Network Working Group
Request for Comments: 5555
Category: Standards Track

H. Soliman, Ed.
Elevate Technologies

June 2009

Mobile IPv6 Support for Dual Stack Hosts and Routers

Status of This Memo

Copyright Notice

Abstract

The current Mobile IPv6 and Network Mobility (NEMO) specifications support IPv6 only. This specification extends those standards to allow the registration of IPv4 addresses and prefixes, respectively, and the transport of both IPv4 and IPv6 packets over the tunnel to the home agent. This specification also allows the mobile node to roam over both IPv6 and IPv4, including the case where Network Address Translation is present on the path between the mobile node and its home agent.

Table of Contents

1. Introduction 3
1.1. Requirements Notation 4
1.2. Motivation for Using Mobile IPv6 Only 4
1.3. Scenarios Considered by This Specification 4
2. Solution Overview 6
2.1. Home Agent Address Discovery 6
2.2. Mobile Prefix Solicitation and Advertisement 7
2.3. Binding Management 8
2.3.1. Foreign Network Supports IPv6 8
2.3.2. Foreign Network Supports IPv4 Only 9
2.4. Route Optimization 11
2.5. Dynamic IPv4 Home Address Allocation 11
3. Extensions and Modifications to Mobile IPv6 11
3.1. Binding Update Extensions 11
3.1.1. IPv4 Home Address Option 11
3.1.2. The IPv4 Care-of Address Option 13
3.1.3. The Binding Update Message Extensions 13
3.2. Binding Acknowledgement Extensions 14
3.2.1. IPv4 Address Acknowledgement Option 14
3.2.2. The NAT Detection Option 16
4. Protocol Operation 17
4.1. Tunnelling Formats 17
4.1.1. Tunnelling Impacts on Transport and MTU 18
4.2. NAT Detection 19
4.3. NAT Keepalives 21
4.4. Mobile Node Operation 22
4.4.1. Selecting a Care-of Address 22
4.4.2. Sending Binding Updates 23
4.4.3. Sending Packets from a Visited Network 25
4.4.4. Movement Detection in IPv4-Only Networks 26
4.5. Home Agent Operation 26
4.5.1. Sending Packets to the Mobile Node 28
4.6. Correspondent Node Operation 29
5. Security Considerations 29
5.1. Handover Interactions for IPsec and IKE 30
5.2. IKE Negotiation Messages between the Mobile Node and Home Agent 33
5.2.1. IKEv2 Operation for Securing DSMIPv6 Signaling 33
5.2.2. IKEv2 Operation for Securing Data over IPv4 36
6. Protocol Constants 38
7. Acknowledgements 38
8. IANA Considerations 38
9. References 39
9.1. Normative References 39
9.2. Informative References 40
10. Contributors 41

1. Introduction

Mobile IPv6 [RFC3775] and NEMO [RFC3963] allow mobile nodes to move within the Internet while maintaining reachability and ongoing sessions, using an IPv6 home address or prefix. However, since IPv6 is not widely deployed, it is unlikely that mobile nodes will initially use only IPv6 addresses for their connections. It is reasonable to assume that mobile nodes will, for a long time, need an IPv4 home address that can be used by upper layers. It is also reasonable to assume that mobile nodes will move to networks that might not support IPv6 and would therefore need the capability to support an IPv4 care-of address. Hence, this specification extends Mobile IPv6 capabilities to allow dual stack mobile nodes to request that their home agent (also dual stacked) tunnel IPv4/IPv6 packets addressed to their home addresses, as well as IPv4/IPv6 care-of address(es).

Using this specification, mobile nodes would only need Mobile IPv6 and [RFC3963] to manage mobility while moving within the Internet, hence eliminating the need to run two mobility management protocols simultaneously. This specification provides the extensions needed in order to allow dual stack mobile nodes to use IPv6 mobility only.

This specification will also consider cases where a mobile node moves into a private IPv4 network and gets configured with a private IPv4 care-of address. In these scenarios, the mobile node needs to be able to traverse the IPv4 NAT in order to communicate with the home agent. IPv4 NAT traversal for Mobile IPv6 is presented in this specification.

In this specification, the term "mobile node" refers to both a mobile host and a mobile router unless the discussion is specific to either hosts or routers. Similarly, we use the term "home address" to reflect an address/prefix format. Note that both mobile host and router functionality have already been defined in [RFC3775] and [RFC3963], respectively. This specification does not change those already defined behaviors, nor does it extend the specific types of hosts and router support already defined, with the following two exceptions: (i) allowing the mobile node to communicate with its home agent even over IPv4 networks, and (ii) allowing the use of IPv4 home addresses and prefixes.

In this specification, extensions are defined for the binding update and binding acknowledgement. It should be noted that all these extensions apply to cases where the mobile node communicates with a Mobility Anchor Point (MAP) as defined in [RFC5380]. The

requirements on the MAP are identical to those stated for the home agent; however, it is unlikely that NAT traversal would be needed with a MAP, as it is expected to be in the same address domain.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Motivation for Using Mobile IPv6 Only

IPv6 offers a number of improvements over today's IPv4, primarily due to its large address space. Mobile IPv6 offers a number of improvements over Mobile IPv4 [RFC3344], mainly due to capabilities inherited from IPv6. For instance, route optimization and dynamic home agent discovery can only be achieved with Mobile IPv6.

One of the advantages of the large address space provided by IPv6 is that it allows mobile nodes to obtain a globally unique care-of address wherever they are. Hence, there is no need for Network Address Translator (NAT) traversal techniques designed for Mobile IPv4. This allows Mobile IPv6 to be a significantly simpler and more bandwidth-efficient mobility management protocol. At the same time, during the transition towards IPv6, NAT traversal for existing private IPv4 networks needs to be considered. This specification introduces NAT traversal for this purpose.

The above benefits make the case for using only Mobile IPv6 for dual stack mobile nodes, as it allows for a long-lasting mobility solution. The use of Mobile IPv6 for dual stack mobility eliminates the need for changing the mobility solution due to the introduction of IPv6 within a deployed network.

1.3. Scenarios Considered by This Specification

There are several scenarios that illustrate potential incompatibilities for mobile nodes using Mobile IPv6. Some of the problems associated with mobility and transition issues were presented in [RFC4977]. This specification considers the scenarios that address all the problems discussed in [RFC4977]. The scenarios considered in this specification are listed below.

All of the following scenarios assume that both the mobile node and the home agent are IPv4- and IPv6-enabled and that only Mobile IPv6 is used between the mobile node and the home agent. We also assume

that the home agent is always reachable through a globally unique IPv4 address. Finally, it's important to note that the following scenarios are not mutually exclusive.

Scenario 1: IPv4-only foreign network

In this scenario, a mobile node is connected to an IPv4-only foreign network. The mobile node can only configure an IPv4 care-of address.

Scenario 2: Mobile node behind a NAT

In this scenario, the mobile node is in a private IPv4 foreign network that has a NAT device connecting it to the Internet. If the home agent is located outside the NAT device, the mobile node will need a NAT traversal mechanism to communicate with the home agent.

It should be noted that [RFC5389] highlights issues with some types of NATs that act as generic Application Level Gateways (ALGs) and rewrite any 32-bit field containing the NAT's public IP addresses. This specification will not support such NATs.

Scenario 3: Home agent behind a NAT

In this scenario, the communication between the mobile node and the home agent is further complicated by the fact that the home agent is located within a private IPv4 network. However, in this scenario, we assume that the home agent is allocated a globally unique IPv4 address. The address might not be physically configured on the home agent interface. Instead, it is associated with the home agent on the Network Address Port Translation (NAPT) device, which allows the home agent to be reachable through address or port mapping.

Scenario 4: Use of IPv4-only applications

In this scenario, the mobile node may be located in an IPv4, IPv6, or dual network. However, the mobile node might be communicating with an IPv4-only node. In this case, the mobile node would need a stable IPv4 address for its application. The alternative to using an IPv4 address is to use protocol translators; however, end-to-end communication with IPv4 is preferred to the use of protocol translators.

The mobile node may also be communicating with an IPv4-only application that requires an IPv4 address.

The cases above illustrate the need for the allocation of a stable IPv4 home address to the mobile node. This is done using an IPv4 home address. Since running Mobile IPv4 and Mobile IPv6

simultaneously is problematic (as illustrated in [RFC4977]), this scenario adds a requirement on Mobile IPv6 to support IPv4 home addresses.

Scenario 5: IPv6 and IPv4-enabled networks

In this scenario, the mobile node should prefer the use of an IPv6 care-of address for either its IPv6 or IPv4 home address. Normal IP-in-IP tunnelling should be used in this scenario as described in [RFC3775]. Under rare exceptions, where IP-in-IP tunnelling for IPv6 does not allow the mobile node to reach the home agent, the mobile node follows the sending algorithm described in Section 4.4.1. UDP tunnelling in IPv6 networks is proposed in this document as a last-resort mechanism when reachability cannot be achieved through normal IP-in-IP tunnelling. It should not be viewed as a normal mode of operation and should not be used as a first resort.

2. Solution Overview

In order to allow Mobile IPv6 to be used by dual stack mobile nodes, the following needs to be done:

- Mobile nodes should be able to use IPv4 and IPv6 home or care-of addresses simultaneously and to update their home agents accordingly.

- Mobile nodes need to be able to know the IPv4 address of the home agent as well as its IPv6 address. There is no need for IPv4 prefix discovery, however.

- Mobile nodes need to be able to detect the presence of a NAT device and traverse it in order to communicate with the home agent.

This section presents an overview of the extensions required in order to allow mobile nodes to use only Mobile IPv6 for IP mobility management.

2.1. Home Agent Address Discovery

Dynamic Home Agent Address Discovery (DHAAD) is defined in [RFC3775] to allow mobile nodes to discover their home agents by appending a well-known anycast interface identifier to their home link’s prefix. However, this mechanism is based on IPv6-anycast routing. If a mobile node (MN) is located in an IPv4-only foreign network, it cannot rely on native IPv6 routing. In this scenario, the solution for discovering the home agent’s IPv4 address is through the Domain Name System (DNS). If the MN is attached to an IPv6-only or dual

stack network, it may also use procedures defined in [CHOWDHURY] to discover home agent information. Note that the use of [CHOWDHURY] cannot give the mobile node information that allows it to communicate with the home agent if the mobile node is located in an IPv4-only network. In this scenario, the mobile node needs to discover the IPv4 address of its home agent through the DNS.

For DNS lookup by name, the mobile node should be configured with the name of the home agent. When the mobile node needs to discover a home agent, it sends a DNS request with QNAME set to the configured name. An example is "ha1.example.com". If a home agent has an IPv4 and IPv6 address, the corresponding DNS record should be configured with both 'AAAA' and 'A' records. Accordingly, the DNS reply will contain 'AAAA' and 'A' records.

For DNS lookup by service, the SRV record defined in [RFC5026] is reused. For instance, if the service name is "mip6" and the protocol name is "ipv6" in the SRV record, the mobile node SHOULD send a DNS request with the QNAME set to "_mip6._ipv6.example.com". The response should contain the home agent's FQDN(s) and may include the corresponding 'AAAA' and 'A' records as well.

If multiple home agents reside on the home link, each configured with a public IPv4 address, then the operation above applies. The correct DNS entries can be configured accordingly.

2.2. Mobile Prefix Solicitation and Advertisement

According to [RFC3775], the mobile node can send a Mobile Prefix Solicitation and receive a Mobile Prefix Advertisement containing all prefixes advertised on the home link.

A dual stack mobile node MAY send a Mobile Prefix Solicitation message encapsulated in IPv4 (i.e., IPv6 in IPv4) in the case where the mobile node has no access to IPv6 within the local network. Securing these messages requires the mobile node to have a security association with the home agent, using IPsec and based on the mobile node's IPv4 care-of address as described in [RFC3775] and [RFC4877].

[RFC3775] requires the mobile node to include the home address option in the solicitation message sent to the home agent. If the mobile node is located in an IPv4 network, it will not be assigned an IPv6 address to include in the source address. In this case, the mobile node MUST use its home address in the source address field of the IPv6 packet, in addition to using the home address option as expected by [RFC3775].

2.3. Binding Management

A dual stack mobile node will need to update its home agent with its care-of address. If a mobile node has an IPv4 and an IPv6 home address, it will need to create a binding cache entry for each address. The format of the IP packet carrying the binding update and acknowledgement messages will vary depending on whether the mobile node has access to IPv6 in the visited network. There are three different scenarios to consider with respect to the visited network:

- The visited network has IPv6 connectivity and provides the mobile node with a care-of address (in a stateful or stateless manner).
- The mobile node can only configure a globally unique IPv4 address in the visited network.
- The mobile node can only configure a private IPv4 address in the visited network.

2.3.1. Foreign Network Supports IPv6

In this case, the mobile node is able to configure a globally unique IPv6 address. The mobile node will send a binding update to the IPv6 address of its home agent, as defined in [RFC3775]. The binding update MAY include the IPv4 home address option introduced in this document. After receiving the binding update, the home agent creates two binding cache entries: one for the mobile node's IPv4 home address and another for the mobile node's IPv6 home address. Both entries will point to the mobile node's IPv6 care-of address. Hence, whenever a packet is addressed to the mobile node's IPv4 or IPv6 home address, the home agent will tunnel it in IPv6 to the mobile node's IPv6 care-of address that is included in the binding update. Effectively, the mobile node establishes two different tunnels, one for its IPv4 traffic (IPv4 in IPv6) and one for its IPv6 traffic (IPv6 in IPv6), with a single binding update.

In this scenario, this document extends [RFC3775] by including the IPv4 home address option in the binding update message. Furthermore, if the network supports both IPv4 and IPv6, or if the mobile node is experiencing problems with IP-in-IP tunnelling, this document proposes some mitigating actions as described in Section 4.4.1.

After accepting the binding update and creating the corresponding binding cache entries, the home agent MUST send a binding acknowledgement to the mobile node as defined in [RFC3775]. In addition, if the binding update included an IPv4 home address option, the binding acknowledgement MUST include the IPv4 address acknowledgment option as described in Section 3.2.1. This option

informs the mobile node whether the binding was accepted for the IPv4 home address. If this option is not included in the binding acknowledgement and the IPv4 home address option was included in the binding update, the mobile node MUST assume that the home agent does not support the IPv4 home address option and therefore SHOULD NOT include the option in future binding updates to that home agent address.

When a mobile node acquires both IPv4 and IPv6 care-of addresses at the foreign network, it SHOULD prioritize the IPv6 care-of address for its MIPv6 binding as described in Section 4.4.1.

2.3.2. Foreign Network Supports IPv4 Only

If the mobile node is in a foreign network that only supports IPv4, it needs to detect whether a NAT is in its communication path to the home agent. This is done while exchanging the binding update and acknowledgement messages as shown later in this document. NAT detection is needed for the purposes of the signaling presented in this specification.

2.3.2.1. Foreign Network Supports IPv4 Only (Public Addresses)

In this scenario, the mobile node will need to tunnel IPv6 packets containing the binding update to the home agent's IPv4 address. The mobile node uses the IPv4 address it gets from the foreign network as a source address in the outer header. The binding update will contain the mobile node's IPv6 home address. However, since the care-of address in this scenario is the mobile node's IPv4 address, the mobile node MUST include its IPv4 care-of address in the IPv6 packet. The IPv4 address is represented in the IPv4 care-of address option defined in this specification. If the mobile node had an IPv4 home address, it MUST also include the IPv4 home address option described in this specification.

After accepting the binding update, the home agent MUST create a new binding cache entry for the mobile node's IPv6 home address. If an IPv4 home address option is included, the home agent MUST create another entry for that address. All entries MUST point to the mobile node's IPv4 care-of address. Hence, all packets addressed to the mobile node's home address(es) (IPv4 or IPv6) will be encapsulated in an IPv4 header that includes the home agent's IPv4 address in the source address field and the mobile node's IPv4 care-of address in the destination address field.

After accepting the binding updates and creating the corresponding entries, the home agent MUST send a binding acknowledgement as specified in [RFC3775]. In addition, if the binding update included

an IPv4 home address option, the binding acknowledgement MUST include the IPv4 address acknowledgment option as described in Section 3.2.1. The binding acknowledgement is encapsulated to the IPv4 care-of address, which was included in the source address field of the IPv4 header encapsulating the binding update.

2.3.2.2. Foreign Network Supports IPv4 Only (Private Addresses)

In this scenario the mobile node will need to tunnel IPv6 packets containing the binding update to the home agent's IPv4 address. In order to traverse the NAT device, IPv6 packets are tunneled using UDP and IPv4. The UDP port allocated for the home agent is 4191 (dsmipv6).

The mobile node uses the IPv4 address it gets from the visited network as a source address in the IPv4 header. The binding update will contain the mobile node's IPv6 home address.

After accepting the binding update, the home agent MUST create a new binding cache entry for the mobile node's IPv6 home address. If an IPv4 home address option is included, the home agent MUST create another entry for that address. All entries MUST point to the mobile node's IPv4 care-of address included in the source address of the IPv4 header that encapsulated the binding update message. In addition, the tunnel used MUST indicate UDP encapsulation for NAT traversal. Hence, all packets addressed to the mobile node's home address(es) (IPv4 or IPv6) will be encapsulated in UDP and then encapsulated in an IPv4 header that includes the home agent's IPv4 address in the source address field and the mobile node's IPv4 care-of address in the destination address field. Note that the home agent MUST store the source UDP port numbers contained in the packet carrying the binding update in order to be able to forward packets to the mobile node.

After accepting the binding updates and creating the corresponding entries, the home agent MUST send a binding acknowledgement as specified in [RFC3775]. In addition, if the binding update included an IPv4 home address option, the binding acknowledgement MUST include the IPv4 address acknowledgment option as described later in this specification. The binding acknowledgement is encapsulated in UDP and then in IPv4 with the home agent's IPv4 address in the source address field and the mobile node's IPv4 care-of address in the destination field. The IPv4 address in the destination field of the IPv4 packet is the source address that was received in the IPv4 header containing the binding update message. The inner IPv6 packet will contain the home agent's IPv6 address as a source address and the mobile node's IPv6 home address in the destination address field.

The mobile node needs to maintain the NAT bindings for its current IPv4 care-of address. This is done through sending the binding update regularly to the home agent.

2.4. Route Optimization

Route optimization, as specified in [RFC3775], will operate in an identical manner for dual stack mobile nodes when they are located in a visited network that provides IPv6 addresses to the mobile node and while communicating with an IPv6-enabled correspondent node. However, when located in an IPv4-only network, or when using the IPv4 home address to communicate with an IPv4 correspondent node, route optimization will not be possible due to the difficulty of performing the return-routability test. In this specification, UDP encapsulation is only used between the mobile node and its home agent. Therefore, mobile nodes will need to communicate through the home agent.

Route optimization will not be possible for IPv4 traffic -- that is, traffic addressed to the mobile node's IPv4 home address. This is similar to using Mobile IPv4; therefore, there is no reduction of features resulting from using this specification.

2.5. Dynamic IPv4 Home Address Allocation

It is possible to allow for the mobile node's IPv4 home address to be allocated dynamically. This is done by including 0.0.0.0 in the IPv4 home address option that is included in the binding update. The home agent SHOULD allocate an IPv4 address to the mobile node and include it in the IPv4 address acknowledgement option sent to the mobile node. In this case, the lifetime of the binding is bound to the minimum of the lifetimes of the IPv6 binding and the lease time of the IPv4 home address.

3. Extensions and Modifications to Mobile IPv6

This section highlights the protocol and implementation additions required to support this specification.

3.1. Binding Update Extensions

3.1.1. IPv4 Home Address Option

This option is included in the mobility header, including the binding update message sent from the mobile node to a home agent or Mobility Anchor Point. The alignment requirement for this option is 4n.

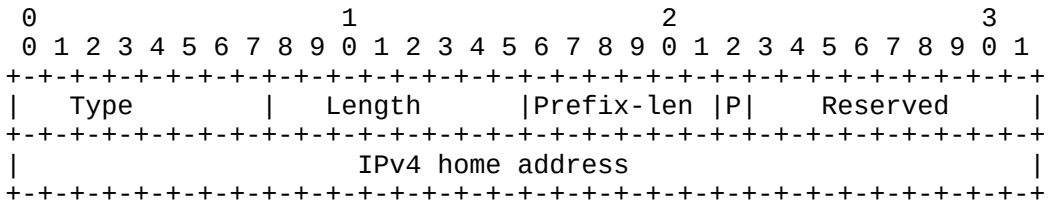

Figure 1: IPv4 Home Address Option

Type

29

Length

6

Prefix-len

The length of the prefix allocated to the mobile node. If only a single address is allocated, this field MUST be set to 32. In the first binding update requesting a prefix, the field contains the prefix length requested. However, in the following binding updates, this field must contain the length of the prefix allocated. A value of zero is invalid and MUST be considered an error.

P

A flag indicating, when set, that the mobile node requests a mobile network prefix. This flag is only relevant for new requests, and must be ignored for binding refreshes.

Reserved

This field is reserved for future use. It MUST be set to zero by the sender and ignored by the receiver.

IPv4 Home Address

The mobile node’s IPv4 home address that should be defended by the home agent. This field could contain any unicast IPv4 address (public or private) that was assigned to the mobile node. The value 0.0.0.0 is used to request an IPv4 home address from the home agent. A mobile node may choose to use this option to request a prefix by setting the address to All Zeroes and setting the P flag. The mobile node could then form an IPv4 home address

based on the allocated prefix. Alternatively, the mobile node may use two different options, one for requesting an address (static or dynamic) and another for requesting a prefix.

3.1.2. The IPv4 Care-of Address Option

This option is included in the mobility header, including the binding update message sent from the mobile node to a home agent or Mobility Anchor Point. The alignment requirement for this option is 4n.

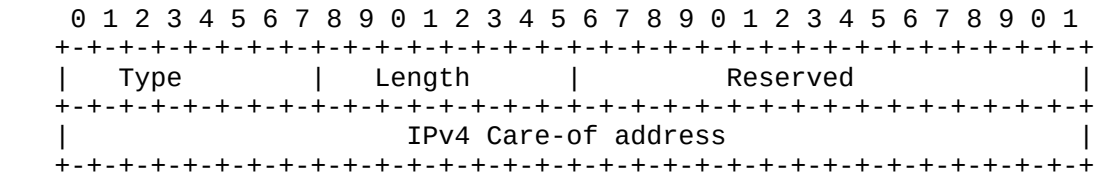

Figure 2: The IPv4 CoA Option

Type

32

Length

6

Reserved

This field is set to zero by the sender and ignored by the receiver.

IPv4 Care-of Address

This field contains the mobile node's IPv4 care-of address. The IPv4 care-of address is used when the mobile node is located in an IPv4-only network.

3.1.3. The Binding Update Message Extensions

This specification extends the binding update message with one new flag. The flag is shown and described below.

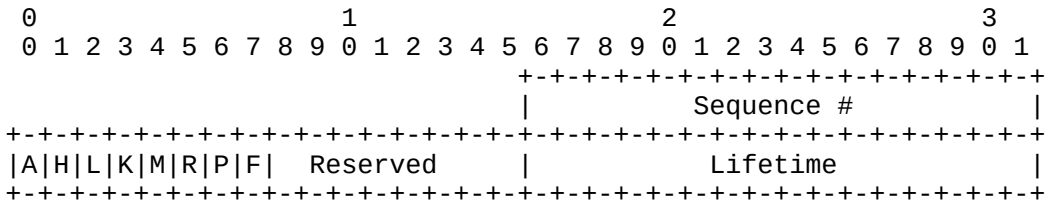

Figure 3: Binding Update Message

F

When set, this flag indicates a request for forcing UDP encapsulation regardless of whether a NAT is present on the path between the mobile node and the home agent. This flag may be set by the mobile node if it is required to use UDP encapsulation regardless of the presence of a NAT. This flag SHOULD NOT be set when the mobile node is configured with an IPv6 care-of address -- with the exception of the scenario mentioned in Section 4.4.1.

3.2. Binding Acknowledgement Extensions

3.2.1. IPv4 Address Acknowledgement Option

This option is included in the mobility header, including the binding acknowledgement message sent from the home agent or Mobility Anchor Point to the mobile node. This option indicates whether a binding cache entry was created for the mobile node's IPv4 address. Additionally, this option includes an IPv4 home address in the case of dynamic IPv4 home address configuration (i.e., if the unspecified IPv4 address was included in the binding update). The alignment requirement for this option is 4n.

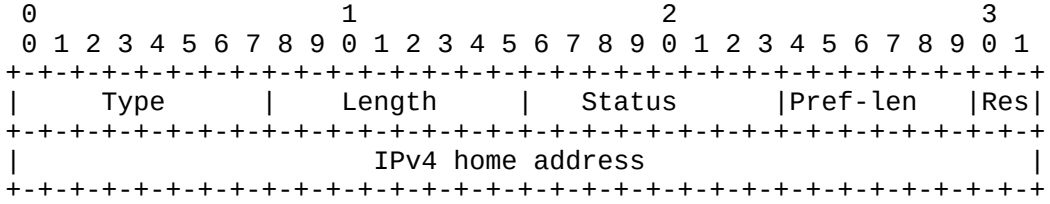

Figure 4: IPv4 Address Acknowledgement Option

Type

30

Length

6

Status

Indicates success or failure for the IPv4 home address binding. Values from 0 to 127 indicate success. Higher values indicate failure.

Pref-len

The prefix length of the address allocated. This field is only valid in case of success and MUST be set to zero and ignored in case of failure. This field overrides what the mobile node requested (if not equal to the requested length).

Res

This field is reserved for future use. It MUST be set to zero by the sender and ignored by the receiver

IPv4 Home Address

The IPv4 home address that the home agent will use in the binding cache entry. This could be a public or private address. This field MUST contain the mobile node's IPv4 home address. If the address were dynamically allocated, the home agent will add the address to inform the mobile node. Otherwise, if the address is statically allocated to the mobile node, the home agent will copy it from the binding update message.

The following values are allocated for the status field:

- 0 Success
- 128 Failure, reason unspecified
- 129 Administratively prohibited
- 130 Incorrect IPv4 home address
- 131 Invalid IPv4 address

- 132 Dynamic IPv4 home address assignment not available

- 133 Prefix allocation unauthorized

3.2.2. The NAT Detection Option

This option is sent from the home agent to the mobile node to indicate whether a NAT was in the path. This option MAY also include a suggested NAT binding refresh time for the mobile node. This might be useful for scenarios where the mobile node is known to be moving within the home agent's administrative domain and, therefore, the NAT timeout is known (through configuration) to the home agent. Section 3.5 of [RFC5405] discusses issues with NAT timeout in some detail.

The alignment requirement for this option is 4n. If a NAT is detected, this option MUST be sent by the home agent.

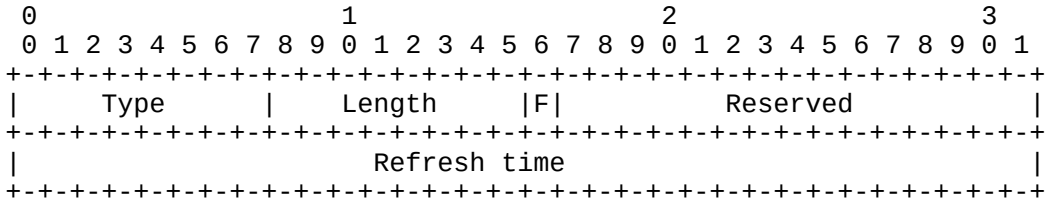

Figure 5: The NAT Detection Option

Type

31

Length

6

F

This flag indicates to the mobile node that UDP encapsulation is required. When set, this flag indicates that the mobile node MUST use UDP encapsulation even if a NAT is not located between the mobile node and home agent. This flag SHOULD NOT be set when the mobile node is assigned an IPv6 care-of address -- with the exception of accommodating the scenarios discussed in Section 4.4.1.

Reserved

This field is reserved for future use. It MUST be set to zero by the sender and ignored by the receiver.

Refresh Time

A suggested time (in seconds) for the mobile node to refresh the NAT binding. If set to zero, it is ignored. If this field is set to all 1s, it means that keepalives are not needed, i.e., no NAT was detected. The home agent MUST be configured with a default value for the refresh time. The recommended value is outlined in Section 6.

4. Protocol Operation

This section presents the protocol operation and processing for the messages presented above. In addition, this section introduces the NAT detection and traversal mechanism used by this specification.

4.1. Tunnelling Formats

This specification allows the mobile node to use various tunnelling formats depending on its location and the visited network's capabilities. The mobile node can tunnel IPv6 in IPv4, IPv4 in IPv6, or use UDP encapsulation to tunnel IPv6 in IPv4. Naturally, this specification also supports tunnelling IPv6 in IPv6 [RFC2473].

This specification allows UDP-based tunnelling to be used between the mobile node and its home agent or MAP. A UDP encapsulation format means the following order of headers:

IPv4/v6

UDP

IP (v4 or v6)

Other headers

Note that the use of UDP encapsulation for IPv6 care-of addresses SHOULD NOT be done except in the circumstances highlighted in Section 4.4.1.

When using this format, the receiver parses the version field following the UDP header in order to determine whether the following header is IPv4 or IPv6. The rest of the headers are processed normally. The above order of headers does not take IPsec headers

into account as they may be placed in different parts of the packet. The above format MUST be supported by all implementations of this specification and MUST always be used to send the binding update message.

UDP tunnelling can also encapsulate an Encapsulating Security Payload (ESP) header as shown below:

IPv4/v6

UDP

ESP

IP (v4 or v6)

Other headers

The negotiation of the secure tunnel format described above is discussed in Section 5.2. The receiver of a UDP tunnel detects whether or not an ESP header is present based on the UDP port used.

4.1.1. Tunnelling Impacts on Transport and MTU

Changing the tunnel format may occur due to movement of the mobile node from one network to another. This can impact the link and path MTU, which may affect the amount of bandwidth available to the applications. The mobile node may use Path MTU Discovery (PMTUD) as specified in [RFC4459].

To accommodate traffic that uses Explicit Congestion Notification (ECN), it is RECOMMENDED that the ECN and Differentiated Services Code Point (DSCP) information be copied between the inner and outer header as defined in [RFC3168] and [RFC2983]. It is RECOMMENDED that the full-functionality option defined in Section 9.1.1 of [RFC3168] be used to deal with ECN.

Note that some implementations may not be able to use ECN over the UDP tunnel. This is due to the lack of access to ECN bits in the UDP API on most platforms. However, this issue can be avoided if UDP encapsulation is done in the kernel.

Note that, when using UDP encapsulation, the Time to Live (TTL) field must be decremented in the same manner as when IP-in-IP encapsulation is used.

4.2. NAT Detection

This section deals with NAT detection for the purpose of encapsulating packets between the mobile node and the home agent when the mobile node is present in a private IPv4 network. Mobile IPv6 uses IKEv2 to establish the IPsec security association (SA) between the mobile node and the home agent. IKEv2 has its own NAT detection mechanism. However, IKEv2's NAT detection is only used for the purpose of setting up the IPsec SA for secure traffic. The interactions between the two NAT traversal mechanisms are described in Section 5.

NAT detection is done when the initial binding update message is sent from the mobile node to the home agent. When located in an IPv4-only foreign link, the mobile node sends the binding update message encapsulated in UDP and IPv4. The source address of the IPv6 packet is the mobile node's IPv6 home address. The destination address is the IPv6 address of the home agent. The IPv4 header contains the IPv4 care-of address in the source address field and the IPv4 address of the home agent in the destination address field.

When the home agent receives the encapsulated binding update, it compares the IPv4 address of the source address field in the IPv4 header with the IPv4 address included in the IPv4 care-of address option. If the two addresses match, no NAT device was in the path. Otherwise, a NAT was in the path and the NAT detection option is included in the binding acknowledgement. The binding acknowledgement and all future packets are then encapsulated in UDP and IPv4. The source address in the IPv4 header is the IPv4 address of the home agent. The destination address is the IPv4 address received in the IPv4 header encapsulating the binding update (this address will be different from the IPv4 care-of address when a NAT is in the path). The source port in the packet is the home agent's source port. The destination port is the source port received in the binding update message. Note that the home agent stores the port numbers and associates them with the mobile node's tunnel in order to forward future packets.

Upon receiving the binding acknowledgement with the NAT detection option, the mobile node sets the tunnel to the home agent to UDP encapsulation. Hence, all future packets to the home agent are tunneled in UDP and IPv4. For all tunneled IPv6 packets, the source address in the IPv6 header is the mobile node's IPv6 home address and the destination address is the correspondent node's IPv6 address. All tunneled IPv4 packets will contain the mobile node's IPv4 home address in the source address field of the inner IPv4 packet and the

correspondent node's IPv4 address in the destination address field. The outer IPv4 header is the same whether the inner packet is IPv4 or IPv6.

If no NAT device was detected in the path between the mobile node and the home agent, then IPv6 packets are tunneled in an IPv4 header unless the home agent forces UDP encapsulation using the F flag. The content of the inner and outer headers are identical to the UDP encapsulation case.

A mobile node MUST always tunnel binding updates in UDP when located in an IPv4-only network. Essentially, this process allows for perpetual NAT detection. Similarly, the home agent MUST encapsulate binding acknowledgements in a UDP header whenever the binding update is encapsulated in UDP.

In conclusion, the packet formats for the binding update and acknowledgement messages are shown below:

Binding update received by the home agent:

IPv4 header (src=V4ADDR, dst=HA_V4ADDR)

UDP header

IPv6 header (src=V6HOA, dst=HAADDR)

ESP header

Mobility header

BU [IPv4 HAO]

IPv4 CoA option

Where V4ADDR is either the IPv4 care-of address or the address provided by the NAT device. V6HOA is the IPv6 home address of the mobile node. The binding update MAY also contain the IPv4 home address option, IPv4 HAO.

Binding acknowledgement sent by the home agent:

IPv4 header (src= HA_V4ADDR, dst=V4ADDR)

UDP header

IPv6 header (src=HAADDR, dst=V6HOA)

ESP header

Mobility header

BA ([IPv4 ACK], NAT DET)

Where V6HOA is the IPv6 home address of the mobile node. The IPv4 ACK is the IPv4 address acknowledgement option, which is only included if the IPv4 home address option is present in the BU. The NAT DET is the NAT detection option, which MUST be present in the binding acknowledgement message if the binding update was encapsulated in UDP.

4.3. NAT Keepalives

If a NAT is detected, the mobile node will need to refresh the NAT bindings in order to be reachable from the home agent. NAT bindings can be refreshed through sending and receiving traffic encapsulated in UDP. However, if the mobile node is not active, it will need to periodically send a message to the home agent in order to refresh the NAT binding. This can be done using the binding update message. The binding update/acknowledgement pair will ensure that the NAT bindings are refreshed in a reliable manner. There is no way for the mobile node to know the exact time of the NAT binding. The default time suggested in this specification is NATKATIMEOUT (see Section 6). If the home agent suggests a different refresh period in the binding acknowledgement, the mobile node SHOULD use the value suggested by the home agent.

If the refresh time in the NAT detection option in the binding acknowledgement is set to all 1s, the mobile node need not send messages to refresh the NAT binding. However, the mobile node may still be required to encapsulate traffic in UDP. This scenario may take place when a NAT is not detected but the home agent still requires the mobile node to use UDP encapsulation.

It should be noted that a mobile node that does not need to be reachable (i.e., one that only cares about the session continuity aspect of Mobile IP) does not need to refresh the NAT binding. In this case, the mobile node would only be able to initiate communication with other nodes. However, this is likely to imply that the mobile node will need to send a binding update before initiating communication after a long idle period as it is likely to be assigned a different port and IPv4 address by the NAT when it initiates communication. Hence, an implementation may choose, for the sake of simplicity, to always maintain the NAT bindings even when it does not need reachability.

Note that keepalives are also needed by IKEv2 over UDP port 4500. This is needed for IKE (Internet Key Exchange Protocol) dead-peer detection, which is not handled by DSMIPv6 keepalives.

4.4. Mobile Node Operation

In addition to the operations specified in [RFC3775] and [RFC3963], this specification requires mobile nodes to be able to support an IPv4 home address. This specification also requires the mobile node to choose an IPv4 or an IPv6 care-of address. We first discuss care-of address selection, then continue with binding management and transmission of normal traffic.

4.4.1. Selecting a Care-of Address

When a mobile node is in a dual stacked, visited network, it will have a choice between an IPv4 and an IPv6 care-of address. The mobile node SHOULD prefer the IPv6 care-of address and bind it to its home address(es). If a mobile node attempted to bind the IPv6 care-of address to its home address(es) and the binding update timed out, the mobile node SHOULD:

- Resend the binding update using the exponential back-off algorithm described in [RFC3775].

- If after three attempts, in total, a binding acknowledgement was not received, the mobile node SHOULD send a new binding update using the IPv4 care-of address. The exponential backoff algorithm described in [RFC3775] should be used for re-transmission of the binding update if needed.

This procedure should be used to avoid scenarios where IPv6 connectivity may not be as reliable as IPv4. This unreliability may take place during early deployments of IPv6 or may simply be due to temporary outages affecting IPv6 routing.

It is RECOMMENDED that upon movement, the mobile node not change the IP address family chosen for the previous binding update unless the mobile node is aware that it has moved to a different administrative domain where previous problems with IPv6 routing may not be present. Repeating the above procedure upon every movement can cause significant degradation of the mobile node’s applications’ performance due to extended periods of packet losses after handover, if the routing outage is still in effect.

When using an IPv4 care-of address and IP-in-IP encapsulation, if the mobile node implementation is made aware by upper layers of persistent packet losses, it may attempt to resend the binding update

with the F flag set, requesting UDP encapsulation for all packets. This may avoid packet losses due to situations where local firewalling policies prevent the use of IP-in-IP encapsulation.

The effect of this address selection mechanism is to allow the following preferences in the absence of NAT:

1. IPv6

2. IPv4 (using IP-in-IP or UDP encapsulation if a NAT is detected)

3. UDP encapsulation when IP-in-IP is not allowed by the local domain.

4.4.2. Sending Binding Updates

When sending an IPv6 packet containing a binding update while connected to an IPv4-only access network, mobile nodes MUST ensure the following:

- The IPv6 packet is encapsulated in UDP.

- The source address in the IPv4 header is the mobile node's IPv4 care-of address.

- The destination address in the IPv4 header is the home agent's IPv4 address.

- The source address in the IPv6 header is the mobile node's IPv6 home address.

- The IPv4 home address option MAY be included in the mobility header. This option contains the IPv4 home address. If the mobile node did not have a static home address, it MAY include the unspecified IPv4 address, which acts as a request for a dynamic IPv4 home address. Alternatively, one or more IPv4 home address options may be included with requests for IPv4 prefixes (i.e., with the P flag set).

- If the mobile node wishes to use UDP encapsulation only, it must set the F flag in the binding update message.

- The IPv6 packet MUST be authenticated as per [RFC3775], based on the mobile node's IPv6 home address.

When sending a binding update from a visited network that supports IPv6, the mobile node MUST follow the rules specified in [RFC3775]. In addition, if the mobile node has an IPv4 home address or needs

one, it MUST include the IPv4 home address option in the mobility header. If the mobile node already has a static IPv4 home address, this address MUST be included in the IPv4 home address option. Otherwise, if the mobile node needs a dynamic IPv4 address, it MUST include the IPv4 0.0.0.0 address in the IPv4 home address option.

In addition to the rules in [RFC3775], the mobile node should follow the care-of address selection guidelines in Section 4.4.1.

When the mobile node receives a binding acknowledgement from the home agent, it follows the rules in [RFC3775] and [RFC3963]. In addition, the following actions MUST be made:

- If the status field indicated failure with error code 144, the mobile node MAY resend the binding update without setting the F flag.

- If the mobility header includes an IPv4 address acknowledgement option indicating success, the mobile node should create two entries in its binding update list: one for the IPv6 home address and another for the IPv4 home address.

- If the NAT detection option is present, the mobile node MUST tunnel future packets in UDP and IPv4. This MUST be indicated in the binding update list.

- If no IPv4 address acknowledgement option is present, and an IPv4 home address option was present in the binding update, the mobile node MUST only create one binding update list entry for its IPv6 home address. The mobile node MAY include the IPv4 home address option in future binding updates.

- If an IPv4 address acknowledgement option is present and it indicates failure for the IPv4 home address binding, the mobile node MUST NOT create an entry for that address in its binding update list. The mobile node MAY include the IPv4 home address option in future binding updates.

4.4.2.1. Removing Bindings

Mobile nodes will remove bindings from the home agent’s binding cache whenever they move to the home link, or simply when mobility support is not needed.

Deregistering the IPv6 home address is described in [RFC3775]. The same mechanism applies in this specification. Mobile nodes may remove the binding for only the IPv4 home address by sending a binding update that does not include the IPv4 home address option.

Upon receiving this binding update, the home agent will replace the existing cache entries with the content of the new message. This ensures that the IPv4 home address binding is removed while maintaining an IPv6 binding.

Note that the mobile node cannot remove the IPv6 home address binding while maintaining an IPv4 home address binding.

A binding update message with a lifetime of zero will remove all bindings for the mobile node.

4.4.3. Sending Packets from a Visited Network

When the mobile node is located in an IPv6-enabled network, it sends and receives IPv6 packets as described in [RFC3775]. In cases where IP-in-IP encapsulation is not providing connectivity to the home agent, the mobile node may choose to encapsulate in UDP as suggested in Section 4.4.1. However, this encapsulation of IPv6 traffic should be used as a last resort, as described. IPv4 traffic is encapsulated in IPv6 packets to the home agent.

When the mobile node is located in an IPv4-only network, it will send IPv6 packets to its home agent according to the following format:

```
IPv4 header (src=V4CoA, dst=HA_V4ADDR)

[UDP header]

IPv6 header (src=V6HoA, dst=CN)

Upper layer protocols
```

Here, the UDP header is only used if a NAT has been detected between the mobile node and the home agent, or if the home agent forced UDP encapsulation. V4CoA is the IPv4 care-of address configured by the mobile node in the visited network.

Similarly, IPv4 packets are sent according to the following format:

```
IPv4 header (src=V4CoA, dst=HA_V4ADDR)

[UDP header]

IPv4 header (src=V4HoA, dst=V4CN)

Upper Layer protocols
```

Here, the UDP header is only used if a NAT has been detected between the mobile node and the home agent, or if the home agent forced UDP encapsulation.

4.4.4. Movement Detection in IPv4-Only Networks

[RFC3775] describes movement detection mostly based on IPv6-specific triggers and Neighbor Discovery [RFC4861] information. These triggers are not available in an IPv4-only network. Hence, a mobile node located in an IPv4-only network SHOULD use [RFC4436] for guidance on movement-detection mechanisms in IPv4-only networks.

The mobile node detects that it's in an IPv4-only network when the IPv6 movement-detection algorithm fails to configure an IPv6 address.

This specification does not support mobile nodes returning home while using IPv4. That is, the IPv4 support is only defined for mobile nodes that are in a visited network.

4.5. Home Agent Operation

In addition to the home agent specification in [RFC3775] and [RFC3963], the home agent needs to be able to process the IPv4 home address option and generate the IPv4 address acknowledgement option. Both options are included in the mobility header. Furthermore, the home agent MUST be able to detect the presence of a NAT device and indicate that presence in the NAT detection option included in the binding acknowledgement.

A home agent must also act as a proxy for address resolution in IPv4 for the registered IPv4 home addresses of mobile nodes it is serving. Moreover, the administrative domain of the home agent is responsible for advertising the routing information of registered IPv4 mobile-network prefixes of the mobile nodes.

In order to comply with this specification, the home agent MUST be able to find the IPv4 home address of a mobile node when given the IPv6 home address. That is, given an IPv6 home address, the home agent MUST store the corresponding IPv4 home address if a static one is present. If a dynamic address is requested by the mobile node, the home agent MUST store that address (associated with the IPv6 home address) after it's allocated to the mobile node.

When the home agent receives a binding update encapsulated in UDP and containing the IPv4 home address option, it needs to follow all the steps in [RFC3775] and [RFC3963]. In addition, the following checks MUST be done:

- If the IPv4 care-of address in the IPv4 CoA option is not the same as the IPv4 address in the source address in the IPv4 header, then a NAT was in the path. This information should be flagged for the binding acknowledgement.

- If the F flag in the binding update is set, the home agent needs to determine whether it accepts forcing UDP encapsulation. If it does not, the binding acknowledgement is sent with error code 144. UDP encapsulation SHOULD NOT be used when the mobile node is located in an IPv6-enabled link, with the exception of the scenarios outlined in Section 4.4.1.

- If the IPv4 home address option contains a valid unicast IPv4 address, the home agent MUST check that this address is allocated to the mobile node that has the IPv6 home address included in the home address option. The same MUST be done for an IPv4 prefix.

- If the IPv4 home address option contained the unspecified IPv4 address, the home agent SHOULD dynamically allocate an IPv4 home address to the mobile node. If none is available, the home agent MUST return error code 132 in the status field of the IPv4 address acknowledgement option. If a prefix is requested, the home agent SHOULD allocate a prefix with the requested length; if prefix allocation (of any length) is not possible, the home agent MUST indicate failure of the operation with the appropriate error code.

- If the binding update is accepted for the IPv4 home address, the home agent creates a binding cache entry for the IPv4 home address/prefix. The home agent MUST include an IPv4 acknowledgement option in the mobility header containing the binding acknowledgement.

- If the binding update is accepted for both IPv4 and IPv6 home addresses, the home agent creates separate binding cache entries, one for each home address. The care-of address is the one included in the binding update. If the care-of address is an IPv4 address, the home agent MUST set up a tunnel to the IPv4 care-of address of the mobile node.

When sending a binding acknowledgement to the mobile node, the home agent constructs the message according to [RFC3775] and [RFC3963]. Note that the routing header MUST always contain the IPv6 home address as specified in [RFC3775].

If the care-of address of the mobile node is an IPv4 address, the home agent includes the mobile node’s IPv6 home address in the destination address field in the IPv6 header. If a NAT is detected, the home agent MUST then encapsulate the packet in UDP and in an IPv4

header. The source address is set to the home agent's IPv4 address and the destination address is set to the address received in the source address of the IPv4 header encapsulating the binding update.

After creating a binding cache entry for the mobile node's home addresses, all packets sent to the mobile node's home addresses are tunneled by the home agent to the mobile node's care-of address. If a NAT is detected, packets are encapsulated in UDP and IPv4. Otherwise, if the care-of address is an IPv4 address and no NAT is detected, packets are encapsulated in an IPv4 header unless UDP encapsulation is forced by the home agent.

4.5.1. Sending Packets to the Mobile Node

The home agent follows the rules specified in [RFC3775] for sending IPv6 packets to mobile nodes located in IPv6 networks. When sending IPv4 packets to mobile nodes in an IPv6 network, the home agent must encapsulate the IPv4 packets in IPv6.

When sending IPv6 packets to a mobile node located in an IPv4 network, the home agent uses the following format:

```
IPv4 header (src= HA_V4ADDR, dst= V4ADDR)

[UDP header]

IPv6 header (src=CN, dst= V6HoA)

Upper layer protocols
```

Where the UDP header is only included if a NAT is detected between the mobile node and the home agent or if the home agent forced UDP encapsulation. V4ADDR is the IPv4 address received in the source address field of the IPv4 packet containing the binding update.

When sending IPv4 packets to a mobile node located in an IPv4 network, the home agent must follow the format negotiated in the binding update/acknowledgement exchange. In the absence of a negotiated format, the default format that MUST be supported by all implementations is:

```
IPv4 header (src= HA_V4ADDR, dst= V4ADDR)

[UDP header]

IPv4 header (src=V4CN, dst= V4HoA)

Upper layer protocols
```

Where the UDP header is only included if a NAT is detected between the mobile node and home agent or if the home agent forced UDP encapsulation.

4.6. Correspondent Node Operation

This specification has no impact on IPv4 or IPv6 correspondent nodes.

5. Security Considerations

This specification allows a mobile node to send one binding update for its IPv6 and IPv4 home addresses. This is a slight deviation from [RFC3775], which requires one binding update per home address. However, like [RFC3775], the IPsec security association needed to authenticate the binding update is still based on the mobile node's IPv6 home address. Therefore, in order to authorize the mobile node's IPv4 home address binding, the home agent MUST store the IPv4 address corresponding to the IPv6 address that is allocated to a mobile node. Therefore, it is sufficient for the home agent to know that the IPsec verification for the packet containing the binding update was valid, provided that it knows which IPv4 home address is associated with which IPv6 home address. Hence, the security of the IPv4 home address binding is the same as the IPv6 binding.

In effect, associating the mobile node's IPv4 home address with its IPv6 home address moves the authorization of the binding update for the IPv4 address to the Mobile IPv6 implementation, which infers it from the fact that the mobile node has an IPv6 home address and the right credentials for sending an authentic binding update for the IPv6 address.

This specification requires the use of IKEv2 as the default mechanism for dynamic keying.

In cases where this specification is used for NAT traversal, it is important to note that it has the same vulnerabilities associated with [RFC3519]. An attacker is able to hijack the mobile node's session with the home agent if it can modify the contents of the outer IPv4 header. The contents of the header are not authenticated and there is no way for the home agent to verify their validity. Hence, a man in the middle attack, where a change in the contents of the IPv4 header can cause a legitimate mobile node's traffic to be diverted to an illegitimate receiver independently of the authenticity of the binding update message, is possible.

In this specification, the binding update message MUST be protected using ESP transport mode. When the mobile node is located in an IPv4-only network, the binding update message is encapsulated in UDP

as described earlier in Section 4.2. However, UDP SHOULD NOT be used to encapsulate the binding update message when the mobile node is located in an IPv6-enabled network. If protection of payload traffic is needed when the mobile node is located in an IPv4-only network, encapsulation is done using tunnel mode ESP over port 4500 as described in [RFC3948]. During the IKE negotiation with the home agent, if the mobile node and home agent support the use of port 4500, the mobile node MUST establish the security association over port 4500, regardless of the presence of a NAT. This is done to avoid switching between ports 500 and 4500 and the potential traffic disruption resulting from this switch.

Handovers within private IPv4 networks or from IPv6 to IPv4 networks will impact the security association between the mobile node and the home agent. The following section presents the expected behaviour of the mobile node and home agent in those situations. The details of the IKE negotiations and messages are illustrated in Section 5.2.

5.1. Handover Interactions for IPsec and IKE

After the mobile node detects movement, it configures a new care-of address. If the mobile node is in an IPv4-only network, it removes binding update list entries for correspondent nodes, since route optimisation cannot be supported. This may cause inbound packet losses, as remote correspondent nodes are unaware of such movement. To avoid confusion in the correspondent node, the mobile node SHOULD deregister its binding with each correspondent node by sending a deregistration binding update. The deregistration binding update message is tunnelled to the home agent and onto the correspondent node. This is done after the mobile node updates the home agent with its new location as discussed below.

The mobile node sends the binding update message to the home agent. If the mobile node is in an IPv6-enabled network, the binding update SHOULD be sent without IPv4/UDP encapsulation, unless UDP encapsulation is needed as described in Section 4.4.1. If the mobile node is in an IPv4-only network, then -- after IPsec processing of the binding update (BU) message -- it encapsulates the BU in UDP/IPv4 as discussed in Sections 4.2 and 4.4. In order to be able to send the binding update while in an IPv4-only network, the mobile node needs to use the new IPv4 care-of address in the outer header, which is different from the care-of address used in the existing tunnel. This should be done without permanently updating the tunnel within the mobile node’s implementation in order to allow the mobile node to receive packets on the old care-of address until the binding acknowledgement is received. The method used to achieve this effect is implementation dependent and is outside the scope of this specification. This implies that the IP forwarding function (which

selects the interface or tunnel through which a packet is sent) is not based solely on the destination address: some IPv6 packets destined to the home agent are sent via the existing tunnel, while BUs are sent using the new care-of address. Since BUs are protected by IPsec, the forwarding function cannot necessarily determine the correct treatment from the packet headers. Thus, the DSMIPv6 implementation has to attach additional information to BUs, and this information has to be preserved after IPsec processing and made available to the forwarding function or to DSMIP extensions included in the forwarding function. Depending on the mobile node's implementation, meeting this requirement may require changes to the IPsec implementation.

Upon receiving the binding update message encapsulated in UDP/IPv4, the home agent processes it as follows. In order to allow the DSMIPv6 implementation in the home agent to detect the presence of a NAT on the path to the mobile node, it needs to compare the outer IPv4 source address with the IPv4 address in the IPv4 care-of address option. This implies that the information in the outer header will be preserved after IPsec processing and made available to the DSMIPv6 implementation in the home agent. Depending on the home agent's implementation, meeting this requirement may require changes to the IPsec implementation.

The home agent updates its tunnel mode security association to include the mobile node's care-of address as the remote-tunnel header address and 4500 as the port number. The IPv4 address and port number are likely to be wrong; the mobile node provides the correct information in a separate exchange as described below. When the mobile node is located in a private IPv4 network (which is detected as described above), the new address and port number are allocated by the NAT. The home agent will also enable or disable UDP encapsulation for outgoing ESP packets for the purpose of NAT traversal.

If the Key Management Mobility Capability (K) bit was set in the binding update, and the home agent supports this feature, the home agent updates its IKE security associations to include the mobile node's care-of address as the peer address and 4500 as the port number. The home agent may also need to change NAT traversal fields in the IKE_SA to enable the dynamic update of the IP address and port number, based on the reception of authenticated IKE messages or authenticated packets using tunnel mode ESP. The dynamic updates are described in Section 2.23 of [RFC4306]. As described above, when the mobile node is located in a private IPv4 network, the address and port number used for IPsec and IKE traffic is not yet known by the home agent at this point.

The mobile node updates the IKE SA in one of two ways. If the K flag was set in the binding acknowledgement message, the mobile node SHOULD send an empty informational message, which results in the IKE module in the home agent dynamically updating the SA information. The IKE implementation in the home agent is REQUIRED to support this feature. Alternatively, the IKE SA should be re-negotiated. Note that updating the IKE SA MUST take place after the mobile node has sent the binding update and received the acknowledgement from the home agent.

It is important to note that the mobile node's IPv4 care-of address seen by the DSMIPv6 module in the home agent upon receiving the binding update may differ from the IPv4 care-of address seen by the IKE module and the care-of address used for forwarding IPsec tunnel mode traffic. Hence, it is probable that different modules in the home agent will have a different care-of address that should be used for encapsulating traffic to the mobile node.

After successfully processing the binding update, the home agent sends the binding acknowledgement to the mobile node's care-of address as received in the outer header of the packet containing the binding update. Note that if the BU was rejected, the binding acknowledgement (BAck) is sent to the same address from which the BU was received. This may require special treatment in IP forwarding and/or IPsec processing that resembles the sending of BUs in the mobile node (described above).

Upon receiving the binding acknowledgement, the mobile node updates its local tunnel mode security association information to include the tunnel header IP source address, which is the mobile node's address, and the tunnel header IP destination, which is the home agent's address. The mobile node may also need to enable or disable UDP encapsulation for outgoing ESP packets for the purpose of NAT traversal and the sending of keepalives.

The mobile node MAY use MOBIKE [RFC4555] to update its IKE SA with the home agent. Using MOBIKE requires negotiating this capability with the home agent when establishing the SA. In this case, the mobile node and the home agent MUST NOT update their IPsec SAs locally, as this step is performed by MOBIKE. Furthermore, the use of MOBIKE allows the mobile node to update the SA independently of the binding update exchange. Hence, there is no need for the mobile node to wait for a binding acknowledgement before performing MOBIKE. The use of MOBIKE is OPTIONAL in this specification.

5.2. IKE Negotiation Messages between the Mobile Node and Home Agent

This specification defines a number of possible data encapsulation formats, depending on the mobile node's connectivity to the visited network. When connected to an IPv6-enabled network, the tunnelling formats are clear. However, when connected to an IPv4-only network, care should be taken when negotiating the IKE association and the consequential tunnelling formats used for secure and insecure traffic. This section illustrates the IKE message exchange between the mobile node and home agent when the mobile node is located in an IPv4-only network. Two different IKE negotiations are considered:

- o IKEv2 operation for securing DSMIPv6 signaling.
- o IKEv2 operation for securing data over IPv4

5.2.1. IKEv2 Operation for Securing DSMIPv6 Signaling

A mobile node connected to an IPv4-only network SHOULD follow the procedures described below in order to establish an SA for the protection of binding update and binding acknowledgement messages. Note that V4ADDR refers to either the mobile node's care-of address in the visited link or the public address allocated to the mobile node by the NAT.

```
Mobile Node                                          Home Agent
-----------                                          ----------
IPv4(source_addr=V4ADDR, dest_addr=HAADDR)
 UDP (500, 500) HDR, SAi1, KEi, Ni
  NAT-D, NAT-D -->

                    <- IPv4(source_addr=HAADDR, dest_addr=V4ADDR)
                             UDP(500,X) HDR, SAr1, KEr, Nr, [CERTREQ]
                              NAT-D, NAT-D

IPv4(source_addr=V4ADDR, dest_addr=HAADDR)
  UDP (4500,4500) <non-ESP Marker > HDR, SK
  {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, N(USE_TRANSPORT_MODE),
  SAi2, TSi, TSr}
 -->

                    <-- IPv4(source_addr=HAADDR, dest_addr=V4ADDR)
                            UDP (4500,Y) <non-ESP Marker > HDR, SK
                            {IDr, [CERT,] AUTH, N(USE_TRANSPORT_MODE),
                            SAr2, TSi, TSr}
```

The corresponding Security Policy Database (SPD) entries are shown below.

Mobile node SPD-S:

```
   IF local_address = home_address_1 &

      remote_address = home_agent_1 &

      proto = MH & local_mh_type = BU &

      remote_mh_type = BAck

  Then use SA ESP transport mode

  Initiate using IDi = user_1 to address home_agent_1
```

Home Agent SPD-S:

```
   IF local_address = home_agent_1 &

      remote_address = home_address_1 &

      proto = MH &

      local_mh_type = BAck &

      remote_mh_type = BU

   Then use SA ESP transport mode
```

Where home_address_1 is the mobile node's registered IPv6 home address and home_agent_1 is the IP address of the home agent.

The above should result in BU/BA messages with the following BU received by the home agent:

```
   IPv4 header (src=V4ADDR, dst=HA_V4ADDR)

   UDP header (sport=Z, dport=DSMIPv6)

   IPv6 header (src=V6HOA, dst=HAADDR)

   ESP header in transport mode

   Mobility header

   BU [IPv4 HAO]
```

IPv4 CoA option

(and others as needed)

At the home agent, following UDP de-capsulation, the binding update is delivered to the IPsec module as shown below:

IPv6 header (src=V6HOA, dst=HAADDR)

ESP header in transport mode

Mobility header

BU [IPv4 HAO]

IPv4 CoA option

(and others as needed)

In addition, V4ADDR and the sport (Z) need to be passed with the packet to ensure correct processing.

Following IPsec processing, the binding update is delivered to the DSMIPv6 home agent module as follows:

IPv6 header (src=V6HOA, dst=HAADDR)

Mobility header

BU [IPv4 HAO]

IPv4 CoA option

(and others as needed)

In addition, V4ADDR and the sport (Z) need to be passed with the packet to ensure correct processing.

The binding acknowledgement sent by the home agent module to the IPsec module is as follows:

IPv6 header (src=HAADDR, dst=V6HOA)

Mobility header

BA ([IPv4 ACK], NAT DET)

(and others as needed)

In addition, V4ADDR, the sport from the BU (Z), and an indication that UDP encapsulation must be used need to be passed with the packet to ensure correct processing.

The binding acknowledgement sent by the home agent to the mobile node is as follows:

IPv4 header (src= HA_V4ADDR, dst=V4ADDR)

UDP header (sport=DSMIPv6, dport=Z)

IPv6 header (src=HAADDR, dst=V6HOA)

ESP header in transport mode

Mobility header

BA ([IPv4 ACK], NAT DET)

5.2.2. IKEv2 Operation for Securing Data over IPv4

To secure data traffic when the mobile node is located in an IPv4-only network, the mobile node MUST establish a child_SA for that purpose. Note that V4ADDR refers to either the mobile node's care-of address in the visited link or the public address allocated to the mobile node by the NAT. The procedure is as follows:

```
Mobile Node                                        Home Agent
-----------                                        ----------
IPv4(source_addr=V4ADDR, dest_addr=HAADDR)
 UDP (4500,4500) < non-ESP Marker > HDR, SK
  {[N], SA, Ni, [KEi], TSi, TSr}    -->

                     <--IPv4(source_addr=HAADDR, dest_addr=V4ADDR)
                            UDP (4500,Y) < non-ESP Marker > HDR, SK
                             SA, Nr, [KEr], TSi, TSr}
```

If no NAT is detected, the encapsulation used will be:

IPv4 (source_addr=v4CoA, dest_addr=HAAddr)

ESP

IP (source_addr=HoA, set_addr=CNAddr)

Upper_layer_HDR

Where IP is either IPv4 or IPv6 and HoA is either the IPv4 HoA or the IPv6 HoA.

If a NAT is detected, the encapsulation used will be:

IPv4 (source_addr=v4Addr, dest_addr=HAAddr)

UDP (sport=Y, dport=4500)

ESP

IP (source_addr=HoA, set_addr=CNAddr)

Upper_layer_HDR

Where v4CoA may be the external IPv4 address of the NAT, IP is either an IPv4 or IPv6 header, and HoA is either the IPv4 or the IPv6 HoA. The above format shows the packet as seen by the home agent.

The SPD, whether a NAT is detected or not, is set as follows. Note that this rule is designed to match all data from the MN to nodes other than the home agent. This is done so that this rule does not overlap with the earlier rule securing BU/BA signaling between the MN and the HA.

Mobile Node SPD-S:

IF local_address = home_address &

remote_address != home_agent &

proto=any

Then use SA ESP tunnel mode

Initiate using IDi = user_1 to address home_agent_1

home agent SPD-S:

IF local_address != home_agent &

remote_address = home_address &

proto=any

Then use SA ESP tunnel mode

Where home_address is the MN's registered IPv6 or IPv4 home address and home_agent is the IPv6 or the IPv4 address of the home agent.

6. Protocol Constants

NATKATIMEOUT = 110 seconds.

7. Acknowledgements

Thanks to the following members (in alphabetical order) of the MIP6 and NEMO Working Groups for their contributions, discussions, and reviews: Jari Arkko, Sri Gundavelli, Wassim Haddad, Alfred Hoenes, Conny Larsson, Acee Lindem, Ahmad Muhanna, Vidya Narayanan, Karen Nielsen, and Keiichi Shima. Thanks to Karen Nielsen, Pasi Eronen, and Christian Kaas-Petersen for raising the issue of IKEv2 interactions and proposing the solution included in this document. Thanks to Pasi Eronen for many thorough reviews of this document.

8. IANA Considerations

IANA has made the following allocations according to this specification:

A UDP port (4191) has been assigned for the NAT traversal mechanism described in Section 4.2.

The IPv4 home address option described in Section 3.1.1 has been assigned value 29. This option is included in the mobility header described in [RFC3775].

The IPv4 address acknowledgement option described in Section 3.2.1 has been assigned value 29. This option is included in the mobility header described in [RFC3775].

The NAT detection option described in Section 3.2.2 has been assigned a value 31. This option is included in the mobility header described in [RFC3775].

The IPv4 care-of address option described in Section 3.1.2 has been assigned value 32. This option is included in the mobility header described in [RFC3775].

The status field in the IPv4 home address option has been allocated by IANA under the new registry: "DSMIPv6 IPv4 Home Address Option Status Codes".

The status field values are allocated using the following procedure:

1. New status field values are allocated through IETF review. This is for all RFC types including standards track, informational, and experimental status that originate from the IETF and have been approved by the IESG for publication.

2. Requests for new option type value assignments from outside the IETF are only made through the publication of an IETF document, per 1 above. Note also that documents published as Independent "RFC Editor contributions" [RFC4844] are not considered to be IETF documents.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4436] Aboba, B., Carlson, J., and S. Cheshire, "Detecting Network Attachment in IPv4 (DNAv4)", RFC 4436, March 2006.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[RFC5026] Giaretta, G., Ed., Kempf, J., and V. Devarapalli, Ed., "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

9.2. Informative References

[CHOWDHURY] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", Work in Progress, April 2008.

[RFC2983] Black, D., "Differentiated Services and Tunnels", RFC 2983, October 2000.

[RFC3344] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3519] Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, April 2003.

[RFC4459] Savola, P., "MTU and Fragmentation Issues with In-the-Network Tunneling", RFC 4459, April 2006.

[RFC4844] Daigle, L., Ed., and Internet Architecture Board, "The RFC Series and RFC Editor", RFC 4844, July 2007.

[RFC4977] Tsirtsis, G. and H. Soliman, "Problem Statement: Dual Stack Mobility", RFC 4977, August 2007.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC5405] Eggert, L. and G. Fairhurst, "Unicast UDP Usage Guidelines for Application Designers", BCP 145, RFC 5405, November 2008.

10. Contributors

This document reflects discussions and contributions from several people including (in alphabetical order):

Vijay Devarapalli: vijay.devarapalli@azairenet.com

James Kempf: kempf@docomolabs-usa.com

Henrik Levkowetz: henrik@levkowetz.com

Pascal Thubert: pthubert@cisco.com

George Tsirtsis: G.Tsirtsis@Qualcomm.com

Ryuji Wakikawa: ryuji@sfc.wide.ad.jp

Author’s Address

Hesham Soliman (editor)
Elevate Technologies

EMail: hesham@elevatemobile.com