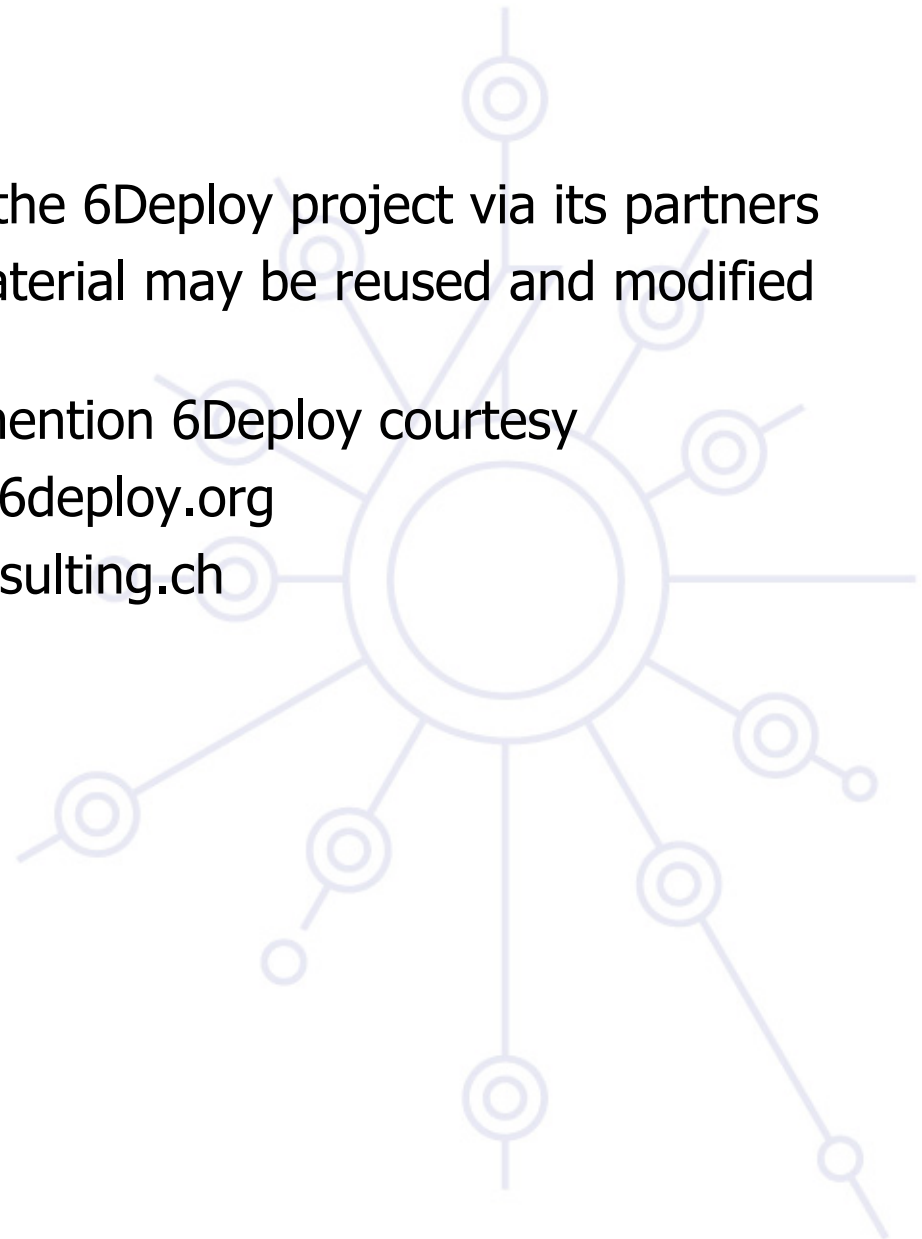


deploy

Mobile IPv6

## Copy ... Rights

- This slide set is the ownership of the 6Deploy 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 6Deploy courtesy
- PDF files are available from [www.6deploy.org](http://www.6deploy.org)
- Mail to : [martin.potts@martel-consulting.ch](mailto:martin.potts@martel-consulting.ch)



# Contributions original slides

- Main authors
  - Jean-Marc Barozet, Cisco, France
  - Faycal Hadj, Cisco, France
  - Patrick Grossetete, Arch Rock, 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



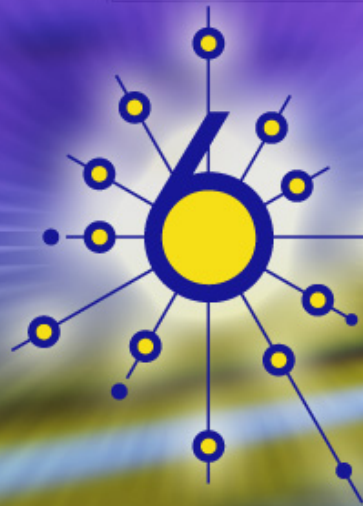


## Contributions 6Deploy Version

- Main authors:
  - Bert Habraken, Cisco, Netherlands







deploy

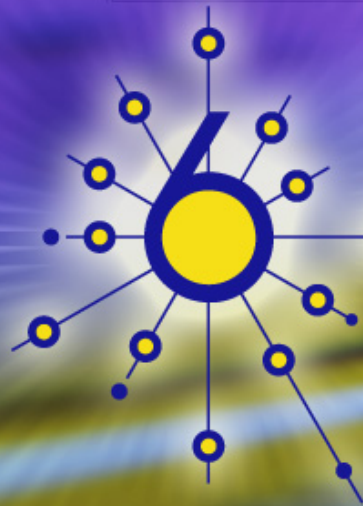
Agenda

IPv6 Mobility Module

## Agenda

- IPv6 Mobility
- Mobile IPv6 Security Overview





deploy

IPv6 Mobility

IPv6 Mobility Module



## Mobility Overview

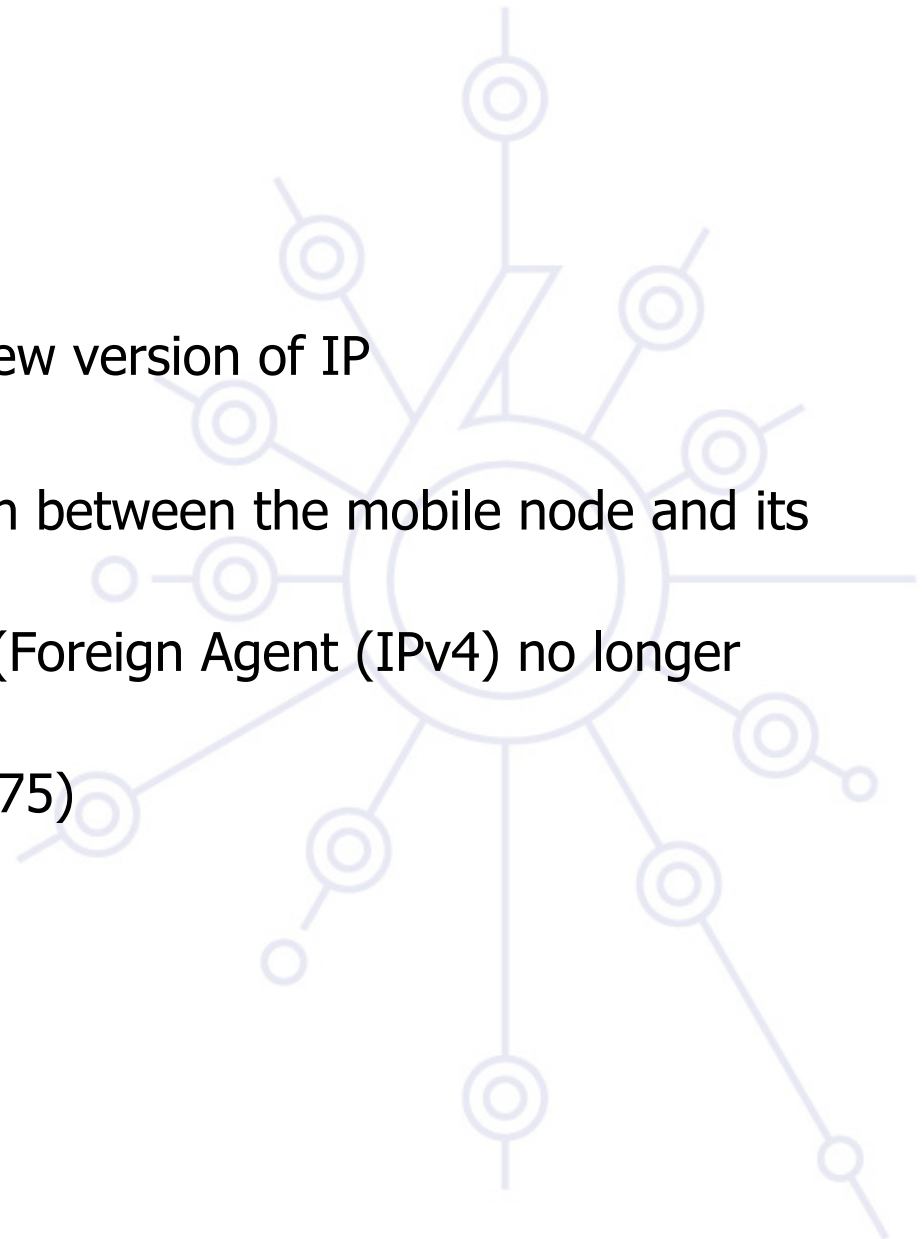
- Mobility is much wider than “nomadism”
- Keep the same IP address regardless of the network the equipment is connected to:
  - reachability
  - configuration
  - real mobility
- Difficult to optimize with Mobile IPv4 (RFC 3344 PS)
- Use facility of IPv6: MIPv6 (RFC 6275 (Original RFC3775))
- Network Mobility (NEMO) Basic Support Protocol: RFC3963



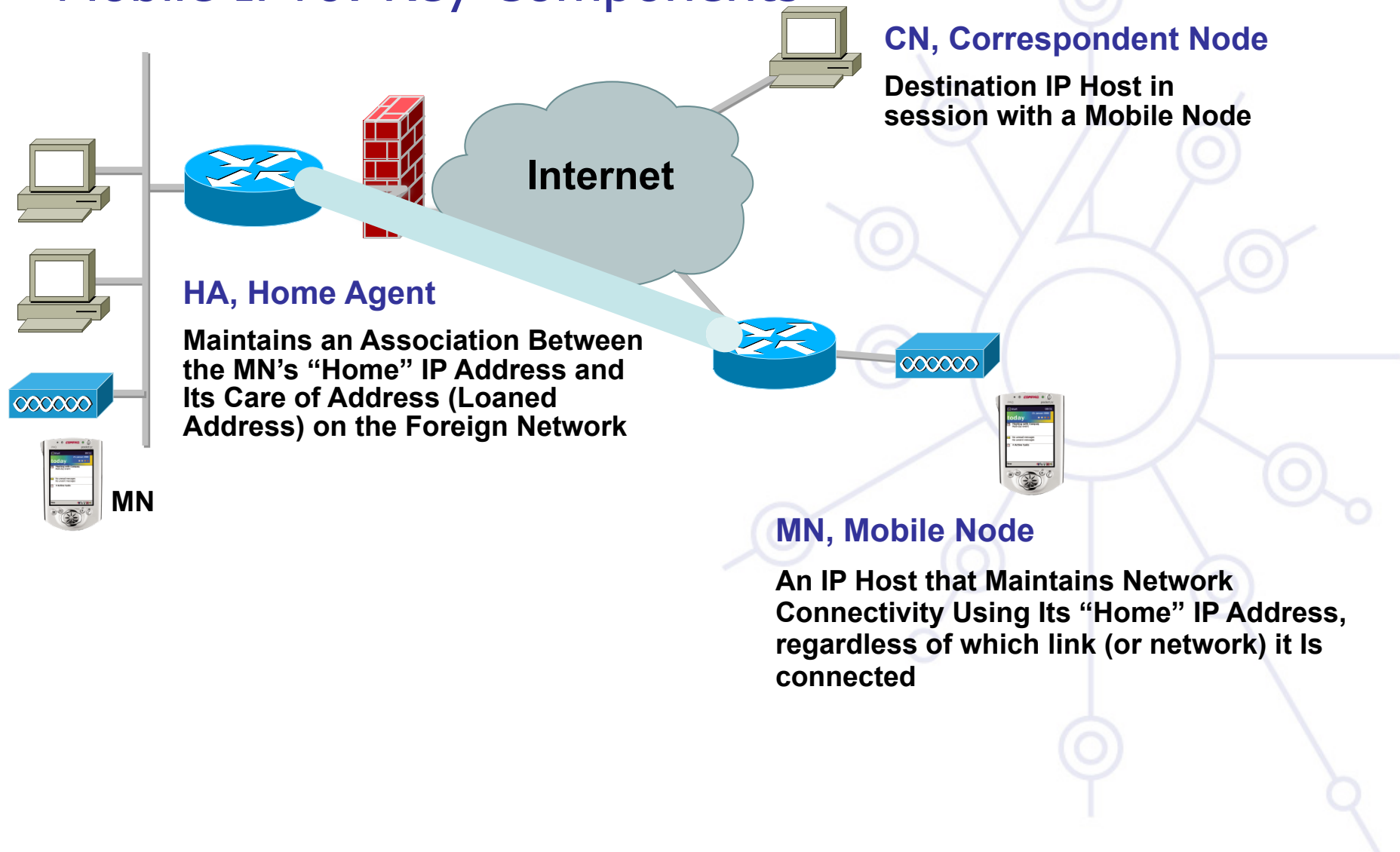


## IPv6 Mobility (MIPv6)

- 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 6275 (Original RFC3775)



# Mobile IPv6: Key Components





## General Considerations

- A globally unique IPv6 address is assigned to each Mobile Node (MN): Home Address
  - This address enables identification of the MN 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
  - MN sends Binding Update (BU) to Home Agent and any CNs

## 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

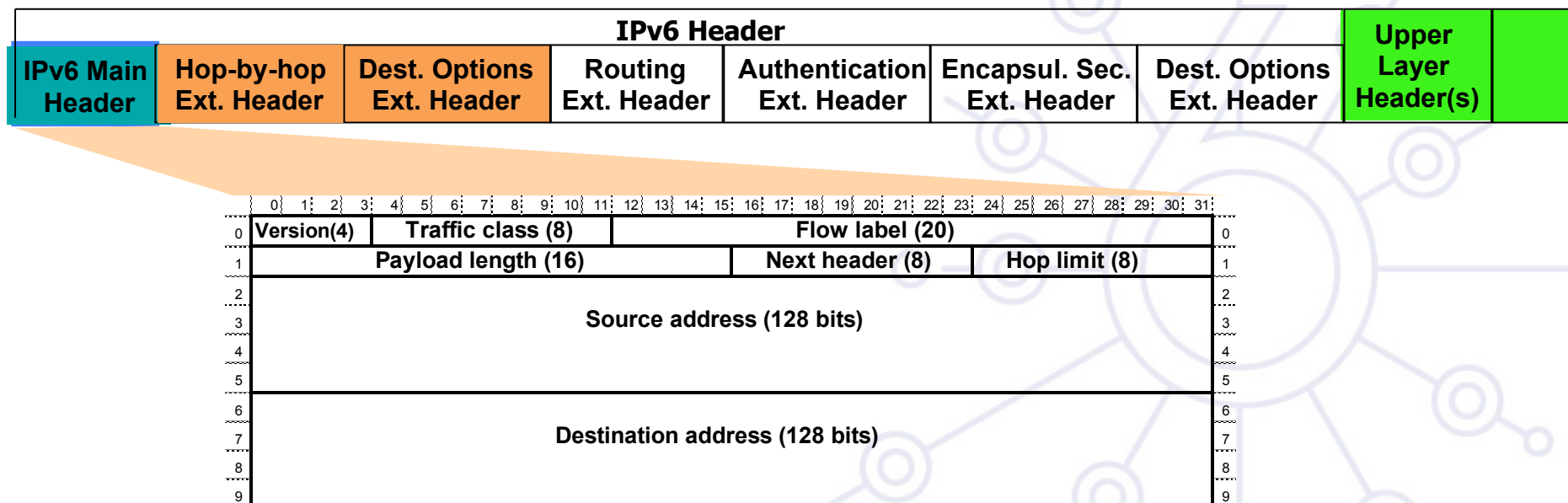
## Main features/requirements of MIPv6

- Correspondent Nodes (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
  - Use Generic IPv6 tunneling (RFC2473)
    - Tunnel (IPv6 encapsulation) those packets directly to the MN
    - Do reverse tunneling (MN → CN)



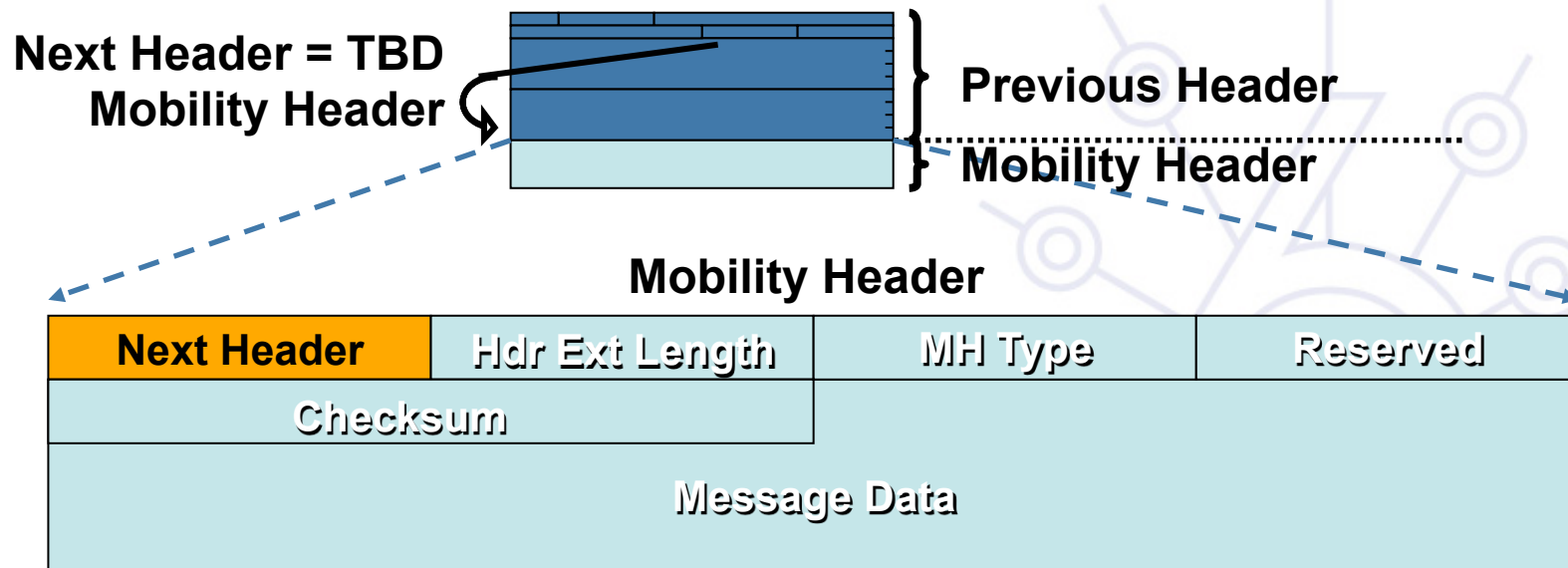
# Mobile IPv6 – a native extension of IPv6

## Un-fragmented Packet Example:



- Utilise 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

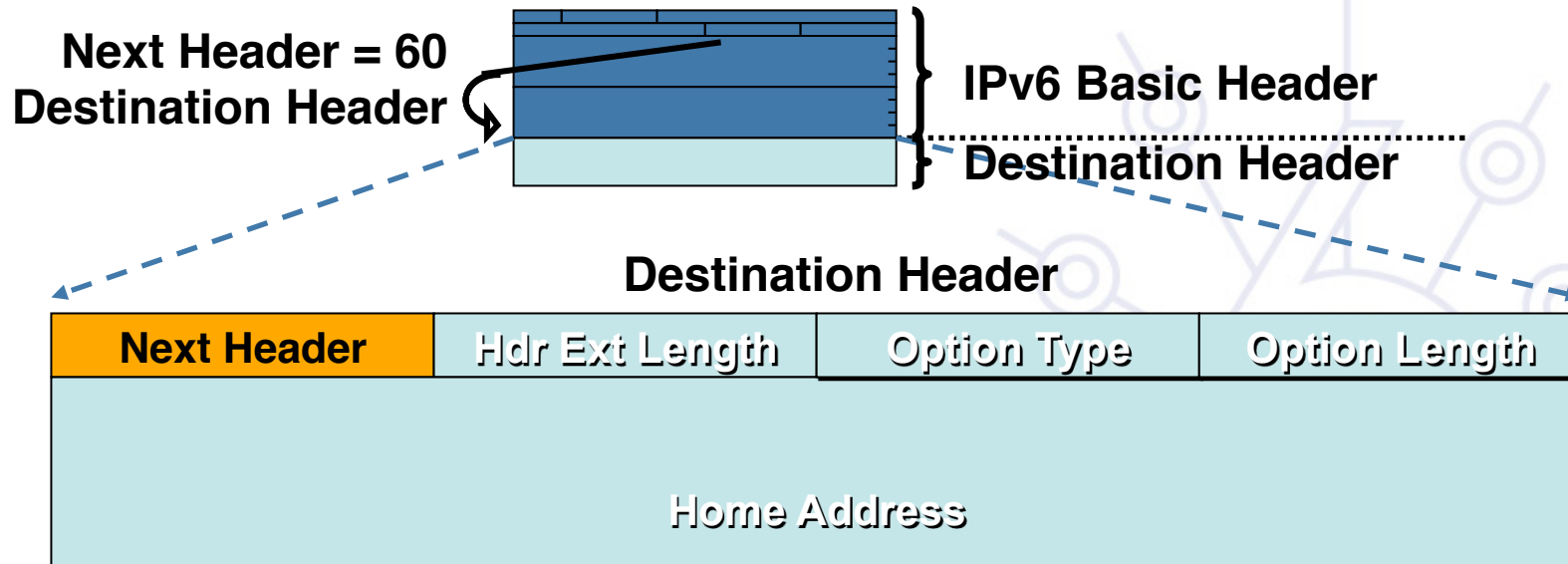




## Mobility Header

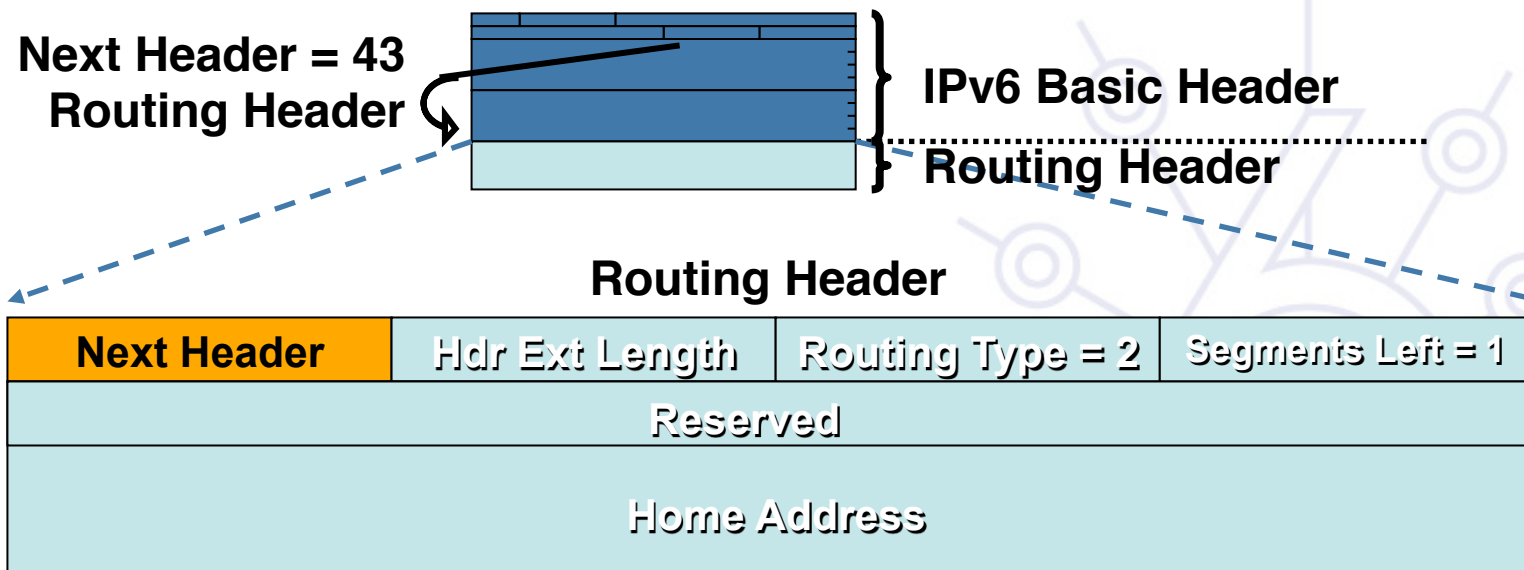
- Mobility header type
  - Binding Refresh Request Message
  - Home Test Init Message (HoTI)—Home Test Message (HoT)
  - Care-of Test Init Message (CoTI)—Care-of Test Message (CoT)
  - Binding Update Message (BU)—Binding Acknowledgement Message (BA)
  - Binding Error Message (BE)
- Message data field 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 Destination Option Header: Home Address Option



- Home Address Option (HAO) is carried by the existing 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: **MN CoA to CN**
  - 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

## New Routing Header Type: Type 2



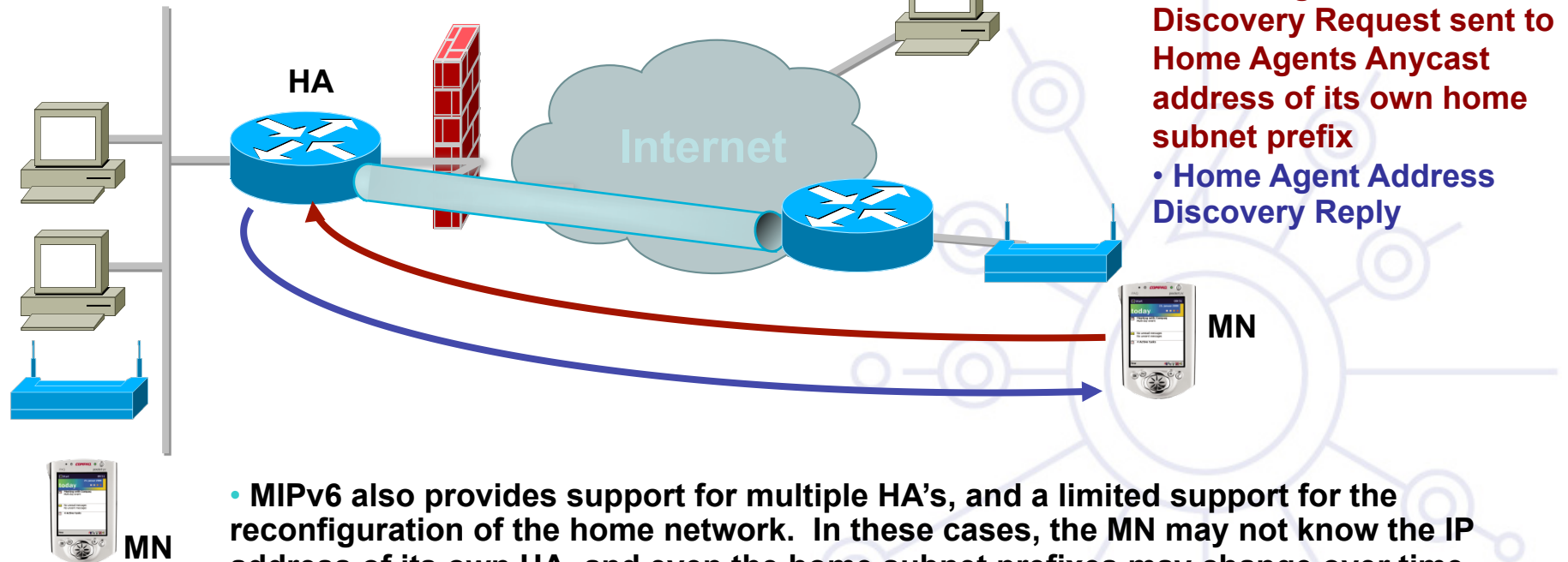
- MIPv6 defines a new routing header variant to allow a packet to be routed directly from a **CN to a MN CoA**
- MN CoA is inserted into the IPv6 destination address field; once the packet arrives at the care-of address, the MN retrieves its home address from the routing header, and this is used as the 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



- 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.

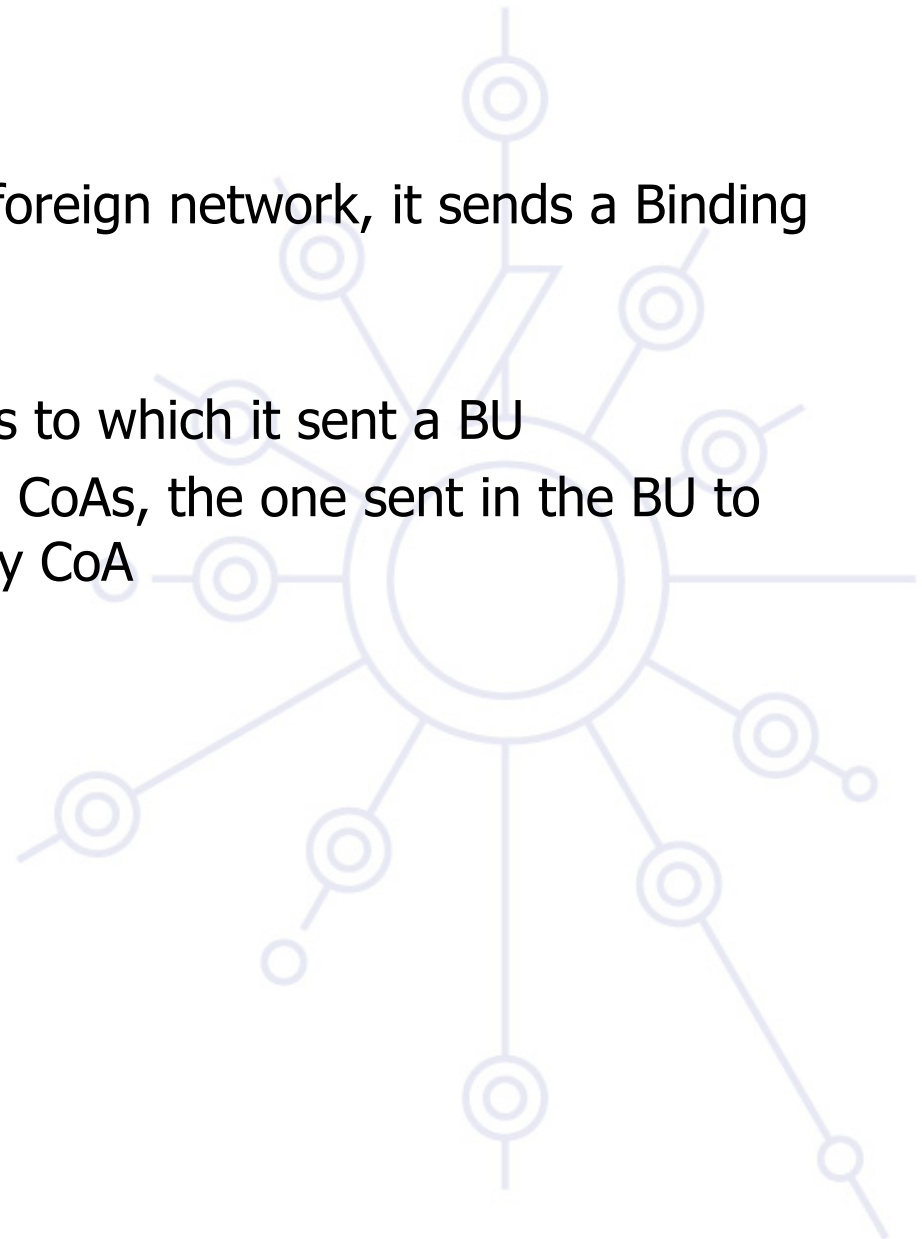
## Modifications to Neighbor Discovery

- 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) to HA and any CNs:
  - 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

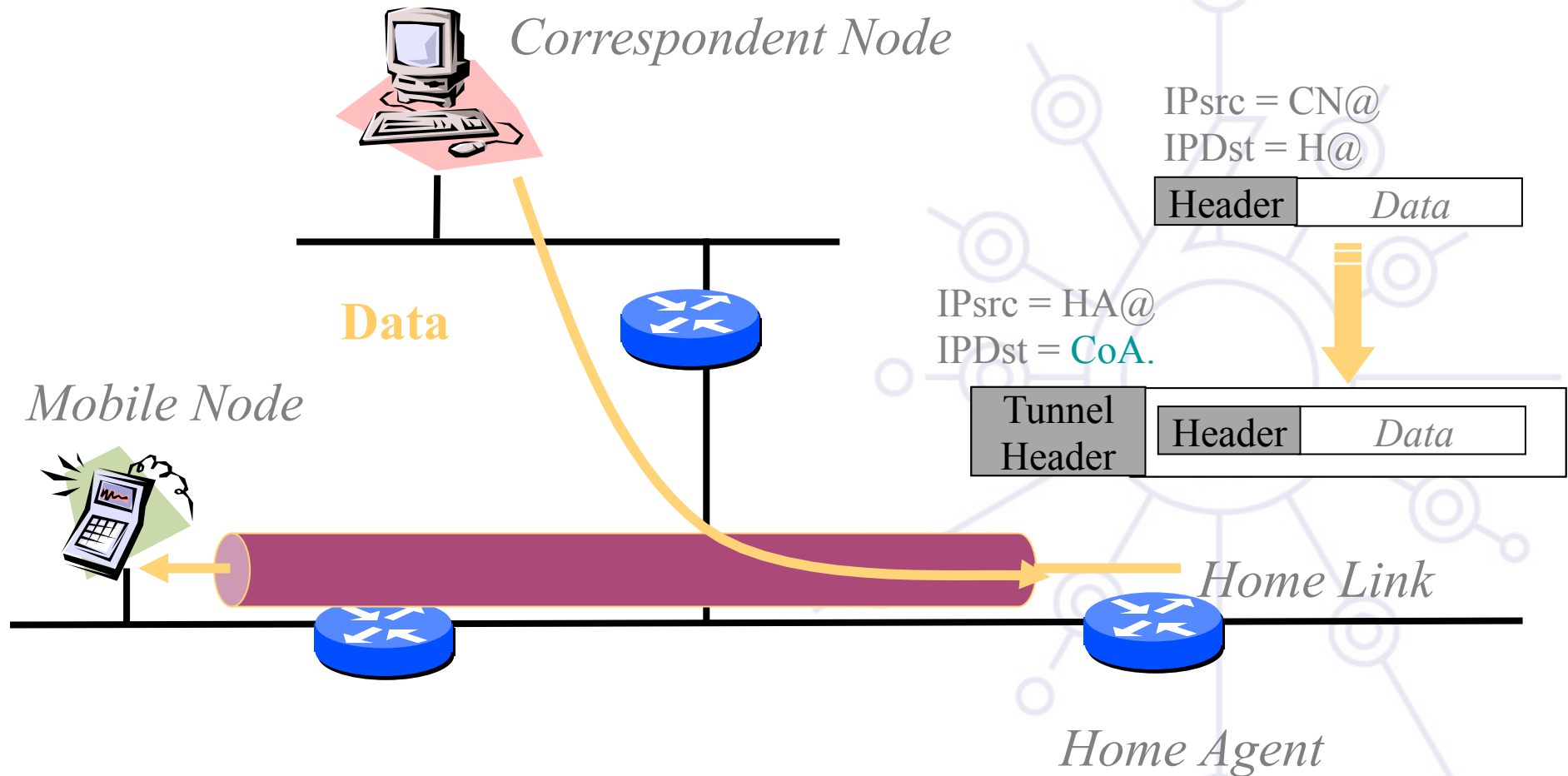


## Communication with a Mobile Node

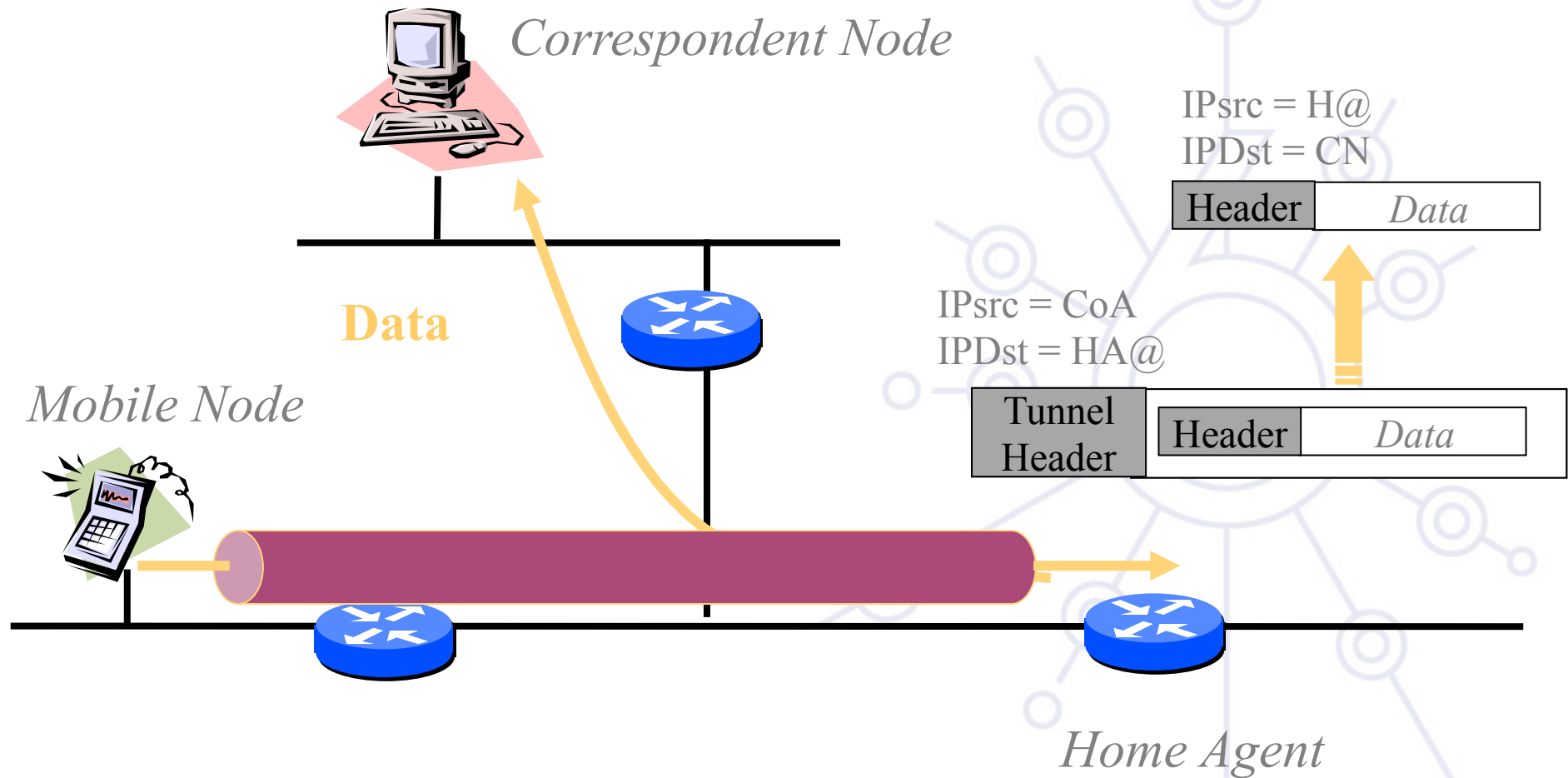
- 2 methods:
  - Bi-directional Tunneling
    - No mobility requirements on CNs
    - No visibility of MNs for CNs
    - Network load increased
    - HA role much reinforced
  - Direct (or Optimized) Routing
    - Much more complex mechanism
    - HA role much alleviated



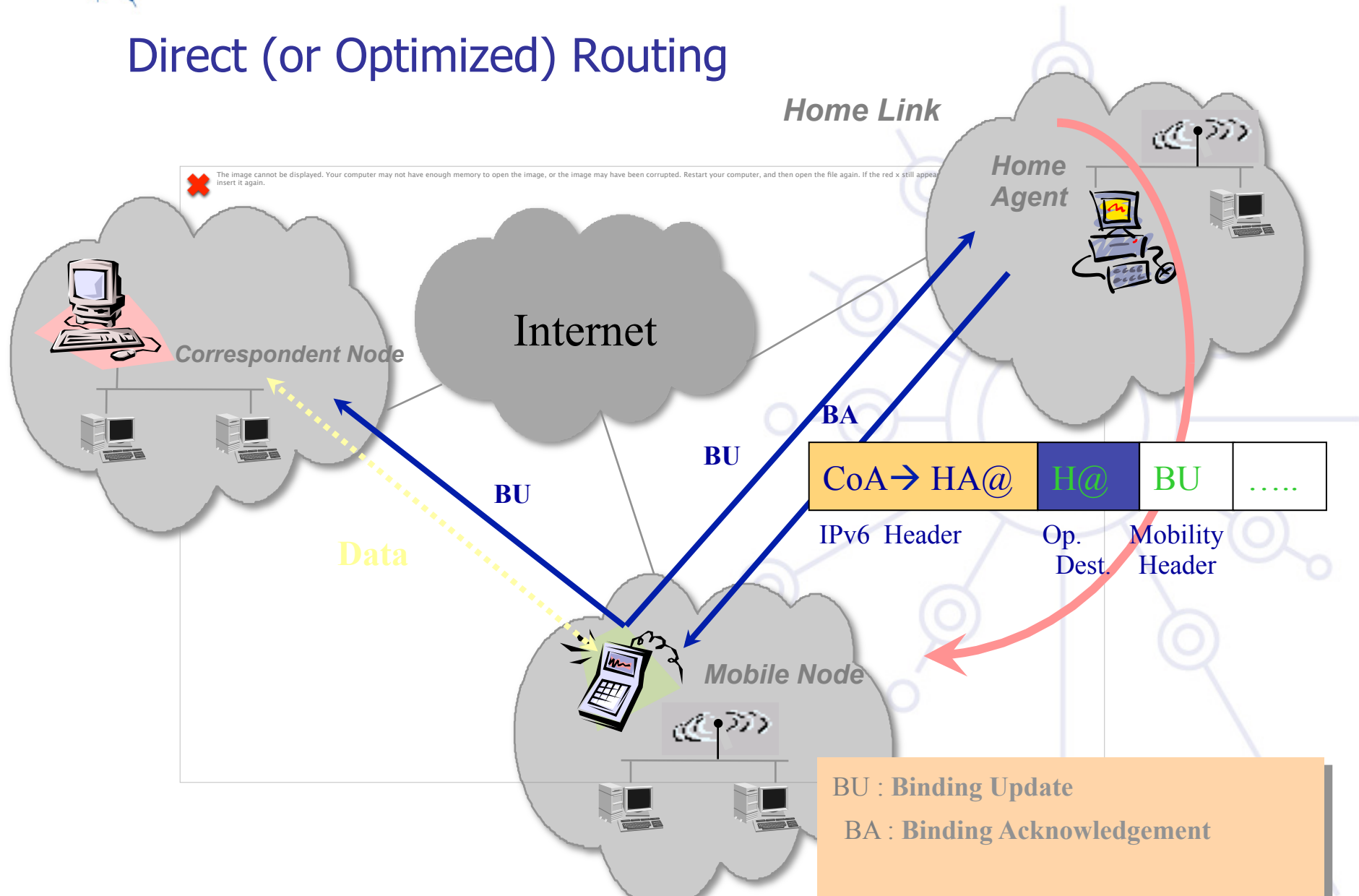
## Bi-directional Tunneling



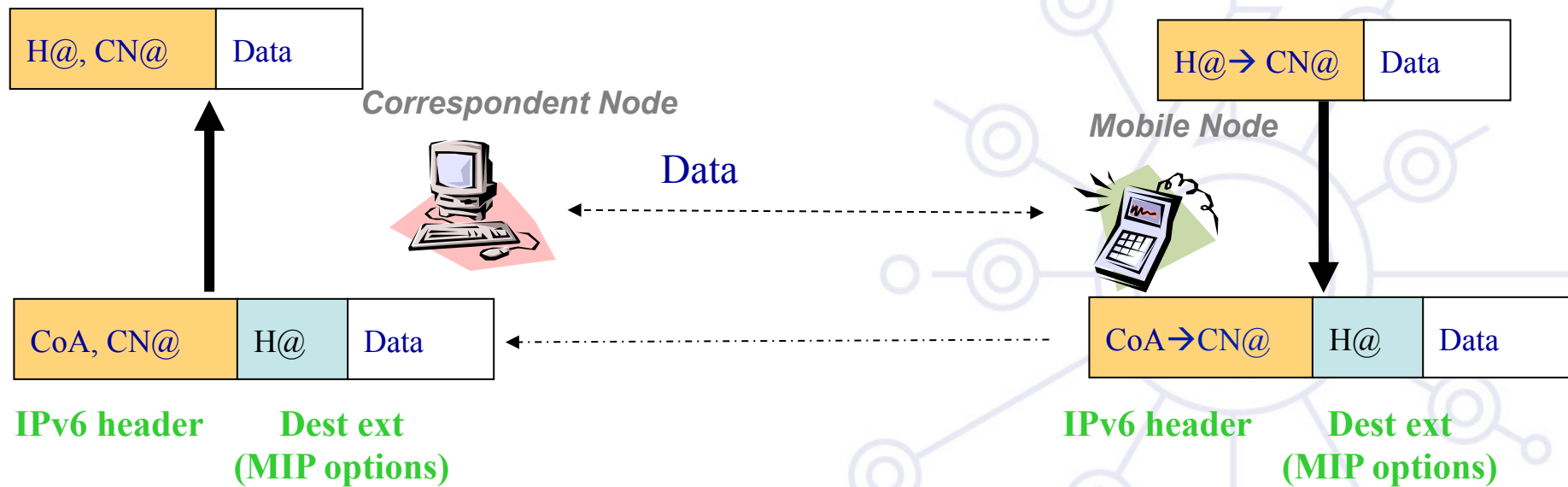
## Bi-directional Tunneling (2)



## Direct (or Optimized) Routing

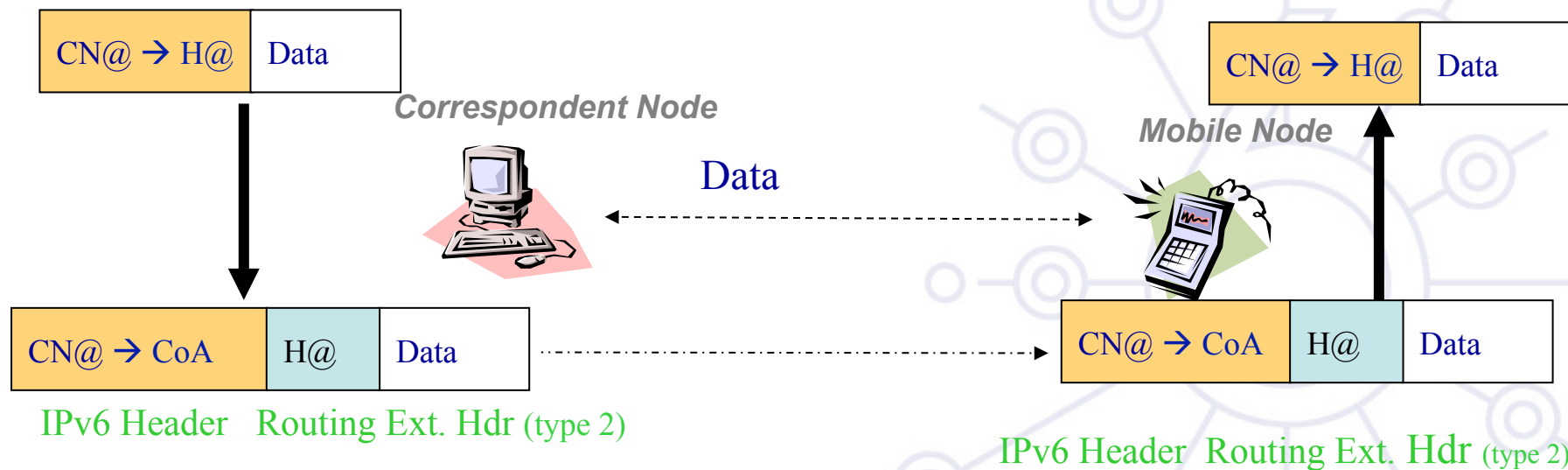


## Direct (or Optimized) Routing: MN → CN





## Direct (or Optimized) 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

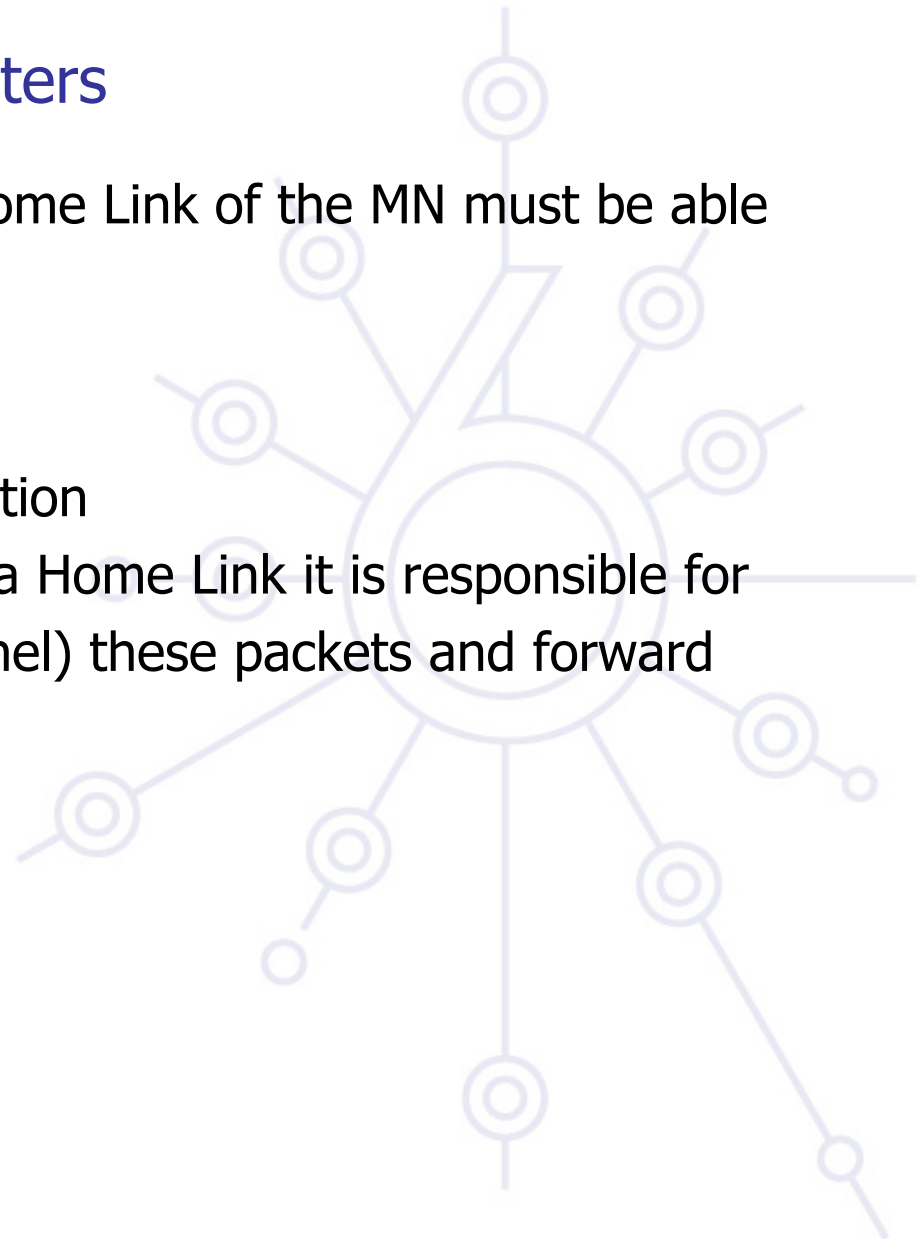


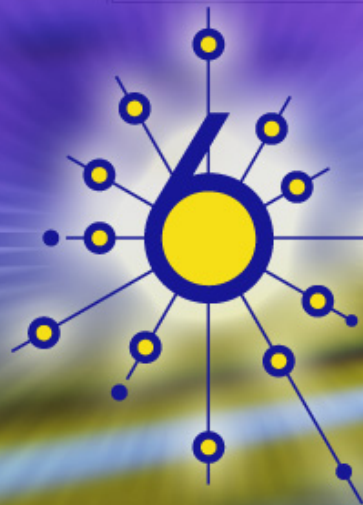
## Mobility Features For IPv6 Hosts

- 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





deploy

## MOBILE IPv6 SECURITY OVERVIEW

IPv6 Mobility Module

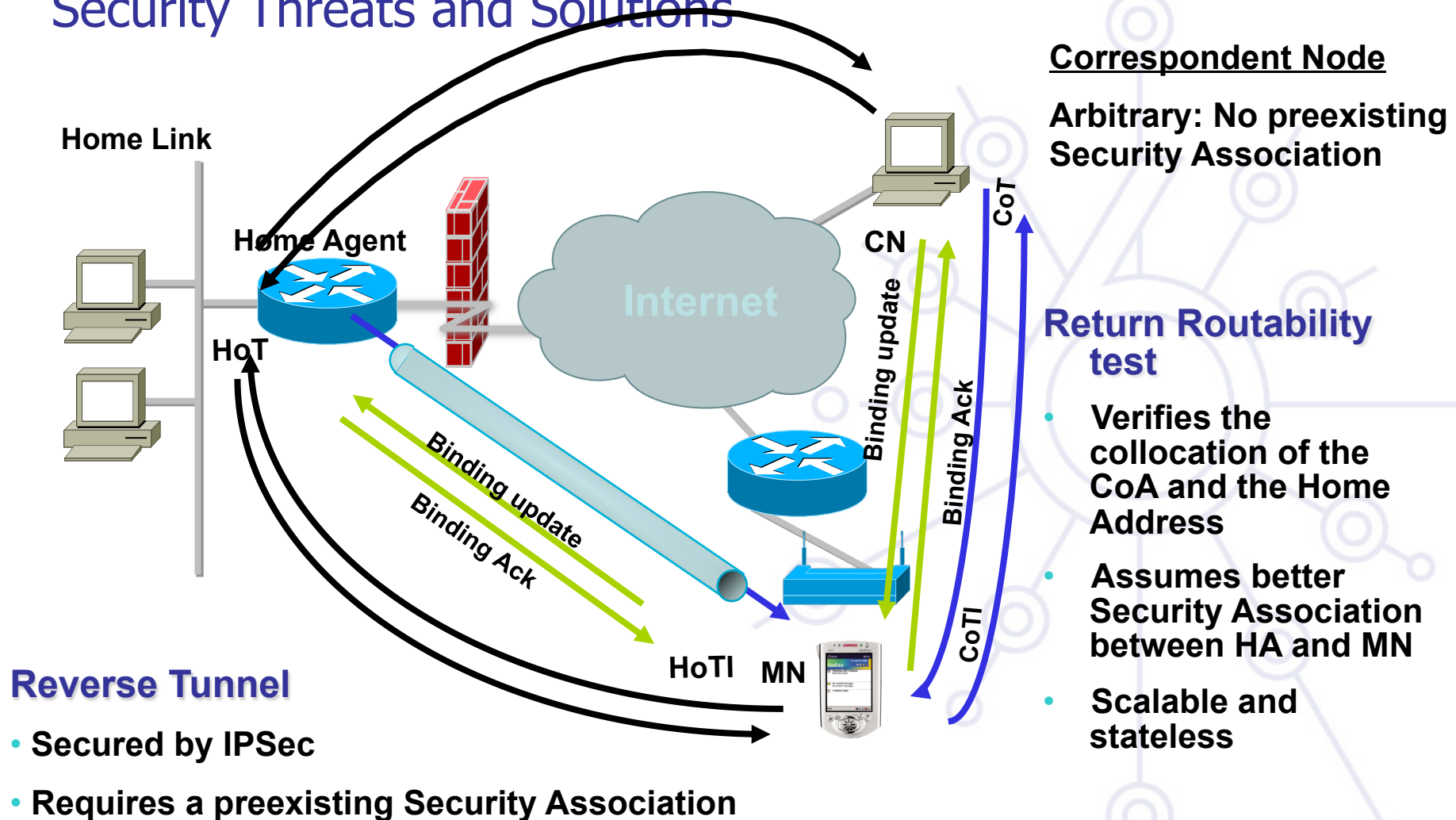


## Mobile IPv6 Security Overview

- MIPv6 RFC 6275/3776 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



# IPSec Technology Primer

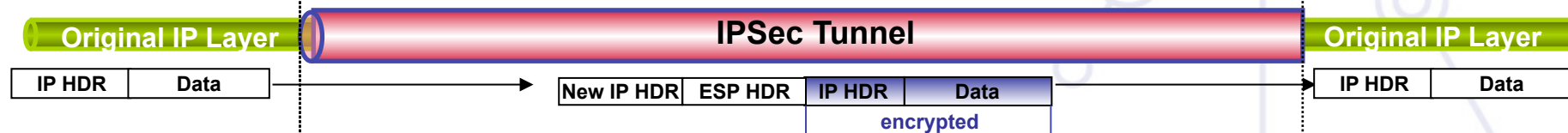
## AH Protocol (RFC 3402)



## ESP Transport Mode (RFC 4303)



## ESP Tunnel Mode (RFC 4303)



## 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.

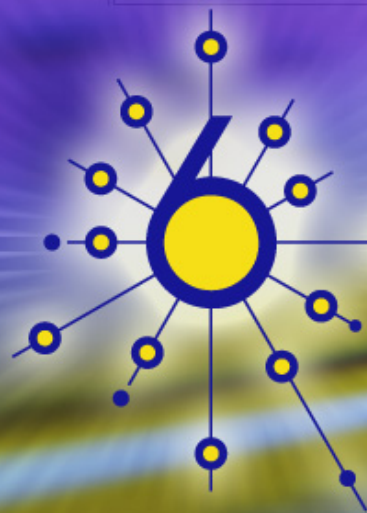


## Mobile Prefix Discovery

- 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 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



deploy

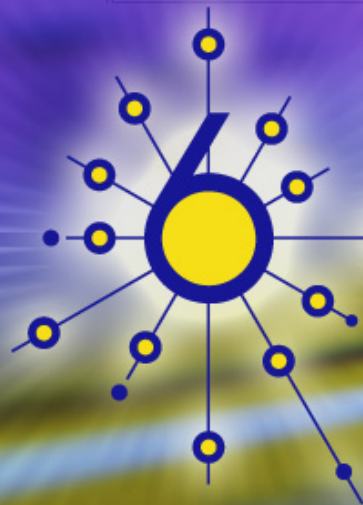
Questions





## 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.



deploy

MOBILE IPv6 @ CISCO

IPv6 Mobility Module



## 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 in 12.4(15)T2
- Mobile IPv6 is part of the planned IPv6 rollouts
  - [http://www.cisco.com/warp/public/732/Tech/ipv6/ipv6\\_learnabout.shtml](http://www.cisco.com/warp/public/732/Tech/ipv6/ipv6_learnabout.shtml)
  - <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, 3200, 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 be 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 suffix 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>
  - Output 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

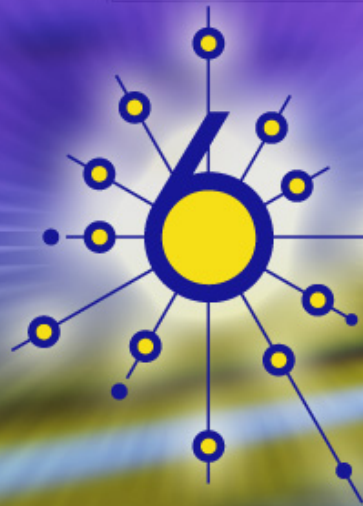
- Router# clear ipv6 mobile binding [home-address <prefix>] [care-of-address <prefix>] [interface <interface>]
  - Clears all bindings with the mobile nodes which match the search criteria. E.g.,
  - router# clear ipv6 mobile binding
  - Clear 27 bindings [confirm]
  - Note that when this command is 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.





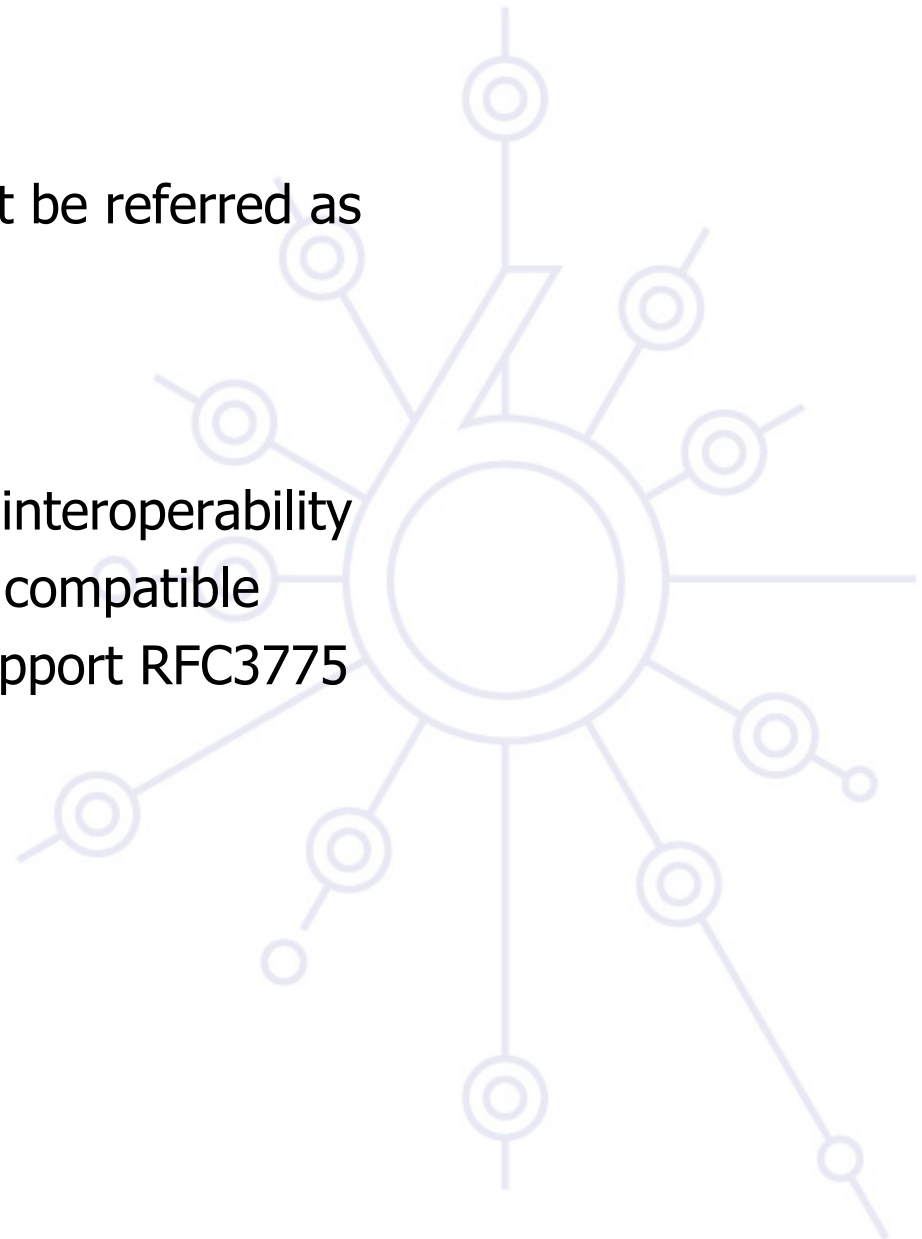
deploy

Implementations and Interoperability

IPv6 Mobility Module

## MIPv6 Implementation

- Mobile IPv6 implementations must be referred as
  - Mobile Node (MN)
  - Home Agent (HA)
  - Correspondent Node (CN)
- MIPv6 draft ID was important for interoperability
  - Draft ID not always backward compatible
  - Now most implementations support RFC3775







# Known Implementations





## Known Implementations

- Cisco – HA
- Elmic systems now Treck Inc. [www.treck.com](http://www.treck.com)  
–[http://www.elmic.com/pdf/MobileIPv6\\_data.pdf](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, Vista
- Mobile IP v4 and v6 implementation <http://www.mip4.org/2004/implementations/>
- NEC – MN, HA, CN and IPsec
- Nokia – MN, HA, CN
- Samsung – MN, CN
- Siemens
- University of Helsinki (Linux) – MN, CN  
–<http://www.mipl.mediapoli.com>
- 6NET MIPv6 implementation survey  
–<http://www.6net.org/publications/deliverables/D4.1.1.pdf>

# Interoperability

- Connectathon
  - <http://www.connectathon.org/>
- Test suites
  - TAHI, UNH
- Previous testing required similar ID compliancy





deploy

Questions

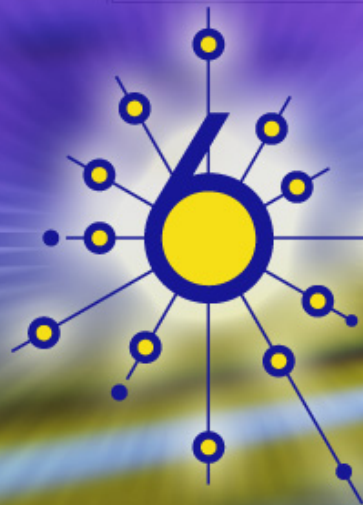


## IPv6 Mobility Module

[6deploy.org](http://6deploy.org)







deploy

CISCO Mobile Networks

IPv6 Mobility Module

## 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

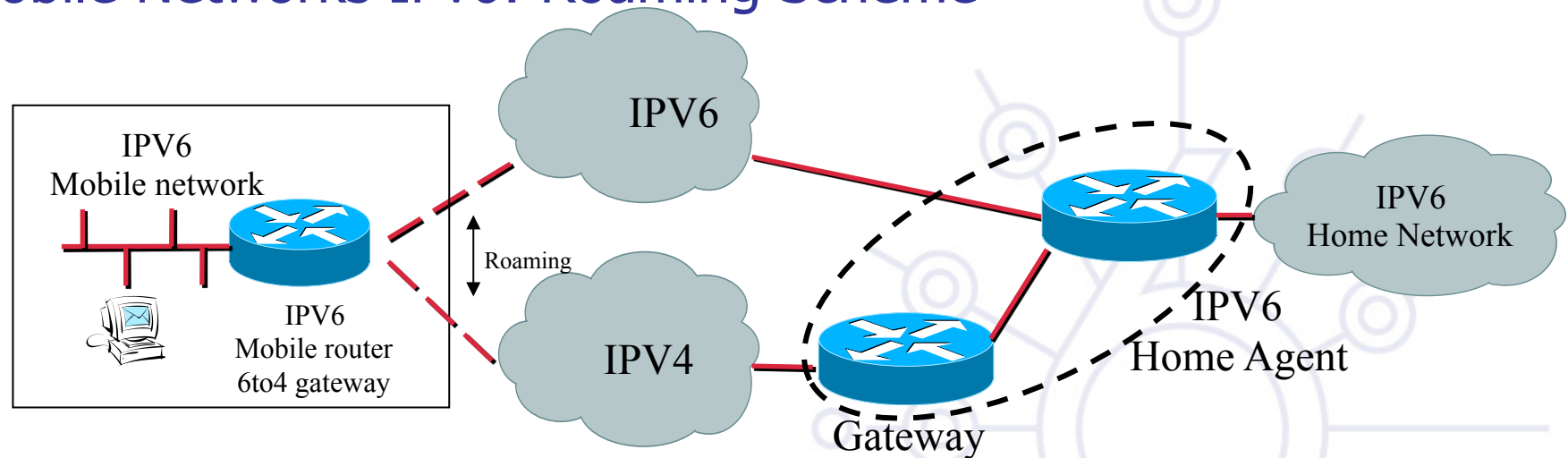


## Cisco Mobile Networks

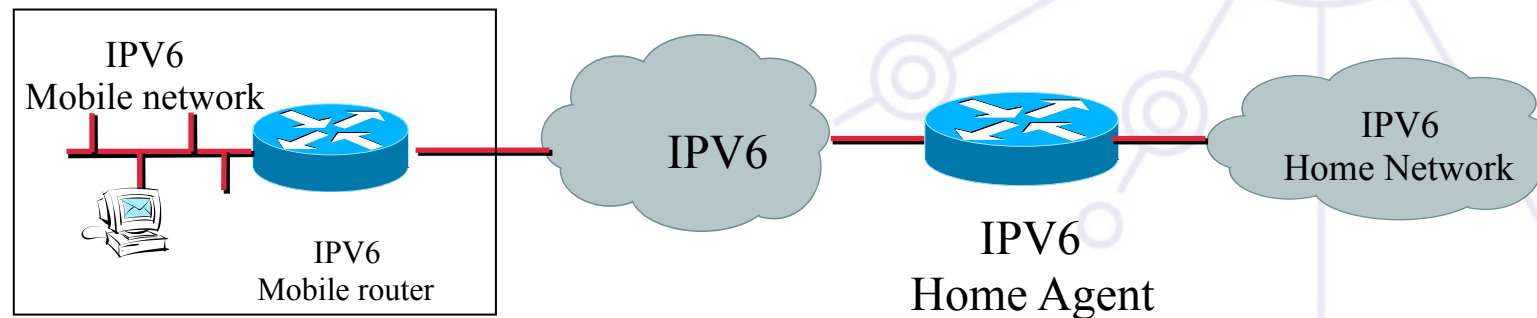
- Available Today on IPv4
- Mobile router feature set on 12.2(4)T and above
- Cisco 2800 to 7600 series
- Cisco MAR 3200 series
- Basic Mobile Router IPv6



## Mobile Networks IPv6: Roaming Scheme

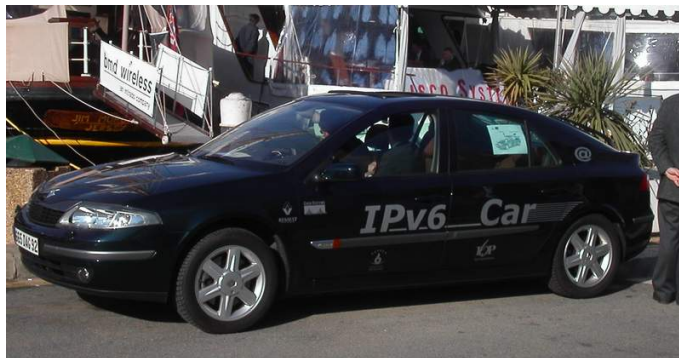


Mobile IPV6 router roaming into a V4 or V6 network

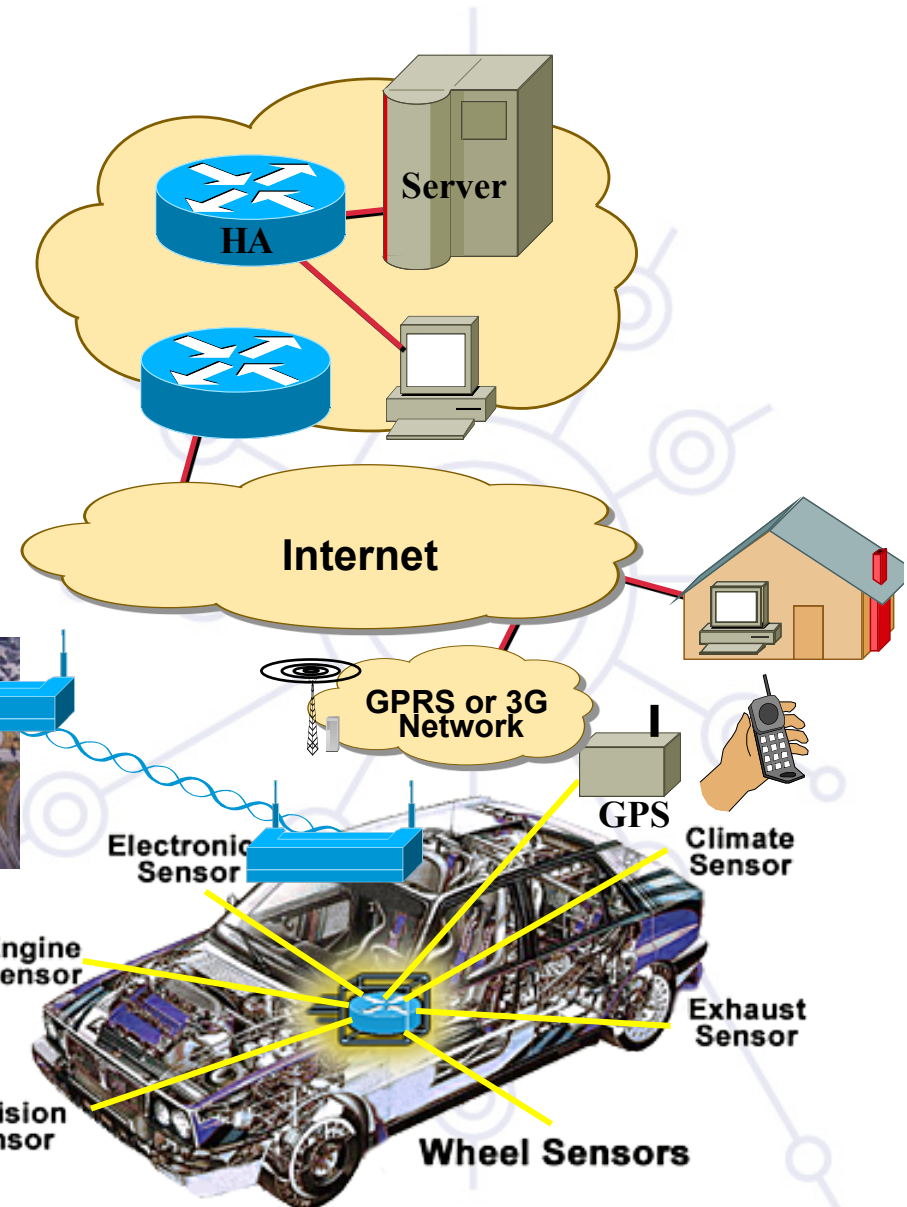
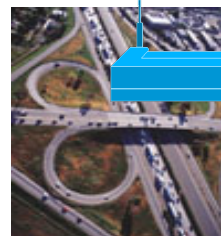


Ideal topology

## Networks in Motion



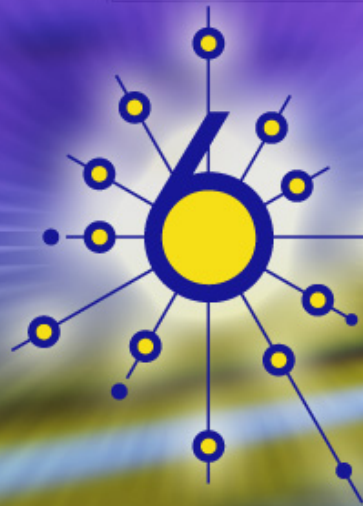
Toll or Gaz  
Station's



## 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-mip6-07.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-hmip6-08.txt>
- Mobile IP implementations for v4 and v6
  - <http://www.mip4.org/2004/implementations/>





deploy

Mobile IPv6 Testbed

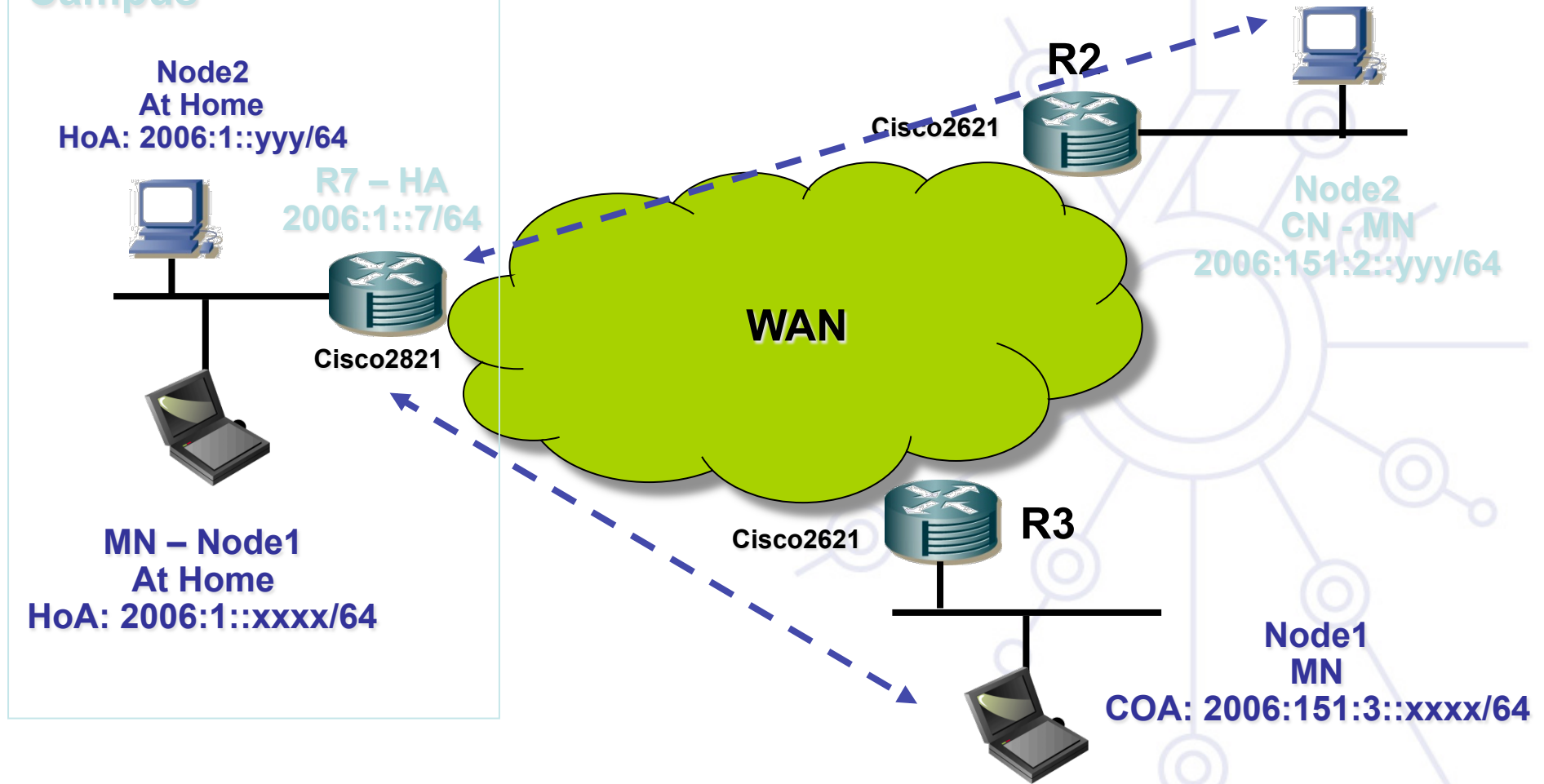
## MIPv6 Devices

- 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

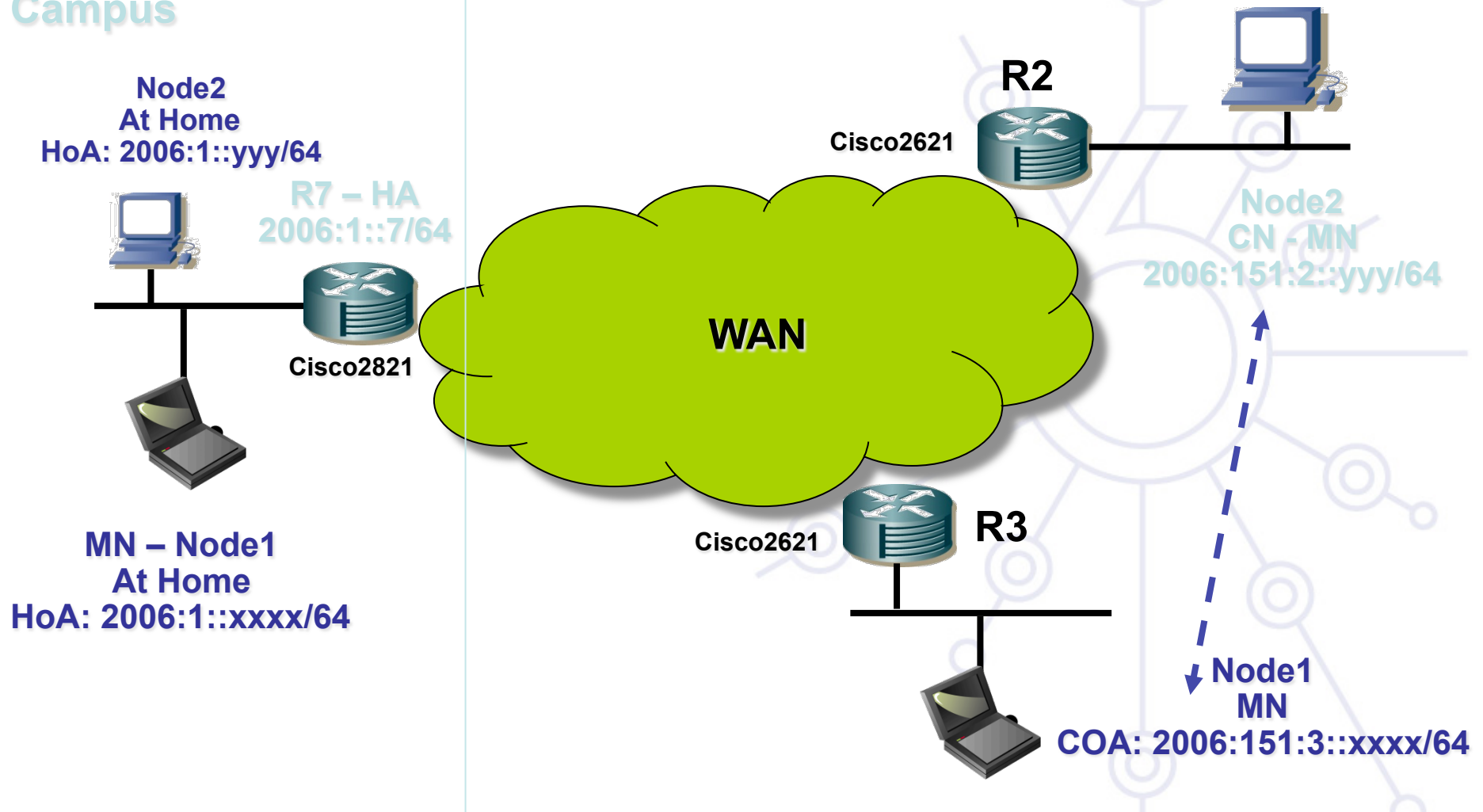
### Campus





## Topology – With Optimized Routing

### Campus





## 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
!
```



## IPv6 Mobility Module

### 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                                     ← Node2
  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                                     ← Node1
  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#
```



## 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\fefef>ipv6 ha
Home Address: 2006:1::20d:60ff:fefa:e15b
Home Agent: 2006:1::7
ESPTunnelSPI: 0
ESPTunnelSPD: 0
```

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



## Node1 : Binding update

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

Node1





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

```
F:\Documents and Settings\fefef>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\fefef>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\fefefe>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\feffe>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\fefefefe>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:fffb9:8d7c, 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

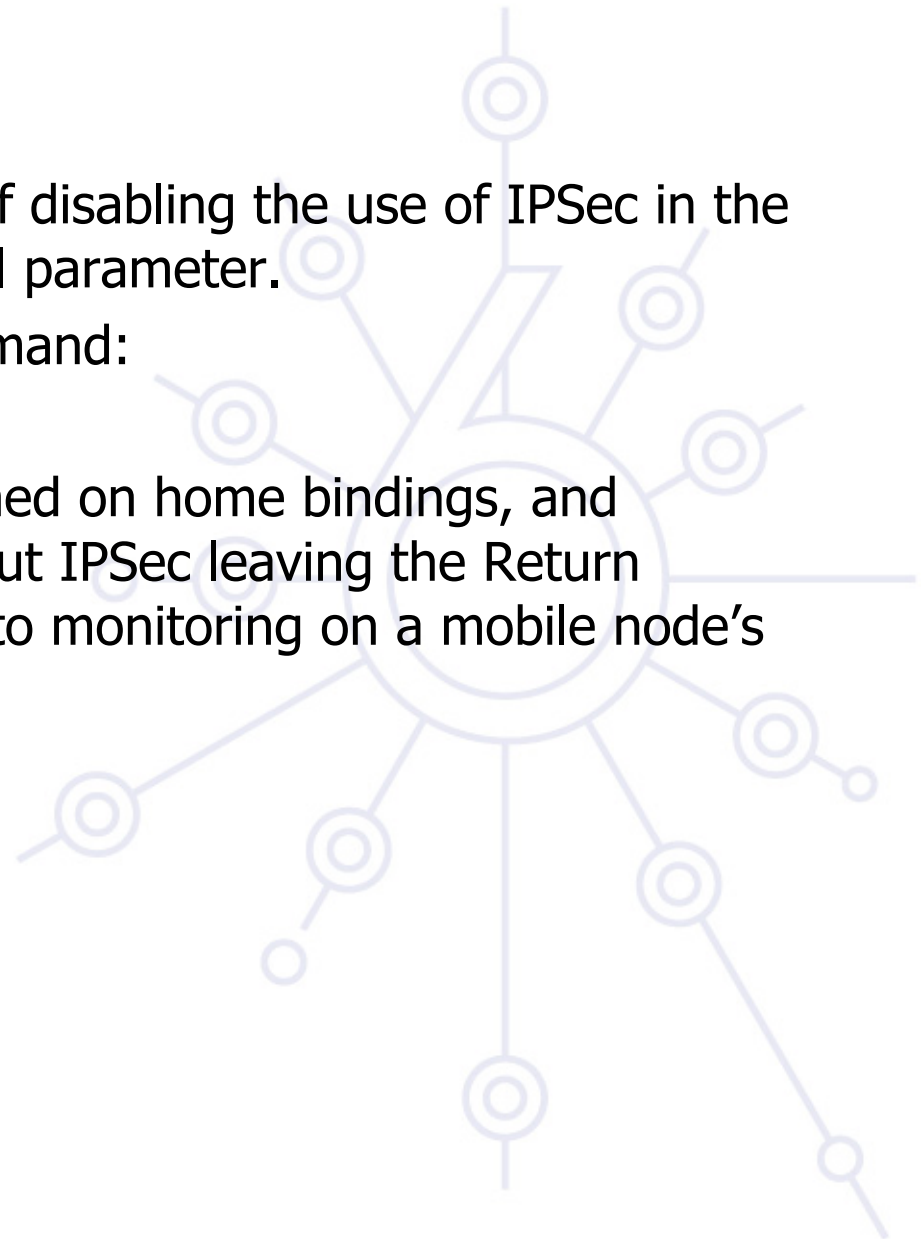
```
C:\JMB>ipv6 hau 2006:1::20c:29ff:feb9:8d7c 2006:1::7
Home address update error: 57
Note: Check that host is in mobile mode (ipv6 gpu MobilityMode [ MN | MN CN ]).
Note: SPI must indicate valid inbound ESP tunnel SPI used by HA for tunnelling to MN.
Note: SPD must indicate valid IPsec SPD entry on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







## IPv6 Mobility Module

### Node2 – D

```
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>h
```



## 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>
```

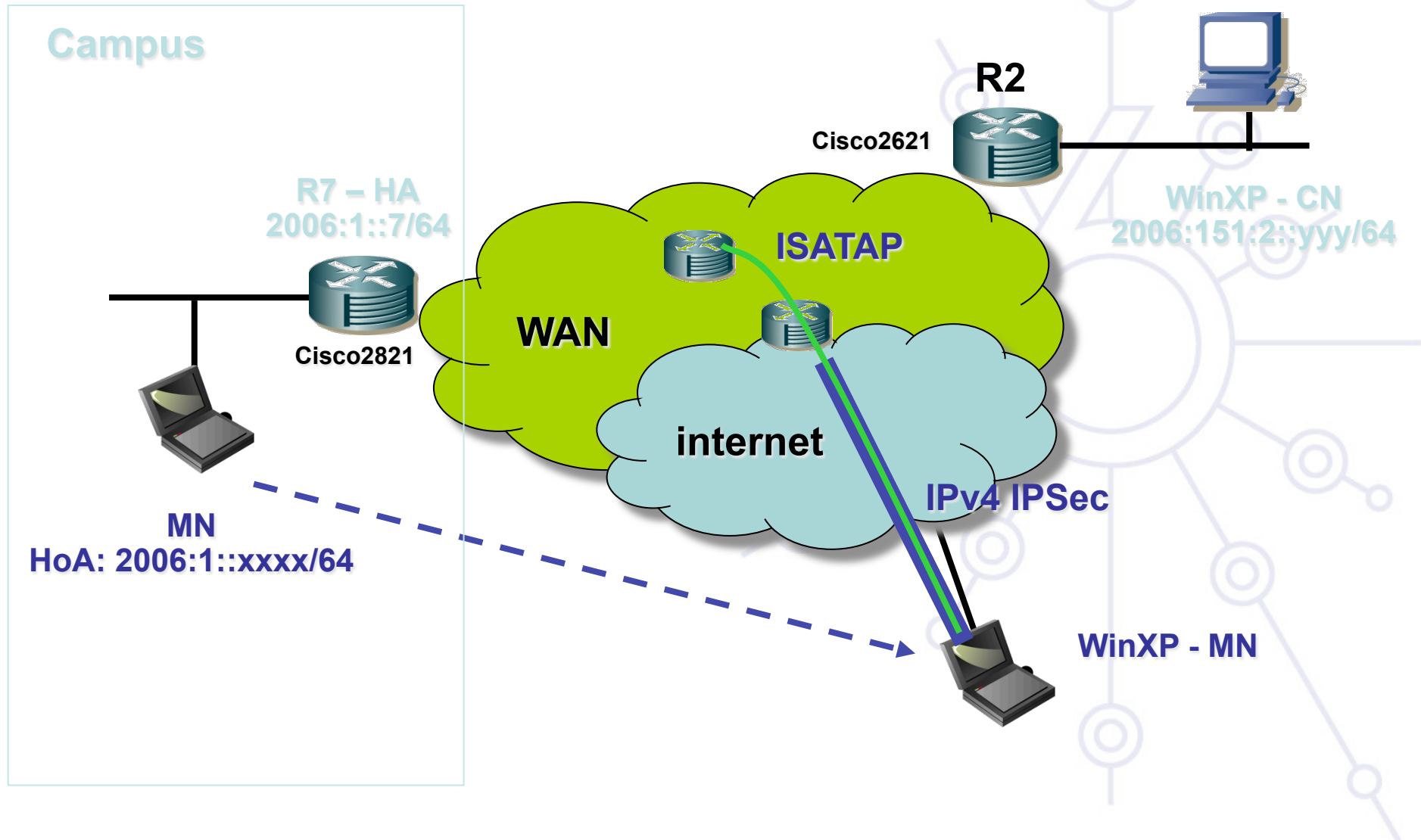


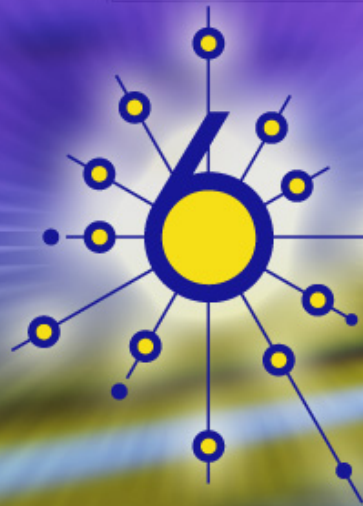
## Node2 – Binding Updates

```
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





deploy

Mobile IPv6 Testbed  
Ethereal Traces

IPv6 Mobility Module



## IPv6 Mobility Module

## Traces after successful pings between MN1 &amp; MN2

traces\_21\_05\_2005\_v2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_c3:e2:0a	Spanning-tree-(for	STP	Conf. Root = 32768/00:06:52:c3:e2:01 Cost = 0 Port = 0x8010
2	1.999973	Cisco_c3:e2:0a	Spanning-tree-(for	STP	Conf. Root = 32768/00:06:52:c3:e2:01 Cost = 0 Port = 0x8010
3	3.999914	Cisco_c3:e2:0a	Spanning-tree-(for	STP	Conf. Root = 32768/00:06:52:c3:e2:01 Cost = 0 Port = 0x8010
4	4.894010	2006:1::20d:60ff:f	2006:1::20c:29ff:f	ICMPv6	Echo request
5	4.904704	2006:1::20c:29ff:f	2006:1::20d:60ff:f	ICMPv6	Echo reply
6	4.904737	2006:1::20d:60ff:f	2006:1::20c:29ff:f	MIPv6	Home Test Init
7	4.904755	2006:151:3:0:20d:6	2006:1::20c:29ff:f	MIPv6	Care-of Test Init
8	4.906517	2006:1::20c:29ff:f	2006:1::20d:60ff:f	MIPv6	Home Test Init
9	4.906547	2006:1::20d:60ff:f	2006:1::20c:29ff:f	MIPv6	Home Test
10	4.907099	2006:151:2:0:20c:2	2006:1::20d:60ff:f	MIPv6	Care-of Test Init
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
14	4.915816	2006:151:3:0:20d:6	2006:1::20c:29ff:f	MIPv6	Binding Update
15	5.936131	2006:151:3:0:20d:6	2006:1::20c:29ff:f	MIPv6	Binding Update
16	5.946121	2006:1::20d:60ff:f	2006:1::20c:29ff:f	ICMPv6	Echo request
17	5.952898	2006:1::20c:29ff:f	2006:1::20d:60ff:f	ICMPv6	Echo reply
18	6.001400	Cisco_c3:e2:0a	Spanning-tree-(for	STP	Conf. Root = 32768/00:06:52:c3:e2:01 Cost = 0 Port = 0x8010
19	7.007675	2006:1::20d:60ff:f	2006:1::20c:29ff:f	ICMPv6	Echo request
20	7.015616	2006:1::20c:29ff:f	2006:1::20d:60ff:f	ICMPv6	Echo reply
21	7.938999	2006:151:3:0:20d:6	2006:1::7	MIPv6	Binding Update
22	7.942397	2006:1::7	2006:151:3:0:20d:6	MIPv6	Binding Acknowledgement
23	7.999816	Cisco_c3:e2:0a	Spanning-tree-(for	STP	Conf. Root = 32768/00:06:52:c3:e2:01 Cost = 0 Port = 0x8010
24	8.069194	2006:1::20d:60ff:f	2006:1::20c:29ff:f	ICMPv6	Echo request
25	8.077161	2006:1::20c:29ff:f	2006:1::20d:60ff:f	ICMPv6	Echo reply
26	8.439761	2006:151:3:0:20d:6	2006:1::20c:29ff:f	MIPv6	Binding Update
27	8.449525	2006:1::20c:29ff:f	2006:151:3:0:20d:6	MIPv6	Binding Acknowledgement
28	8.553819	2006:151:2:0:20c:2	2006:1::20d:60ff:f	MIPv6	Binding Update
29	8.553909	2006:1::20d:60ff:f	2006:151:2:0:20c:2	MIPv6	Binding Acknowledgement

Frame 4 (134 bytes on wire, 134 bytes captured)

Internet Protocol Version 6

Version: 6

0000 00 07 50 5e 79 00 00 0d 60 fa e1 5b 86 dd 60 00 ..Pay...[...]

0010 00 00 00 50 29 40 20 06 01 51 00 03 00 00 02 0d ...P)@...Q.....

0020 60 ff fe fa e1 5b 20 06 00 01 00 00 00 00 00 00 .....[.....]

0030 00 00 00 00 00 07 60 00 00 00 00 28 3a 40 20 06 .....[.....](@...

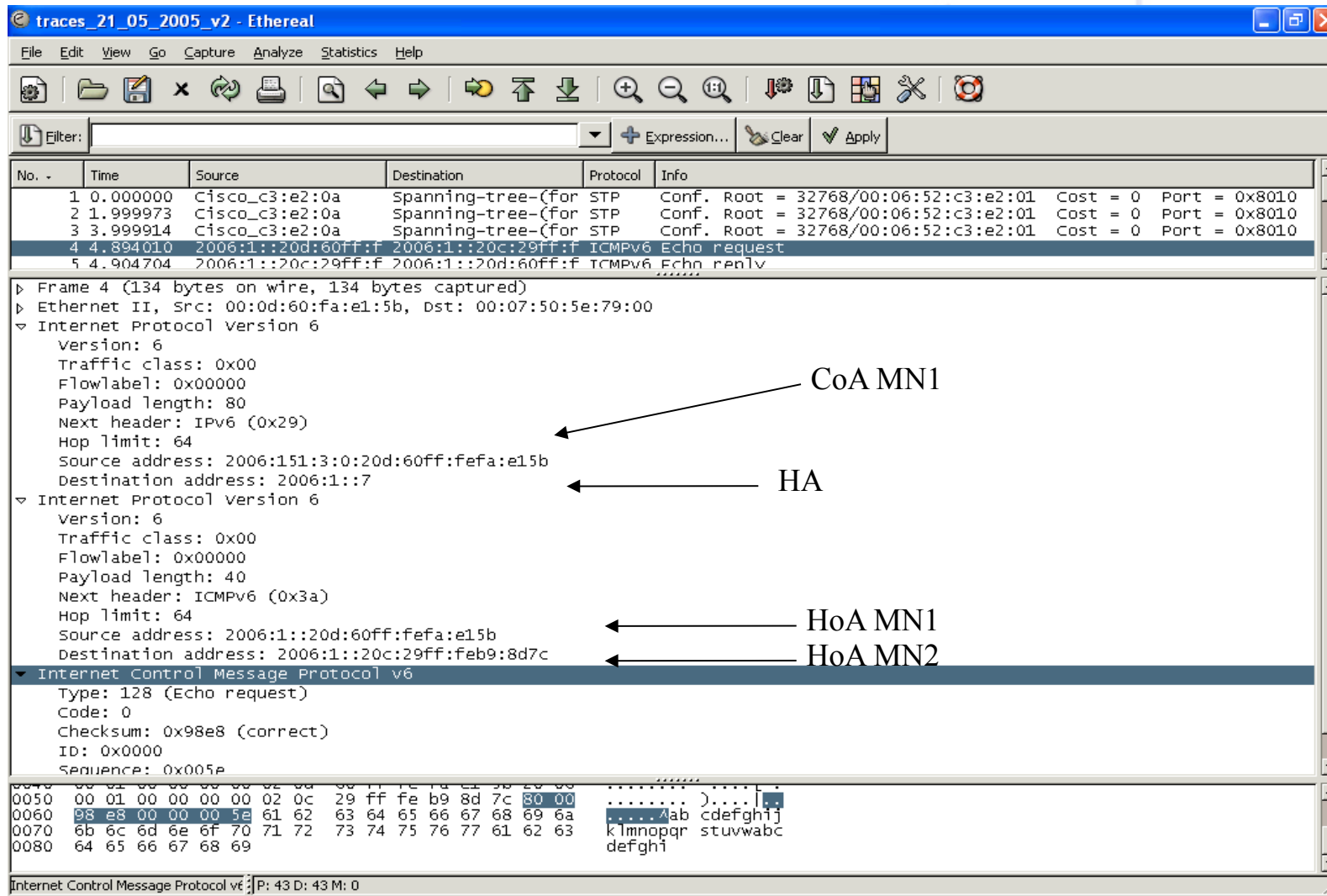
0040 00 01 00 00 00 00 02 0d 60 ff fe fa e1 5b 20 06 .....[.....]

0050 00 01 00 00 00 00 02 0d 60 ff fe fa e1 5b 20 06 .....[.....]

File: traces\_21\_05\_2005\_v2 5272 b; P: 43 D: 43 M: 0



## Ping without direct routing IPv6 tunnelled in IPv6



The screenshot shows a Wireshark packet capture of an ICMPv6 Echo request (ping) from CoA MN1 to HA. The packet is then forwarded to HoA MN1 and HoA MN2. The packet details are as follows:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_c3:e2:0a	Spanning-tree-(for STP	Conf. Root = 32768/00:06:52:c3:e2:01	Cost = 0 Port = 0x8010
2	1.999973	Cisco_c3:e2:0a	Spanning-tree-(for STP	Conf. Root = 32768/00:06:52:c3:e2:01	Cost = 0 Port = 0x8010
3	3.999914	Cisco_c3:e2:0a	Spanning-tree-(for STP	Conf. Root = 32768/00:06:52:c3:e2:01	Cost = 0 Port = 0x8010
4	4.894010	2006:1::20d:60ff:f	2006:1::20c:29ff:f	ICMPv6 Echo request	
5	4.904704	2006:1::20c:29ff:f	2006:1::20d:60ff:f	ICMPv6 Echo reply	

Frame 4 (134 bytes on wire, 134 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: 80
- Next header: IPv6 (0x29)
- Hop limit: 64
- Source address: 2006:151:3:0:20d:60ff:feffa:e15b
- Destination address: 2006:1::7

Internet Protocol version 6

- Version: 6
- Traffic class: 0x00
- Flowlabel: 0x00000
- Payload length: 40
- Next header: ICMPv6 (0x3a)
- Hop limit: 64
- Source address: 2006:1::20d:60ff:feffa:e15b
- Destination address: 2006:1::20c:29ff:feb9:8d7c

Internet Control Message Protocol v6

- Type: 128 (Echo request)
- Code: 0
- Checksum: 0x98e8 (correct)
- ID: 0x0000
- Sequence: 0x005e

0050 00 01 00 00 00 00 02 0c 29 ff fe b9 8d 7c 80 00 ..... ).....  
0060 98 e8 00 00 00 5e 61 62 63 64 65 66 67 68 69 6a .....ab cdefghij  
0070 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 klmnopqr stuvwabc  
0080 64 65 66 67 68 69 defghi

Internet Control Message Protocol v6 [P: 43 D: 43 M: 0]



## IPv6 Mobility Module

## Echo reply w/o 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
4	4.894010	2006:1::20d:60ff:f	2006:1::20c:29ff:f	ICMPv6	Echo request
5	4.904704	2006:1::20c:29ff:f	2006:1::20d:60ff:f	ICMPv6	Echo reply
6	4.904737	2006:1::20d:60ff:f	2006:1::20c:29ff:f	MIPv6	Home Test Init
7	4.904755	2006:151:3:0:20d:6	2006:1::20c:29ff:f	MIPv6	Care-of Test Init
8	4.906517	2006:1::20c:29ff:f	2006:1::20d:60ff:f	MIPv6	Home Test Init

Ethernet II, Src: 00:07:30:3e:79:00, Dst: 00:0d:60:fa:e1:5b

Internet Protocol Version 6

- Version: 6
- Traffic class: 0x00
- Flowlabel: 0x00000
- Payload length: 80
- Next header: IPv6 (0x29)
- Hop limit: 60
- Source address: 2006:1::7
- Destination address: 2006:151:3:0:20d:60ff:fe fa:e15b

Internet Protocol Version 6

- Version: 6
- Traffic class: 0x00
- Flowlabel: 0x00000
- Payload length: 40
- Next header: ICMPv6 (0x3a)
- Hop limit: 63
- Source address: 2006:1::20c:29ff:feb9:8d7c
- Destination address: 2006:1::20d:60ff:fe fa:e15b

Internet Control Message Protocol v6

- Type: 129 (Echo reply)
- Code: 0
- Checksum: 0x97e8 (correct)
- ID: 0x0000
- Sequence: 0x005e
- Data (32 bytes)

0000 00 0d 60 fa e1 5b 00 07 50 5e 79 00 86 dd 60 00 ...[... P... ..

0010 00 00 00 50 29 3c 20 06 00 01 00 00 00 00 00 ...P)< . ....

0020 00 00 00 00 00 07 20 06 01 51 00 03 00 00 02 0d .....Q.....

0030 60 ff fe fa e1 5b 60 00 00 00 00 28 3a 3f 20 06 .....[...(:?...

0040 00 01 00 00 00 00 02 0c 29 ff fe b9 8d 7c 20 06 ..... )....| .

HA

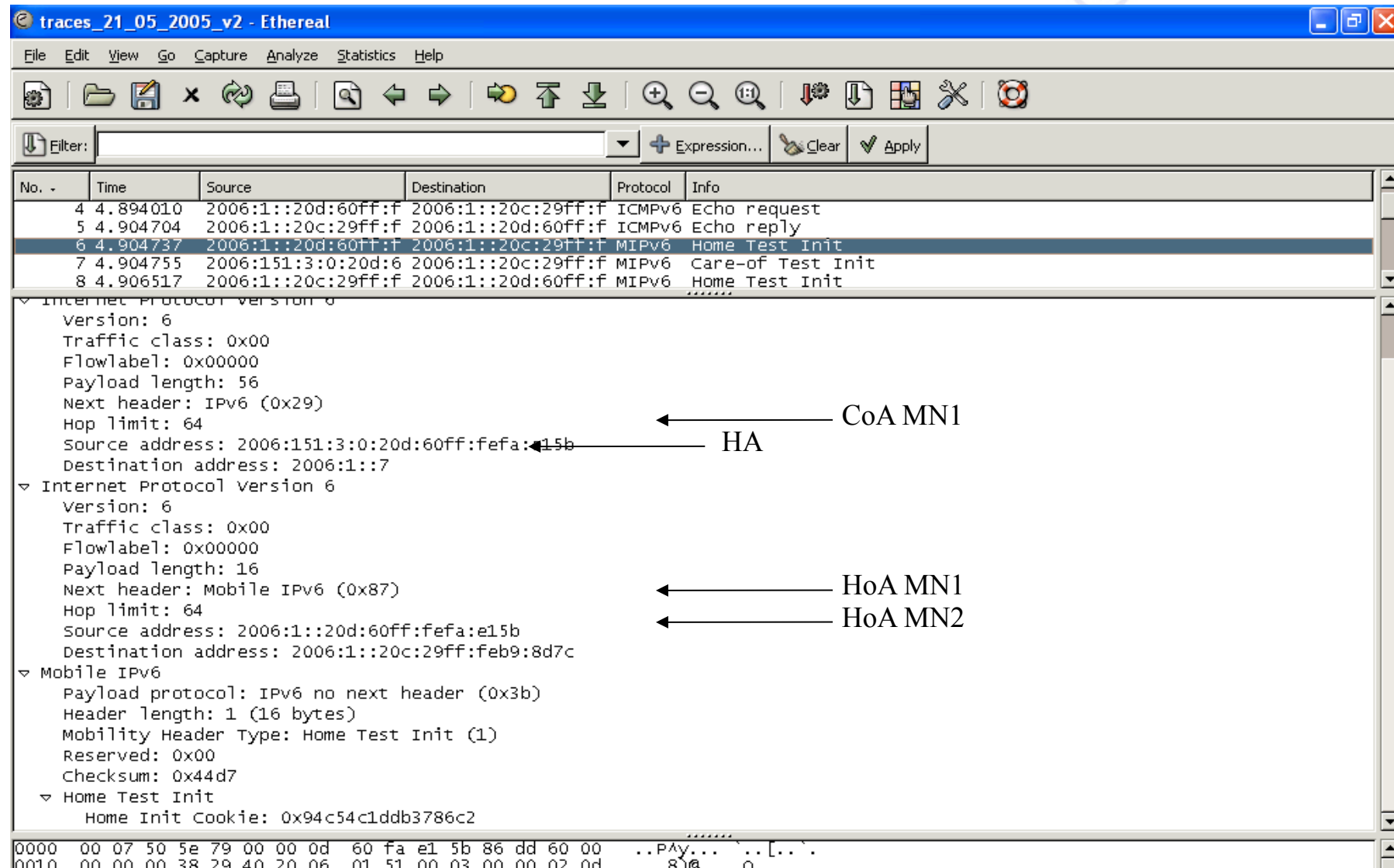
CoA MN1

HoA MN2

HoA MN1



## Home test init



The image shows a Wireshark packet capture window titled "traces\_21\_05\_2005\_v2 - Ethereal". The packet list shows a sequence of ICMPv6 Echo request/reply and MIPv6 Home Test Init/Care-of Test Init messages. The selected packet (No. 6) is a MIPv6 Home Test Init message. The packet details pane shows the following structure:

- Internet Protocol Version 6
  - Version: 6
  - Traffic class: 0x00
  - Flowlabel: 0x00000
  - Payload length: 56
  - Next header: IPv6 (0x29)
  - Hop limit: 64
  - Source address: 2006:151:3:0:20d:60ff:fefa:e15b ← HA
  - Destination address: 2006:1::7
- Internet Protocol Version 6
  - Version: 6
  - Traffic class: 0x00
  - Flowlabel: 0x00000
  - Payload length: 16
  - Next header: Mobile IPv6 (0x87)
  - Hop limit: 64
  - Source address: 2006:1::20d:60ff:fefa:e15b ← HoA MN1
  - Destination address: 2006:1::20c:29ff:feb9:8d7c ← HoA MN2
- Mobile IPv6
  - Payload protocol: IPv6 no next header (0x3b)
  - Header length: 1 (16 bytes)
  - Mobility Header Type: Home Test Init (1)
  - Reserved: 0x00
  - Checksum: 0x44d7
  - Home Test Init
    - Home Init Cookie: 0x94c54c1ddb3786c2

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.



## Care-of test init

traces\_21\_05\_2005\_v2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter:  + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
4	4.894010	2006:1::20d:60ff:f	2006:1::20c:29ff:f	ICMPv6	Echo request
5	4.904704	2006:1::20c:29ff:f	2006:1::20d:60ff:f	ICMPv6	Echo reply
6	4.904737	2006:1::20d:60ff:f	2006:1::20c:29ff:f	MIPv6	Home Test Init
7	4.904755	2006:151:3:0:20d:6	2006:1::20c:29ff:f	MIPv6	Care-of Test Init
8	4.906517	2006:1::20c:29ff:f	2006:1::20d:60ff:f	MIPv6	Home Test Init

▶ Frame 7 (70 bytes on wire, 70 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: 16
- Next header: Mobile IPv6 (0x87)
- Hop limit: 64
- Source address: 2006:151:3:0:20d:60ff:fefa:e15b ← CoA MN1
- Destination address: 2006:1::20c:29ff:feb9:8d7c ← HoA MN2

▼ Mobile IPv6

- Payload protocol: IPv6 no next header (0x3b)
- Header length: 1 (16 bytes)
- Mobility Header Type: Care-of Test Init (2)
- Reserved: 0x00
- Checksum: 0xc936
- ▼ Care-of Test Init
  - Care-of Init Cookie: 0x80efaf7ec315c8a6

0000 00 07 50 5e 79 00 00 0d 60 fa e1 5b 86 dd 60 00 ..Ply... ..[...  
0010 00 00 00 10 87 40 20 06 01 51 00 03 00 00 02 0d .....@...Q.....  
0020 60 ff fe fa e1 5b 20 06 00 01 00 00 00 00 02 0c .....[... ..  
0030 29 ff fe b9 8d 7c 3b 01 02 00 c9 36 00 00 80 ef .....|... ..6....



# Home 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
8	4.906517	2006:1::20c:29ff:f	2006:1::20d:60ff:f	MIPv6	Home Test Init
9	4.906547	2006:1::20d:60ff:f	2006:1::20c:29ff:f	MIPv6	Home Test
10	4.907099	2006:151:2:0:20c:2	2006:1::20d:60ff:f	MIPv6	Care-of Test Init

Version: 6  
Traffic class: 0x00  
Flowlabel: 0x00000  
Payload length: 64  
Next header: IPv6 (0x29)  
Hop limit: 64  
Source address: 2006:151:3:0:20d:60ff:fefa:e15b  
Destination address: 2006:1::7

Internet Protocol Version 6  
Version: 6  
Traffic class: 0x00  
Flowlabel: 0x00000  
Payload length: 24  
Next header: Mobile IPv6 (0x87)  
Hop limit: 64  
Source address: 2006:1::20d:60ff:fefa:e15b  
Destination address: 2006:1::20c:29ff:feb9:8d7c

Mobile IPv6  
Payload protocol: IPv6 no next header (0x3b)  
Header length: 2 (24 bytes)  
Mobility Header Type: Home Test (3)  
Reserved: 0x00  
Checksum: 0xc585

Home Test  
Home Nonce Index: 167  
Home Init Cookie: 0x6f9ae52791247899  
Home Keygen Token: 0xc43641d828873268

0000 00 07 50 5e 79 00 00 0d 60 fa e1 5b 86 dd 60 00 ..PAY...[...]  
0010 00 00 00 40 29 40 20 06 01 51 00 03 00 00 02 0d ...@a...O.....

CoA MN1  
HA  
HoA MN1  
HoA MN2



## IPv6 Mobility Module

## 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 ← HoA MN2
- Destination address: 2006:151:3:0:20d:60ff:fefa:e15b ← 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 ... Pay...  
0010 00 00 00 18 87 3c 20 06 00 01 00 00 00 02 0c .....<..  
0020 29 ff fe b9 8d 7c 20 06 01 51 00 03 00 00 02 0d .....|.Q.....  
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 .....~.....





# Binding update

traces\_21\_05\_2005\_v2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter:  + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
14	4.915816	2006:151:3:0:20d:60ff:fe15b	2006:1::20c:29ff:f	MIPv6	Binding Update
15	5.026121	2006:151:3:0:20d:60ff:fe15b	2006:1::20c:29ff:f	MIPv6	Binding Update

Source address: 2006:151:3:0:20d:60ff:fe15b ← CoA MN1  
Destination address: 2006:1::20c:29ff:feb9:8d7c ← HoA MN2

Destination option Header  
Next header: Mobile IPv6 (0x87)  
Length: 2 (24 bytes)  
PadN: 4 bytes  
Option Type: 201 (0xc9) - Home Address option  
Option Length: 16  
Home Address: 2006:1::20d:60ff:fe15b (2006:1::20d:60ff:fe15b) ← HoA MN1

Mobile IPv6  
Payload protocol: IPv6 no next header (0x3b)  
Header length: 3 (32 bytes)  
Mobility Header Type: Binding Update (5)  
Reserved: 0x00  
Checksum: 0x15ab

Binding Update  
Sequence number: 8  
1... = Acknowledge (A) flag: Binding Acknowledgement requested  
.0... = Home Registration (H) flag: No Home Registration  
..0... = Link-Local Compatibility (L) flag: No Link-Local Address Compatibility  
...0... = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility  
Lifetime: 3 (12 seconds)

Mobility Options  
Nonce Indices  
Home nonce index: 62  
Care-of nonce index: 62  
Binding Authorization Data  
Authenticator: 02E2D2F7606C24EE854503E6

0000 00 07 50 5e 79 00 00 0d 60 fa e1 5b 86 dd 60 00 ..PAY... ..[...]  
0010 00 00 00 38 3c 40 20 06 01 51 00 03 00 00 02 0d ...8<@ . .Q.....  
0020 60 ff fe fa e1 5b 20 06 00 01 00 00 00 00 02 0c .....[ . ....  
0030 20 ff fe fa e1 5b 20 06 00 00 00 00 00 00 00 00 .....[ . ....



## Binding acknowledgement ...

The image shows a Wireshark packet capture window titled "traces\_21\_05\_2005\_v2 - Ethereal". The packet list shows two packets: packet 21 is a "Binding Update" and packet 22 is a "Binding Acknowledgement". Packet 22 is selected, and its details are shown in the packet pane. The packet is an IPv6 packet with a source address of 2006:1::7 and a destination address of 2006:151:3:0:20d:60ff:fefa:e15b. The packet is a Binding Acknowledgement message. The details pane shows the following structure:

- Frame 22 (94 bytes on wire, 94 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: 40
  - Next header: IPv6 routing (0x2b)
  - Hop limit: 61
  - Source address: 2006:1::7
  - Destination address: 2006:151:3:0:20d:60ff:fefa:e15b
- Routing Header, Type 2
  - Next header: Mobile IPv6 (0x87)
  - Length: 2 (24 bytes)
  - Type: 2
  - Segments left: 1
  - Home Address : 2006:1::20d:60ff:fefa:e15b (2006:1::20d:60ff:fefa:e15b)
- Mobile IPv6
  - Payload protocol: IPv6 no next header (0x3b)
  - Header length: 1 (16 bytes)
  - Mobility Header Type: Binding Acknowledgement (6)
  - Reserved: 0x00
  - Checksum: 0x39a9
  - Binding Acknowledgement
    - Status: Binding update accepted (0)
    - 0... .. = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
    - Sequence number: 53
    - Lifetime: 15 (60 seconds)

Annotations with arrows point to specific fields:

- HA (Home Agent) points to the Source address: 2006:1::7.
- CoA MN1 (Care-of Address Mobile Node 1) points to the Destination address: 2006:151:3:0:20d:60ff:fefa:e15b.
- HoA MN1 (Home Address Mobile Node 1) points to the Home Address: 2006:1::20d:60ff:fefa:e15b.

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 00 0d 60 fa e1 5b 00 07 50 5e 79 00 86 dd 60 00 ...[.. P^y...
0010 00 00 00 28 2b 3d 20 06 00 01 00 00 00 00 00 00 ...(+...
0020 00 00 00 00 00 07 20 06 01 51 00 03 00 00 02 0d .....Q.....
```



## Binding acknowledgement

The image shows a Wireshark packet capture window titled "traces\_21\_05\_2005\_v2 - Ethereal". The packet list shows two packets: packet 21 is a "Binding Update" and packet 22 is a "Binding Acknowledgement". Packet 22 is selected, and its details are expanded.

**Packet 22: 7.942397 2006:1::7 → 2006:151:3:0:20d:60ff:fefa:e15b MIPv6 Binding Acknowledgement**

- Internet Protocol Version 6
  - Version: 6
  - Traffic class: 0x00
  - Flowlabel: 0x00000
  - Payload length: 40
  - Next header: IPv6 routing (0x2b)
  - Hop limit: 61
  - Source address: 2006:1::7
  - Destination address: 2006:151:3:0:20d:60ff:fefa:e15b
- Routing Header, Type 2
  - Next header: Mobile IPv6 (0x87)
  - Length: 2 (24 bytes)
  - Type: 2
  - Segments left: 1
  - Home Address : 2006:1::20d:60ff:fefa:e15b (2006:1::20d:60ff:fefa:e15b)
- Mobile IPv6
  - Payload protocol: IPv6 no next header (0x3b)
  - Header length: 1 (16 bytes)
  - Mobility Header Type: Binding Acknowledgement (6)
  - Reserved: 0x00
  - Checksum: 0x39a9
  - Binding Acknowledgement
    - Status: Binding Update accepted (0)
    - 0... .. = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
    - Sequence number: 53
    - Lifetime: 15 (60 seconds)
  - Mobility options
    - PadN: 4 bytes

Annotations with arrows pointing to the packet details:

- HA (Home Agent) points to the Source address: 2006:1::7.
- CoA MN1 (Care-of Address for Mobile Node 1) points to the Destination address: 2006:151:3:0:20d:60ff:fefa:e15b.
- HoA MN1 (Home Address for Mobile Node 1) points to the Home Address: 2006:1::20d:60ff:fefa:e15b.

The packet bytes are shown at the bottom:

```
0000  00 0d 60 fa e1 5b 00 07 50 5e 79 00 86 dd 60 00  ...[.. P...
0010  00 00 00 28 2b 3d 20 06 00 01 00 00 00 00 00 00  ...(+...
0020  00 00 00 00 00 07 20 06 01 51 00 03 00 00 02 0d  ...Q...
0030  60 ff fe fa e1 5b 87 02 02 01 00 00 00 00 20 06  ....[..
```

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:60ff:fe fa:e15b	2006:151:2:0:20c:29ff:feb9:8d7c	ICMPv6	Echo request
33	9.136794	2006:151:2:0:20c:29ff:feb9:8d7c	2006:151:3:0:20d:60ff:fe fa:e15b	ICMPv6	Echo reply

▶ 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:fe fa:e15b ← CoA MN1
- Destination address: 2006:151:2:0:20c:29ff:feb9:8d7c ← CoA MN2

▼ 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) ← HoA MN2

▼ 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:fe fa:e15b (2006:1::20d:60ff:fe fa:e15b) ← HoA MN1

▼ 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 ..Pay... ..[...]

0010 00 00 00 58 2b 40 20 06 01 51 00 03 00 00 02 0d ...x+@ .Q.....

0020 60 ff fe fa e1 5b 20 06 01 51 00 02 00 00 02 0c .....[ .Q.....

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 ..... ).....|..

0050 01 02 00 00 00 00 20 06 00 01 00 00 00 00 02 0d ..... ).....|..

File: traces\_21\_05\_2005\_v2 5272 b; P: 43 D: 43 M: 0



## Icmp reply 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	9.136692	2006:151:3:0:20d:60ff:fefb:8d7c	2006:151:2:0:20c:29ff:feb9:e15b	ICMPv6	Echo request
33	9.136794	2006:151:2:0:20c:29ff:feb9:e15b	2006:151:3:0:20d:60ff:fefb:8d7c	ICMPv6	Echo reply

Frame 33 (142 bytes on wire, 142 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: 88
- Next header: IPv6 routing (0x2b)
- Hop limit: 60
- Source address: 2006:151:2:0:20c:29ff:feb9:8d7c ← CoA MN2
- Destination address: 2006:151:3:0:20d:60ff:fefb:e15b ← CoA MN1

Routing Header, Type 2

- Next header: IPv6 destination option (0x3c)
- Length: 2 (24 bytes)
- Type: 2
- Segments left: 1
- Home Address : 2006:1::20d:60ff:fefb:e15b (2006:1::20d:60ff:fefb:e15b) ← HoA MN1

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::20c:29ff:feb9:8d7c (2006:1::20c:29ff:feb9:8d7c) ← HoA MN2

Internet Control Message Protocol v6

- Type: 129 (Echo reply)
- Code: 0
- Checksum: 0x97e4 (incorrect, should be 0x953f)

0000 00 0d 60 fa e1 5b 00 07 50 5e 79 00 86 dd 60 00 ...[..] Pay...  
0010 00 00 00 58 2b 3c 20 06 01 51 00 02 00 00 02 0c ...X< . .Q.....  
0020 29 ff fe b9 8d 7c 20 06 01 51 00 03 00 00 02 0d )....| . .Q.....  
0030 60 ff fe fa e1 5b 3c 02 02 01 00 00 00 00 20 06 .....[< .....



# Icmp reply 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
33	9.136794	2006:151:2:0:20c:2	2006:151:3:0:20d:6	ICMPv6	Echo reply
34	9.441138	fe80::20d:60ff:fe5	fe80::207:50ff:fe5	ICMPv6	Neighbor solicitation

Version: 6  
Traffic class: 0x00  
Flowlabel: 0x00000  
Payload length: 88  
Next header: IPv6 routing (0x2b)  
Hop limit: 60  
Source address: 2006:151:2:0:20c:29ff:feb9:8d7c  
Destination address: 2006:151:3:0:20d:60ff:fe5a:e15b

CoA MN1  
CoA MN2

Routing Header, Type 2  
Next header: IPv6 destination option (0x3c)  
Length: 2 (24 bytes)  
Type: 2  
Segments left: 1  
Home Address : 2006:1::20d:60ff:fe5a:e15b (2006:1::20d:60ff:fe5a:e15b)

HoA MN2

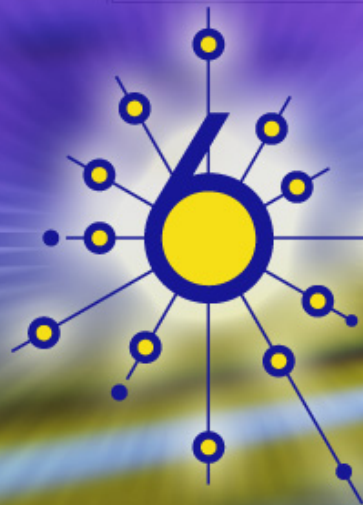
Destination Option Header  
Next header: ICMPv6 (0x3a)  
Length: 2 (24 bytes)  
PadN: 4 bytes  
option Type: 201 (0xc9) - Home Address Option  
option Length : 16  
Home Address : 2006:1::20c:29ff:feb9:8d7c (2006:1::20c:29ff:feb9:8d7c)

HoA MN1

Internet Control Message Protocol v6  
Type: 129 (Echo reply)  
Code: 0  
Checksum: 0x97e4 (incorrect, should be 0x953f)  
ID: 0x0000  
Sequence: 0x0062  
Data (32 bytes)

0000 00 0d 60 fa e1 5b 00 07 50 5e 79 00 86 dd 60 00 ..[... Pay...  
0010 00 00 00 58 2b 3c 20 06 01 51 00 02 00 00 02 0c ...X+<...Q.....  
0020 29 ff fe b9 8d 7c 20 06 01 51 00 03 00 00 02 0d ).....Q.....  
0030 60 ff fe fa e1 5b 3c 02 02 01 00 00 00 00 20 06 .....f<.....





deploy

Reference Slides

IPv6 Mobility Module



## IPv6 Mobility Module

## Direct routing

105 29.467988 2006:151:3:0:20d:60ff:fefa:e15b 2006:151:2:0:20c:29ff:feb9:8d7c ICMPv6 Echo request

▶ Frame 105 (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

← CoA MN1  
← CoA MN2

▼ 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: 0x8239 (incorrect, should be 0x7f94)  
ID: 0x0000  
Sequence: 0x170d  
Data (32 bytes)

0020 60 ff fe fa e1 5b 20 06 01 51 00 02 00 00 02 0c .....Q.....  
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 .....). ....|:  
0050 01 02 00 00 00 00 00 06 00 01 00 00 00 00 02 0d .....). ....|:

# Direct routing

106 29.474610 2006:151:2:0:20c:29ff:feb9:8d7c 2006:151:3:0:20d:60ff:fefa:e15b ICMPv6 Echo reply

Frame 106 (142 bytes on wire, 142 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: 88
- Next header: IPv6 routing (0x2b)
- Hop limit: 60
- Source address: 2006:151:2:0:20c:29ff:feb9:8d7c
- Destination address: 2006:151:3:0:20d:60ff:fefa:e15b

Routing Header, Type 2

- Next header: IPv6 destination option (0x3c)
- Length: 2 (24 bytes)
- Type: 2
- Segments left: 1
- Home Address : 2006:1::20d:60ff:fefa:e15b (2006:1::20d:60ff:fefa:e15b)

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::20c:29ff:feb9:8d7c (2006:1::20c:29ff:feb9:8d7c)

Internet Control Message Protocol v6

- Type: 129 (Echo reply)
- Code: 0
- Checksum: 0x8139 (incorrect, should be 0x7e94)
- ID: 0x0000
- Sequence: 0x170d
- Data (32 bytes)

CoA MN2  
CoA MN1

0000 00 0d 60 fa e1 5b 00 07 50 5e 79 00 86 dd 60 00 ..[..[.. Pay...  
0010 00 00 00 58 2b 3c 20 06 01 51 00 02 00 00 02 0c ...X< . .Q.....  
0020 50 ff fe b9 8d 7c 20 06 01 51 00 02 00 00 02 0d .....



## HA with ACL

Configuration 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

!

CoA MN1

CoA MN2

[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

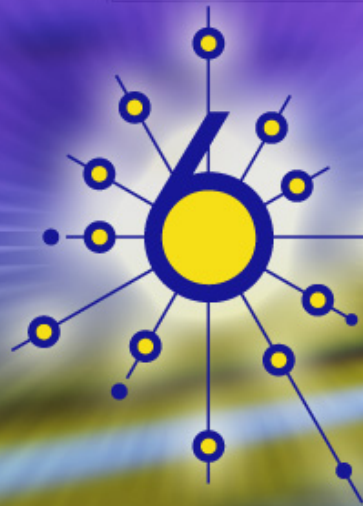
deny ipv6 host 2006:151:2:0:20C:29FF:FEB9:8D7C host  
2006:151:3:0:20D:60FF:FEFA:E15B sequence 20

permit ipv6 any any (162 matches) sequence 30

R7#

R7#





deploy

NEMO NETwork MObility

IPv6 Mobility Module



## What is NEMO?

“The NEMO Working Group is concerned with managing the mobility of an entire network, which changes, as a unit, its point of attachment to the Internet and thus its reachability in the topology. The mobile network includes one or more mobile routers (MRs) which connect it to the global Internet.

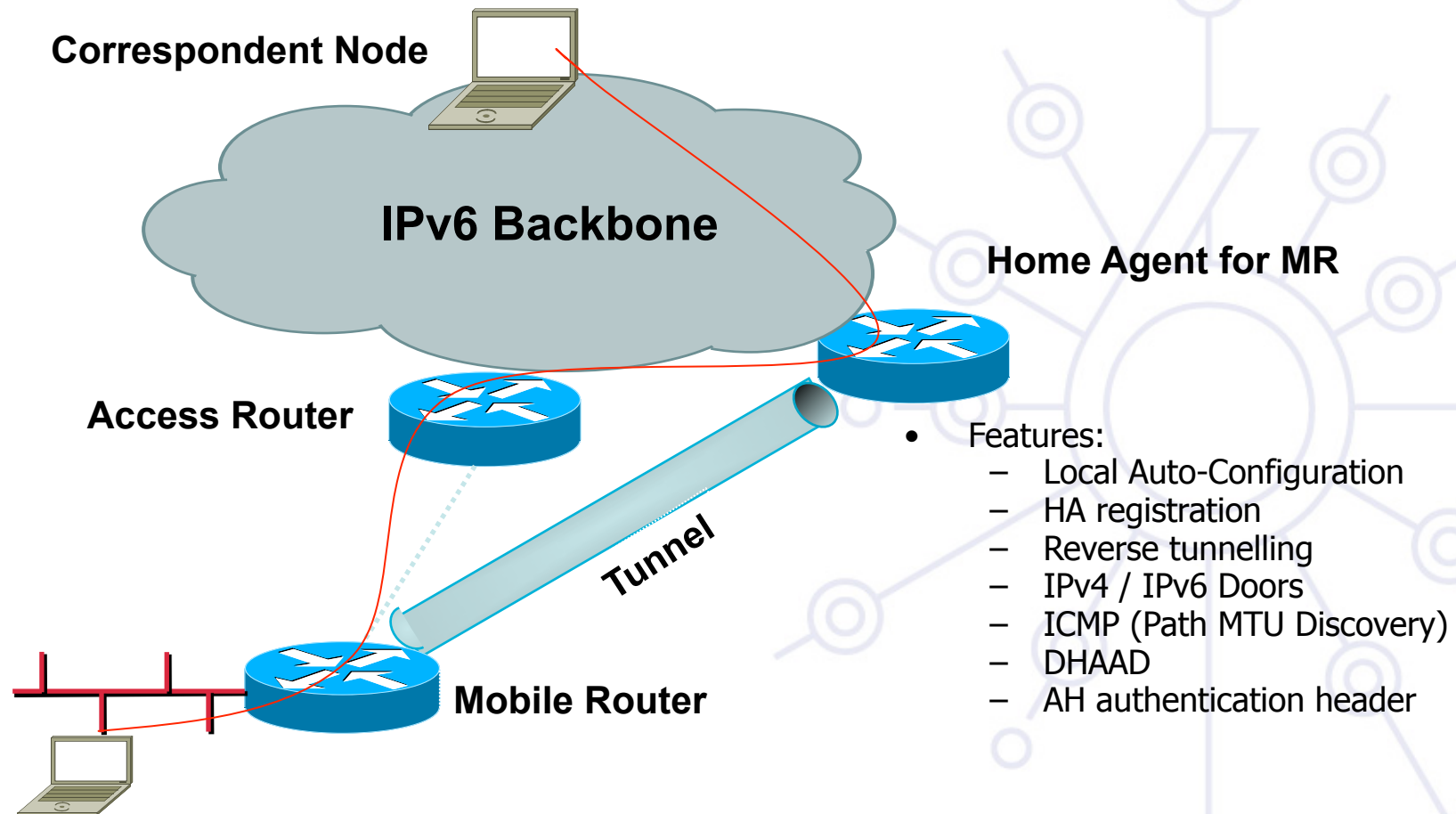
A mobile network is assumed to be a leaf network, i.e. it will not carry transit traffic. However, it could be multihomed, either with a single MR that has multiple attachments to the internet, or by using multiple MRs that attach the mobile network to the Internet.”

Network Mobility (nemo) IETF Working Group Charter

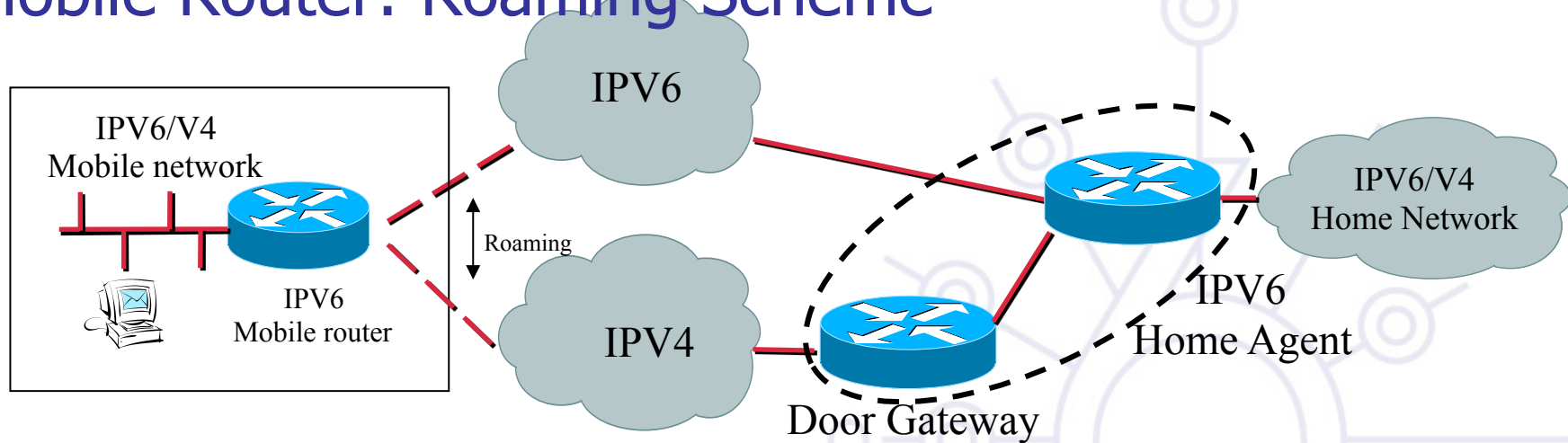
<http://www.ietf.org/html.charters/nemo-charter.html>



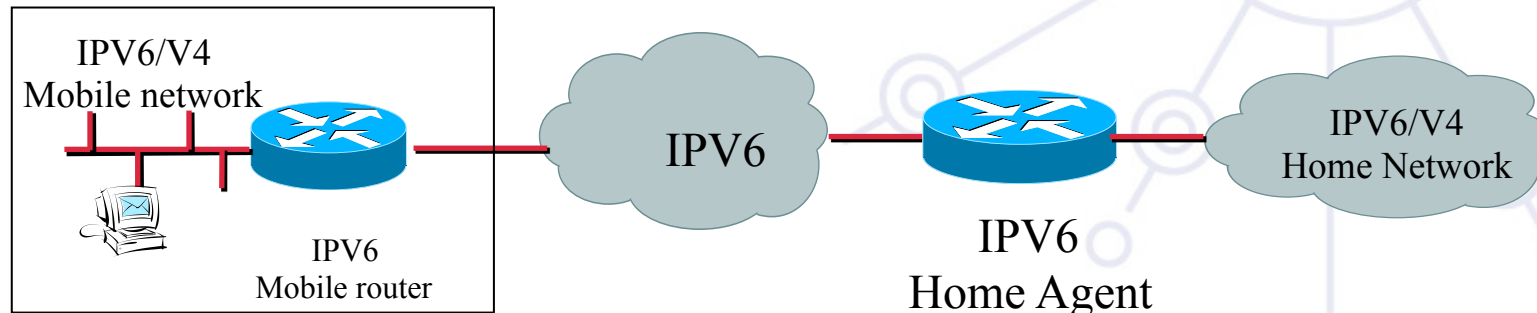
# Mobile Router IPv6: NEMO Basic



## Mobile Router: Roaming Scheme



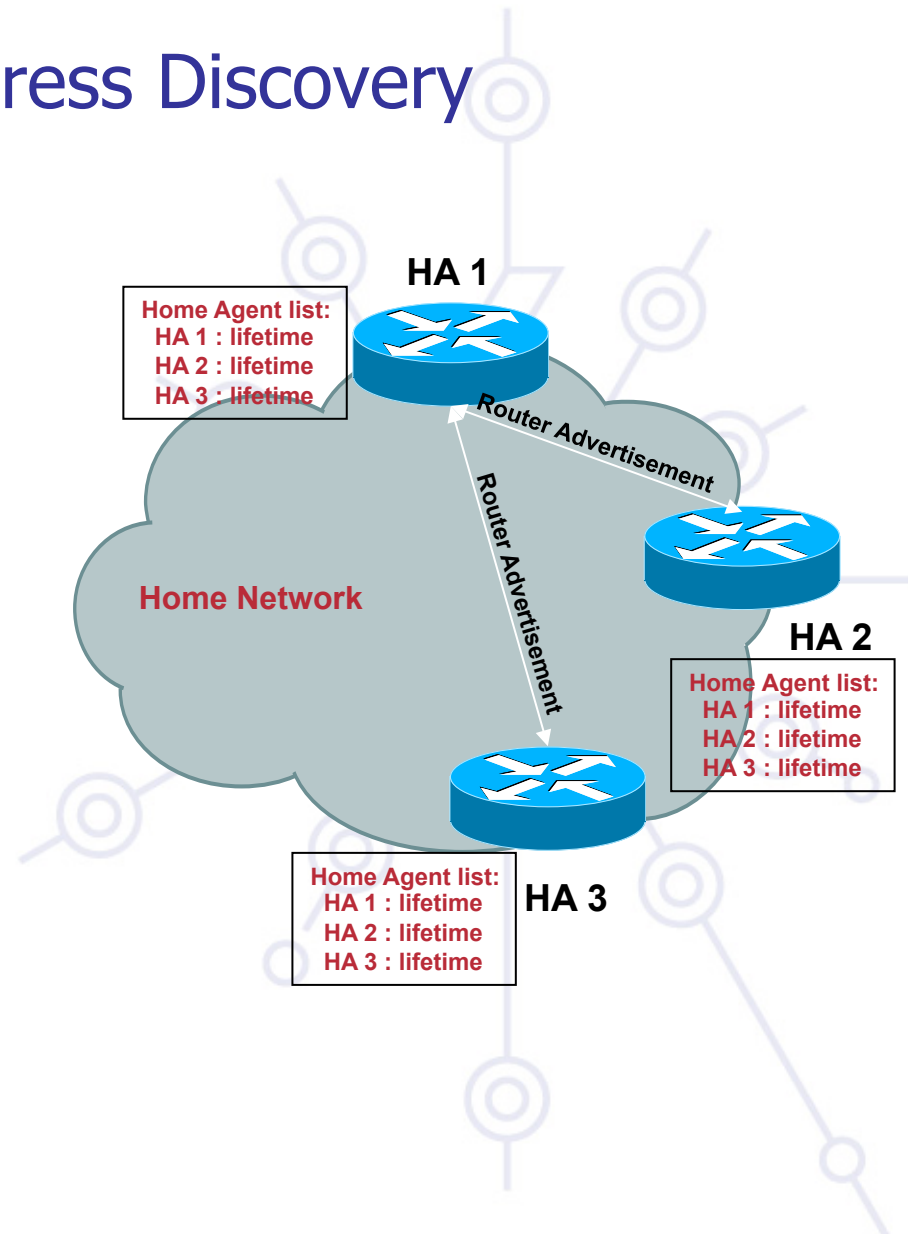
Mobile IPv6 router roaming into a V4 or V6 network



Ideal topology

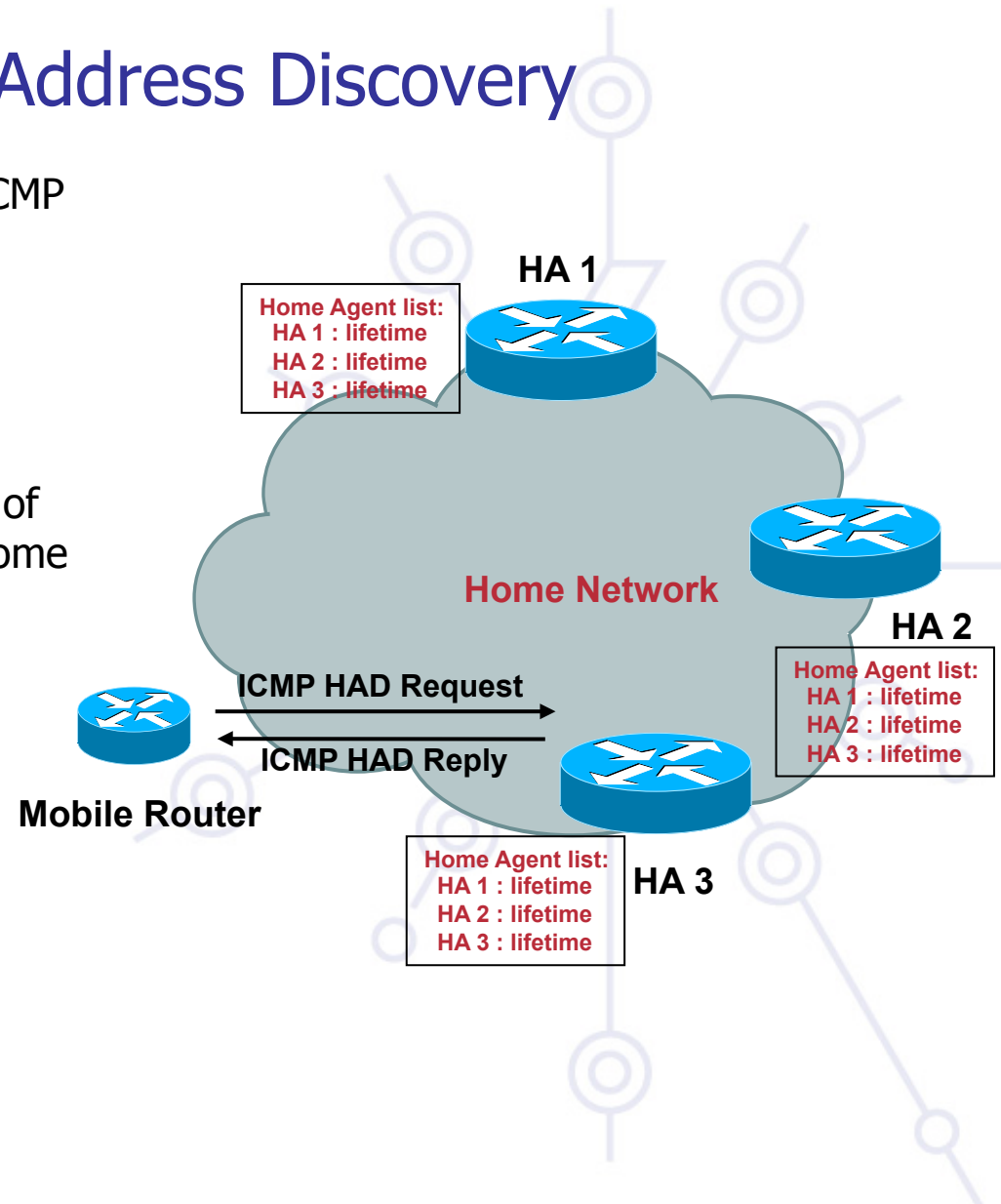
# Dynamic Home Agent Address Discovery

- Step 1: Each Home Agent receives Router Advertisement from all the other HAs on the Home Network using standard Neighbor Discovery protocol.
- Step2: Each Home Agent maintains an ordered list of the Current Home Agents with their lifetime and preference.



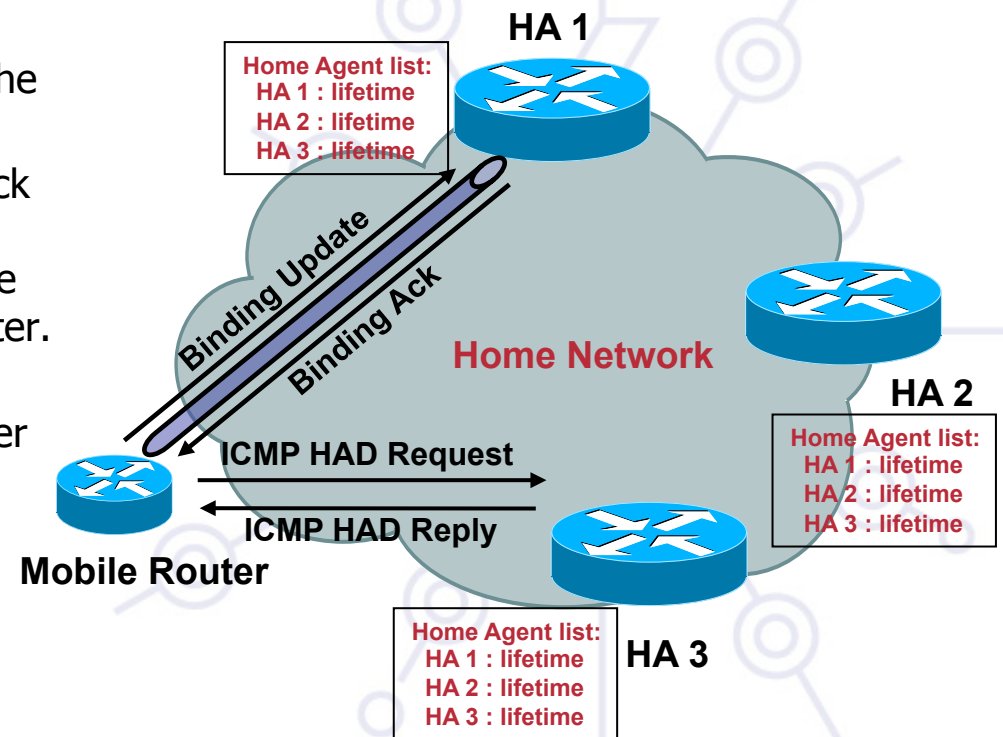
# Dynamic Home Agent Address Discovery

- Step 3: The Mobile Router send a ICMP Home Agent Discovery Request message to the Mobile IPv6 Home-Agents Anycast address.
- Step 4: The first HA to receive the message reply with an ICMP Home Agent Discovery Reply with the list of all the Global IP addresses of the Home Agents in the order of preference.



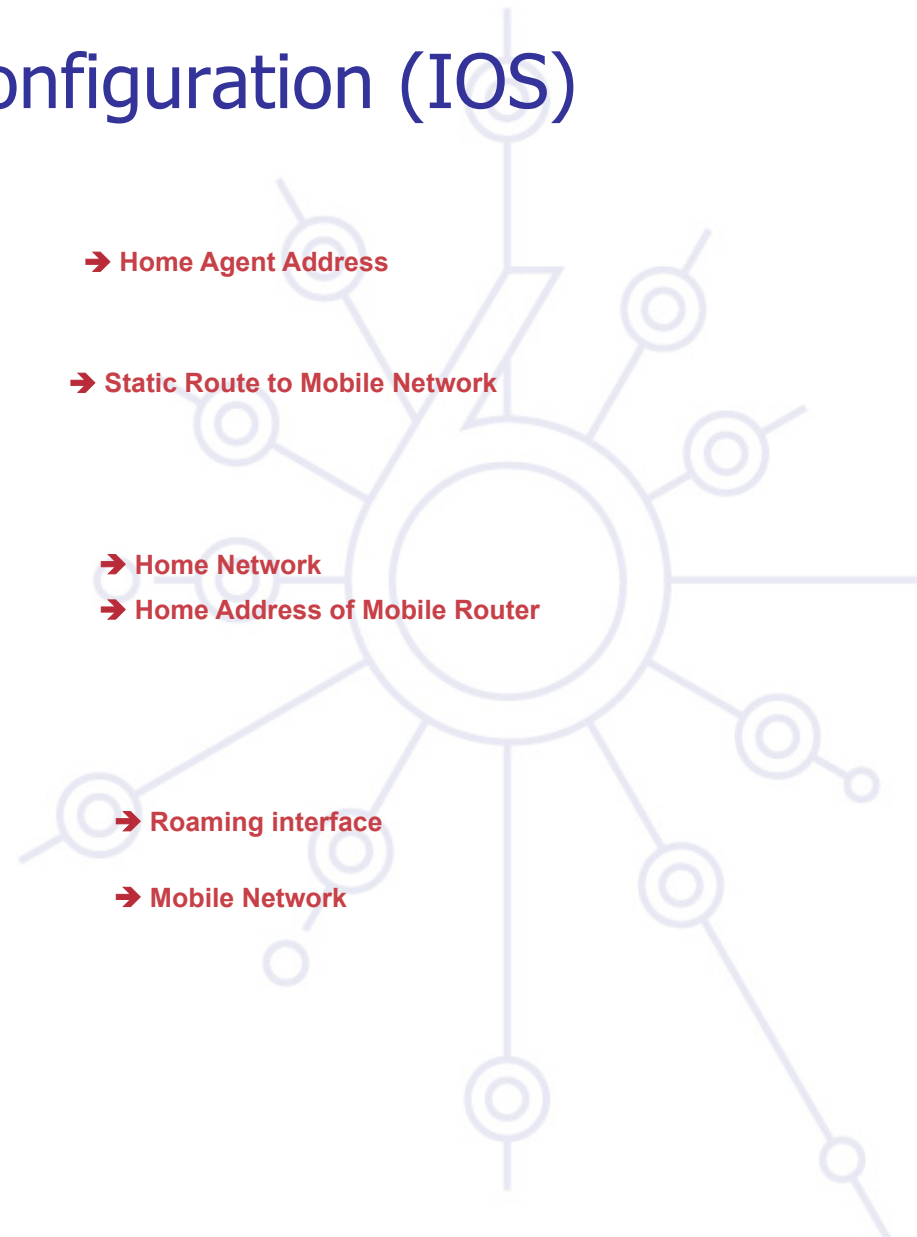
# Dynamic Home Agent Address Discovery

- Step 5: The Mobile Router having acquired a Care Of Address by auto-configuration sends a Binding Update message to the first Home Agent in the list.
- Step 6: The Home Agent answers back with a Binding Acknowledgment message. It updates its Binding Cache table with the CoA of the Mobile Router.
- Step 7: A bidirectional tunnel is established between the Mobile Router and the Home Agent.

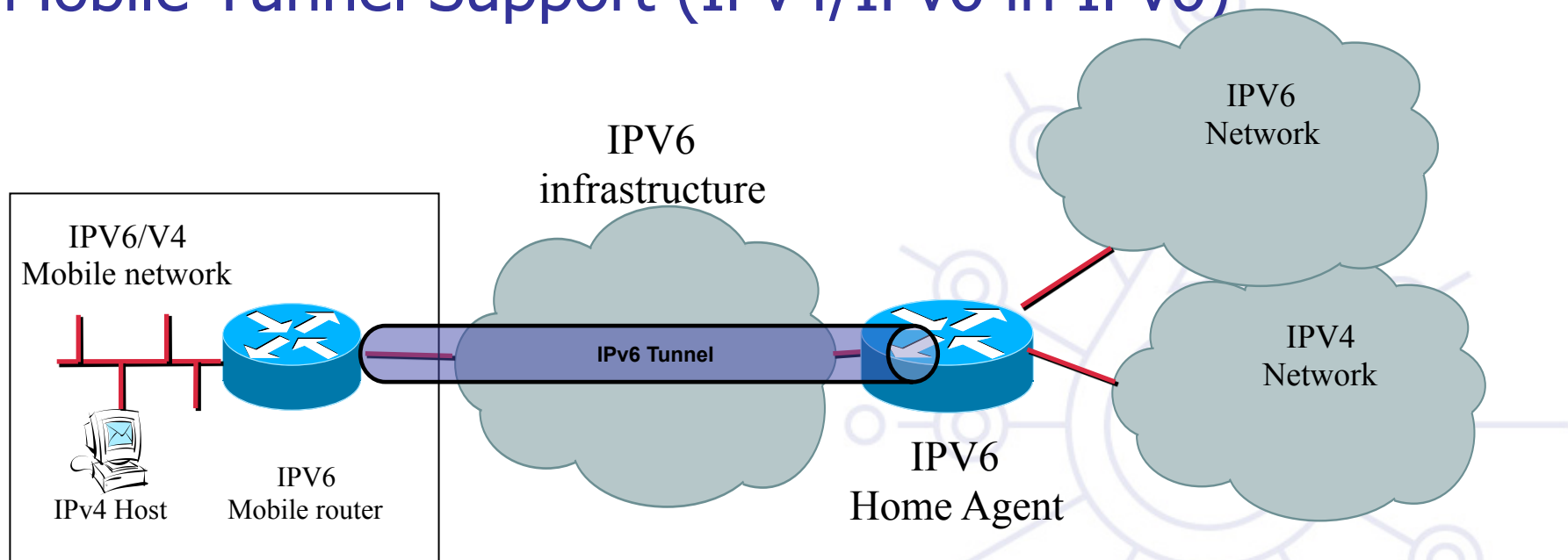


# Mobile Network Sample Configuration (IOS)

- Home Agent configuration:
  - interface Ethernet1
    - ipv6 address CA5A:4::BB4/64
    - ipv6 enable
    - ipv6 mobile home-agent run
  - ipv6 route D093::/64 CA5A:4::9
- Mobile Router Configuration:
  - ipv6 unicast-routing
  - ipv6 mobile router
    - home-network CA5A:4::BB4/64
    - home-address home-network ::9
  - interface FastEthernet0/1
    - ipv6 address autoconfig
    - ipv6 enable
    - ipv6 nd suppress-ra
    - ipv6 mobile router-service roam
  - interface FastEthernet1/0
    - ipv6 address D093::1/64
    - ipv6 enable



## Mobile Tunnel Support (IPv4/IPv6 in IPv6)

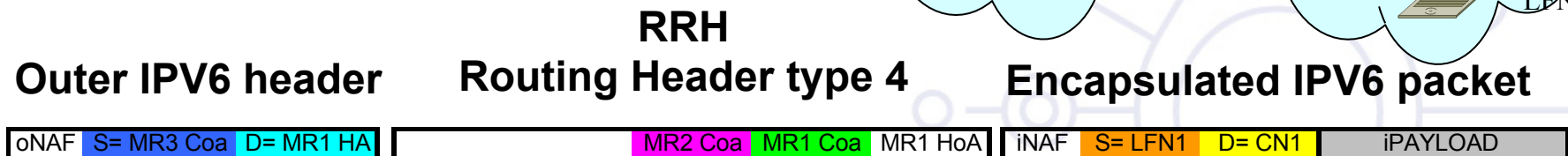
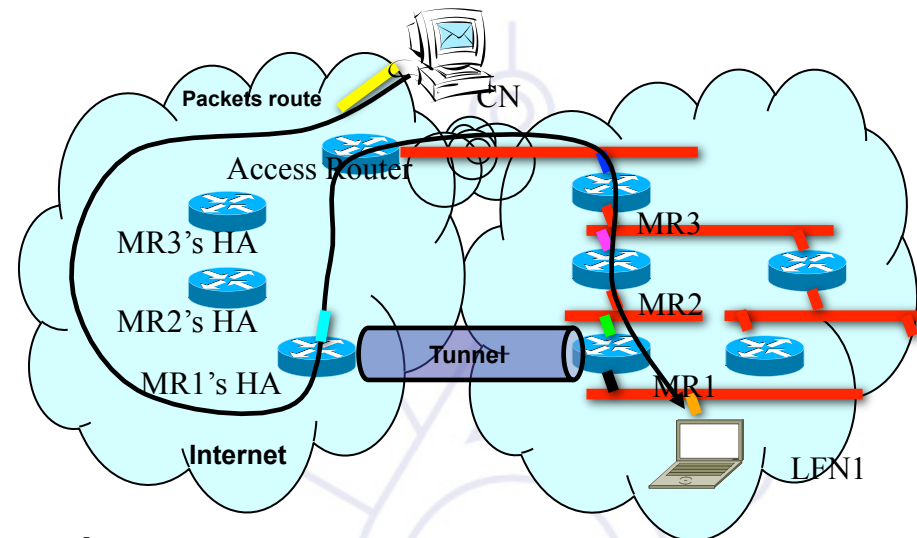


- Configuration of IPv6 tunnel between the Mobile Router and its Home Agent.
- Both IPv4 and IPv6 traffics can go thru this mobile tunnel
- The mobility being handled at the IPv6 level.



# Reverse Routing Header

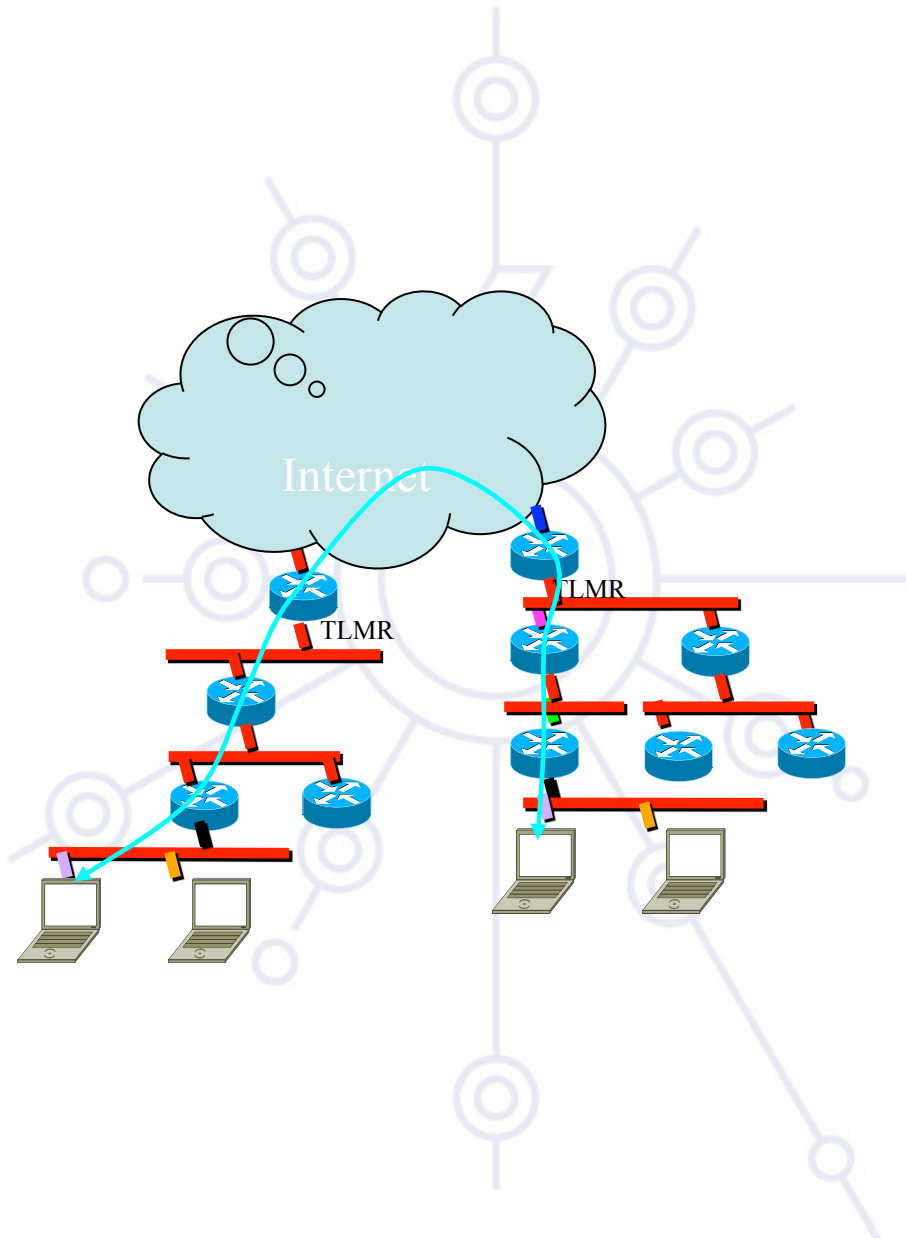
- **Routing Header: type 4**



- Works with plain V6 hosts on both ends
- Home Equivalent Privacy option via HA
- First MR or MN builds a tunnel with RRH
- Next MRs add the source to the RRH and overwrite source with their COA
- A combination of IP Routing in Infrastructure and of On Demand Source Route in the mobile cloud to adapt faster to topology changes

# Tree Discovery

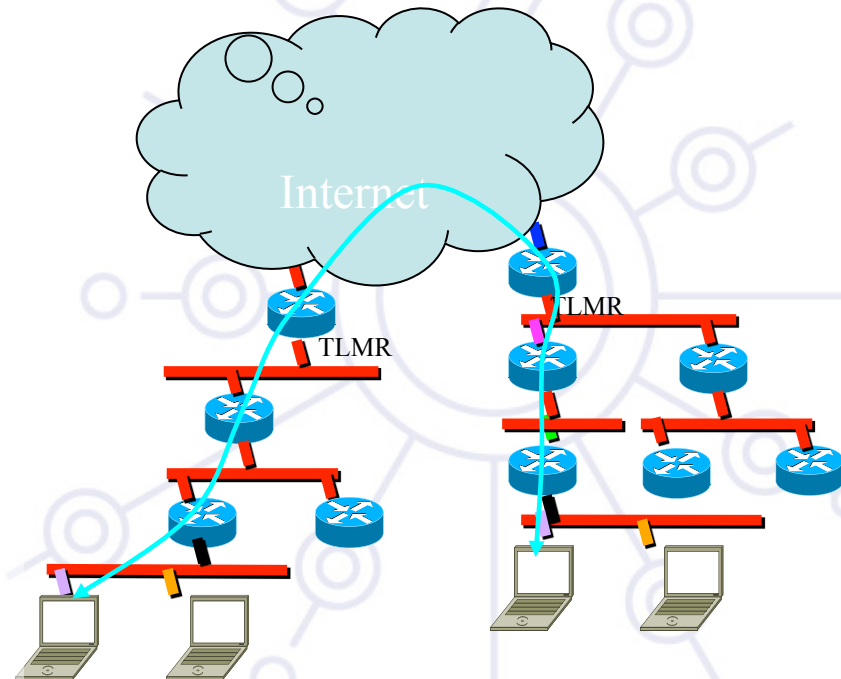
- Each Mobile router has only one COA (MIPv6)
- Each Mobile Router attaches to another one following rules that force Tree topology
  - Based on autonomous decision of each Mobile router
  - Based on Loop avoidance mechanism



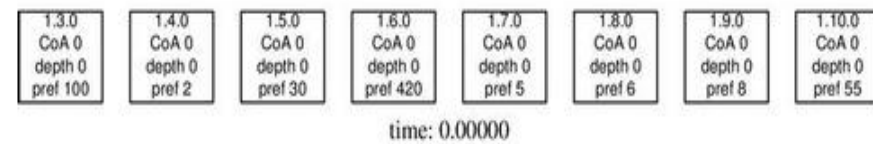
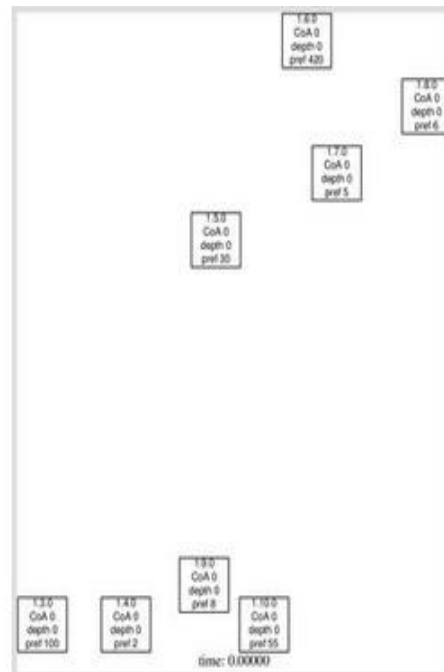
- ```

0                               1                               2                               3
0 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+
|          Type            | Length = 5   | Tree_Prefer. | TreeDepth
+-+
|F|H| Reserved    | Bandwidth      | DelayTime
+-+
| MRPreference     | BootTimeRandom
+-+
|                                     PathCRC
+-+
|
+
|
+
Tree TLMR Identifier
|
+
|
+
Tree Group
|
+

```

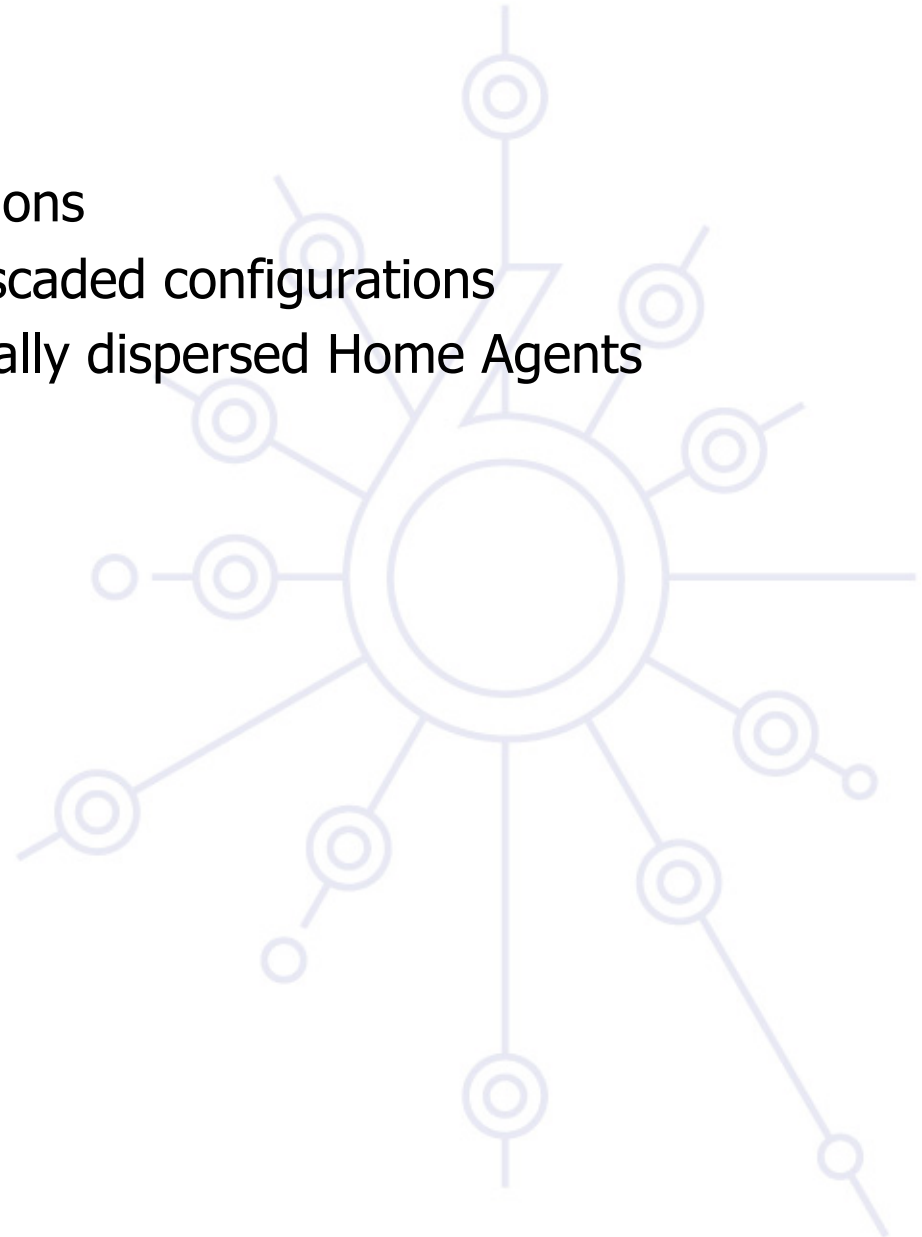


# Tree Discovery



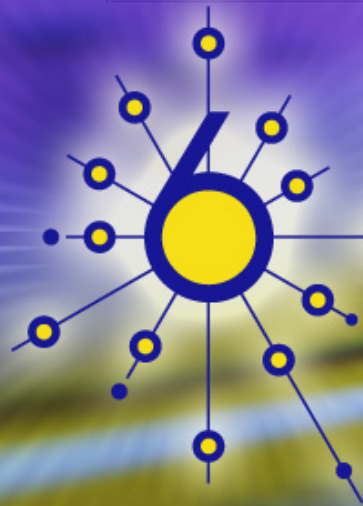
## Summary

- Support for IETF NEMO specifications
- Mobile Router Trees allow for cascaded configurations
- Dynamic HA allow for Geographically dispersed Home Agents



## References

- IETF NEMO Working Group
  - <http://www.ietf.org/html.charters/nemo-charter.html>
- IETF Mobility for IPv6 Working Group
  - <http://www.ietf.org/html.charters/mip6-charter.html>
- Selected NEMO Drafts:
  - <http://www.ietf.org/internet-drafts/draft-ietf-nemo-basic-support-03.txt>
  - <http://www.ietf.org/internet-drafts/draft-thubert-nemo-basic-usages-01.txt>
  - <http://www.ietf.org/internet-drafts/draft-thubert-nemo-ro-taxonomy-02.txt>
  - <http://www.ietf.org/internet-drafts/draft-thubert-tree-discovery-00.txt>
  - <http://www.ietf.org/internet-drafts/draft-thubert-nemo-reverse-routing-header-05.txt>



deploy

Mobile Ad-Hoc Network routing

IPv6 Mobility Module

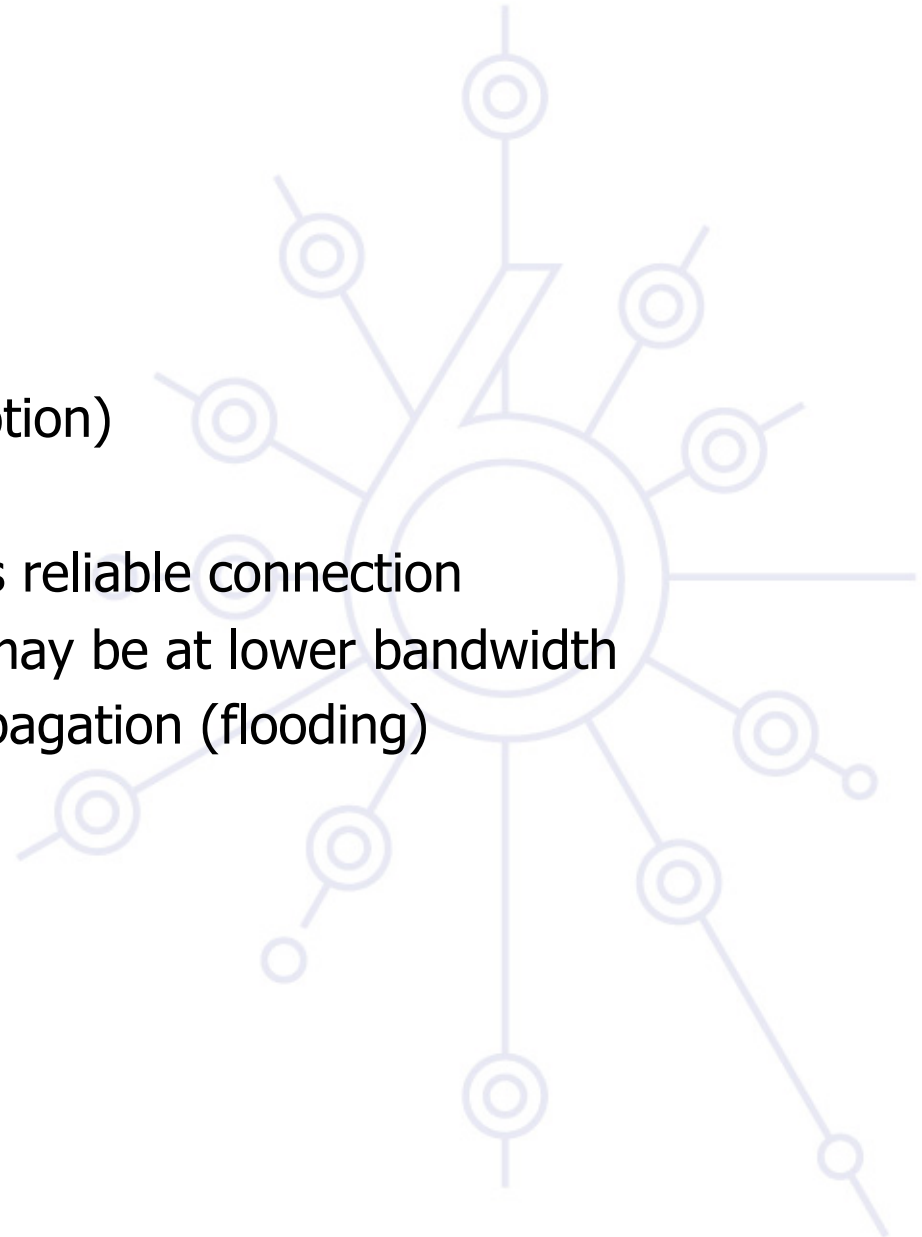


## Characteristics of MANETs (RFC2501)

- Dynamic topologies
  - Nodes are free to move arbitrarily. Network topology may change randomly and rapidly at unpredictable times.
- Bandwidth-constrained, variable capacity links
  - Wireless links have significantly lower capacity than their hardwired counterparts. After accounting for the effects of multiple access, fading, noise, and interference conditions, etc.; the actual throughput is often much less than a radio's maximum transmission rate.
- Energy-constrained operation
  - Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. Network & routing optimization must be cognizant of energy conservation.
- Limited physical security
  - Mobile wireless networks are more prone to physical security threats (i.e. eavesdropping, spoofing, and DOS attacks) than hardwired networks.

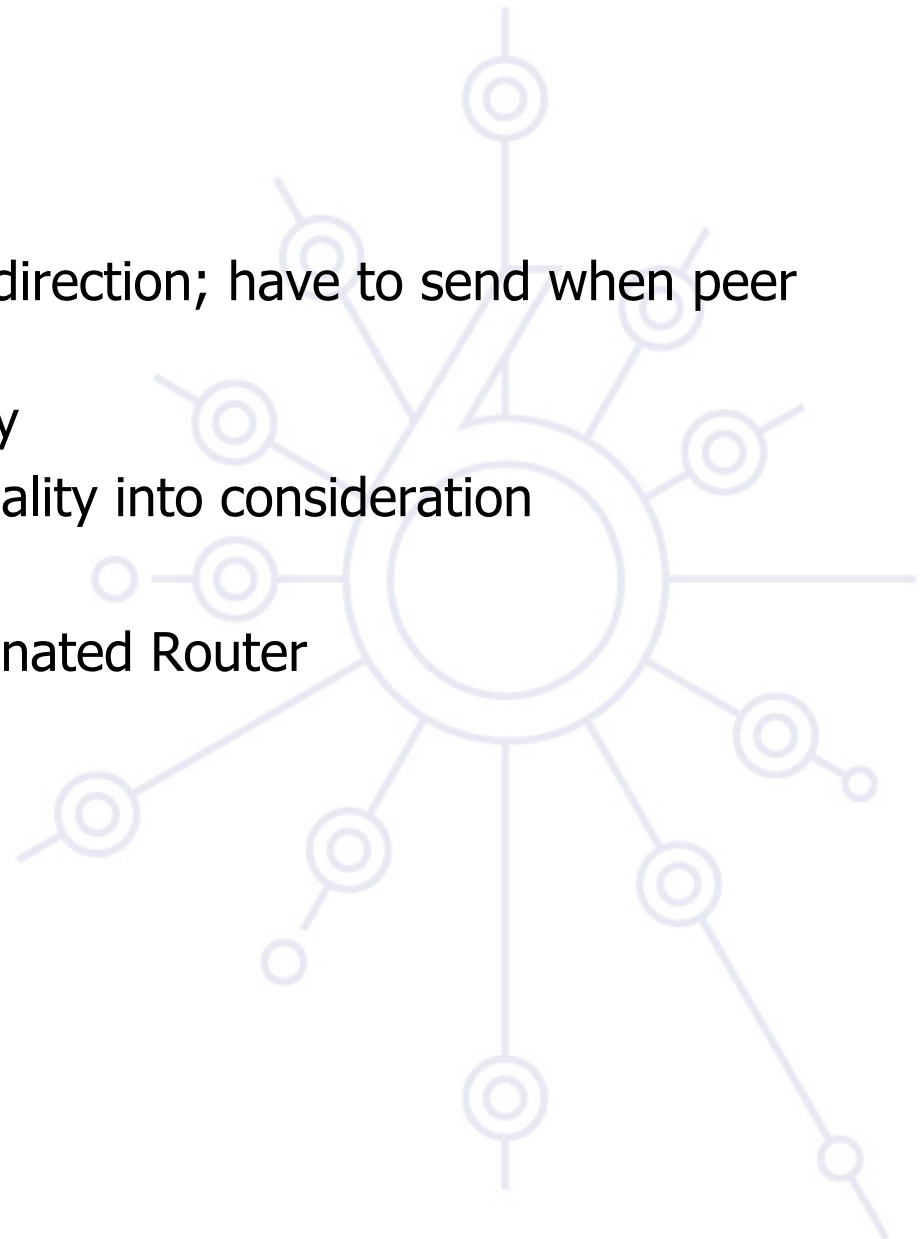
## Dynamic Topology

- Random interconnection
  - Minimal or no engineering
  - Low bandwidth links
- Constant or frequent change (motion)
  - Neighbor changes;
    - New neighbor may be less reliable connection
    - More reliable connection may be at lower bandwidth
    - Resulting information propagation (flooding)

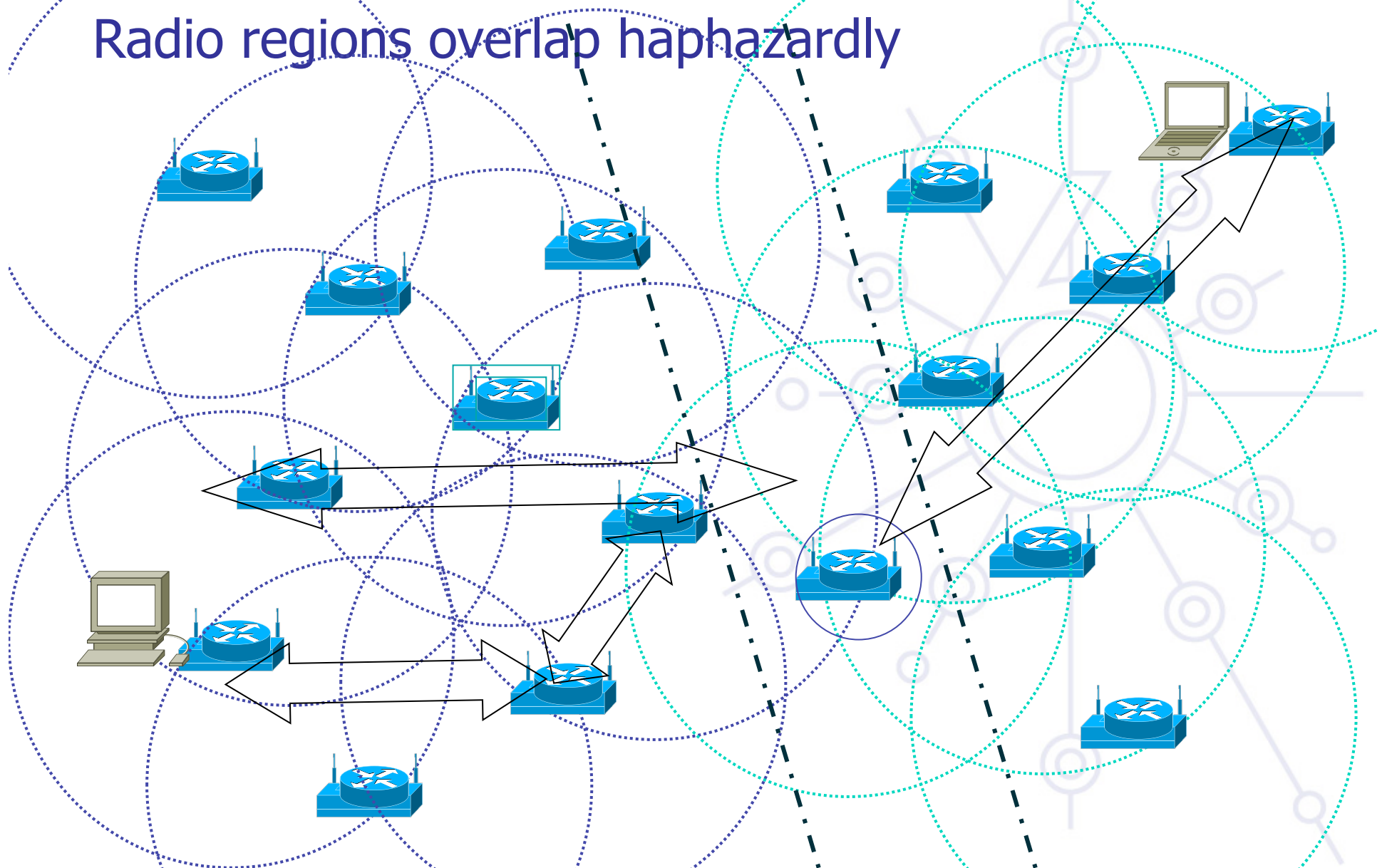


## Radio Characteristics

- Directional Antenna
  - Some radios send in a stated direction; have to send when peer is listening in that direction
- Varying signal strength, link quality
  - Route cost *should* take link quality into consideration
- Overlapping connectivity
  - No unifying concept like Designated Router
  - Haphazard connections



# Radio regions overlap haphazardly

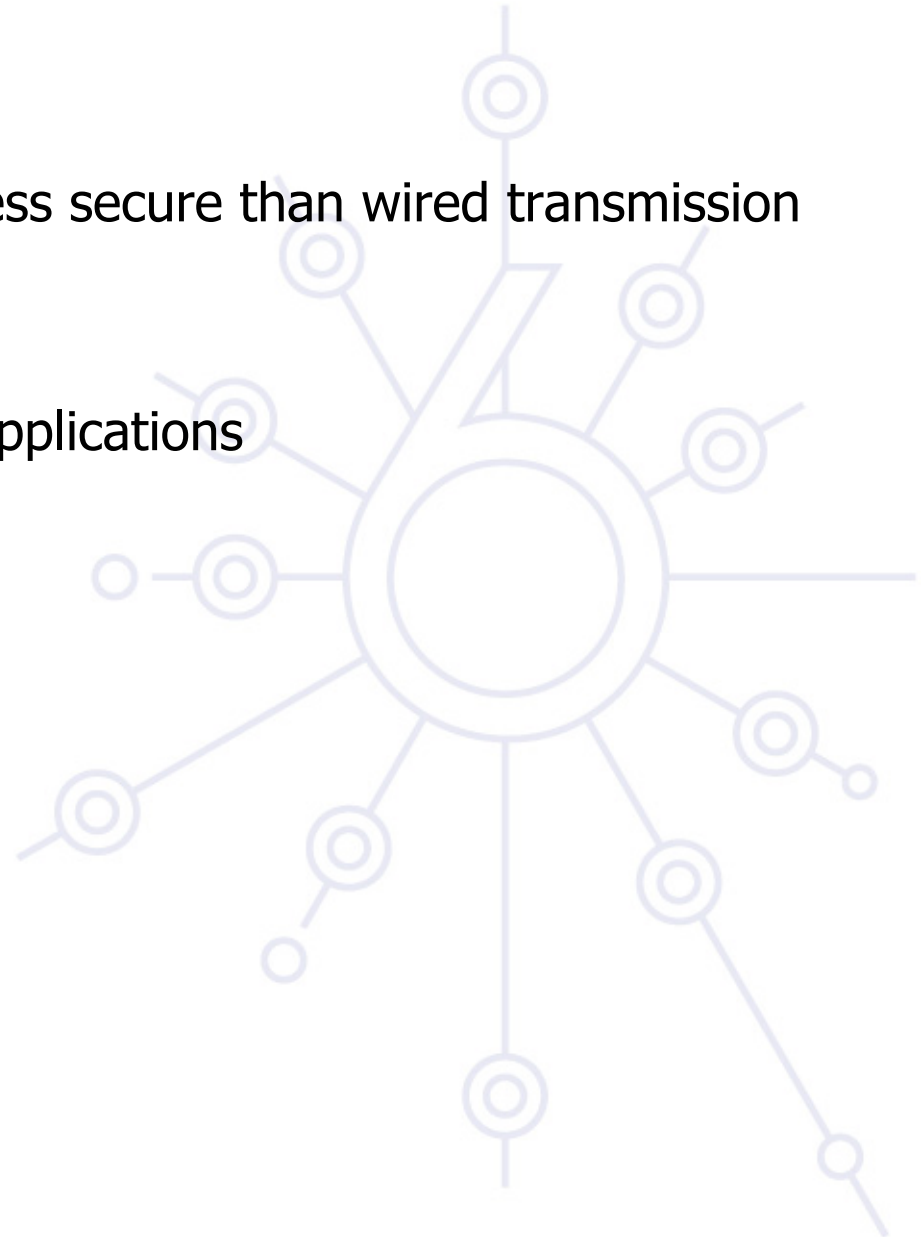


## Energy-constrained Operation

- Some nodes (e.g. hand-held, or laptop devices) are powered by batteries
- Others (e.g. vehicle-based) may be able to rely on a “constant” power source
- Battery drain will influence a node’s ability to participate as a routing next-hop
  - You could suspend a node if it hasn’t participated in a MANET for some period of time, but then how do you wake it up when appropriate?
  - Route cost *should* take energy constraints into consideration
- Inefficient data link, MAC, or network layer design can result in additional packets being transmitted, hence, more battery power being consumed.

## Limited Physical Security

- Radio transmission is inherently less secure than wired transmission
  - Easier to snoop or eavesdrop
- More susceptible to DoS attacks
- Detection avoidance for military applications



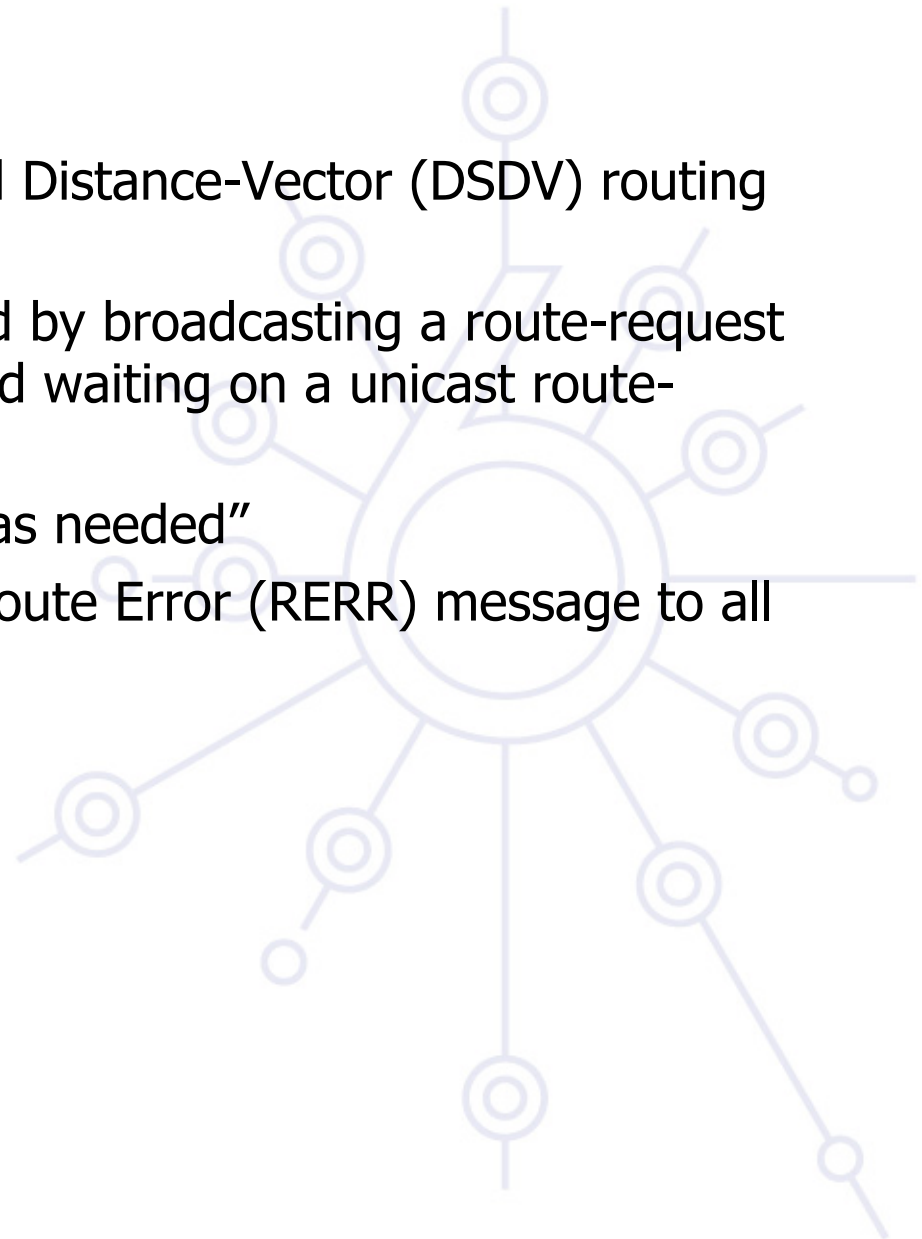
## MANET Protocols in IETF

- Numerous protocols have been proposed over the years; four remain active in the MANET IETF working group
- Protocols fall into two categories: Proactive and Reactive
  - Proactive – Protocols that actively maintain network topology whether a specific route has been requested or not
  - Reactive – Protocols that defer route discovery until it is needed
- Proactive
  - Optimized Link State Routing (OLSR – RFC3626)
  - Topology Dissemination Based on Reverse-Path Forwarding (TBRPF – RFC3684)
- Reactive
  - Ad Hoc On Demand Distance Vector Routing (AODV – RFC3561)
  - Dynamic Source Routing Protocol for Ad Hoc Networks (DSR – Internet Draft, no RFC number assigned, last updated 15 April 2003)



## AODV

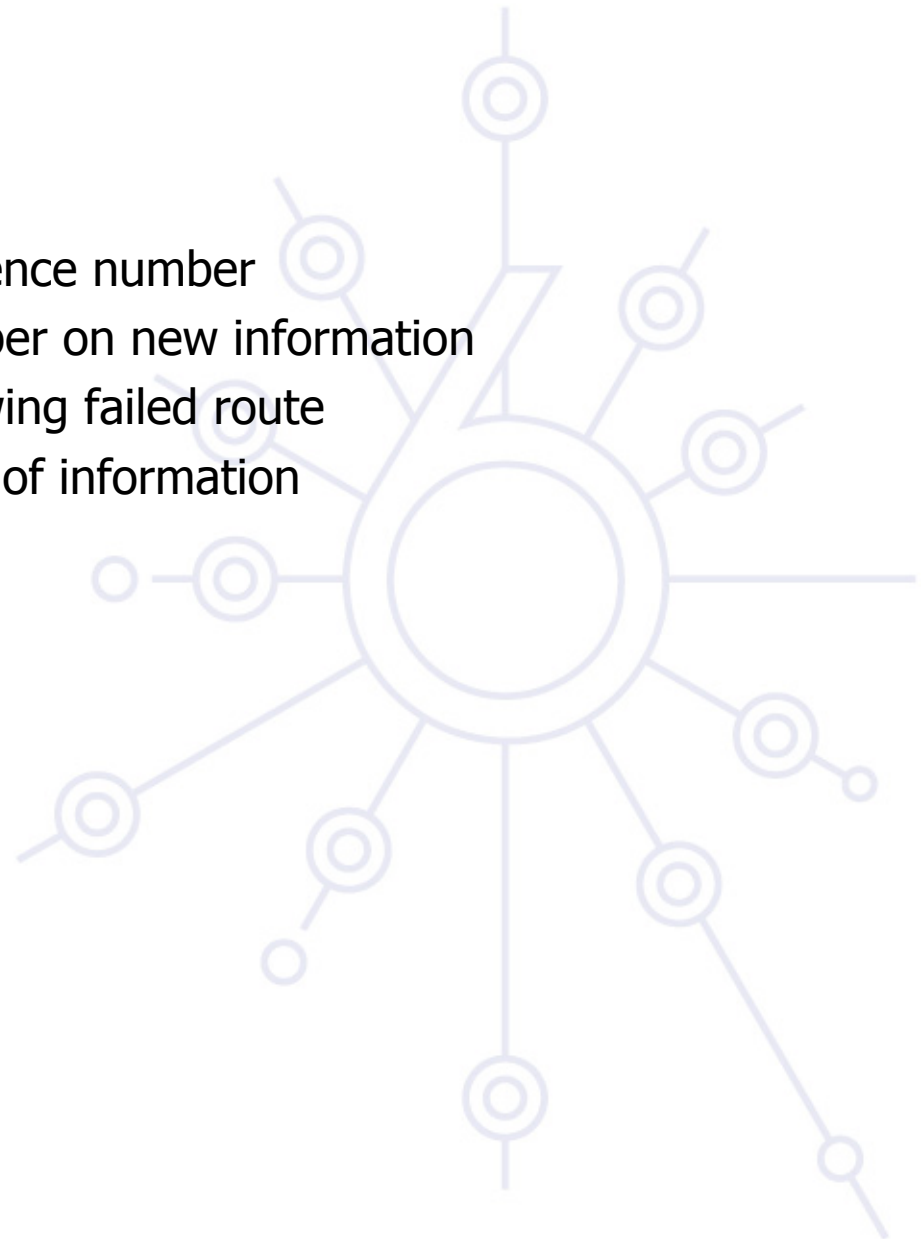
- Based on Destination-Sequenced Distance-Vector (DSDV) routing algorithm
- Routes are discovered as-needed by broadcasting a route-request (RREQ) through the network, and waiting on a unicast route-reply (RREP)
- Routes are maintained “as long as needed”
- Route errors are signaled by a Route Error (RERR) message to all effected destinations



- # Distance Vector (AODV)
- Nodes is found by sending locality  
all, grows with failure  
larger than the locality
- sary  
outing node if possible to  
e  
te
- 
- The diagram illustrates a network topology for Distance Vector (AODV) routing. It features three laptops labeled A, B, and C, and ten routers labeled d, e, f, g, h, i, j, k, l, and m. The routers are arranged in a grid-like structure. Laptop A is at the bottom left, Laptop B is at the bottom right, and Laptop C is at the top center. The routers are connected by blue dashed lines representing network links. Purple dashed lines represent the local neighborhood of each node, which grows as the network changes. Arrows indicate the flow of information or data between nodes.

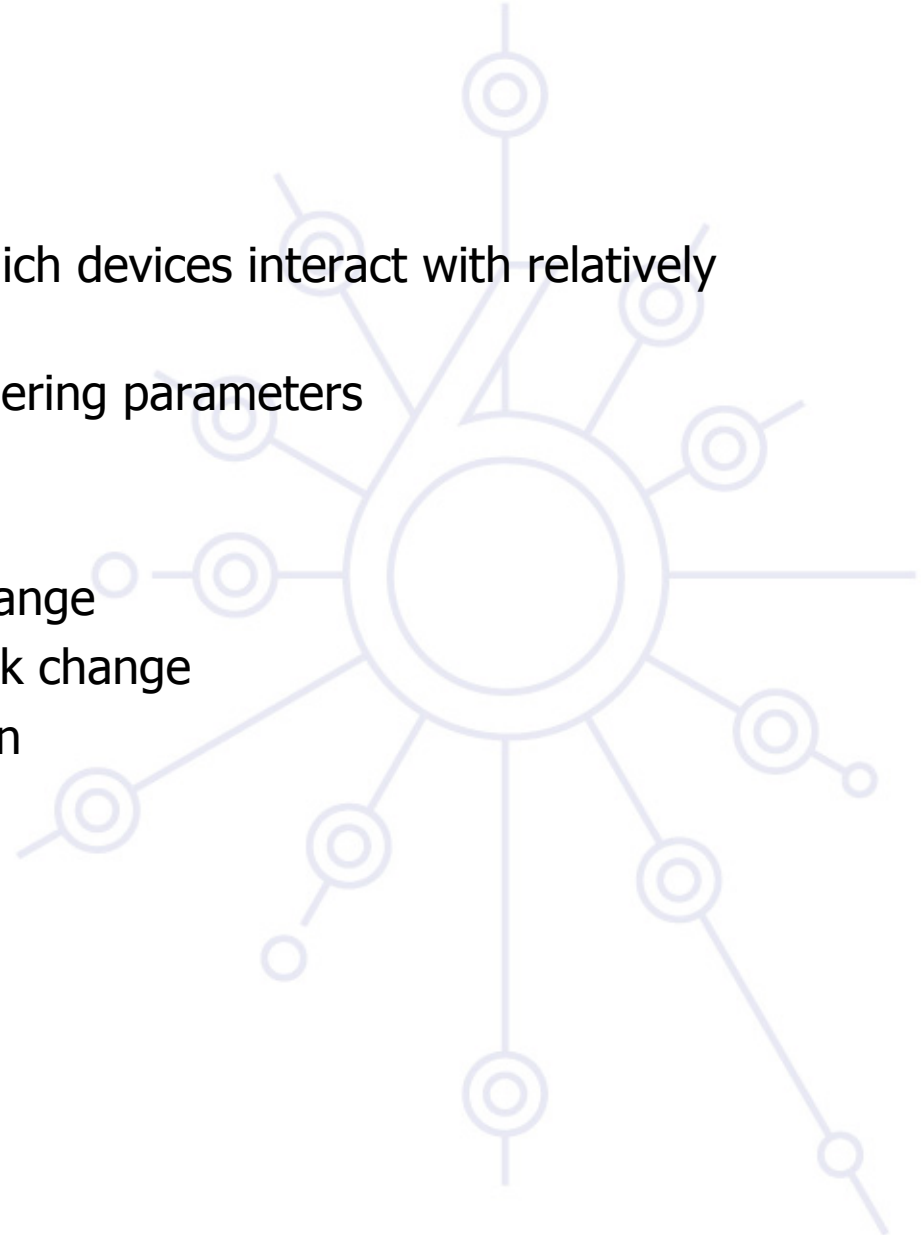
## AODV Continued

- Each route is to a router
- Each route advertisement has a sequence number
  - Originator bumps sequence number on new information
  - Others bump only when withdrawing failed route
- Effect: we always know relative order of information
  - No count to infinity
  - No looping routes



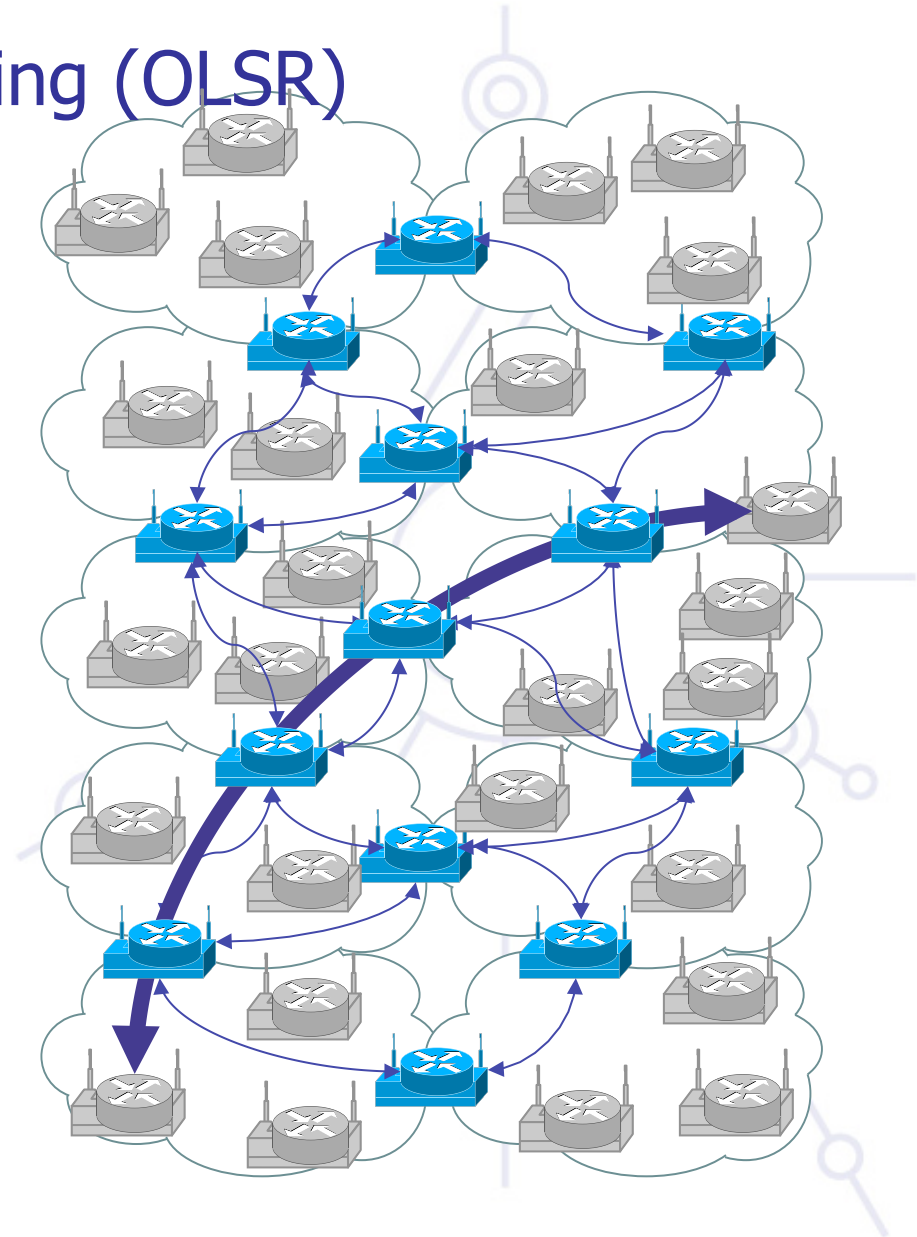
## AODV Analysis

- Opportunities
  - Perhaps good in application in which devices interact with relatively small number of others
  - Possibility of adding traffic engineering parameters
  - Device knowledge minimized
- Issues
  - Delay during route installation/change
  - Heavy multicasting during network change
  - Route authentication/authorization



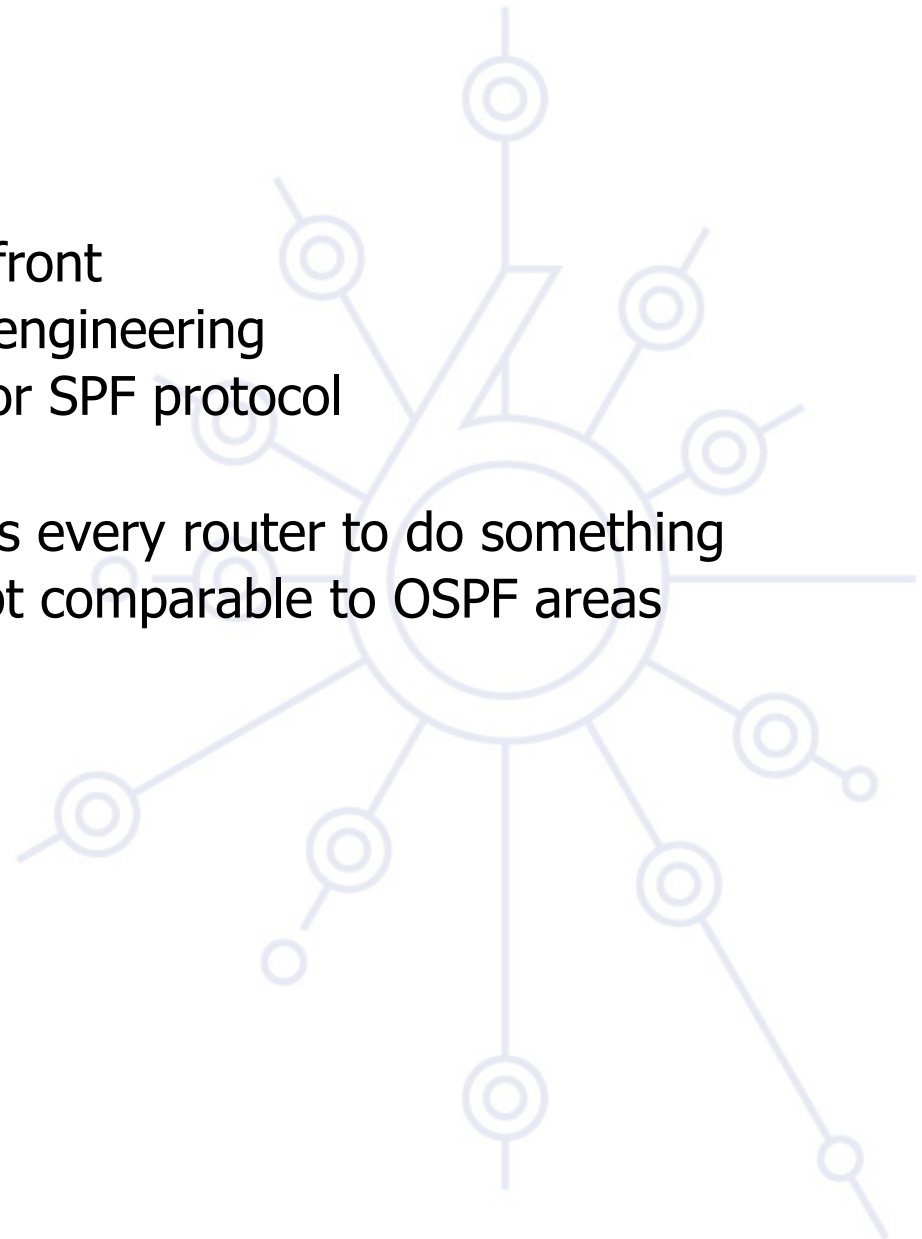
# Optimized Link State Routing (OLSR)

- Systems trade
  - Some form routing backbone
  - Some act as “hosts”
- As devices move
  - Topological relationships change
  - Routes change
  - Backbone shape and composition changes



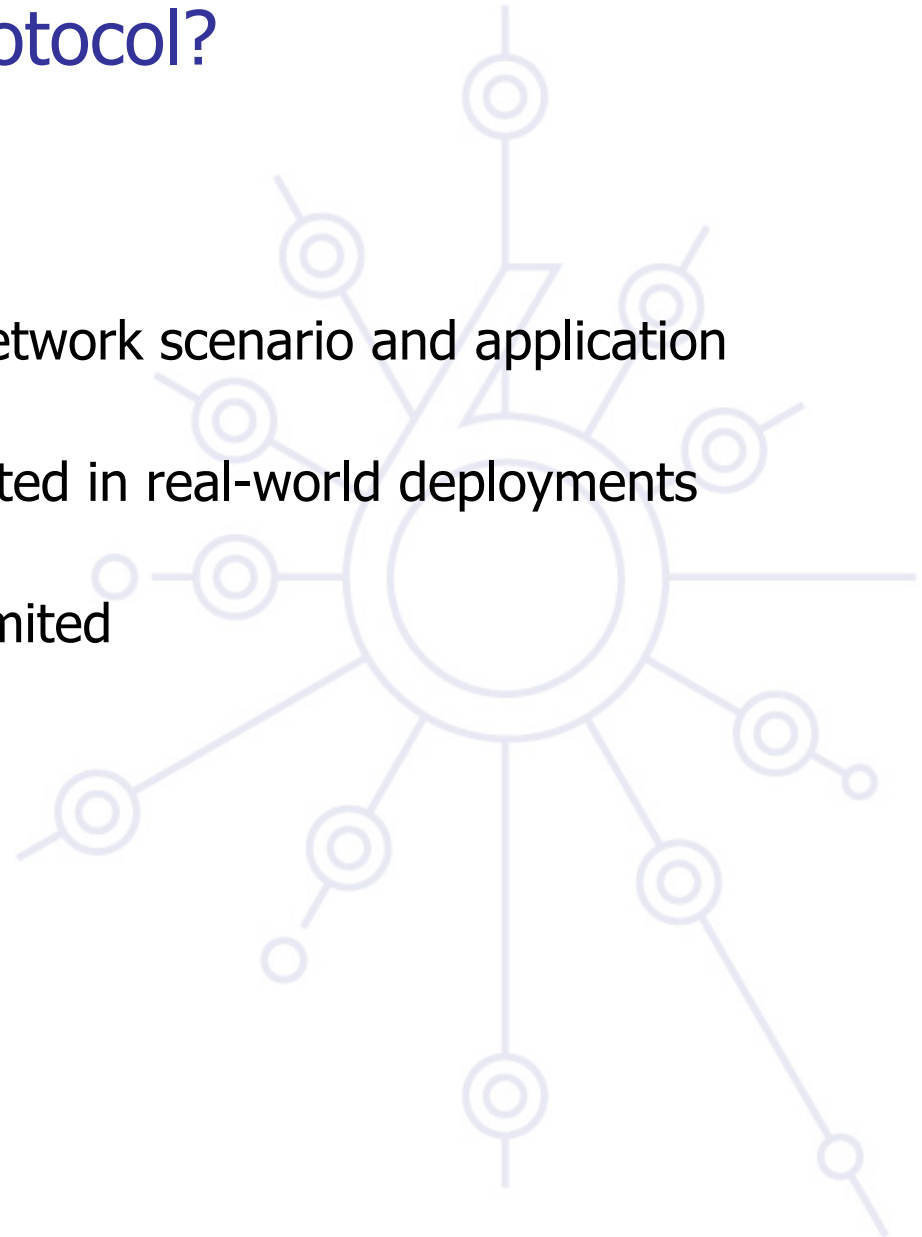
## OLSR Analysis

- Opportunities
  - Proactive: knows network up front
  - Parameters can be added for engineering
  - Minimizes distribution traffic for SPF protocol
- Issues
  - Every network change requires every router to do something
  - No hierarchical routing concept comparable to OSPF areas



# What's the best MANET protocol?

- When looking at IETF protocols;
  - No 'optimal' protocol
  - Performance depends on network scenario and application (traffic patterns)
  - Testing studies – not validated in real-world deployments (research community)
  - Live implementations are limited
  - Experimental RFCs







How about one of the *other* protocols available?

**LUNAR**

**FISHEYE**

**MOSAIC**

**TORA**

**ABR**

**SSA**

**LAR**

**LANMAR**

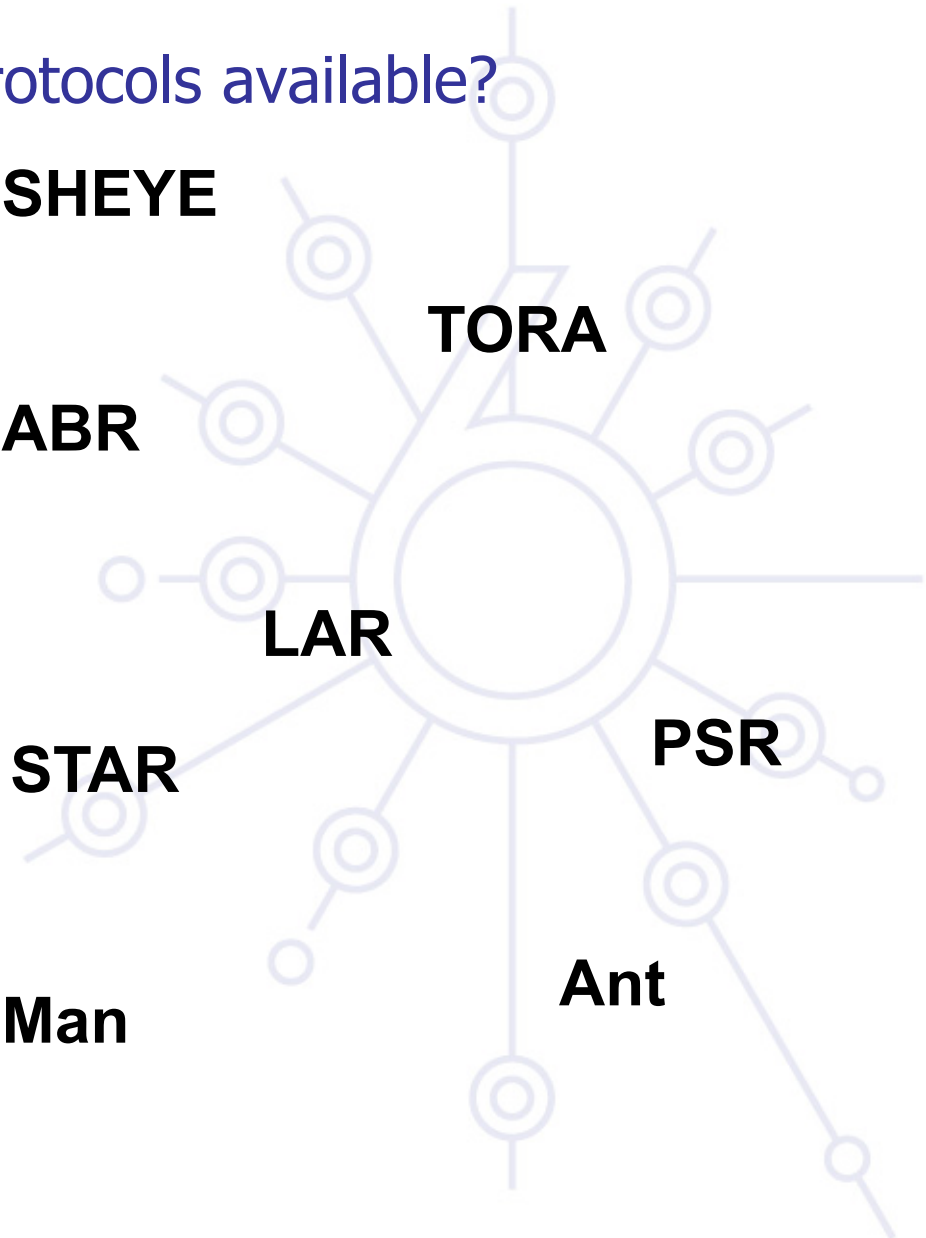
**STAR**

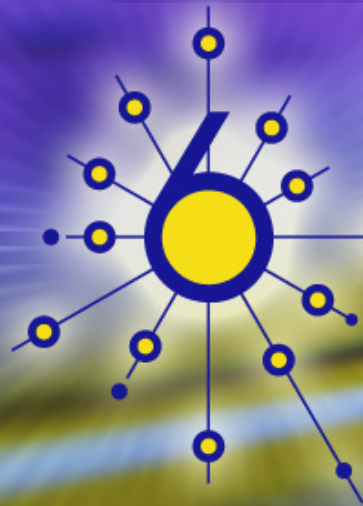
**PSR**

**ZRP**

**Ant**

**MobileMan**





deploy

MANET OSPFv3 extensions

IPv6 Mobility Module



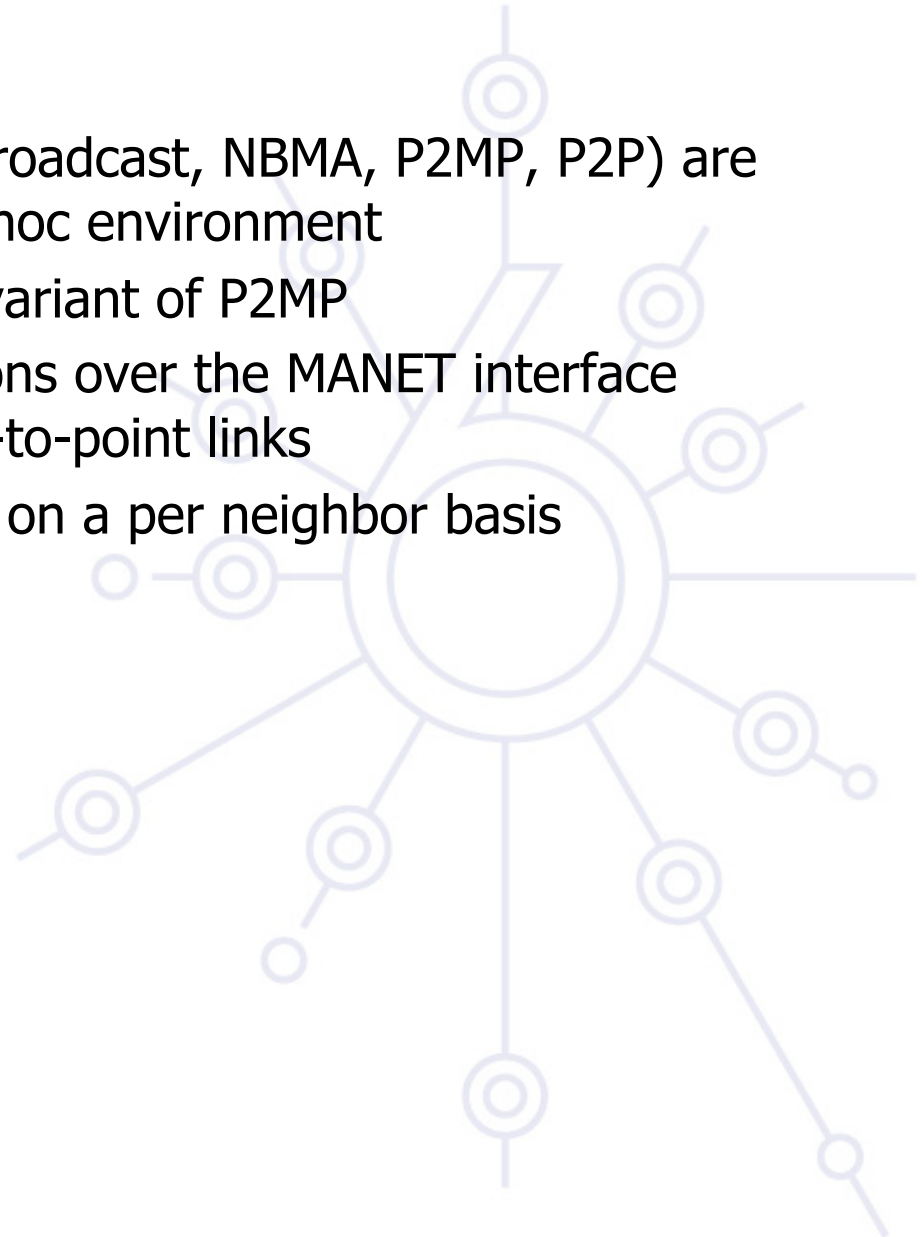
## Areas of OSPFv3 inefficiency addressed with MANET Extensions

- Interface Types
- Neighbor adjacencies
- Database synchronization
- Flooding of routing updates



## Interface Type

- Existing OSPF interface types (Broadcast, NBMA, P2MP, P2P) are not efficient for operation in ad-hoc environment
- New MANET interface type is a variant of P2MP
  - All router-to-router connections over the MANET interface behave as if they were point-to-point links
  - Route cost metric can be set on a per neighbor basis



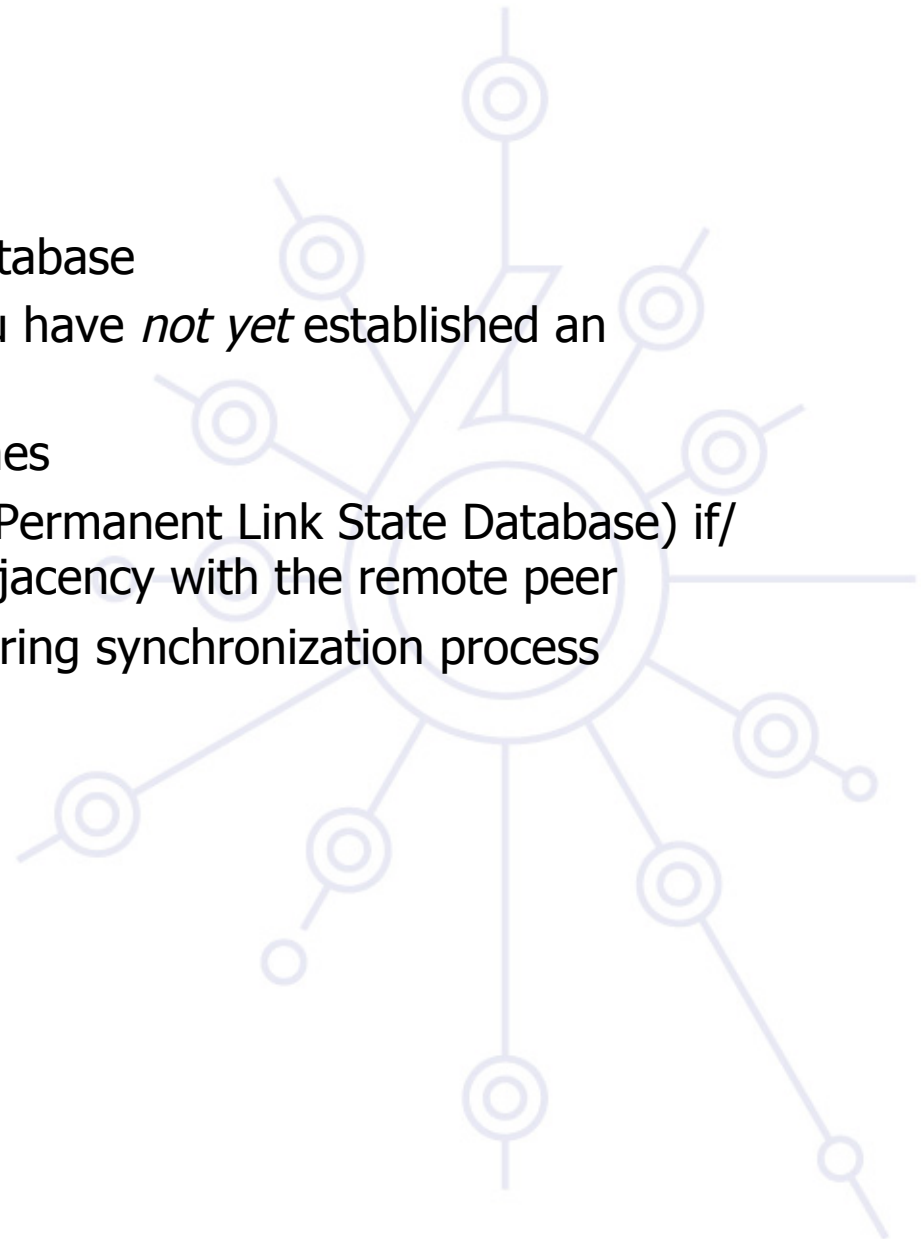
## Neighbor Adjacency Issues

- Nodes may have varied capabilities
- Periodic Hello messages – overhead increases with size and density of network, and with rate of Hello message exchanges
- Potential large size of neighbor list to be advertised in Hello
  - Unnecessary overhead and possible size issues (packets larger than interface MTU)
- Solution is implemented in 'Incremental Hello' messages
  - Allows for varied participation levels
  - Two-way connectivity check
  - Include selection of 'active' overlapping relays for optimized flooding
  - Include Willingness to serve as an 'active' overlapping relay
- Don't include full neighbor list on Hello packets; incrementally update as neighbor state changes



## Database Synchronization

- Implement a Temporary Link State Database
- Keeps valid LSAs from routers that you have *not yet* established an adjacency with
- LSAs are multicasted, local router caches
- LSAs are “promoted” (moved into the Permanent Link State Database) if/when the local OSPF establishes an adjacency with the remote peer
- Keeps them from be re-transmitted during synchronization process



## Flooding Issues

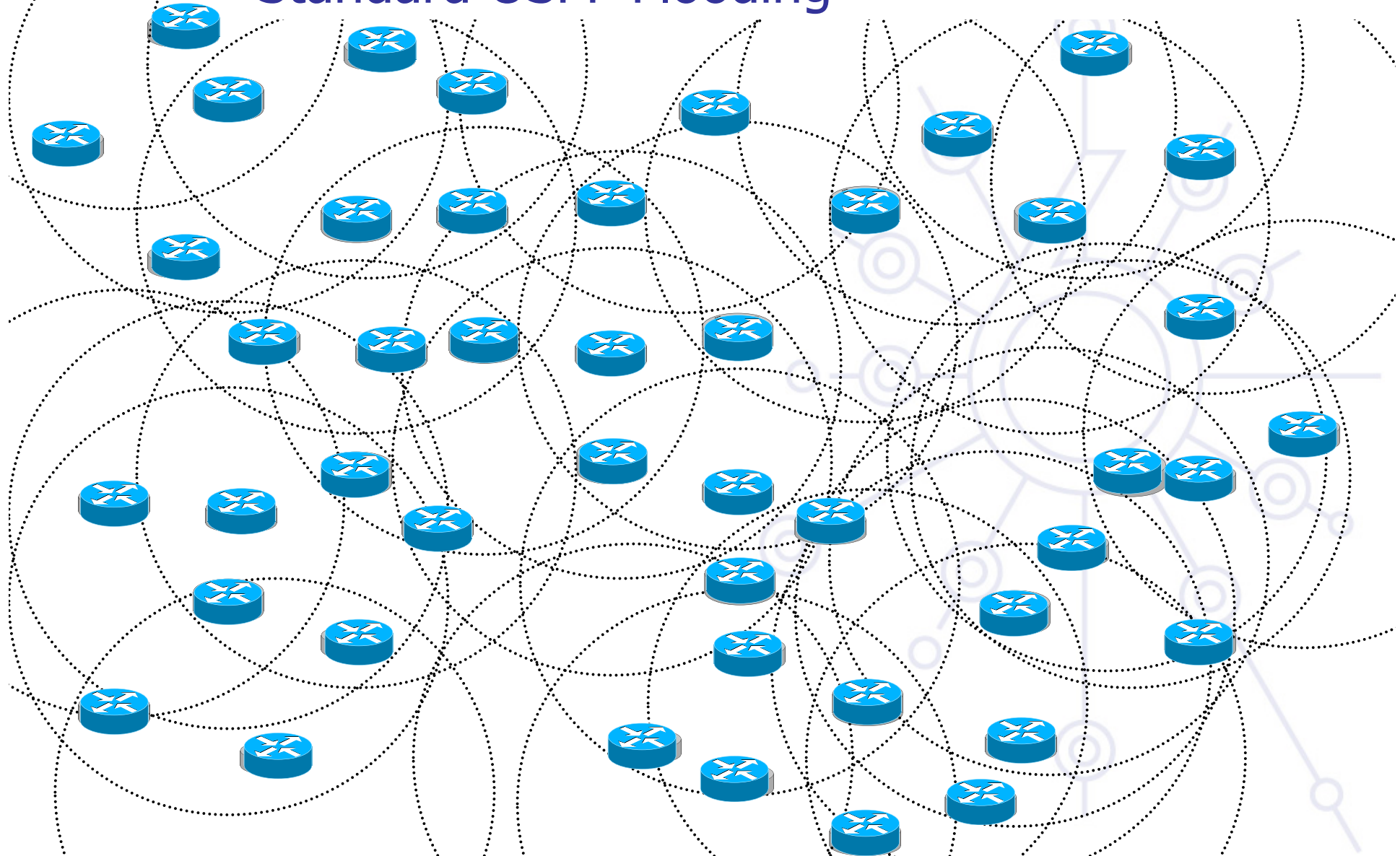
- Flooding Overhead
  - Current flooding occurs on all interfaces other than the receiving interface
  - All routers flood received updates
- Flooding optimization (Overlapping Relays)
  - Minimize propagating link-state information to routers who have already received it
  - Use knowledge of two-hop neighborhood, allowing more intelligent flooding decisions and intelligent ACKing decisions to be made
  - Goal is to minimize control overhead



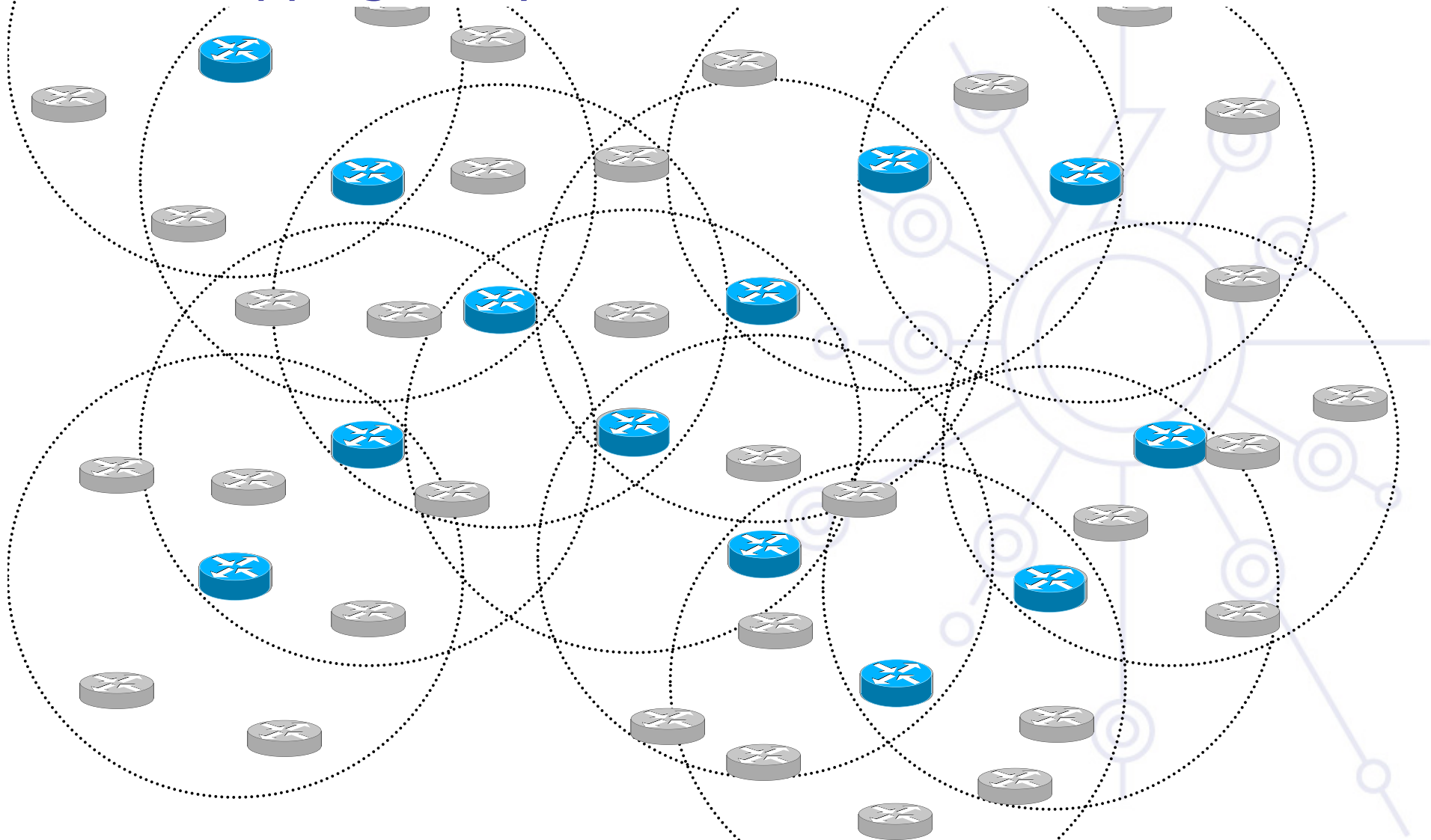


IPv6 Mobility Module

# Standard OSPF Flooding

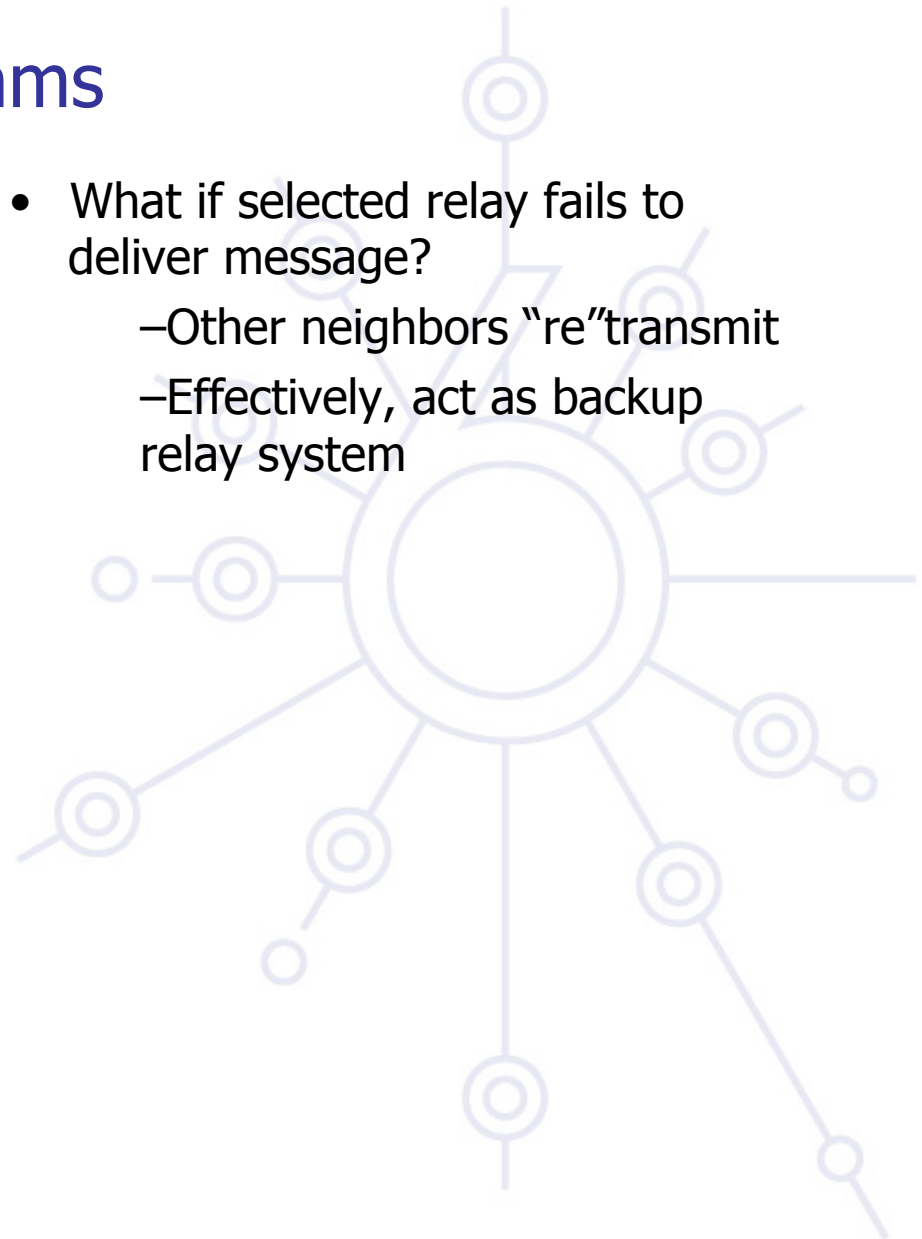


# Overlapping Relays



# Overlapping Relay Algorithms

- Concept drawn from OLSR MPR
- Who gets to be a relay system?
  - Router advertises willingness (policy)
  - Neighbors select neighbor with most “two hop” neighbors
- What if selected relay fails to deliver message?
  - Other neighbors “re”transmit
  - Effectively, act as backup relay system



## Intelligent Acking

- All ACKs are multicast.
- Reflood of LSA serves an implicit ACK
- Node should only ACK first LSA received on link
- Relays should only expect ACKS (implicit or explicit) from peers that have not already ACKed this LSA.
- Several ACKS bundled in single packet
- ACKs reset RouterDeadInterval at receiver
- ACKs reset HelloInterval at sender if no state is waiting to be sent in a Hello packet
- LSA received unicast is ACKed via multicast

## ITEF References

- MANET Characteristics - <http://www.ietf.org/rfc/rfc2501.txt>
- AODV - <http://www.ietf.org/rfc/rfc3561.txt>
- OLSR - <http://www.ietf.org/rfc/rfc3626.txt>
- TBRPF - <http://www.ietf.org/rfc/rfc3684.txt>
- DSR -  
<http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt>
- OSPFv3 MANET-  
<http://www.ietf.org/internet-drafts/draft-chandra-ospf-manet-ext-04.txt>

## ITEF References cont'd.

- PPP - <http://www.ietf.org/rfc/rfc1661.txt>
- PPPoE – <http://www.ietf.org/internet-drafts/draft-bberrypppoe-credit-06.txt>

