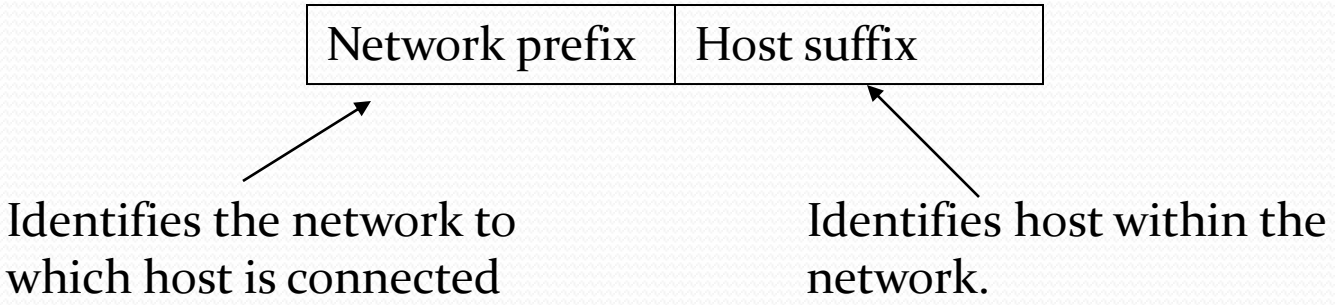
Mobility Support in IPv6

IPv6 addressing and mobility

- IPv6 addresses consist of two parts: a 64-bit network prefix and a 64-bit host suffix.



- Network prefix of address depends on location.
- When a host moves from one IP network to another, it needs to change the network part of its address.

→Issues with reachability, session continuity.

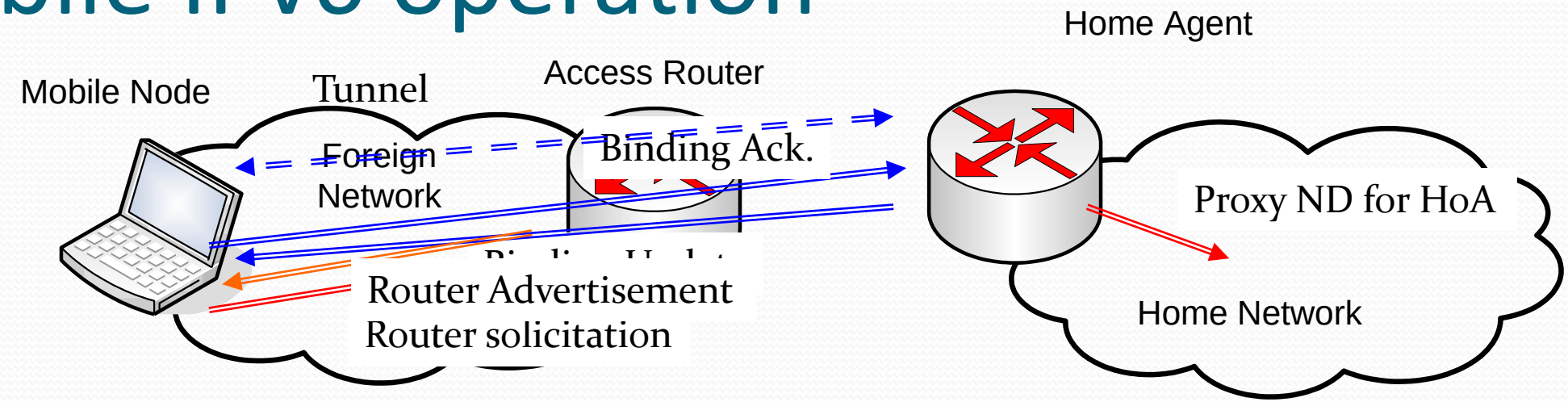
Terminology

- *Mobile node* (MN) is a mobile device with an IPv6 *home address*
  - Mobile IPv6 is dedicated to host mobility
- *Correspondent node (CN)* is any node that communicates with the mobile node
- *Home Address* is based on the 64-bit prefix assigned to the *home link combined with the mobile node's interface* identifier
- *Home Link* is the link to which Home Address prefix is assigned
- *Home Agent* (HA) helps MN to manage its mobility:
  - Mobile node can always be reached at its home address, regardless of its point of attachment (care-of address) to the Internet.
  - Connections made with home address survive movement between different IP networks

Terminology

- *Foreign Link* refers to any link (other than the home link) visited by a mobile node
- *Care-of Address* is based on the prefix of the foreign link combined with the mobile node's interface identifier
- *Binding* is the association of the mobile node's home address with a care-of address for a certain period of time
- *Binding cache* is stored in volatile memory containing a number of bindings for one or more mobile nodes
  - A binding cache is maintained by both the correspondent node and the home agent
- *Binding Update List (BUL)* is a list maintained by the mobile node in volatile memory
  - This list contains all bindings that were sent to the mobile node's home agent and correspondent nodes

Mobile IPv6 operation



MN forms
Care-of address

How Mobile IPv6 Works

- When the mobile node is away from home it acquires a care-of address through the use of "Address Autoconfiguration"
- It informs its correspondent nodes of its new address through the use of a "Binding Update"
- The correspondent nodes are required to maintain a cache of such mobility bindings and uses the IPv6 routing header to send datagrams to the care-of address
- The mobile node always registers its care-of addresses with its home agent

How Mobile IPv6 Works

- The home agent intercepts and tunnels all traffic, destined for the mobile node, arriving at the home network through *proxy neighbor advertisement*
  - The home agent also defends the mobile node's addresses in case another node configures an address that collides with a mobile node's home address (or addresses)
- Mobile IPv6 specification prohibits the home agent from tunneling packets addressed to the mobile node's link-local address
- The protocol uses IPsec for all security functions
  - The home agent may choose to secure the tunnel to the mobile node using an Authentication Header, depending on local policies within the home network.

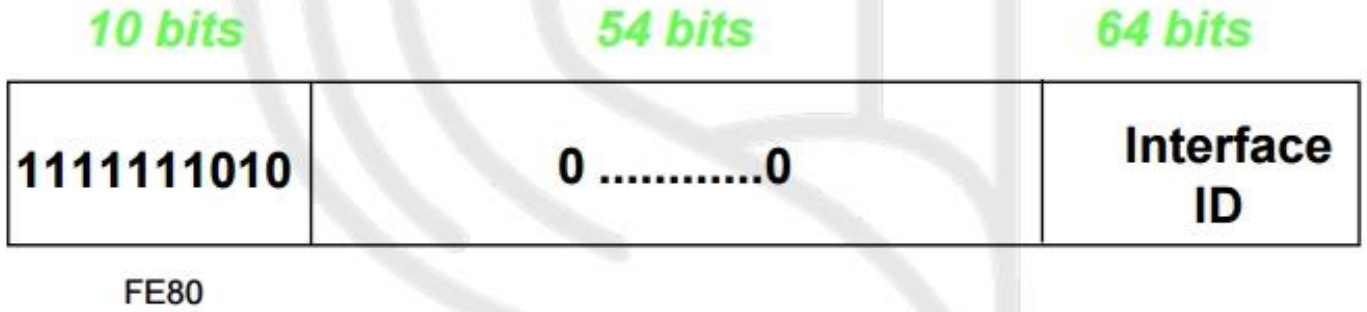
Data Structures

- Data Structures
  - Binding Cache
    - A cache of bindings for other nodes.
    - This cache is maintained by home agents and correspondent nodes.
  - Binding Update List
    - This list is maintained by each mobile node.
    - The list has an item for every binding that the mobile node has or is trying to establish with a specific other node.
    - Both correspondent and home registrations are included in this list.
    - Using the binding update list, the mobile node monitors the lifetimes of its bindings and refreshes them before they expire
  - Home Agents List
    - Home agents need to know which other home agents are on the same link

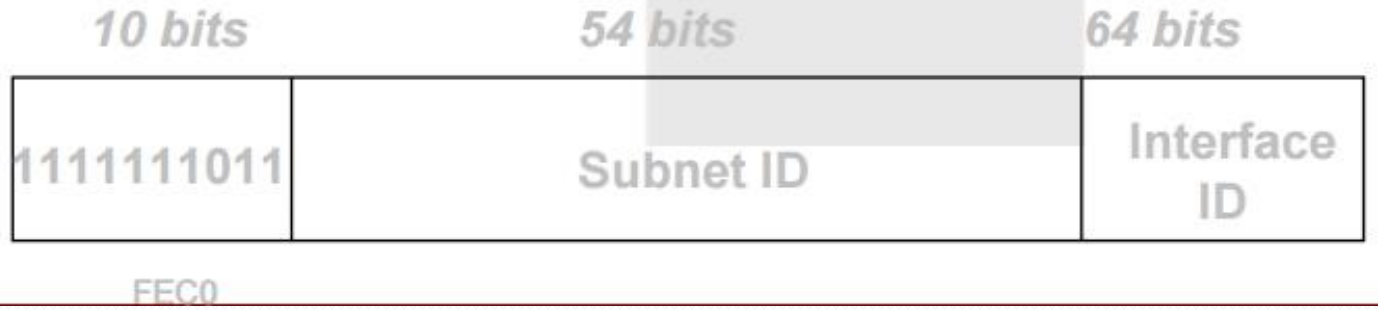
Addressing

- Unicast
- Multicast
- Anycast
  - This address type allows for services that are provided by multiple servers where only one server has to respond
  - In routing, anycast addresses are used to route packets to the closest routers
  - These are allocated from the unicast address space, using any of the defined unicast address formats
- Global Unicast Addresses
  - a public IP address in IPv4
- Local use, Unicast Addresses
  - Site Local Address
    - Equivalent to private IP addresses in IPv4
    - The address space reserved for these addresses, which are only routed within an organization and not on the public Internet
  - Link Local Address
    - In IPv6, link-local addresses always begin with 11111010 (FE80)
    - Link-local addresses are never forwarded by routers and therefore can only be reached on the link (local network on which hosts communicate without intervening routers)

Link-local



Site-local (in the process of being deprecated)

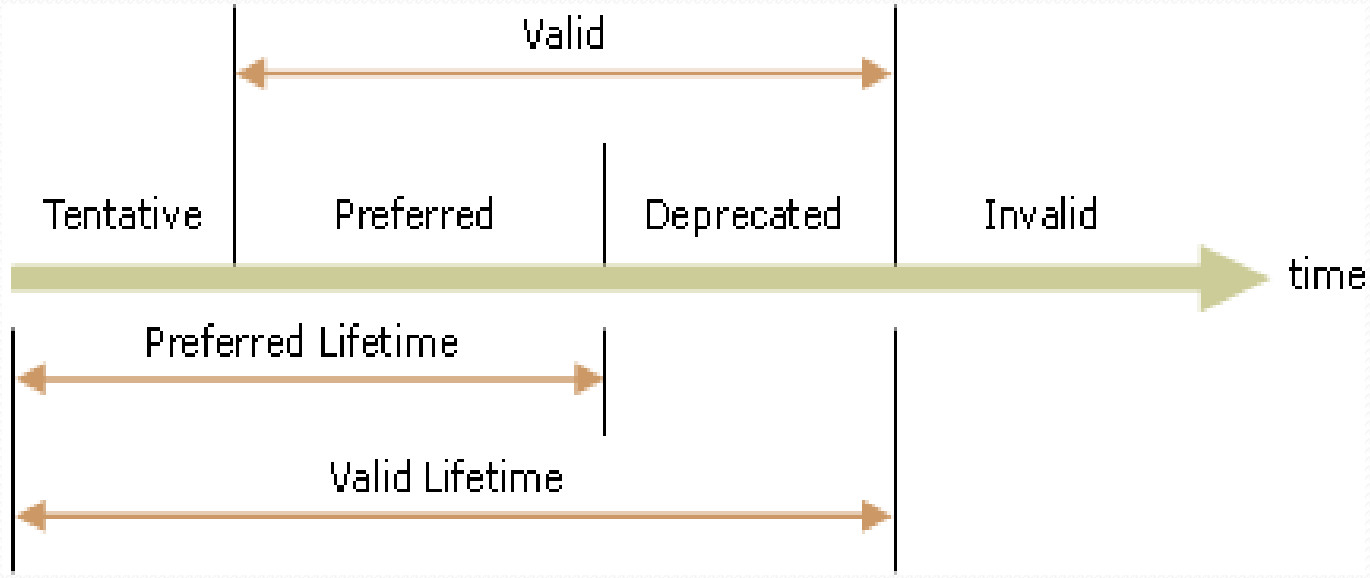


Ref: https://www.6diss.org/tutorials/addressing.pdf

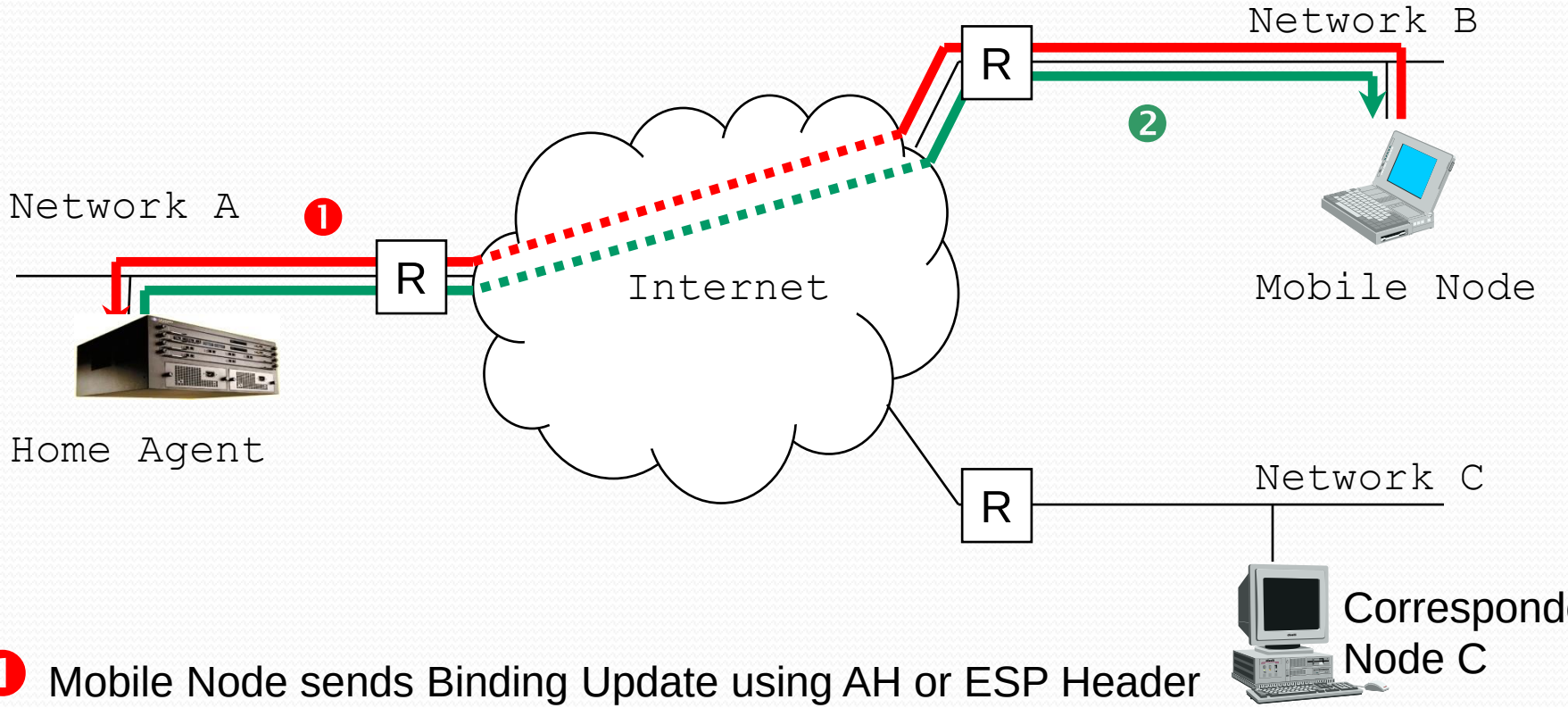
Address Autoconfiguration

- The host sends a Router Solicitation message.
- If a Router Advertisement message is received, the routing information is set on the host.
- For each stateless autoconfiguration address prefix that is included, the following processes occur:
  - The address prefix and the appropriate 64-bit interface identifier are used to derive a tentative address.
  - Duplicate address detection is used to verify the uniqueness of the tentative address. If the tentative address is in use, the address is not initialized for the interface. If the tentative address is not in use, the address is initialized. This includes setting the valid and preferred lifetimes based on information included in the Router Advertisement message.

States


Valid
Tentative
Preferred
Deprecated
Invalid
time
Preferred Lifetime
Valid Lifetime

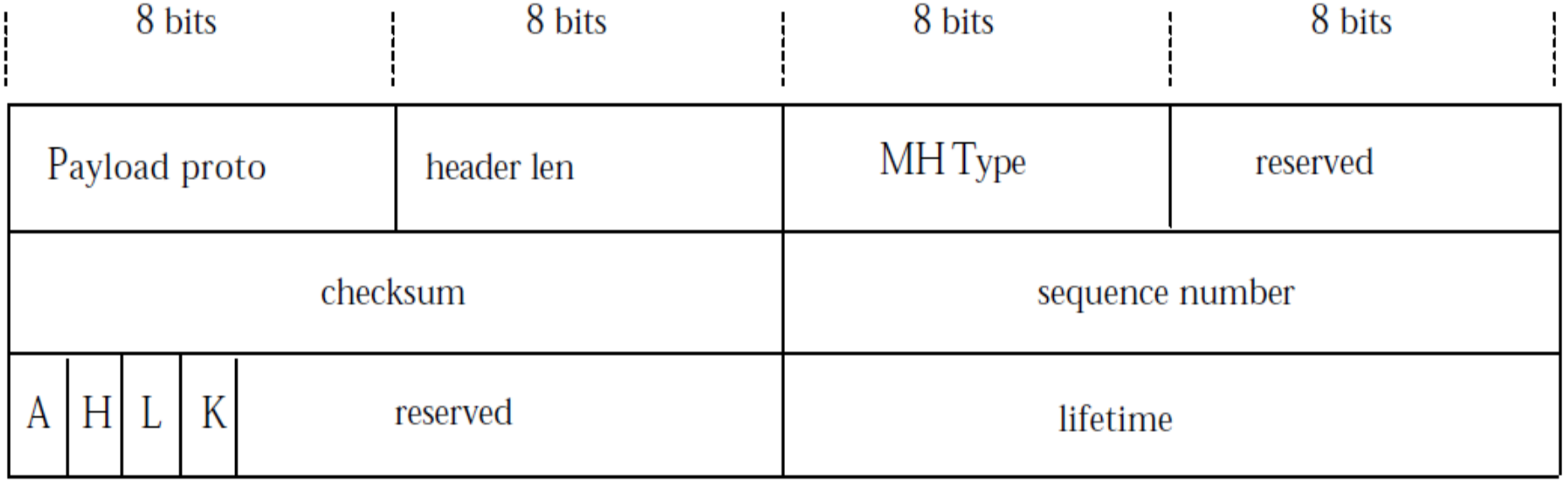
Mobile Node registers at its Home Agent



1. Mobile Node sends Binding Update using AH or ESP Header
2. Home Agent replies with Binding Acknowledgement using AH or ESP Header

Binding

- A reliable protocol is required to install a binding in the home agent's binding cache
- *Payload proto* is always set to the decimal value 59, indicating that the mobility header is the last header
- *Header len* gives length in 8octets excluding the first 8 octets
- The *mobility header type* field is used as a switch to indicate which message is included in the mobility header
  - The value is set to 5 for BU



- *A flag* indicates Acknowledgement required
- *H flag* indicates BU is sent to Home Agent
- *L Flag* indicates to the home agent that its link-local address' interface identifier is the same as that included in its home address
  - Hence, the home agent can defend the link-local address by appending the interface identifier to the well-known link-local prefix.
- The *K flag* indicates whether the protocol used to establish a security association between the mobile node and its home agent must be rerun every time the mobile node moves
- *The Lifetime field* indicates the requested lifetime (in 4-second units) for the binding cache entry created by the receiver of the binding update

Binding Update

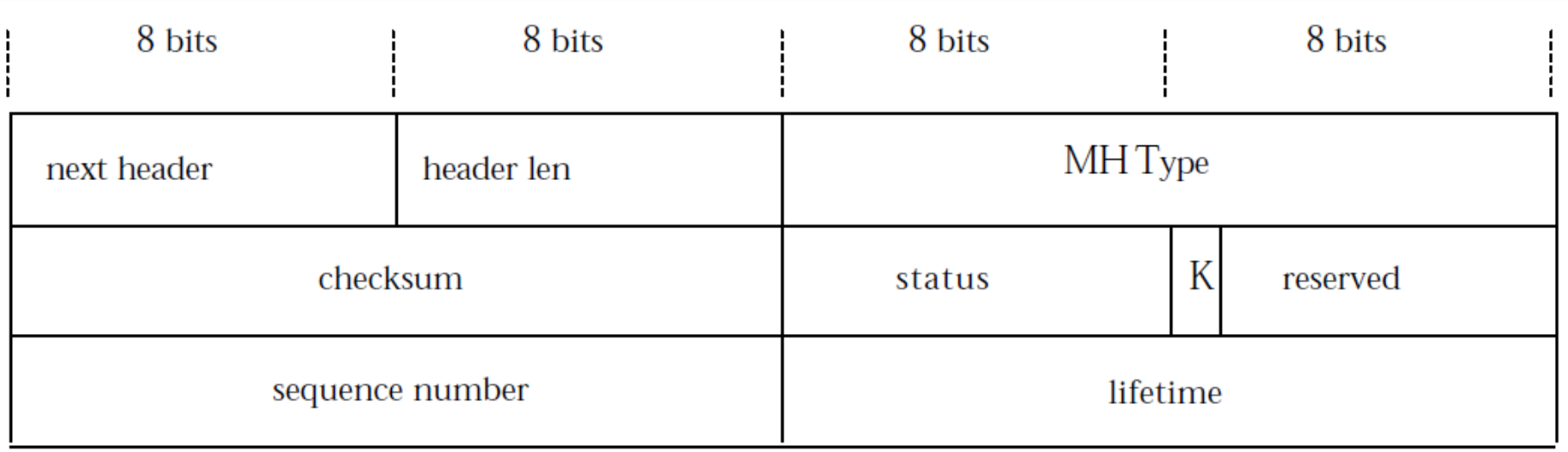
- When the home agent receives the first binding update from a mobile node, it performs DAD for the mobile node's home addresses included in the binding update
- The home agent copies the contents of the message into an existing binding cache entry or creates a new one if this was the first binding update
- If a binding cache entry already exists, the home agent updates it with the contents of the new message
- The care-of address can be retrieved through two different fields:
  - the source address included in the IP header or an alternate-care-of address option included in the mobility header containing the binding update

Binding Cache Entries

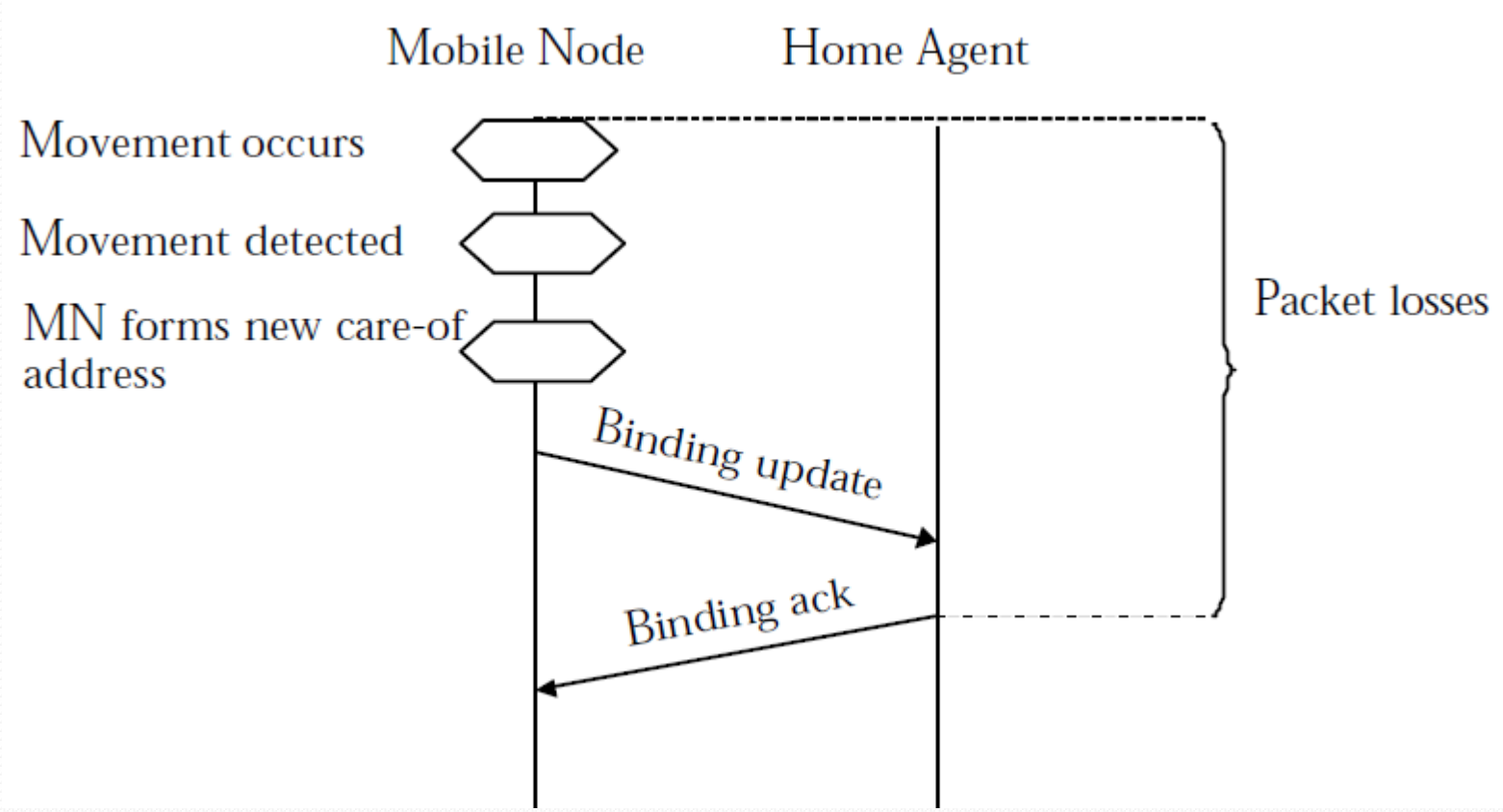
Home address	Care-of address	Sequence no.	Lifetime	Flags
3ffe:200:8:1:A:B:C:D	3ffe:200:1:5:A:B:C:D	11	250	A/H/K/L
3ffe:200:8:1:D:E:F:9	3ffe:100:3:1:D:E:F:9	2000	400	A/H/L

Binding ACK

- The lifetime fields in the binding update and acknowledgment messages may not have the same values
- The binding acknowledgment contains the sequence number of the binding update being acknowledged
- Mobile nodes continue to retransmit the binding update (increasing the sequence number for each retransmission) to the home agent until an ack is received following exponential back-off



Movement Detection



Routers periodically advertise
After noticing that a new prefix has appeared on link, the mobile node must check if it still shares a link with its default router

Returning Home

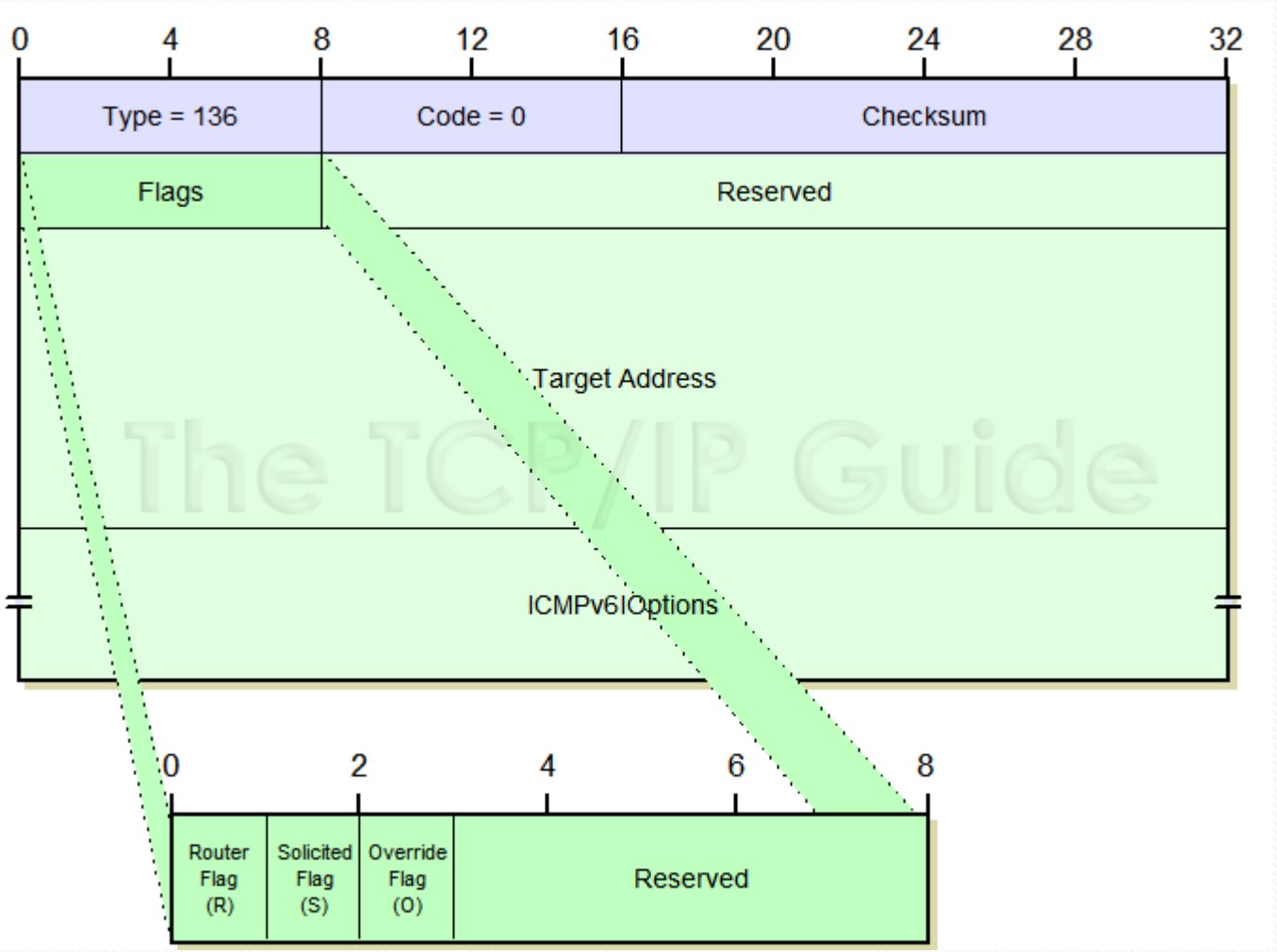
- The mobile node must send a binding update to the home agent with a lifetime of zero and a care-of address (source address) equal to the mobile node's home address
- DAD at home agent fails
- To avoid it, the mobile node sends a binding update with its home address as a source and the home agent's address as a destination.
- This is done without performing DAD on the mobile node's home address (an exception to address autoconfiguration).

Returning Home

- The mobile node sends a neighbor advertisement to the *all-nodes multicast address with the O flag set*.
- The purpose of this advertisement is to inform all nodes that they should send traffic directly to the mobile node (i.e., override the home agent's earlier proxy advertisements)

Neighbor Advertisement

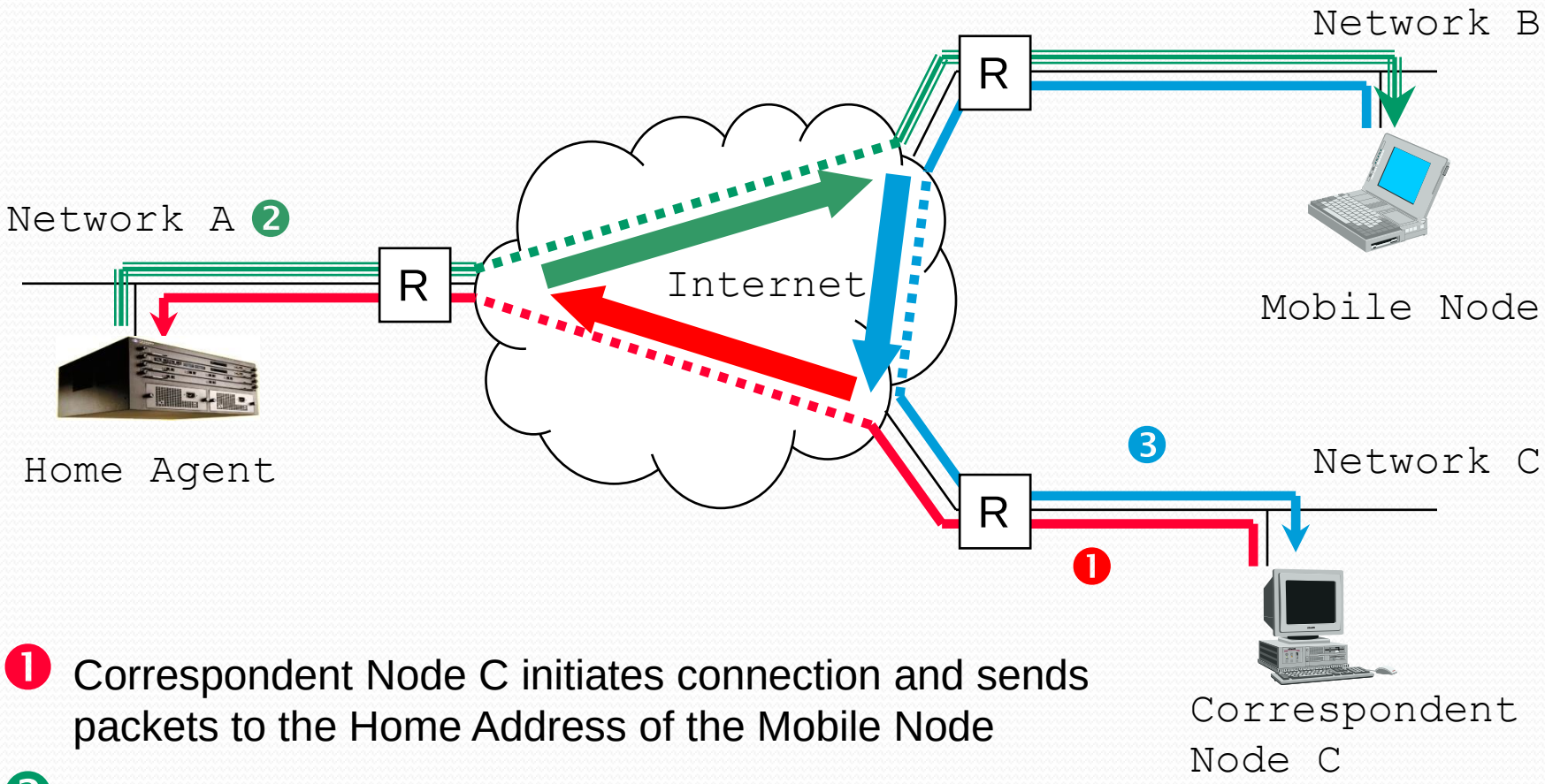
- In order to intercept packets, when a node begins serving as the home agent it MUST multicast onto the home link a Neighbor Advertisement message on behalf of the mobile node.
- All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it were sending this Neighbor Advertisement while at home, with the following exceptions:
  - The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.
  - The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.
  - The Router (R) bit in the Advertisement MUST be set to zero.
  - The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.
  - The Override Flag (O) in the Adv MUST be set, indicating that the Adv SHOULD override any existing Neighbor Cache entry at any node receiving it.
  - The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.
- When a home agent receives a Neighbor Solicitation, it MUST check if the Target Address specified in the message matches the address of any mobile node for which it has a valid entry marked as a home registration.
  - If such an entry exists in the home agent's Binding Cache, the home agent MUST reply to the Neighbor Solicitation with a Neighbor Advertisement giving the home agent's own link-layer address as the link-layer address for the specified Target Address.


0
4
8
12
16
20
24
28
32
Type = 136
Code = 0
Checksum
Flags
Reserved
Target Address
ICMPv6IOptions
0
2
4
6
8
Router Flag (R)
Solicited Flag (S)
Override Flag (O)
Reserved

Packet Processing

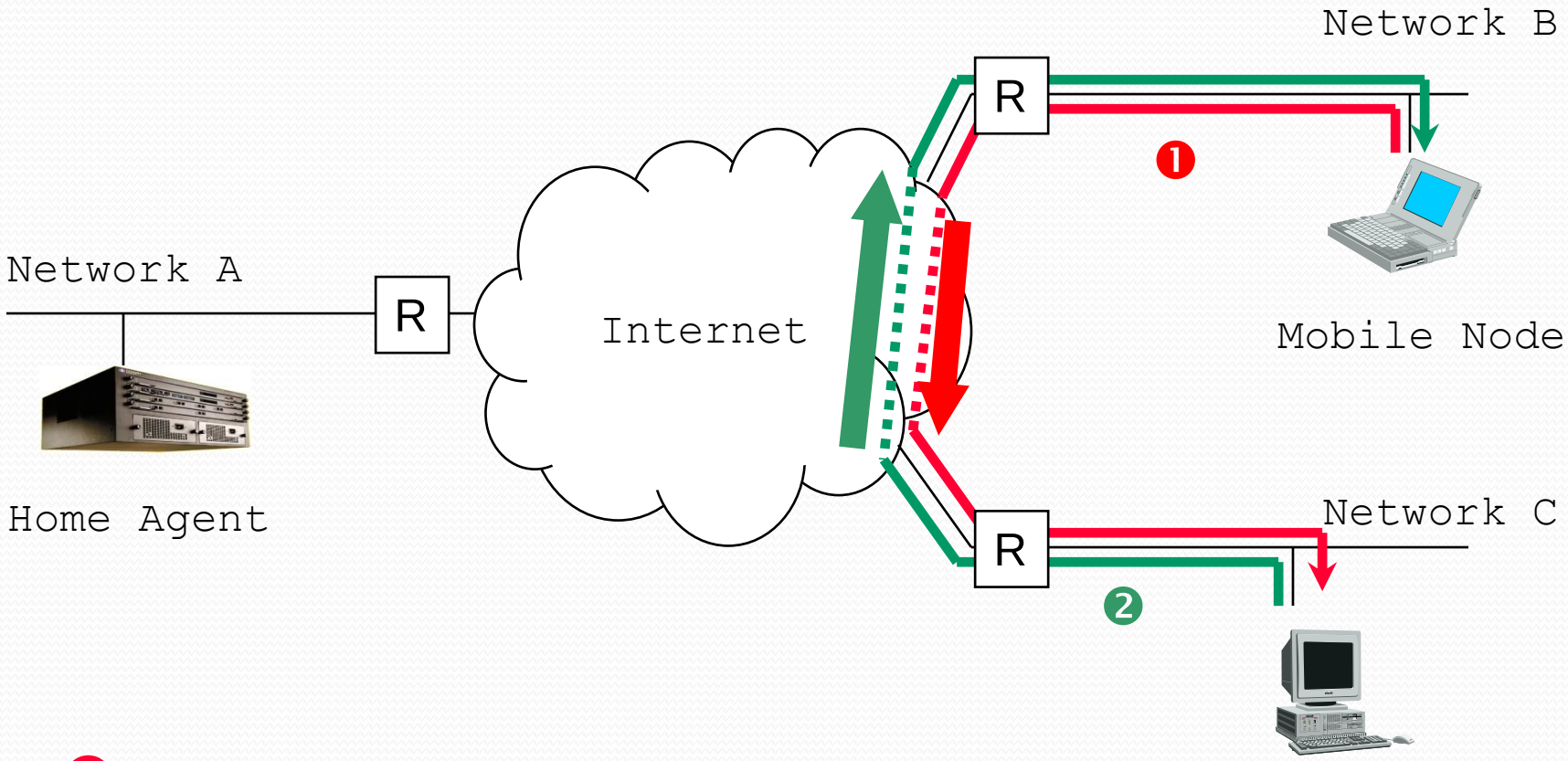
- When received by the mobile node, normal processing of the tunnel header will result in decapsulation and processing of the original packet by the mobile node.
- However, packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node. Instead, these packets MUST be discarded and the home agent SHOULD return an ICMP Destination Unreachable, Code 3, message to the packet's Source Address (unless this Source Address is a multicast address).
- Multicast packets addressed with a global scope, to which the mobile node has successfully subscribed, MUST be tunneled to the mobile node.

Triangular Routing during Initial Phase



1. Correspondent Node C initiates connection and sends packets to the Home Address of the Mobile Node
2. Home Agent intercepts packets and tunnels them to the Mobile Node
3. Mobile Node sends answer directly to Host C

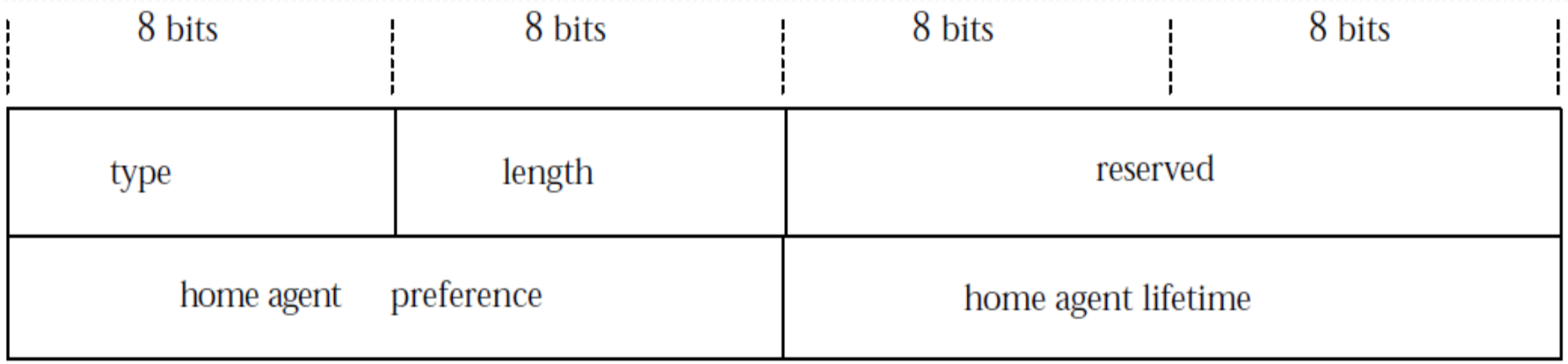
Normal Operation by Route Optimization



1. Mobile Node sends Binding Update to Correspondent Node C
2. Now Correspondent Node can address the CoA of the Mobile Node directly

Dynamic Home Agent Address Discovery

- Home Agents advertise
  - If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists).
  - It allows home agents to share the load between them, in cases where multiple home agents are located on the same link, by utilizing a *preference parameter* in router advertisements
  - Larger values indicate higher availability of the home agent.
  - Every home agent on a link keeps a list (the *home agents list) containing* an IP address of each home agent on the link and its preference.
  - Home agents can change their preference values dynamically and communicate them in router advertisements, depending on their availability or other load-related parameters.
- The mobile node sends a message requesting a list of global IP addresses for possible home agents on its home link.
- The message is sent to the *home agents' anycast address*
- The home agents' IP addresses are arranged in order of preference in the reply, with the most preferred home agent on top of the list


8 bits
8 bits
8 bits
8 bits
type
length
reserved
home agent preference
home agent lifetime

Differences between Mobile IPv4 and Mobile IPv6

- There is no need to deploy special routers as "foreign agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router

- Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions

- Mobile IPv6 route optimization can operate securely even without pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes

- Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering"
- The IPv6 Neighbor Unreachability Detection assures symmetric reachability between the mobile node and its default router in the current location

Differences between Mobile IPv4 and Mobile IPv6

- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4
- Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP. This also improves the robustness of the protocol
- The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state"
- The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent

Conclusion

- The operation of Mobile IPv6, starting with the role of each element: the mobile node, the correspondent node, and the home agent is described.

Course Objective

The aim of the course is to acquaint the students with the basics of internet technologies.

Course Outcomes

The students will be able to

1. Understand how Internet is controlled and managed through different policy formulation and implementation agencies.
2. Describe the protocols and standards adopted by the Internet at the transport layer and networking layer and understand and analyse various performance issues.
3. Describe the commonly used application layer services, such as http and https, World Wide Web, and email with an understanding of client-server architecture.
4. Analyse and develop Internet applications based on client-server programming model.
5. Understand the security threats over the Internet and design and develop technologies to counter the threats.

CO-PO Mapping *(3 – Strong, 2 – Moderate and 1 – Weak)*

CO	PO1	PO2	PO3	PO4	PO 5	PO 6	PO 7	PO8	PO9	PO10	PO11	PO12
1	2						1					
2		3										
3	2				1							
4		1	1									
5			1	1								