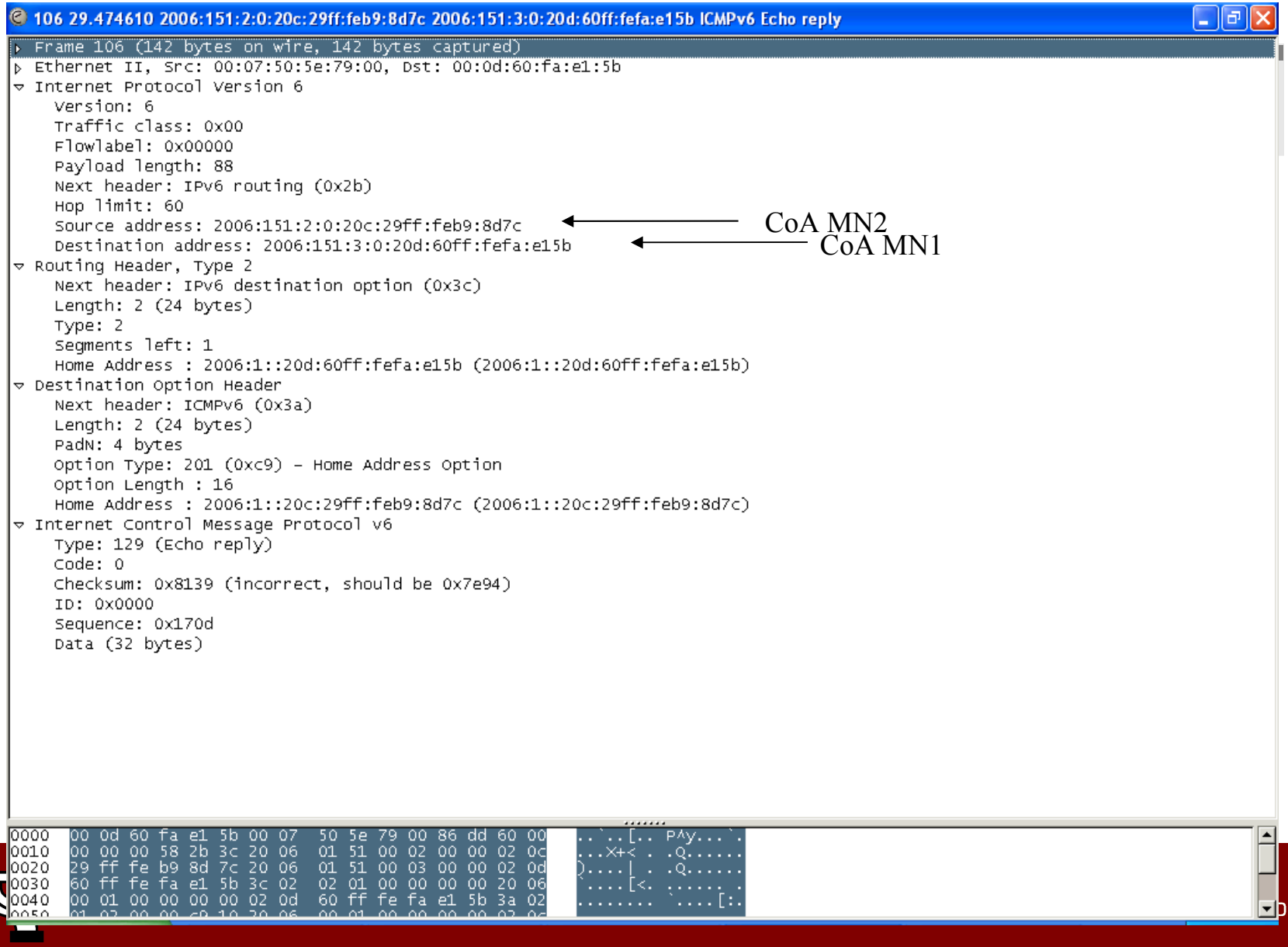


Slides for reference only

Direct routing

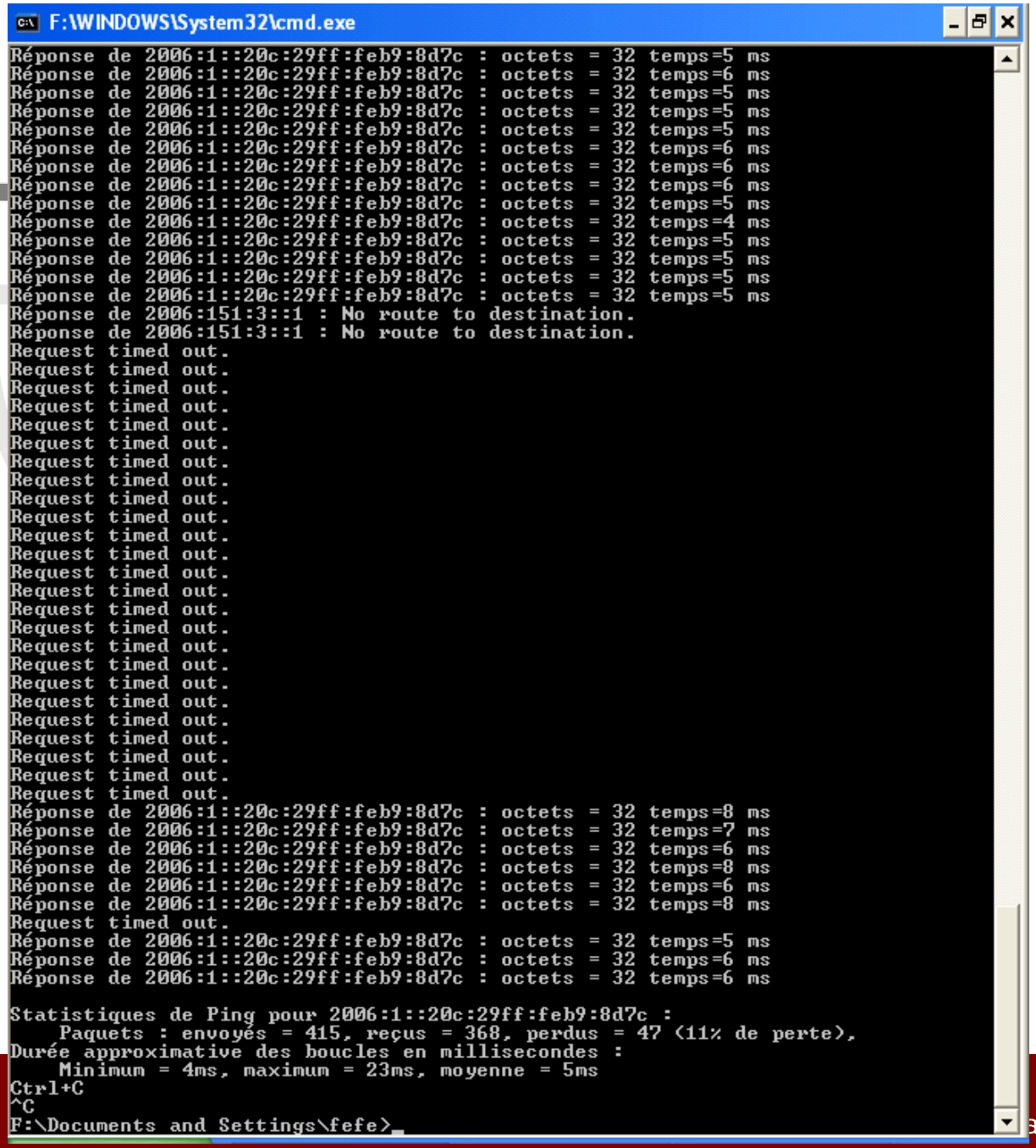


Direct routing



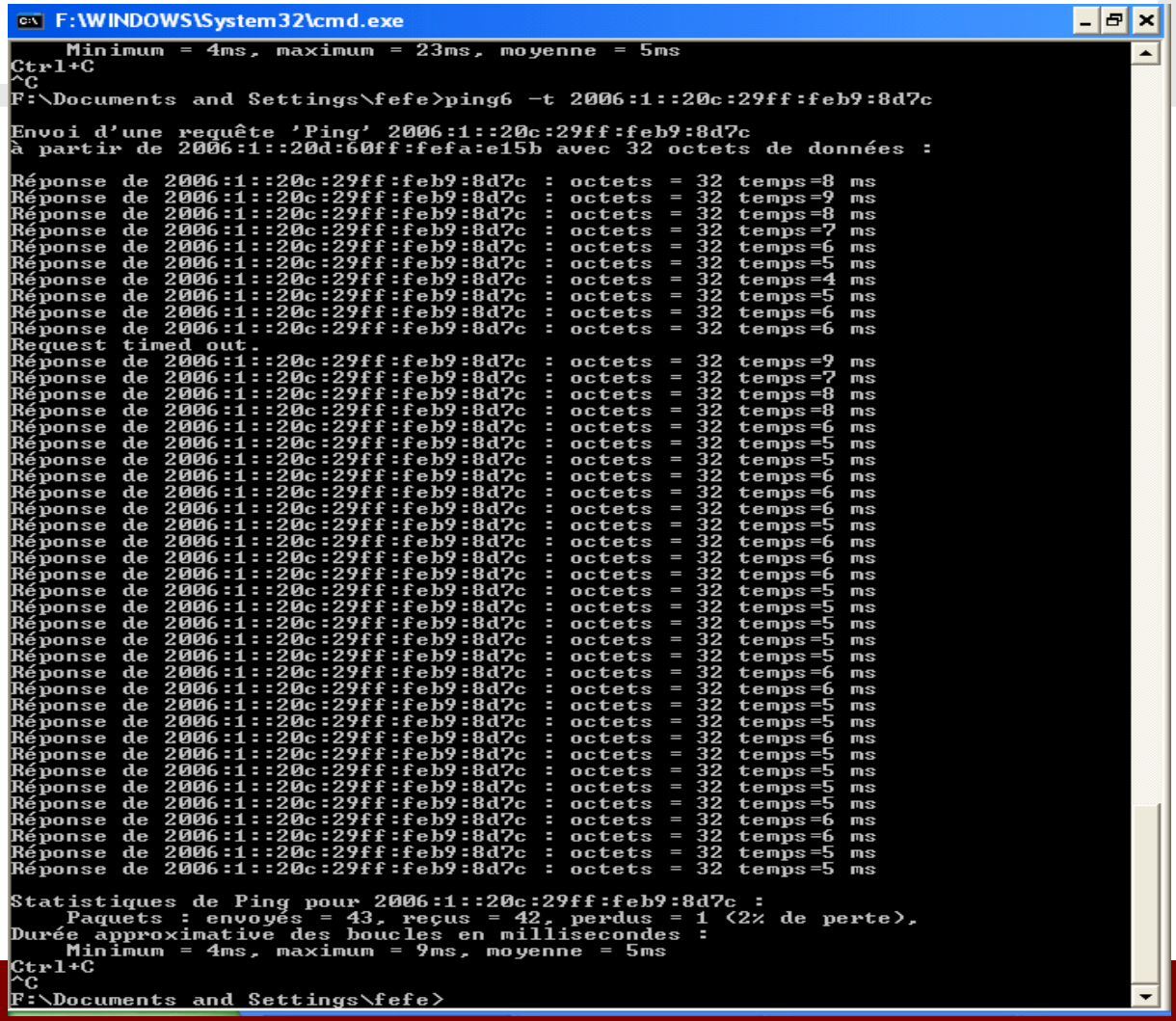
Power off HA →

Power on HA →



After applying ACL concerning both CoA MN in the HA interface

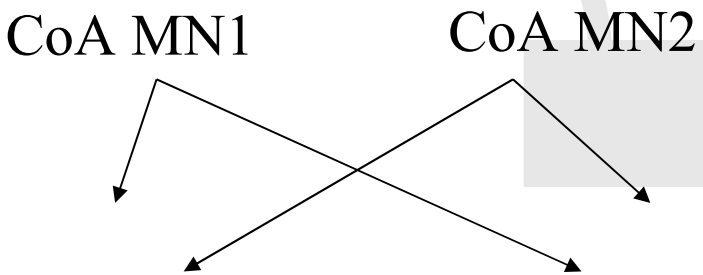
Directing routing allow MN1 to ping MN2 even if HA is not cross



HA with ACL

onfiguration Sample :

```
!
interface GigabitEthernet0/1
 description ==== Vers le WAN ===
 ip address 10.151.17.7 255.255.255.0
 ip nbar protocol-discovery
 duplex auto
 speed auto
 ipv6 address 2006:151:17::7/64
 ipv6 traffic-filter MIP in
 ipv6 ospf 200 area 0
!
[snip]
!
ipv6 access-list MIP
 deny ipv6 host 2006:151:3:0:20D:60FF:FEFA:E15B host 2006:151:2:0:20C:29FF:FEB9:8D7C
 deny ipv6 host 2006:151:2:0:20C:29FF:FEB9:8D7C host 2006:151:3:0:20D:60FF:FEFA:E15B
 permit ipv6 any any
!
```



HA with ACL

```
R7#sh access-list
IPv6 access list MIP
    deny ipv6 host 2006:151:3:0:20D:60FF:FEFA:E15B host 2006:151:2:0:20C:29FF:FEB9:8D7C
      sequence 10
    deny ipv6 host 2006:151:2:0:20C:29FF:FEB9:8D7C host 2006:151:3:0:20D:60FF:FEFA:E15B
      sequence 20
    permit ipv6 any any (162 matches) sequence 30
R7#
R7#
```