IPv6 Mobility

Athanassios Liakopoulos (aliako@grnet.gr)

IPv6 Training, Skopje, June 2011

Copy ... Rights

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

- Main authors (6DEPLOY)
  - Bert Habraken, Cisco, Netherlands

Agenda

IPv6 Mobility Module

Agenda

- IPv6 Mobility
- Mobile IPv6 Security Overview
- Mobile IPv6 @ Cisco
- Implementations and Interoperability
- Network Mobility - NEMO

IPv6 Mobility

Mobility Overview

- Mobility is much wider than “nomadism”
- Keep the same IP address regardless of the network the node is connected to:
  - reachability
  - configuration
  - real mobility
- Difficult to optimize with IPv4 (RFC 3344 PS)
- Use facility of IPv6: MIPv6 (RFC 3776)
- Network Mobility (NEMO) Basic Support Protocol (RFC 3963)

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, e.g. the *Foreign Agent* (IPv4) is 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

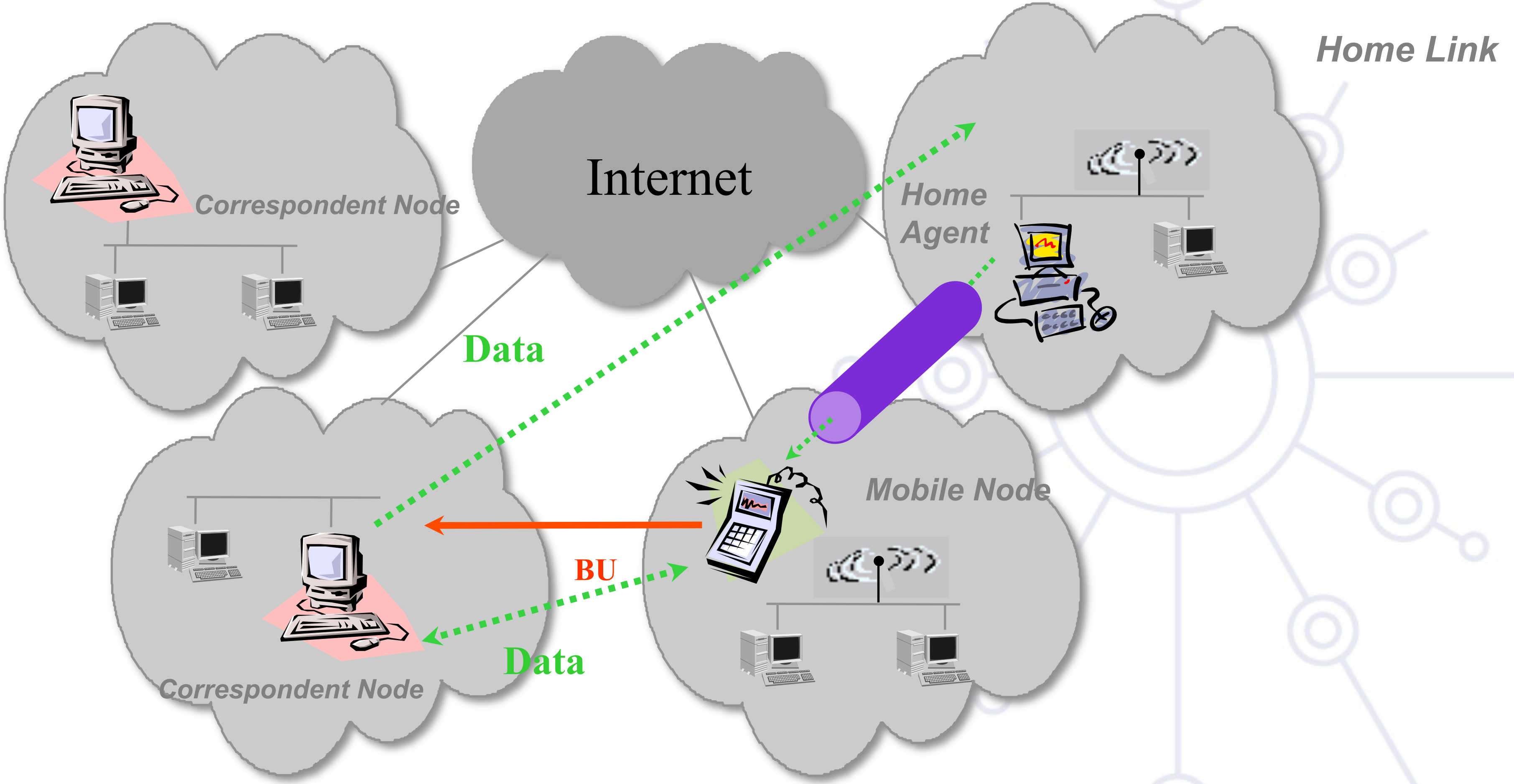
- Correspondent Node (CN) can:
  - Put/get a Binding Update (BU) in/from their Binding Cache
  - Learn the position of a mobile node by processing BU options
  - Perform direct packet routing toward the MN (Routing Header)

- 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)

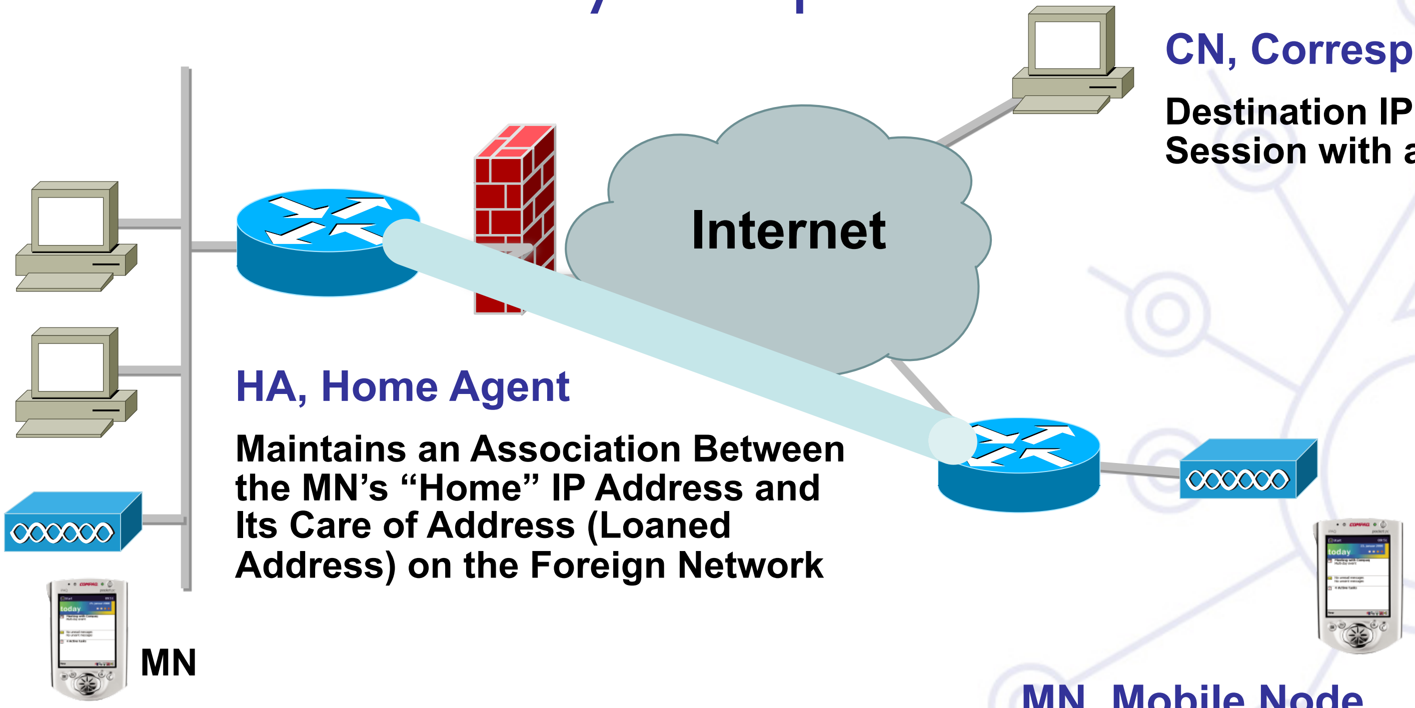
Mobile Node Addressing

- 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 (ND RA's) 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

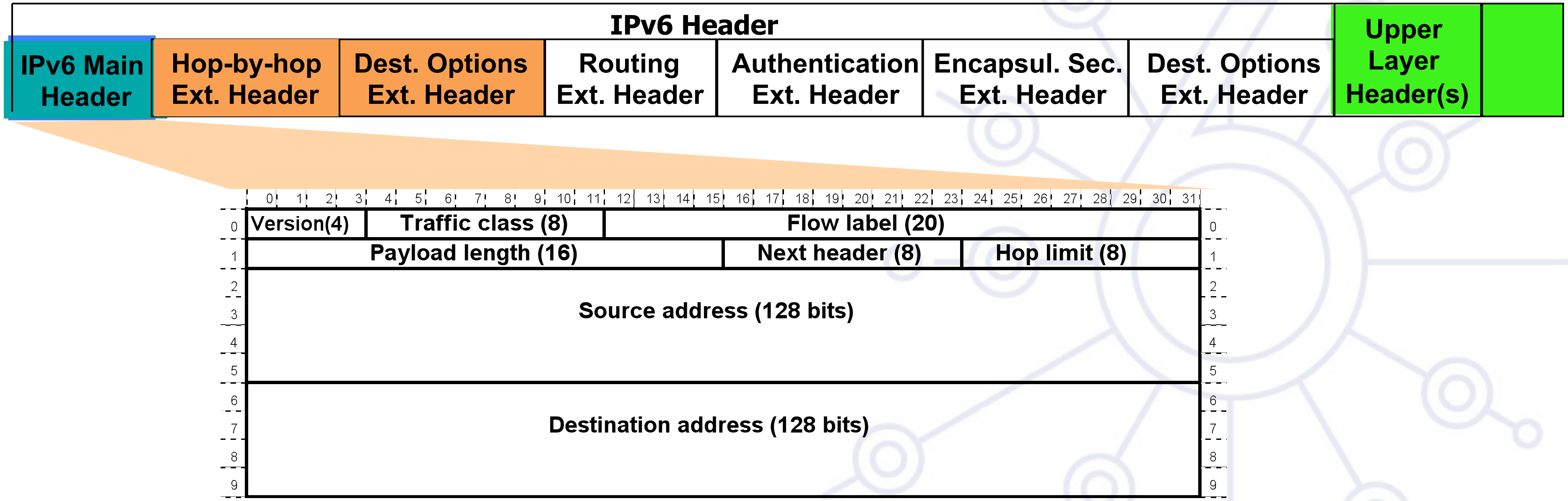
Maintains an Association Between the MN’s “Home” IP Address and Its Care of Address (Loaned Address) on the Foreign Network

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:

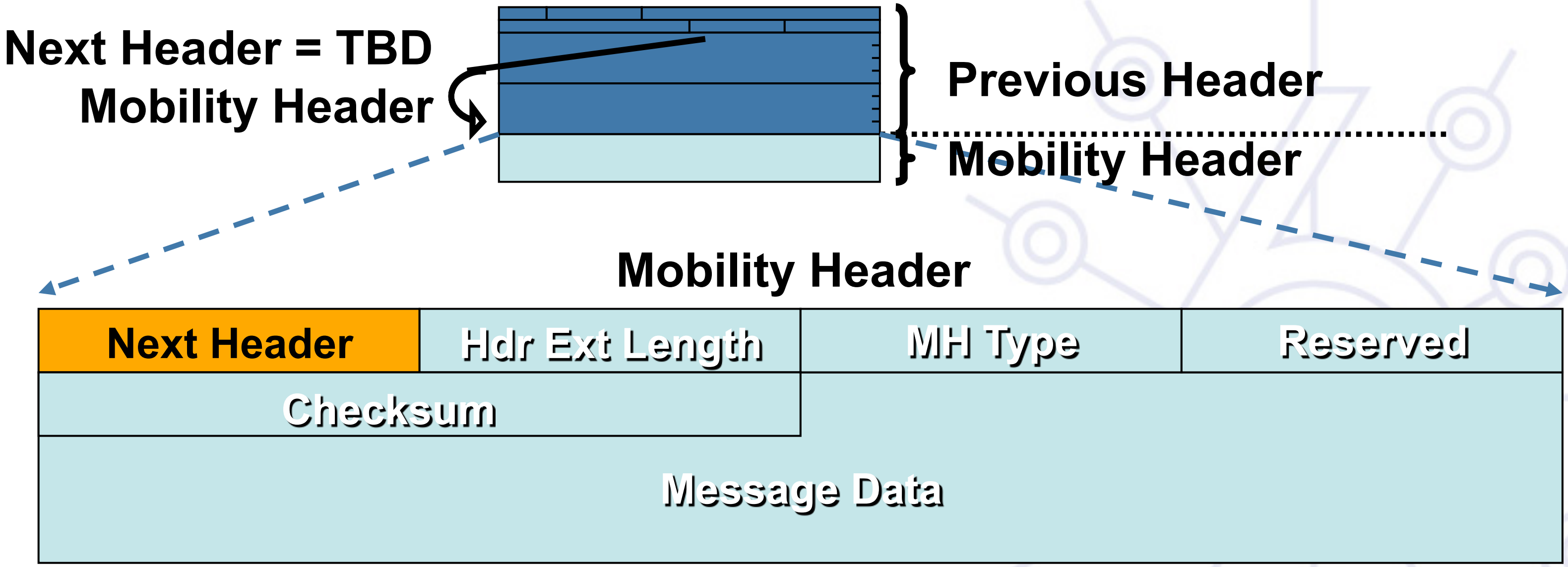


IPv6 Header							Upper Layer Header(s)	
IPv6 Main Header	Hop-by-hop Ext. Header	Dest. Options Ext. Header	Routing Ext. Header	Authentication Ext. Header	Encapsul. Sec. Ext. Header	Dest. Options Ext. Header		

Bits 0–3	Bits 4–11	Bits 12–31	
Version(4)	Traffic class (8)	Flow label (20)	
Payload length (16)		Next header (8)	Hop limit (8)
Source address (128 bits)			
Destination address (128 bits)			

- 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

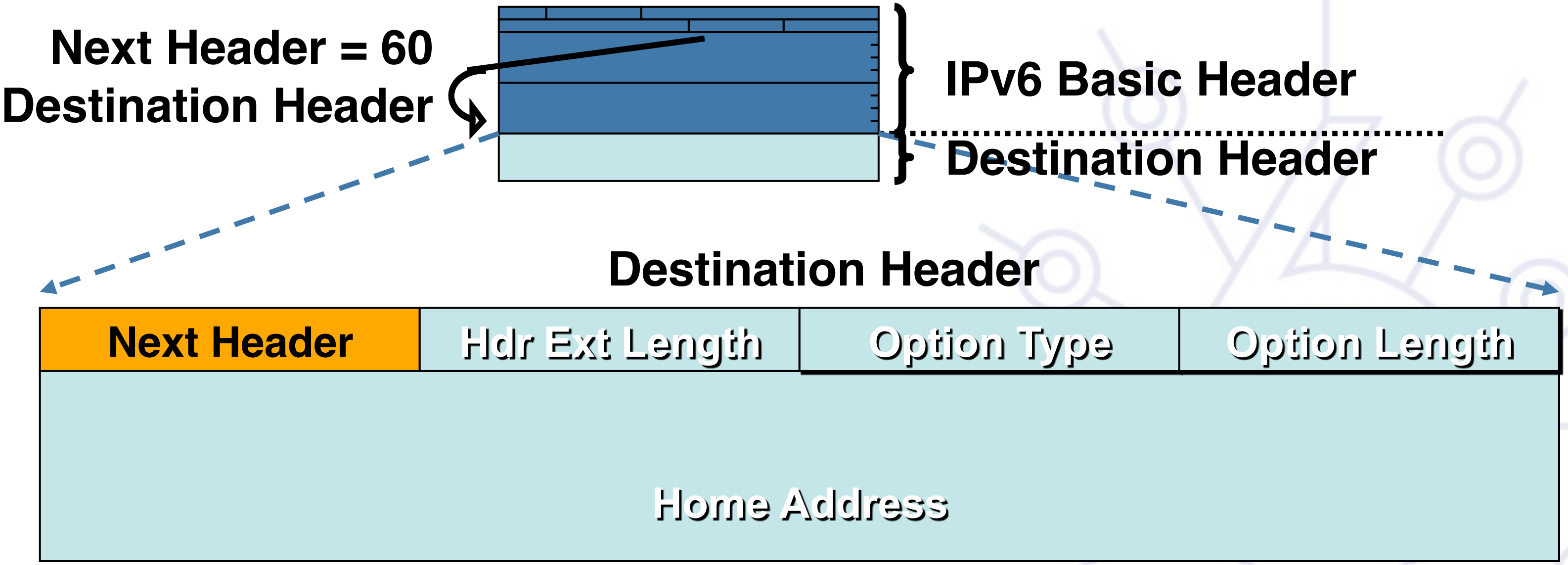


- New extension header to be used by MN, HA and CN in all messaging related to the creation and management of bindings
- IPv6 option header may allow piggybacking of these messages
  - Another advantage over IPv4

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



Next Header = 60

Destination Header

IPv6 Basic Header

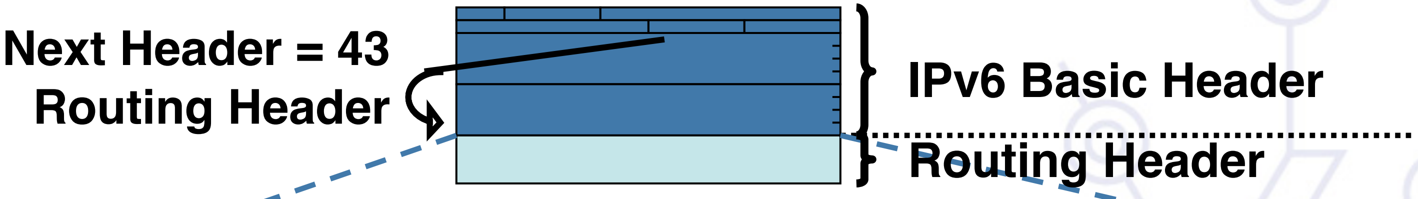
Destination Header

Destination Header

Next Header	Hdr Ext Length	Option Type	Option Length
Home Address			

- 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



Routing Header

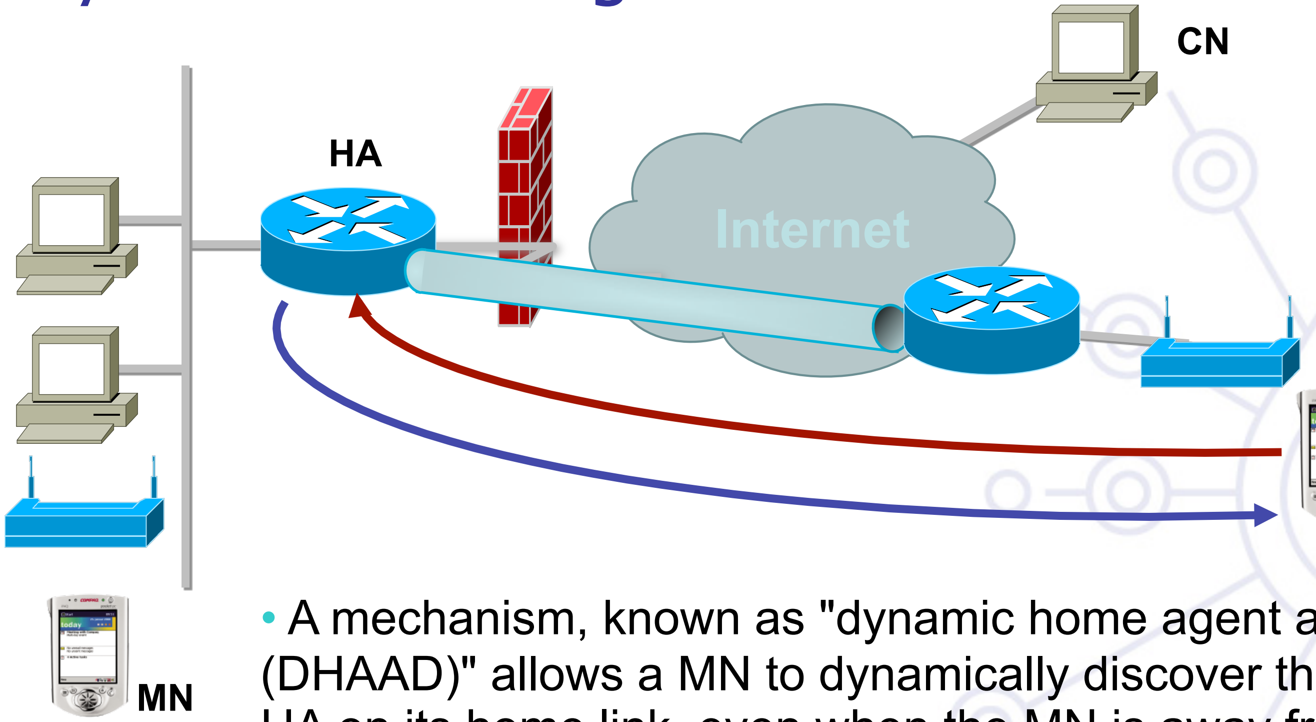
Next Header	Hdr Ext Length	Routing Type = 2	Segments Left = 1
Reserved			
Home Address			

- 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

- 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.
  - 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.
  - 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

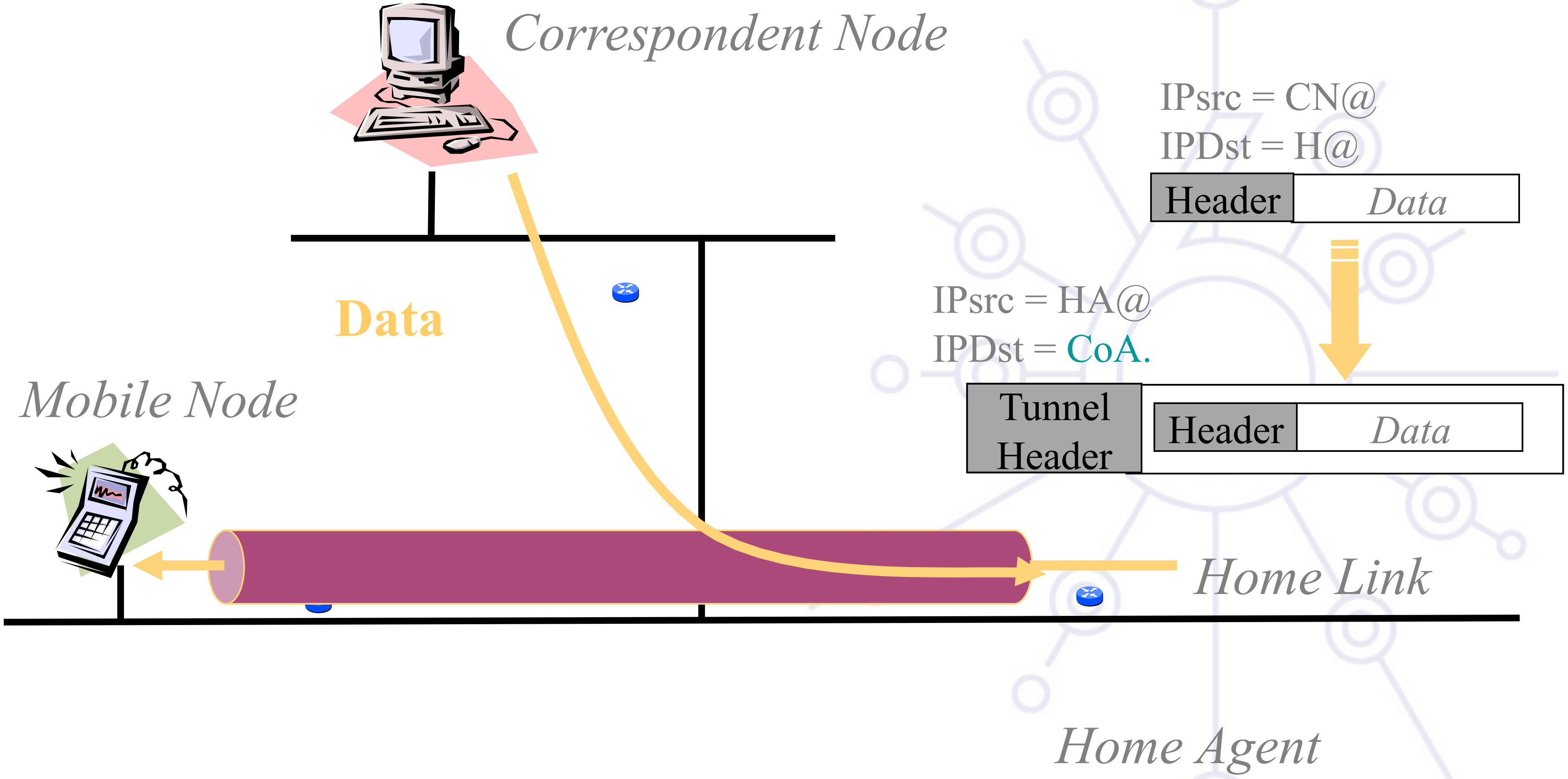
Binding Cache Management

- 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

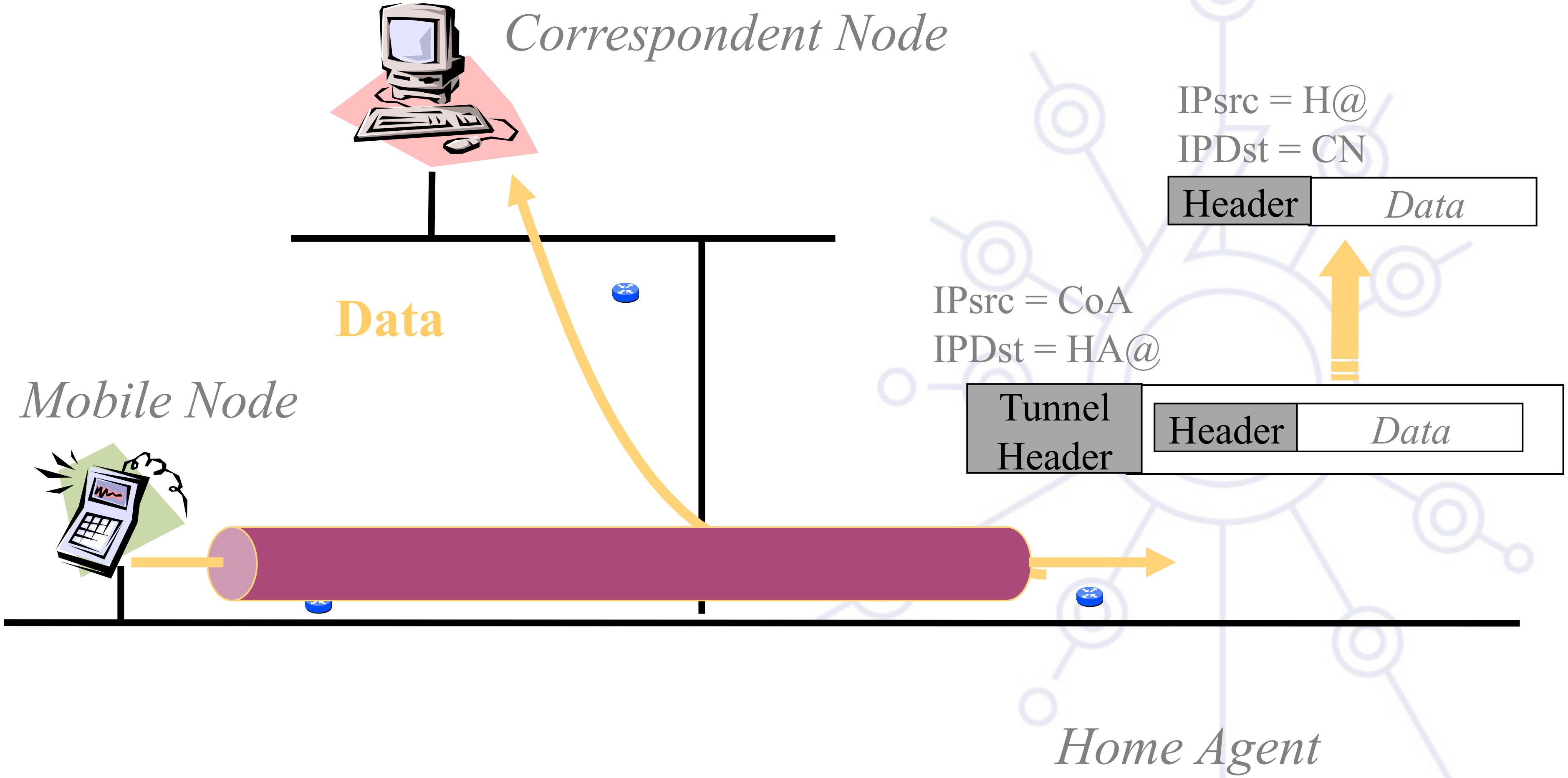
Communication with a Mobile Node

- Two methods are possible:
  - **Bi-directional Tunneling**
    - No mobility requirements on CNs
    - No visibility of MNs for CNs
    - Network load increased
    - Home Agent (HA) role much reinforced
  - **Direct Routing**
    - Much more complex mechanism
    - Home Agent (HA) role much alleviated (simplified)

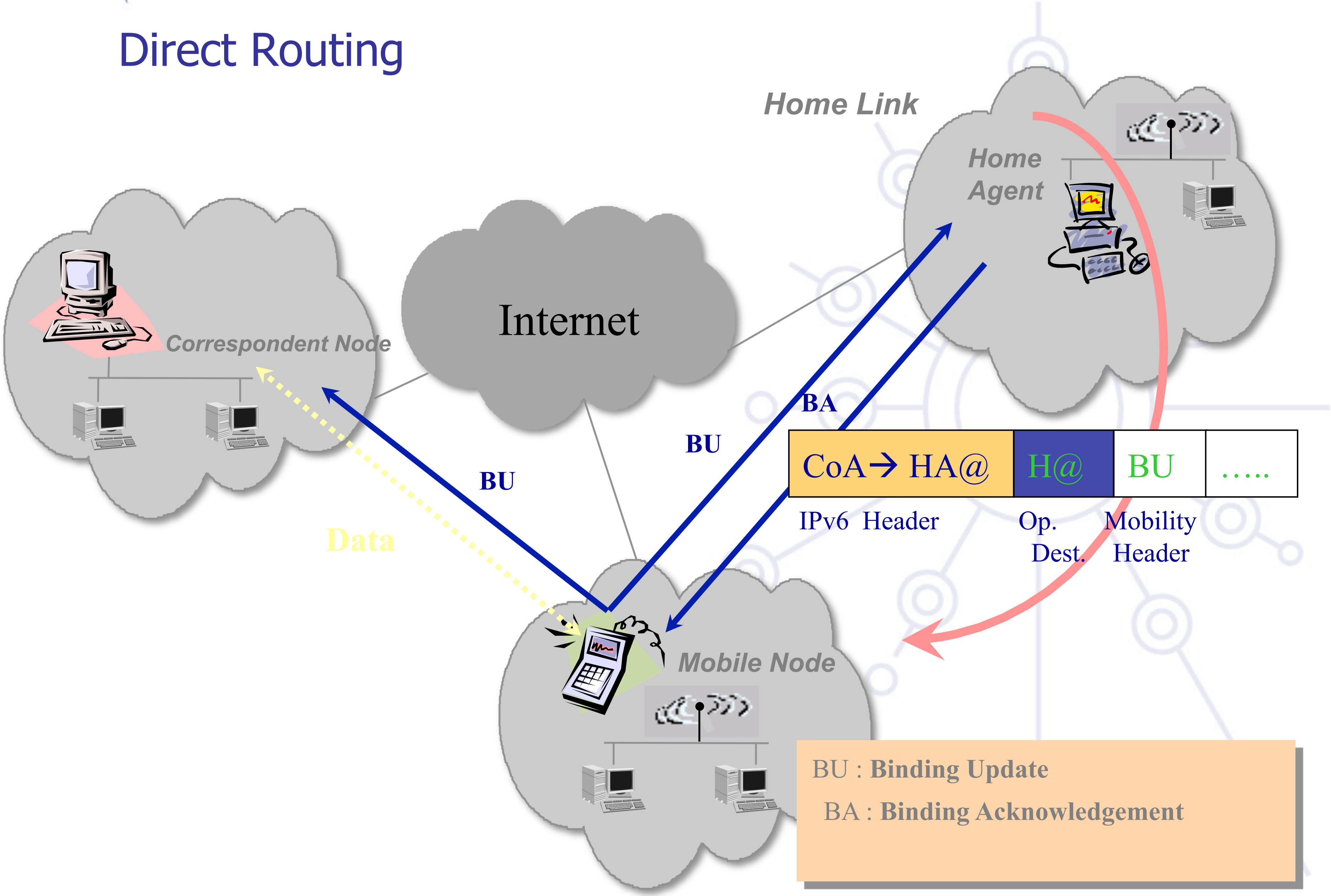
Bi-directional Tunneling



Bi-directional Tunneling (2)



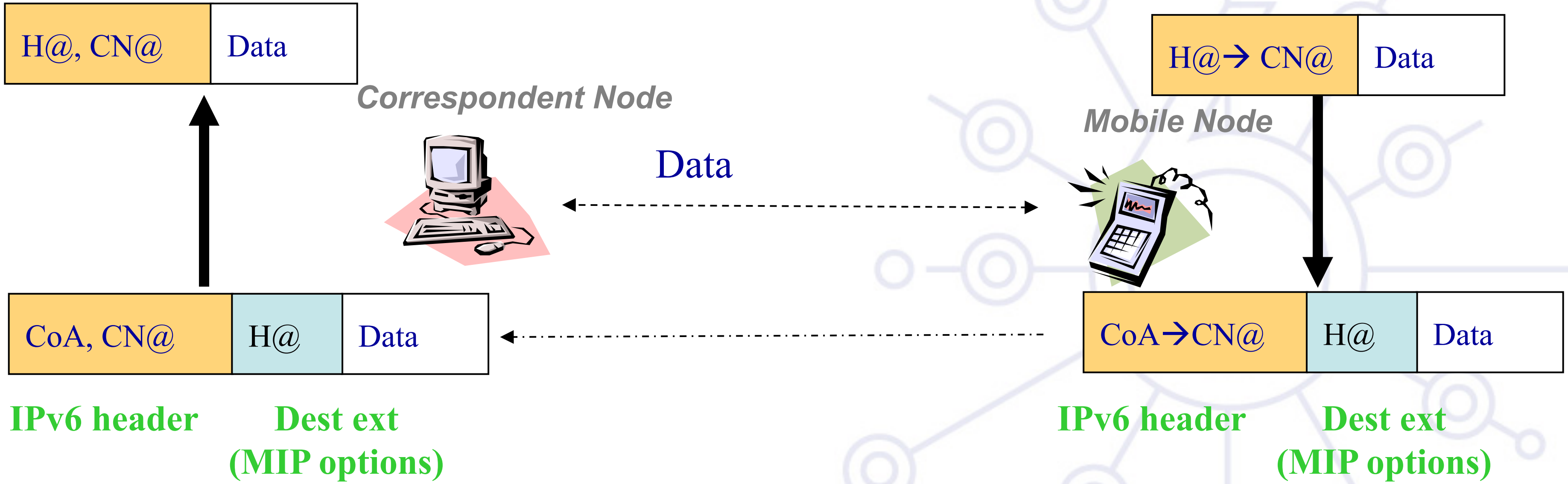
Direct Routing



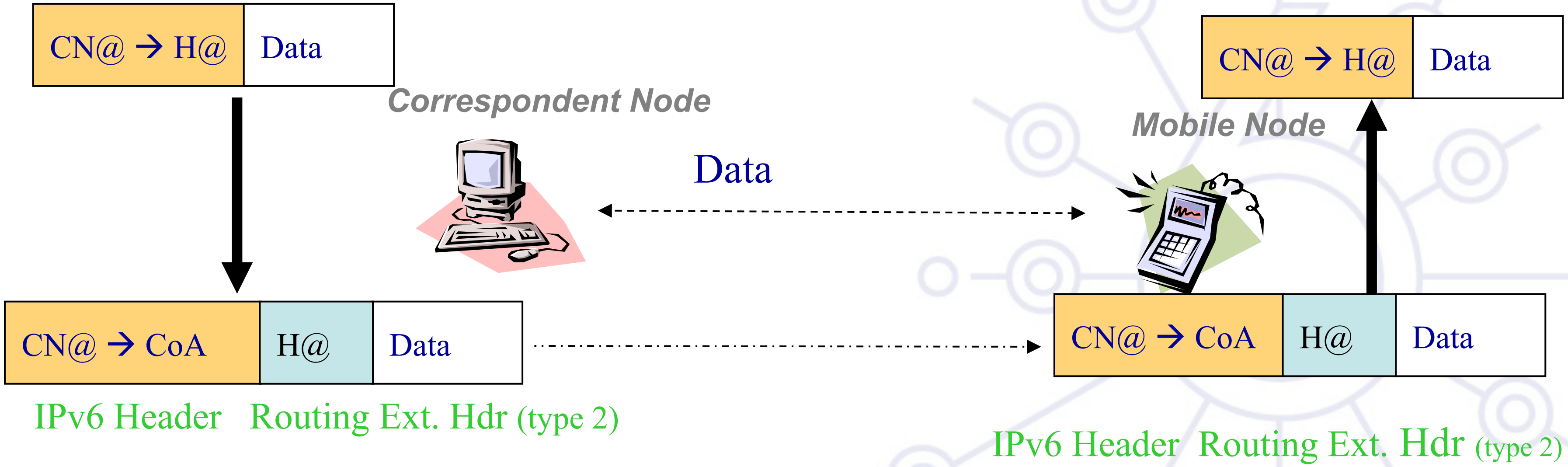
BU : **Binding Update**

BA : **Binding Acknowledgement**

Direct Routing: MN → CN



Direct Routing: CN → MN



CN@ → H@ | Data

Correspondent Node

Data

Mobile Node

CN@ → H@ | Data

CN@ → CoA | H@ | Data

IPv6 Header   Routing Ext. Hdr (type 2)

CN@ → CoA | H@ | Data

IPv6 Header   Routing Ext. Hdr (type 2)

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 / de-encapsulate (tunnel) these packets and forward them to the CoA of the MN

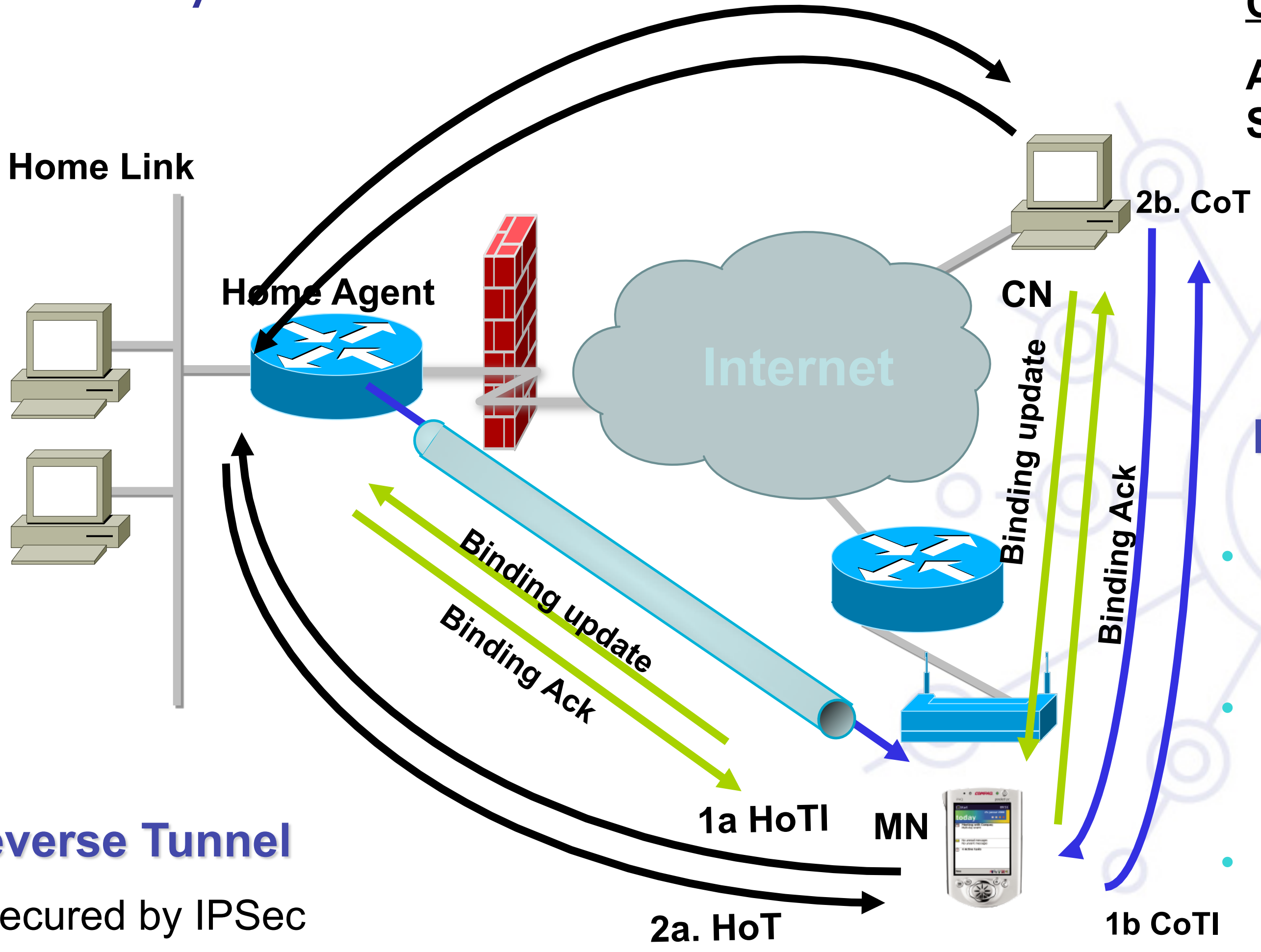
MOBILE IPv6 SECURITY OVERVIEW

IPv6 Mobility Module

Mobile IPv6 Security Overview

- MIPv6 RFC 3775/3776 provides a number of security features.
- Protection of binding updates (BU) both to home agents and correspondent nodes
  - by 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 (RRP)
- 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 (RRT)

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

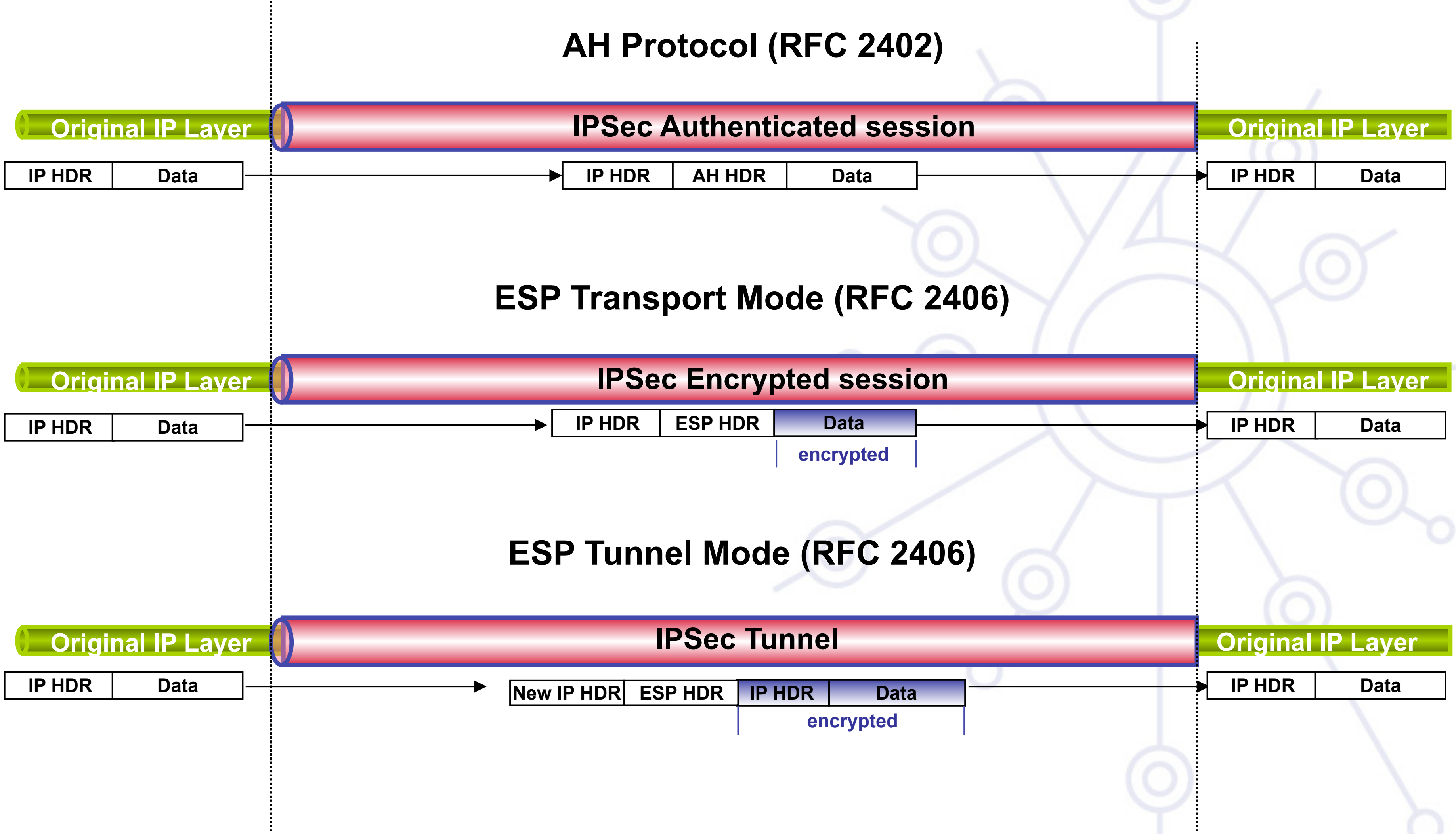
Reverse Tunnel

- Secured by IPSec
- Requires a preexisting Security Association

Mobile IPv6 Terms

- Binding management key (Kbm)
  - Kbm is a key used for authorizing a binding cache management message (e.g., BU or BA). Return routability procedure provides a way to create a binding management key (Kbm).
- 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.

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

Questions?