NEMO Working Group
Internet-Draft
Expires: January 10, 2005

C. Ng
Panasonic Singapore Labs
J. Hirano
Panasonic

July 12, 2004

Securing Nested Tunnels Optimization with Access Router Option
draft-ng-nemo-access-router-option-01

Status of this Memo

Copyright Notice

Abstract

Network Mobility (NEMO) Basic Support provides global connectivity to mobile network through the establishment of bi-directional tunnels between a mobile router and home agent. However, this sub-optimal routing, especially when nesting of mobile networks or Mobile IPv6 (MIPv6) host occurs within a mobile network. This memo proposes using a new mobility header option called the Access Router Option to allow a mobile node (host/router) to inform its home agent (HA) or corespondent node (CN) the home-address (HoA) of the access router it

is currently attached to. From there, this memo lays out a mechanism that allows mobile nodes to securely achieve nested tunnels optimization, and even full route optimization.

Table of Contents

1. Introduction 4
1.1 Terms Used 5
1.2 Organization 5
1.3 Change Log 6
2. Overview of Operation 7
2.1 Router Advertisement 7
2.2 Binding Update from MR1 to HA1 7
2.3 Binding Update from MR2 to HA1 8
2.4 Forwarding Packets from HA1 to MR1 8
2.5 Forwarding Packets from MR1 to HA1 9
2.6 Scenario with a Local Fixed Router 9
2.7 Route Optimization with Mobile Network Hosts 10
3. Changes to Existing Protocols 12
3.1 Modifications to NEMO Basic Support / Mobile IPv6 12
3.1.1 Addition of Access Router Option 12
3.1.2 Extending Type 2 Router Header 13
3.1.3 Modification to Conceptual Data Structures 14
3.2 Modifications to IPv6 Neighbor Discovery 15
3.2.1 Addition of New Option in Router Advertisement 15
3.3 Modifications to ICMPv6 16
3.3.1 New Router Global Address ICMP Message 16
3.4 Extending the Router Alert Option 18
4. Operation of ARO-Enabled Mobile Routers 20
4.1 Operation When Mobile Router is At Home 20
4.1.1 Sending Router Advertisement 20
4.1.2 Processing Outbound Packets 20
4.1.3 Processing Inbound Packets 20
4.2 Operation When Mobile Router is Away 21
4.2.1 Sending Router Advertisement 21
4.2.2 Receiving Router Advertisement 21
4.2.3 Sending Binding Updates 21
4.2.4 Processing Outbound Packets 22
4.2.5 Processing Inbound Packets 23
4.3 IPSec Processing 24
4.3.1 IPSec Processing on Inbound Packets 24
4.3.2 IPSec Processing on Outbound Packets 24

5. Operation of ARO-Enabled Home Agents 25
5.1 Receiving Binding Updates 25
5.2 Receiving Tunneled Packets from Away Nodes 25
5.3 Tunneling Packets to Away Nodes 26
5.4 IPSec Processing 28
5.4.1 IPSec Processing on Inbound Packets 28

5.4.2 IPSec Processing on Outbound Packets 28
6. Operation of ARO-Enabled Mobile Network Nodes 29
6.1 Nested Tunnel Optimization with Home Agent 29
6.2 Receiving Router Advertisement 29
6.3 Sending Binding Updates 29
6.4 Sending Data Packets 30
6.5 Processing Inbound Packets 30
6.6 IPSec Processing 31
6.6.1 IPSec Processing on Inbound Packets 31
6.6.2 IPSec Processing on Outbound Packets 31
7. Operation of ARO-Enabled Correspondent Node 32
7.1 Receiving Binding Updates 32
7.2 Receiving Route Optimized Packets from Mobile Nodes . . . 32
7.3 Sending Route Optimized Packets to Mobile Nodes 32
7.4 IPSec Processing 33
7.4.1 IPSec Processing on Inbound Packets 33
7.4.2 IPSec Processing on Outbound Packets 33
8. Design Considerations 34
8.1 Considerations in the Use of Mutable Router Alert Option 34
8.1.1 Overview of Router Alert Option 34
8.1.2 Example where an Immutable RAO is Used 34
8.1.3 The Need for Mutable RAO 36
8.1.4 Alternatives to the Mutable Router Alert Option . . . 36
8.2 Change of Source Address 37
8.2.1 Justifications 37
8.2.2 Alternatives 38
9. Security Considerations 39
9.1 Addition of Access Router Option 39
9.2 Router Global Address Option 40
9.3 Accepting Tunnel with a Source Address not Directly Bound to the Home Address 40
9.4 Use of Extended Routing Header Type 2 41
9.5 Mutable Router Alert Option 42
9.6 IPSec Processing 43

9.6.1 Processing of Extended Routing Header Type 2 43
9.6.2 Processing of Home Address Destination Option 43
9.6.3 Processing of Mutable Router Alert Option 43
10. References 45
Authors' Addresses 46
A. Acknowledgement 46
Intellectual Property and Copyright Statements 47

1. Introduction

This memo describes a proposed solution for provisioning route optimization in Network Mobility (NEMO). This solution is built on top of Mobile IPv6 (MIPv6) [1] and NEMO Basic Support [2][3]. The general problem of route optimization in NEMO is analyzed and summarized in [4].

The proposed solution described in this memo aims to solve the following route optimizations problems:

- Nested Tunnel Optimization

  This optimization problem is to eliminate the nesting of tunnels for a nested mobile network. The proposed solution requires changes to the mobile router (MR) and home agent (HA) implementation so that no matter how many level of nesting a mobile network has, there is only one tunnel between the innermost MR and its HA.

- Nested Tunnel Optimization for MIPv6

  This optimization problem is to eliminate the nesting of tunnels for a MIPv6 host in a mobile network. The proposed solution requires changes to the MR, MIPv6 host, and HA (for both the MR and MIPv6 host) implementation so that for a visiting mobile host in a mobile network, the only tunnel necessary is the one between the MIPv6 host and its HA, without additional encapsulation at the

MR.

- MIPv6 over NEMO Optimization

  This optimization problem is to allow the MIPv6 route optimization to work between a MIPv6 host in a mobile network (i.e. visiting mobile host) and its correspondent node (CN). The proposed solution requires changes to the MR, MIPv6 host, and CN implementation so that a visiting mobile host in a mobile network can perform route optimization with a CN, without any tunneling back to the home agents of either the MIPv6 host or MR.

Various different proposals have been submitted to the NEMO Working Group to solve different aspects of the route optimization problem of network mobility. Readers are encouraged to look at <http://www.mobilenetworks.org/nemo/> for a complete list of Internet Drafts that have been published.

1.1 Terms Used

It is assumed that readers are familiar with the NEMO terminology described in [5] and those defined in [4]. In addition, [4] also presents a detailed description of the problem of route optimization in NEMO.

Apart from the terms described in [5] and [4], we further define the following terminology:

Access Router (AR)

Any router that is the point of attachment to the Internet of one or more visiting mobile node (VMN). We use the phrase "access router of node X" to loosely refer to the router a node X attaches to. An access router can be a MR.

ARO-Solution, ARO-enabled

To aid our illustration, we refer to the solution proposed in this memo as the "ARO-Solution". Any network nodes that implements the

"ARO-Solution" is referred to as a "ARO-enabled" node.

1.2 Organization

In this memo, we first begin in Section 2 by giving a general overview of the proposed ARO Solution in operation. This is followed by a detailed description of the modifications to existing protocols in Section 3. Following which, the operation of each entity: mobile router, home agent, mobile network node, and correspondent node that support the ARO Solution are detailed respectively from Section 4 through Section 7. In Section 8, we list some of the design considerations when formulating the ARO Solution. Finally, security considerations in discussed in Section 9.

1.3 Change Log

- Changes from version -00 to -01
  - Extended solution to be able to optimized over local fixed router with inclusion of NEMO-BU RAO
  - Inclusion of NEMO-BU RAO and a new ICMPv6 message
  - Extended solution for optimization between MR and CN
  - Extended solution for optimization between VMN and CN/HA
  - Included operations of CN and VMN

2. Overview of Operation

This section gives an overview of the operation of the proposed solution. We use the scenario illustrated in Figure 1 below as an example to describe the operation of the ARO-solution.

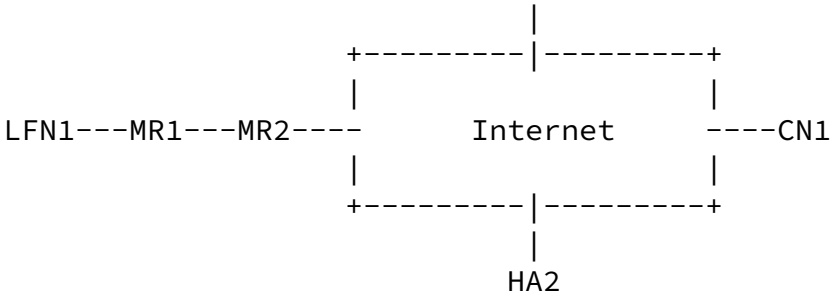


Figure 1: Example Scenario

In Figure 1, LFN1 is a local fixed node attached to the ingress interface of the visiting mobile router (VMR) MR1. MR1 is itself attached to the ingress interface of another mobile router, MR2. HA1 is the home agent of MR1, and HA2 is the home agent of MR2. LFN1 is communicating with a correspondent node CN1.

2.1 Router Advertisement

When MR1 first obtains a Router Advertisement (RA) from MR2, it checks if MR2 supports the ARO-Solution. This is determined by an additional option (known as Router Global Address Option, or RGAO) that advertises the home-address (HoA) of MR2.

2.2 Binding Update from MR1 to HA1

After MR1 obtains a care-of-address (CoA), it sends Binding Update (BU) to its home agent, HA1. The BU message, beside having the prefix informations as detailed in [2], also contains an important extension, known as the "Access Router Option" (ARO). This ARO specifies the global address of MR2, thus informing HA1 the access router MR1 is currently attached to. In this case, since MR2 is itself a mobile router, the global address is the HoA of MR2.

HA1 records this together with the binding update in the corresponding binding cache entry (BCE). When returning the Binding Acknowledgment (BA), HA1 can then made use of the extended Type 2 Routing Header (RH2) to forward the BA message to MR1 via the HoA of MR2. Here, the RH2 as defined by Mobile IPv6 specification [1] is extended so that it can store more than one address. In addition, HA1 should insert the same ARO in BA message to indicate that the BU

with ARO is accepted.

Since the BA message is addressed to the HoA of MR2, the BA message will be intercepted by HA2. Here, we assume that the BCE of HA2 contains a binding of the current CoA and HoA of MR2. Thus, HA2 will tunnel the packet to the CoA of MR2. When MR2 receives and decapsulates the BA message, it notices that there is an extended RH2. It proceeds to swap the destination address with the appropriate entry in the RH2 (which should be the CoA of MR1), and forward it to MR1. MR1 receives the packet, verifies that it is the final destination of the packet, and consumes the BA message.

2.3 Binding Update from MR2 to HA1

From the processing of the extended RH2 as described previously, MR2 can deduce the following two facts:

1. the sender (i.e. HA1) does not have a BCE of MR2's current CoA, since the received packet is encapsulated in a tunnel from HA2, and

2. HA1 is ARO-enabled, since an extended RH2 is used.

Having established these, MR2 may then send a BU to HA1. In this case, HA1 is treated as a correspondent node from the perspective of MR2. Thus, the Return Routability (RR) procedure specified in [1] must be carried out before sending the BU message. Note also that since HA1 is treated as a correspondent node, MR2 should not insert any prefix information (i.e. Mobile Network Prefix Option [2]) in the BU message. Once the binding update is successful, MR2 should add the host address of HA1 to a locally maintained Binding Update List. This list contains a list of hosts that have an active binding cache entry of MR2's current CoA.

Note that if the access router (fixed or mobile) of MR2 is ARO-enabled, MR2 should add an ARO in the BU it sent to HA1 to inform HA1 the global address of the access router MR2 is currently attached to. To simply our description, we assume that this is not the case.

2.4 Forwarding Packets from HA1 to MR1

After receiving the BU message from MR2, the bi-directional tunnel between HA1 and MR1 need not go through the tunnel between HA2 and MR2. Instead, tunnel packets from HA1 to MR1 can be sent directly to the CoA of MR2 with an attached extended RH2.

As an illustration, suppose CN1 now sends a packet to LFN1. The packet will be intercepted by HA1. HA1 checks its routing table and

notices that the packet should be forwarded to MR1. However, a check of its binding cache reveals that MR1 is away. Hence, HA1 needs to tunnel the packet to the current CoA of MR1. Furthermore, HA1 knows that MR1 is currently attached to MR2, and HA1 has a BCE of MR2. Thus, the tunnel should be configured, with an extended RH2, such that it reaches CoA of MR1 via CoA MR2. In this case, the destination address of the outer packet is set to the CoA of MR2, and the entries in the RH2 are the CoA and HoA of MR1, in that order. When MR2 receives such a packet, it updates the RH2 (i.e. swap the destination address with the next entry in the RH2), and forward the packet to the new destination (i.e. CoA of MR1). MR1 upon receiving the packet will verify that it is the final destination of the outer packet, and decapsulates the packet. The inner packet is addressed to LFN1, a valid address in the subnet of MR1. Hence, MR1 forwards the packet to its appropriate ingress interface.

2.5 Forwarding Packets from MR1 to HA1

When LFN1 sends a packet to CN1, MR1 will encapsulate the packet to be sent through the reverse tunnel with its home agent HA1. The outer packet is appended with a mutable Router Alert Option (RAO) [6], in addition to the Home Address destination Option (HAO). This RAO requests upstream routers that are ARO-enabled to forward packet directly to the destination. When MR2 receives this packet and noticed the RAO, it checks if it has a binding update with the specified destination (from its Binding Update List). If so, it changes the source address to its CoA and sends the packet to the destination. Else, the packet is tunneled to HA2, i.e. normal reverse tunneling between MR2 and HA2. For the latter case, MR2 might want to send a BU message to the destination (i.e. HA1) so that subsequent packets can be forwarded directly to the destination (without going through an additional level of encapsulation).

When HA1 receives an encapsulated packet, it verifies that the outer packet originated from authentic source. This is done by checking that the originator (that is specified by the HAO) has a BCE that indicates the mobile router identified by the source address is a valid access router of the originator. HA1 then overwrites the source address with the HoA specified in HAO and processes it as per MIPv6 specifications [1].

Section 4 describes in greater detail the operation of an ARO-enabled mobile router, and Section 5 describes the operation of an

ARO-enabled home agent.

2.6 Scenario with a Local Fixed Router

The ARO-Solution is designed such that it will work even across a non

ARO-enabled router, such as in the case where there is a local fixed router in between two ARO-enabled MR. Figure 2 show the scenario with a non ARO-enabled router LFR1 in between MR1 and MR2. Again, HA1 and HA2 are the home-agents of MR1 and MR2 respectively. LFR1 simply route packets between its ingress and egress interfaces, and does not do any reverse tunneling.

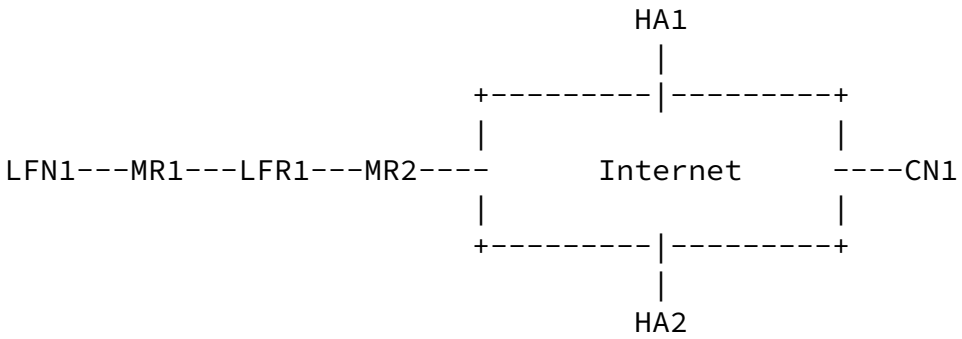


Figure 2: Example Scenario with a LFR

The problem here is that although MR2 advertises its HoA in the RA messages it broadcast, LFR1 being non ARO-enabled will ignore such information. Also, MR1 will not see any RGAO in the RA messages broadcasted by LFR1. Thus MR1 will not add in any RAO in the tunnel packet to HA1, and hence MR2 will not attempt to send BU to HA1. This will result in all packets sent between LFN1 and CN1 to go through two levels of encapsulation.

To overcome this problem, when an ARO-enabled mobile router (eg MR1) does not detect its access router to be ARO-enabled, it should try to determine if there is any ARO-enabled router in its upstream. This is done by adding a new RAO in the initial BU message it sent to its HA. Any upstream ARO-enabled router (eg MR2) will detect this RAO, and respond to MR1 with an ICMP message conveying its global address. This way, MR1 can immediately send a new BU with the global address of the MR2 in the ARO. This imply that for the purpose of route optimization, MR1 treats MR2 as its access router.

2.7 Route Optimization with Mobile Network Hosts

The same mechanism can be extended to be used between a MIPv6 mobile host and its home agent or correspondent node (CN). Here, the MIPv6 host needs to extract the RGAO from the RA messages it receives from its access router, and insert the ARO in the BU messages it sent to its HA or CN. After a successful binding, data packets sent from the mobile host can be prepend with a RAO to request upstream routers to attempt to route packets directly to the destination. The RAO can be inserted when tunneling a packet back to its HA, or inserted when the packet is sent directly to the CN using MIPv6 route optimization

mechanism. In this way, a visiting mobile host (VMH) can perform route optimization over NEMO.

When attempting to use ARO-Solution for full route optimization with a CN, the mobile host must first determine if the CN is ARO-enabled. One possible way of such capability detection is to send a BU with the ARO, and check if the BA returned contains the same ARO. An ARO-enabled CN would return a BA with the same ARO found in a BU message.

Section 6 describes in greater detail the operation of an ARO-enabled mobile node, and Section 7 describes the operation of an ARO-enabled correspondent node.

3. Changes to Existing Protocols

3.1 Modifications to NEMO Basic Support / Mobile IPv6

3.1.1 Addition of Access Router Option

The Access Router Option (ARO) is a new option for Mobility Header defined in Mobile IPv6 and NEMO Basic Support. Its format is shown below.

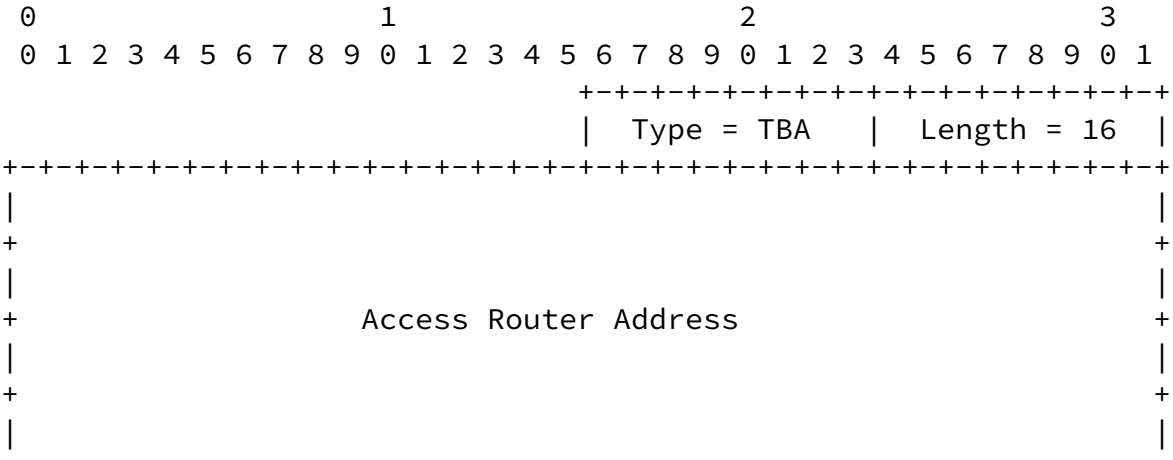


Figure 3: Access Router Option

Type

8-bit identifier of the Mobility Header option type. The value that identifies an Access Router Option is yet to be assigned.

Length

8-bit unsigned integer that specifies the length of the mobility option in octets, excluding Type and Length fields. Always 16 for the Access Router Option.

Access Router Address

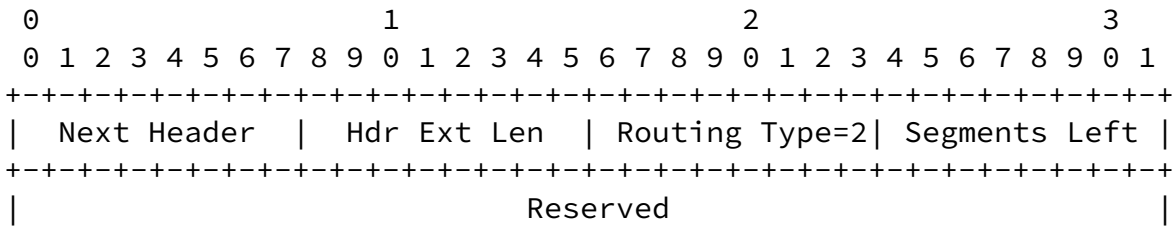
Global address of the access router that the sender is currently attached to.

The Access Router Option is only valid in a BU and BA message. The purpose of this option is to inform the recipient that the sender is currently attached to the specified access router. Using this information, recipient can route packets to the sender via the access router by making use of extended Type 2 Routing Header. Section 9.1 addresses some security considerations on the use of the Access

Router Option.

3.1.2 Extending Type 2 Router Header

The Type 2 Routing Header (RH2) is now extended such that it can contain more than one entry. This extension makes it more similar to the type 0 routing header. The format of the modified Type 2 Routing Header is shown below.



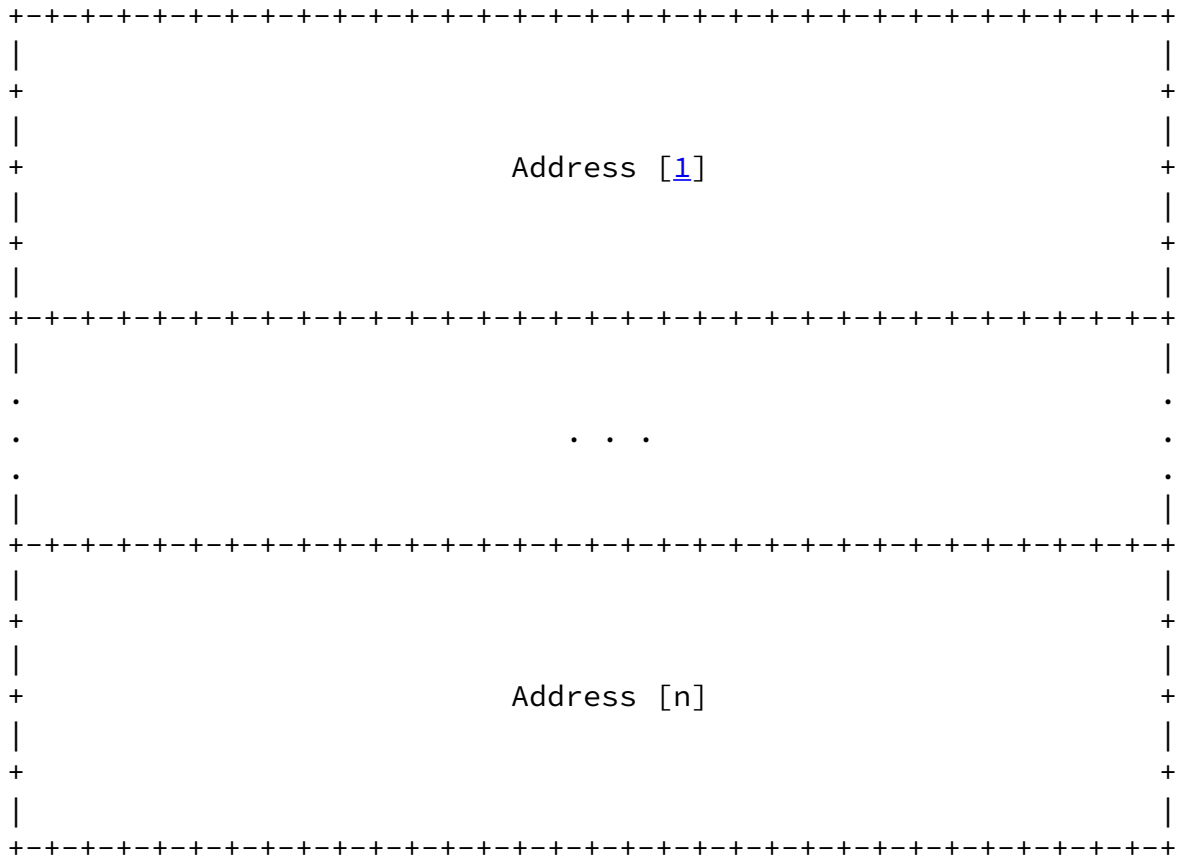


Figure 4: Extended Type 2 Routing Header

Next Header

8-bit selector. Identifies the type of header immediately following the Routing Header. Uses the same value as the IPv6 Next Header field [7].

Hdr Ext Len

8-bit unsigned integer. Length of the routing header in 8- octet units, not including the first 8 octets. This value is always equal to twice the number of addresses in the Address vector.

Routing Type

8-bit unsigned integer that contains the value 2.

Segments Left

8-bit unsigned integer. Number of route segments remaining; i.e. number of explicitly listed intermediate nodes still to be visited before reaching its final destination.

Address[1..n]

Vector of 128-bit addresses, numbered 1 to n.

This routing header is used by the sender to direct the packet to the mobile node via a sequence of routers. The addresses of the sequence of routers are placed in the order of visit to the Address[1..n] vector. The last address, Address[n], must be the HoA of the intended recipient. Note also that Hdr Ext Len field must always contain an even number.

Each MR that receives a packet with the Type 2 Routing Header and the destination field equals to its address must checked if Segments Left field is equal to 1. If yes, the last address in the Address[] vector must be its HoA. Else the packet is discarded. If Segments-Left is non-zero, it decrements the Segment-Left field, and swaps the destination field with the next address in the Address[] vector. To work out which address to swap, the MR can divide the Hdr Ext Len field by 2 (which gives the number of entries in Address[] vector), and subtract Segment Left from it.

The extended Type 2 Routing Header is a mutable but predictable IPv6 header. Thus IP Security (IPSec) [8] protocols such as Authentication Header (AH) [9] and Encapsulating Security Payload (ESP) [10] can be used with the routing header. Security considerations on the extension of Type 2 Routing Header are presented in Section 9.4.

3.1.3 Modification to Conceptual Data Structures

In Mobile IPv6 [1], the Binding Cache data structure is defined to contain entries of HoA to CoA bindings. NEMO Basic Support [2]

suggested the extension of each BCE to contain information on

prefixes injected by mobile routers. This ARO-Solution further extends each BCE to contain an additional field known as the Access Router Address. This field is used to store the global address of the access router specified in the Access Router Option in a Binding Update message.

When updating the BCE, the Access Router Address field is overwritten with the address specified in the Access Router Option. If the Access Router Option is absent, the Access Router Address field should be marked to be invalid.

3.2 Modifications to IPv6 Neighbor Discovery

3.2.1 Addition of New Option in Router Advertisement

A new option, Router Global Address Option (RGAO) is defined here. This new option can only appear in a Router Advertisement message, its format is defined below.

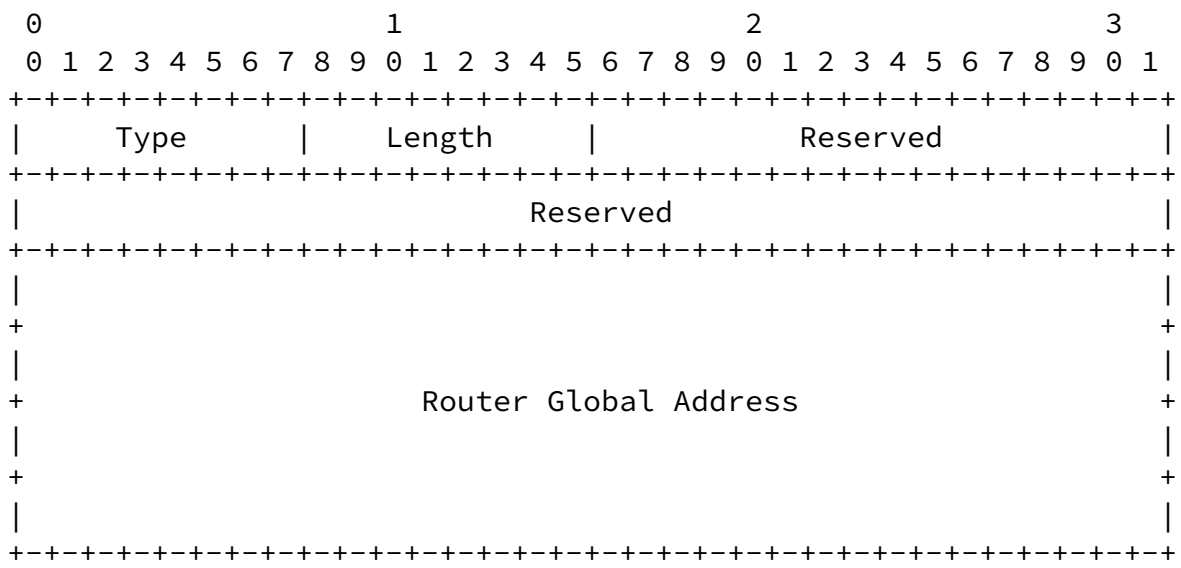


Figure 5: Router Global Address Option

Type

8-bit identifier to identify the type of the option. The value used to identify the Router Global Address Option is yet to be assigned.

Length

8-bit unsigned integer that gives the length of the option in 8-octet units. Always equals to 3 for the Router Global Address

Option.

Router Global Address

128-bit address. Contains the global address of the egress interface of the sender. Should the sender be a mobile router, this global address is the home-address of the sender.

This option allows the sender to advertise its egress interface global address to nodes attached to its ingress interface(s). This allows mobile nodes to include an Access Router Option when sending BU. Inclusion of this option in a RA message would imply the sender is ARO-enabled.

Security considerations for the Router Global Address Option are listed in Section 9.2. According to Section 4.2 of IPv6 Neighbor Discovery [11], receivers that do not understand this new option MUST silently ignore the option and continue processing the Router Advertisement message.

3.3 Modifications to ICMPv6

3.3.1 New Router Global Address ICMP Message

A new ICMP message to convey the global address of a mobile router is needed in the ARO-Solution. This message, called the Router Global Address Message, has a format as defined below.

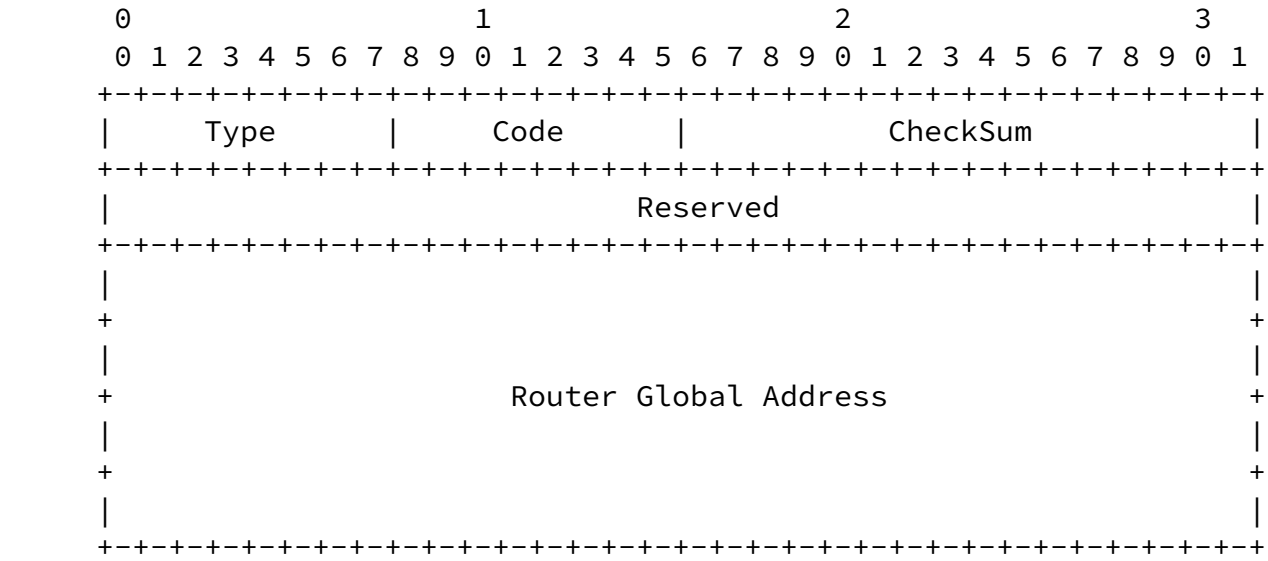


Figure 6: Router Global Address ICMP Message

Type

8-bit identifier to identify the type of the ICMP Message. The value used to identify the Router Global Address Message is yet to be assigned.

Code

8-bit unsigned integer that gives the finer granularity on message type differentiation. Set to 0 for the Router Global Address Message.

CheckSum

8-bit ICMP Checksum (see [12]

Router Global Address

128-bit address. Contains the global address of the egress interface of the sender. Should the sender be a mobile router, this global address is the home-address of the sender.

This message is sent when a ARO-enabled router intercepts a packet from its ingress interface containing a NEMO-BU RAO. This occurs when a nested MR does not know its access router's global address, and is attempting to learn its access router's global address. The ARO-enabled router intercepting such a packet would send the Router Global Address ICMP message to the source, revealing its global address (or home-address if the ARO-enabled router is also a mobile router).

3.4 Extending the Router Alert Option

The router alert option [6] has the following format:

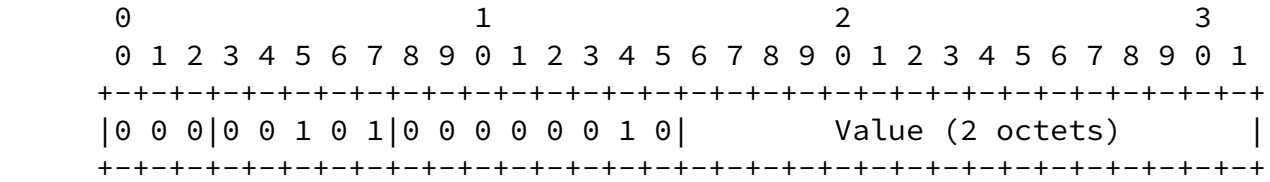


Figure 7: Router Alert Option

The first three bits of the first byte are zero and the value 5 in the remaining five bits is the Hop-by-Hop Option Type number. By zeroing all three, this specification requires that nodes not recognizing this option type should skip over this option and continue processing the header, and that the option must not change en route.

In this memo, we require the value field to be mutable en-route. Specifically, the router that is not attached to a ARO- enabled access router will change the value code. Thus, this memo propose a mutable Router Alert Option, of the following format:

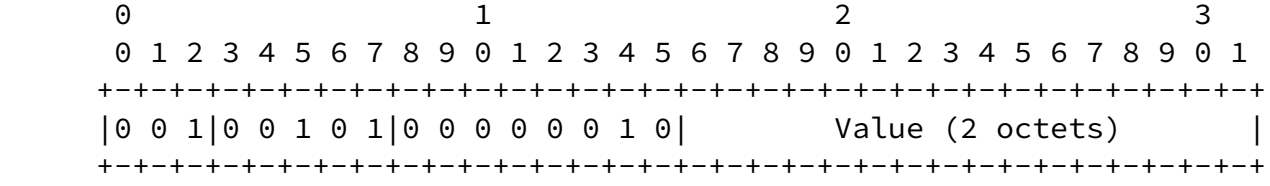


Figure 8: Mutable Router Alert Option

The first two bits of the first byte are zero, the third bit is 1 and the value 5 in the remaining five bits. Thus the Hop-by-Hop Option Type number is 0x25 (hexadecimal). By zeroing the first two bits, this memo requires that nodes not recognizing this option type should skip over this option and continue processing the header.

The Value code in the mutable Router Alert Option is extended to contain three extra values to be assigned. For purpose of description, we call these values the NEMO-Forward, NEMO-No-Forward, and NEMO-BU. Hereafter, mutable Router Alert Option with Value code equal to NEMO- Forward will be known as a NEMO-Forward Router Alert Option, or simply, NEMO-Fwd RAO; mutable Router Alert Option with Value code equal to NEMO-No-Forward will be known as a NEMO-No-Forward Router Alert Option, or simply, NEMO-NoFwd RAO; and mutable Router Alert Option with Value code equal to NEMO-BU will be known as a NEMO-BU Router Alert Option, or simply, NEMO-BU RAO.

Intermediate routers that support the ARO-Solution should recognize the NEMO-Fwd RAO and attempt to forward the packet directly to the destination without using a reverse tunnel. If necessary, the router can change the source address of the packet to the current CoA of the router in order to pass through ingress filters of subsequent routers/gateways.

Intermediate routers that support the ARO-Solution should recognize the NEMO-NoFwd RAO, and behave as if the RAO is not present. Specifically, the router MUST NOT change the source address of the packet.

Intermediate routers that support the ARO-Solution should recognize the NEMO-BU RAO, and realize that the sender (indicated by the source address), is attempting to discover the global address of its access router. The ARO-enabled intermediate router should then change the NEMO-BU RAO to a NEMO-NoFwd RAO before forwarding the packet. In addition, it should send a Router Global Address ICMP message (see Section 3.3.1) to the source of the packet containing the NEMO-BU RAO. This allows the source to learn the HoA of the MR.

Section 8.1 discusses some of the design considerations that lead to the use of a mutable Router Alert Option.

4. Operation of ARO-Enabled Mobile Routers

4.1 Operation When Mobile Router is At Home

This section describes the operation of a MR when it is attached to its home link.

4.1.1 Sending Router Advertisement

When the MR sends RA message, it should advertise its HoA by adding a RGAO in the RA message. This also indicates to the recipients that the MR is ARO-enabled.

4.1.2 Processing Outbound Packets

When the MR intercepts an outbound packet from its ingress interface, it first checks if the packet contains a NEMO-Fwd RAO or a NEMO-BU RAO. Packets that do not contain a NEMO-Fwd RAO, or packets that

contain a NEMO-NoFwd RAO are simply forwarded to its egress interface. For packet that contains a NEMO-Fwd RAO, since the MR is at home, it changes the NEMO-Fwd RAO to a NEMO-NoFwd RAO and forwards the packet to its egress interface.

If the packet contains a NEMO-BU RAO, it implies that the originator of that packet is an ARO-enabled node trying to learn if there is an ARO-enabled access router in its upstream. The MR should send to this originator a Router Global Address ICMP message (see Section 3.3.1). In addition, the MR should change the NEMO-BU RAO to a NEMO-NoFwd RAO, and forward the packet to its egress interface.

4.1.3 Processing Inbound Packets

When the MR is at home, it functions like a normal router. Thus it will consume any packet that is addressed to its HoA, forward any packet with a destination address that is a valid address in one of its ingress interface (e.g. the destination address must contain the same network prefix as one of the ingress interface), and discard any packet with an invalid destination address.

When the packet is addressed to the MR's HoA, the packet may contain an extended RH2. The Segments Left field of RH2 is checked. If Segments Left field is 0, the packet is consumed. If Segments Left field is non-zero, it is checked to be smaller or equal to the number of addresses in the Type 2 Routing Header (which can be calculated by dividing the Ext Hdr Len field by two). If Segments Left field is bigger, the packet is discarded, and an ICMP error may be returned to the sender. Else, the Segments Left field is decremented by one and the destination address is swapped with the next entry in the

Address[] vector of the RH2.

The new destination address is then checked if it is a valid address in one of the ingress interfaces of the MR. If yes, the packet is forwarded to the new destination. Else, the packet is silently discarded.

4.2 Operation When Mobile Router is Away

This section describes the operation of a MR when it is away from its home link.

4.2.1 Sending Router Advertisement

The MR would continue to send RA messages to its ingress interface(s) when it is away. It should behave as specified in Section 4.1.1. There is no difference in the RA message whether the MR is at home or away.

4.2.2 Receiving Router Advertisement

The MR should solicit RA from its access router whenever it changes its point of attachment to the Internet. When the MR receives the RA, it should check if the access router has included the RGAO in the RA message. If an RGAO is present, the access router is ARO-enabled. If no RGAO is present, the access router is not ARO-enabled.

4.2.3 Sending Binding Updates

When the MR sends BU to other hosts, either its own HA or other correspondent nodes, it should add an ARO to the BU messages if its access router is ARO-enabled. The ARO should contain the global address of the access router it learned from the RGAO in the RA message. Otherwise, if its access router is not ARO-enabled, the MR will not include the ARO in the BU messages.

When sending BU with the ARO, especially to nodes that the MR does not know to be ARO-enabled, the MR should request for a BA so that it can determine if the recipient supports the ARO-Solution by checking if the ARO is present in the BA message. If the ARO is present, the node is ARO-enabled.

If the access router is not ARO-enabled, a MR may attempt to discover if there are any ARO-enabled routers upstream by prepending a NEMO-BU RAO to the BU message it sends out. If there exist an ARO-enabled router upstream, the ARO-enabled router will send an ICMP message containing the global address (eg HoA) of the ARO-enabled router. For this case, the MR can send another BU message with an ARO

containing this global address.

If no response is received after a short timeout period, the MR should concede that there is no ARO-enabled router upstream.

4.2.4 Processing Outbound Packets

When the MR received a packet from its ingress interface for outbound forwarding, the behavior of the MR will be different depending on whether the outbound packet contains a RAO or not.

1. Packet does not have any RAO

   When the MR intercepts a packet from one of its ingress interfaces, it first checks if there is a NEMO-Fwd RAO or NEMO-BU RAO attached to the packet. When the NEMO-Fwd RAO is absent (or a NEMO- NoFwd RAO is present), the MR has to route this packet through its own HA. The packet is encapsulated in an outer packet addressed to the HA of the mobile router. If the MR's access router is not ARO-enabled, the outer packet is sent to the MR's home agent. The outer packet has the normal mobility characteristics, i.e. the source field contains the CoA of the MR and the destination field contains the address of the HA of the MR.

   If the MR's access router is ARO-enabled, reverse tunneling is still necessary. However, in this case, the mobile router will add a NEMO-Fwd RAO to the outer packet. The outer packet is then marked with source address set to the CoA of the MR, destination address set to the address of the MR's HA. and attached with a Home Address destination Option containing the HoA of the MR.

2. Packet has a NEMO-NoFwd RAO

   Processing of an outbound packet with a NEMO-NoFwd RAO is identical to that when the packet contains no RAO.

3. Packet has a NEMO-Fwd RAO

   On the other hand, when the MR received a packet with a NEMO-Fwd RAO from one of its ingress interfaces, the MR will then attempt to forward the packet directly to the destination. To do so, the MR has to check if it has a binding update with the specified destination (by checking its Binding Update List). If it does not have an active binding update with the specified destination, the MR will have to tunnel the received packet to its HA using reverse tunneling. In this case, the NEMO-Fwd RAO is changed to a NEMO-NoFwd RAO, and the packet is processed as though it does

not contain a NEMO-Fwd RAO (as described previously).

The presence of a NEMO-Fwd RAO should suggest to the MR that it could perform a Return Routability Procedure and BU with the specified destination, so that subsequent packets from the same source to the same destination need not go through the bi-directional tunnel.

If the MR does have an active binding update with the specified destination, the source address of the packet is changed to the CoA of the MR. In addition, if the access router of the MR is not ARO-enabled, the NEMO-Fwd RAO is changed to a NEMO-NoFwd RAO. The packet is then forwarded through the egress interface of the MR.

4. Packet has a NEMO-BU RAO

When the MR intercepts a packet from one of its ingress interfaces with a NEMO-BU RAO, it implies that the originator of that packet is an ARO-enabled node trying to learn if there is an ARO-enabled access router in its upstream. The MR should send to this originator a Router Global Address ICMP message (see Section 3.3.1). In addition, the MR should change the NEMO-BU RAO to a NEMO-NoFwd RAO, and process the packet as though it does not contain a NEMO-BU RAO (as described previously).

4.2.5 Processing Inbound Packets

When the MR received a packet from its egress interface, the MR checks if the packet is addressed to itself. Packets not addressed to its CoA or HoA are discarded. When the packet is addressed to its CoA, the MR checks for the presence of type 2 routing header (RH2). Packets without the RH2 are processed as per specified in [2]. If the packet contains a RH2 and is addressed to its CoA, the packet must be sent from a host that has a BCE of the MR. If security measures warrant it, the MR may want to verify the sender is indeed a node in the MR's Binding Update List, and discard the packet if it isn't.

The Segments Left field of RH2 is then checked. If Segments Left field is 0, the packet is discarded. If Segments Left field is non-zero, it is checked to be smaller or equal to the number of addresses in the RH2 (which can be calculated by dividing the Ext Hdr Len field by two). If Segments Left field is bigger, the packet is discarded, and an ICMP error may be returned to the sender. Else, the Segments Left field is decremented by one and the destination address is

swapped with the next entry in the Address[] vector of the RH2.

If the new destination address is the HoA of the MR, the Segments Left field is checked if it is 0 (after decrementing). If so, the packet is consumed by the MR. Otherwise, the packet is silently discarded.

Alternatively, the new destination address may be an address in one of the MR's ingress interfaces. If yes, the packet is forwarded to the new destination. Else, if the new destination field of the packet is neither the HoA nor a valid address in one of the MR's ingress interfaces, the packet is silently discarded.

When a packet is consumed by the MR, the payload may be an encapsulated packet. In this case, sender of the outer packet must be the HA of the MR, or a node in MR's Binding Update List. Processing of the inner packet is the same as though the mobile router is at home.

4.3 IPSec Processing

It is recommended that the MR uses IPSec protocols such as AH [9] or ESP [10] to secure the reverse tunnel with its HA [13]. This section highlights changes to the IPSec processing for inbound and outbound packets.

4.3.1 IPSec Processing on Inbound Packets

Inbound packets may contain a RH2 with an AH/ESP. The RH2 should be processed before AH. If the MR is the final destination, the packet is passed to the IPSec module for AH/ESP processing. Since the HA or CN will generate the AH/ESP in a such a way that it is consistent with the state of the packet headers when the receiver received the packet (see Section 5.4.2), no additional processing needs to be done before the AH/ESP processing.

4.3.2 IPSec Processing on Outbound Packets

For outbound packets, the new options added to the packets by the ARO-Solution are the NEMO-Fwd, NEMO-BU and NEMO-NoFwd Router Alert Options. For simplicity, it is best that all IPSec implementations ignore these options and treat their values as all zero when

processing.

5. Operation of ARO-Enabled Home Agents

5.1 Receiving Binding Updates

When a HA receives a BU message, it needs to check for the necessary security measures as specified in Mobile IPv6 specifications [1] or NEMO Basic Support [2]. The only change this ARO Solution requires is for the HA to add a field to its Binding Cache: access router's address. Every valid BU is checked for the Access Router Option field. If one is absent, the corresponding BCE will have the access router field invalidated. If one is present, the corresponding BCE will have the access router field updated.

In addition, when returning a BA for a BU that contains an Access Router Option, the ARO-Solution requires that the HA return a the BA with the same Access Router Option if the binding is successful. Note also that the HA MUST accept BU with Access Router Option regardless of whether the Home Registration bit is set.

5.2 Receiving Tunneled Packets from Away Nodes

When the HA received a packet that contains an encapsulated packet, it may choose to perform certain security checks. The obvious check is to ensure that the source address is either a valid CoA of the HoA in its binding cache, or the source address is a valid CoA or HoA of an access router that is in the upstream of the mobile node with the specified HoA in the Home Address Destination option. Section 9.3 discusses the security considerations on accepting tunnels with a source address that is not directly bound to the HoA specified in the Home Address destination option.

To establish this, the HA can use the pseudo algorithm depicted in Figure 9. The algorithm returns TRUE if the source address in a

valid address, and FALSE otherwise. When the algorithm returns TRUE, the source address is a valid address, and the packet is decapsulated and processed as normal. Should the algorithm evaluates to FALSE, the packet is discarded.


```
set start-address =  HoA in HAO
while (TRUE) do
{
  find an entry in Binding Cache with HoA field == start-address
  if (no BCE is found)
  {
     return (FALSE)
  }
  if (CoA field in the BCE
        == source-address of outer packet)
  {
     return (TRUE)
  }
  if (the BCE does not contain a valid access
        router address)
  {
     return (FALSE)
  }
  if (access router address field in the BCE
        == source-address of outer packet)
  {
     return (TRUE)
  }
  set start-address = access router address field in the BCE
}
```

Figure 9: Algorithm to check source address is valid

5.3 Tunneling Packets to Away Nodes

When the HA intercepted a packet addressed to a node in its home domain, it checks the next hop to forward the packet from its routing table. This sub-section describes the operation of the HA when the next hop is away, i.e. the next hop is a mobile node, and the mobile node is away from home.

In this case, the HA will forward the packet to the mobile node at the CoA of the mobile node. This is done by encapsulating the intercepted packet into a new packet. According to standard MIPv6 specification [1], the packet will have the source address set to the address of the HA, destination set to the CoA of the mobile router, and a RH2 with only one address entry equals to the HoA of the mobile node.

This ARO-Solution extends the RH2 to include addresses of access routers, and the pseudo algorithm depicted in Figure 10 can be used to construct such a routing header. In Figure 10, src-address and

dst-address are the abbreviations for the source address and destination address fields of the outer packet respectively.

```
initialize an empty stack
set src-address = address of home agent
set dst-address = HoA of mobile node
set Finished = FALSE
while (not Finished)
{
   find BCE with HoA field = dst-address
   if (no BCE is found)
   {
      Finished = TRUE
   }
   else
   {
      if (dst-address == HoA of mobile node)
      {
         push dst-address to stack
```

```
            }
            set dst-address = CoA field of the found BCE
            if (the found BCE contains a valid access router address)
            {
               push dst-address to stack
               set dst-address = access router address field of BCE found
            }
            else
            {
               Finished = TRUE
            }
         }
      }
      if (stack is not empty)
      {
         prepare a type 2 routing header
         set Hdr Ext Len field of RH2 = (size of stack) x 2
         set Segments Left field of RH2 = size of stack
         for n=1 to (Segments Left field of RH2)
         {
            pop top of stack to Address[n] of RH2
         }
      }
```

Figure 10: Algorithm to construct extended RH2

The outer packet is then sent to the destination. If secure tunnel is used, the IPSec protocol used must be able to recognize that the RH2 is a mutable but predictable header, such that the two end-points

use the same routing header and IPv6 destination field for IPSec processing. Particularly, the sender should calculate the IPSec parameters using values in the IPv6 headers that the receiver will receive.

5.4 IPSec Processing

It is recommended that the HA uses IPSec protocols such as AH [9] or ESP [10] to protect the tunnel with a mobile node [13]. This section highlights changes to the IPSec processing for inbound and outbound packets.

5.4.1 IPSec Processing on Inbound Packets

Packets that are inbound may have their source address modified en-route by access routers. Thus, all home-agents SHOULD use the algorithm shown in Figure 9 to establish the authenticity of the source address. Once the source address is verified, the source address field will be replaced by the HoA specified in the Home Address Destination option, and the Home Address field of the Home Address Destination option MUST be replaced with the CoA of the sender. In MIPv6, this CoA can be obtained from the source address field in the packet. However, the ARO-Solution allows intermediate mobile routers to modify the source address field. Thus, the home agent MUST obtain the CoA from its BCE.

The above processing MUST be carried out before AH processing.

5.4.2 IPSec Processing on Outbound Packets

Outbound packets may contain an extended RH2. The extended RH2 is a mutable but predictable header. According to the usual norm of generating AH authentication data, the HA must order the contents of the RH2 as it will appear at the final destination when generating the AH authentication data.

6. Operation of ARO-Enabled Mobile Network Nodes

The operation of an ARO-enabled MNN is very similar to that of a MR. When the MNN is at home, there is no additional operation requirements imposed by the ARO Solution (i.e. the ARO-enabled MNN

operation is similar to a normal MNN when it is at home). This section described the operation of MNN when it is away (i.e. it is a VMN).

6.1 Nested Tunnel Optimization with Home Agent

In this case, the MNN is VMN using MIPv6 bi-direction tunneling with its HA. If it is ARO-enabled, and its HA is also ARO-enabled, then the number of nested tunnel can be reduced to one.

The MNN basically follows the same procedure as an ARO-enabled MR. It needs to detect the RGAO in the RA messages broadcasted by its access router to determine if its access router is ARO-enabled. When sending BU message to its HA, the MNN will insert an ARO to the BU message containing the home-address of its access router.

After the binding is successful, the MNN can then attached a NEMO-Fwd RAO in the tunnel packets sent to its HA. Note that when doing so, the MNN needs to attach a Home Address Destination Option in the tunnel packet.

6.2 Receiving Router Advertisement

The MNN should solicit RA from its access router whenever it changes its point of attachment to the Internet. When the MNN receives the RA, it should check if the access router has included the RGAO in the RA message. If an RGAO is present, the access router is ARO-enabled. If no RGAO is present, the access router is not ARO-enabled.

6.3 Sending Binding Updates

When the MNN sends BU to other hosts, either its own HA or other correspondent nodes, it should add an ARO to the BU messages if its access router is ARO-enabled. The ARO should contain the global address of the access router it learned from the RGAO in the RA message. Otherwise, if its access router is not ARO-enabled, the MNN will not include the ARO in the BU messages.

When sending BU with the ARO, especially to nodes that the MNN does not know to be ARO-enabled, the MNN should request for a BA so that it can determine if the recipient supports the ARO-Solution by checking if the ARO is present in the BA message. If the ARO is present, the node is ARO-enabled.

If the access router is not ARO-enabled, a MNN may attempt to discover if there are any ARO-enabled routers upstream by prepending a NEMO-BU RAO to the BU message it sends out. If there exist an ARO-enabled router upstream, the ARO-enabled router will send an ICMP message containing the global address of the ARO-enabled router. For this case, the MNN can send another BU message with an ARO containing this global address.

If no response is received after a short timeout period, the MNN should concede that there is no ARO-enabled router upstream.

6.4 Sending Data Packets

When the MNN is tunneling data packets to its HA, the MNN can add a NEMO-Fwd RAO to the tunnel packet (i.e. outer packet) if (1) its HA is ARO-enabled, and (2) its access router is ARO-enabled. Otherwise, the MNN should use the normal MIPv6 bi-directional tunneling to forward the data packet to its HA. When adding the NEMO-Fwd RAO, the MNN should also include a Home Address Destination Option in the tunnel packet.

When the MNN knows (by other means) that the CN it is communicating with is ARO-enabled, the MNN can choose to employ full route optimization with the CN. This is done by adding a NEMO-Fwd RAO to the data packet. Note that the MNN should also include a Home Address Destination Option in the data packet.

6.5 Processing Inbound Packets

When the MNN received a packet from its egress interface, the MNN checks if the packet is addressed to itself. Packets not addressed to its CoA or HoA are discarded. When the packet is addressed to its CoA, the MNN checks for the presence of type 2 routing header (RH2). Packets without the RH2 are processed as per specified in [2]. If the packet contains a RH2 and is addressed to its CoA, the packet must be sent from a host that has a BCE of the MNN. If security measures warrant it, the MR may want to verify the sender is indeed a node in the MR's Binding Update List, and discard the packet if it isn't.

The Segments Left field of RH2 is then checked. If Segments Left field is 0, the packet is discarded. If Segments Left field is non-zero, it is checked to be smaller or equal to the number of addresses in the RH2 (which can be calculated by dividing the Ext Hdr Len field by two). If Segments Left field is bigger, the packet is discarded, and an ICMP error may be returned to the sender. Else, the Segments Left field is decremented by one and the destination address is swapped with the next entry in the Address[] vector of the RH2.

Being a host, the MNN must be the final destination of the packet. Thus, if the new destination address is not the HoA of MNN, or the Segments Left field is non-zero after decrementing, the packet is silently discarded. Else if the new destination address is the HoA of MNN, and the Segments Left field is zero after decrementing the packet is consumed.

When a packet is consumed by the MNN, the payload may be an encapsulated packet. In this case, sender of the outer packet must be the HA of the MNN. Processing of the inner packet is the same as though the MNN is at home.

6.6 IPSec Processing

6.6.1 IPSec Processing on Inbound Packets

Inbound packets may contain a RH2 with an AH/ESP. The routing header should be processed before AH. If the MNN is the final destination, the packet is passed to the IPSec module for AH/ESP processing. Since the HA or CN will generate the AH/ESP in a such a way that it is consistent with the state of the packet headers when the receiver received the packet (see Section 5.4.2), no additional processing needs to be done before the AH/ESP processing.

6.6.2 IPSec Processing on Outbound Packets

For outbound packets, the new options added to the packets by the ARO-Solution are the NEMO-Fwd, NEMO-BU and NEMO-NoFwd Router Alert Options. For simplicity, it is best that all IPSec implementations ignore these options and treat their values as all zero when processing.

7. Operation of ARO-Enabled Correspondent Node

7.1 Receiving Binding Updates

When a CN receives a BU message, it needs to check for the necessary security measures as specified in Mobile IPv6 specifications [1] or NEMO Basic Support [2]. The only change this ARO Solution requires is for the CN to add a field to its Binding Cache: access router's address. Every valid BU is checked for the Access Router Option field. If one is absent, the corresponding BCE will have the access router field invalidated. If one is present, the corresponding BCE will have the access router field updated.

In addition, when returning a BA for a BU that contains an Access Router Option, the ARO-Solution requires that the CN returns a the BA with the same Access Router Option if the binding is successful. Note that a BU sent to the CN MUST be preceded with a return routability procedure. Section 9.1 discusses possibility of extending the return routability procedure to protect the Access Router Option.

7.2 Receiving Route Optimized Packets from Mobile Nodes

When the CN received a packet that contains a Home Address Destination Option, it will have to perform certain security checks to ensure that the source address is either a valid CoA of the HoA in its binding cache, or the source address is a valid CoA or HoA of an access router that is in the upstream of the mobile node with the specified HoA in the Home Address Destination option. Section 9.3 discusses the security considerations on accepting tunnels with a source address that is not directly bound to the HoA specified in the Home Address destination option.

To establish this, the CN can use the pseudo algorithm depicted in Figure 9 shown in Section 5.2. The algorithm returns TRUE if the

source address in a valid address, and FALSE otherwise. When the algorithm returns TRUE, the source address is a valid address, and the source address is replaced with the HoA contained in the Home Address Destination Option and processed as normal. Should the algorithm evaluates to FALSE, the packet is silently discarded.

7.3 Sending Route Optimized Packets to Mobile Nodes

When the CN sends a packet, it should check if the destination address is in its BCE. If the destination is not in the BCE, then the packet is sent as per normal IPv6 operation. If the destination is in its BCE, normal MIPv6 will require that the source address be set to the address of the CN, destination set to the CoA of the MR,

and a RH2 with only one address entry equals to the HoA of the mobile node.

This ARO-Solution extends the RH2 to include addresses of access routers, and the pseudo algorithm depicted in Figure 10 shown in Section 5.3 can be used to construct such a routing header. In Figure 10, src-address and dst-address are the abbreviations for the source address and destination address fields of the outer packet respectively.

If IPSec protocol is used to protect the packet, the IPSec protocol used must be able to recognize that the RH2 is a mutable but predictable header, such that the two end-points use the same routing header and IPv6 destination field for IPSec processing. Particularly, the sender should calculate the IPSec parameters using values in the IPv6 headers that the receiver will receive.

7.4 IPSec Processing

7.4.1 IPSec Processing on Inbound Packets

Packets that are inbound may have their source address modified en-route by access routers. Thus, all ARO-enabled correspondent nodes SHOULD use the algorithm depicted in Figure 9 shown in Section 5.2 to establish the authenticity of the source address. Once the source address is verified, the source address field will be replaced by the HoA specified in the Home Address Destination option, and the Home Address field of the Home Address Destination option MUST be replaced

with the CoA of the sender. In MIPv6, this CoA can be obtained from the source address field in the packet. However, the ARO-Solution allows intermediate mobile routers to modify the source address field. Thus, the CN MUST obtain the CoA from its BCE.

The above processing MUST be carried out before AH processing.

7.4.2 IPSec Processing on Outbound Packets

Outbound packets may contain an extended RH2. The extended RH2 is a mutable but predictable header. According to the usual norm of generating AH authentication data, the CN must order the contents of the RH2 as it will appear at the final destination when generating the AH authentication data.

8. Design Considerations

This section describes the rational behind some design decision made in the formulation of the ARO Solution. Some justifications are given, and in some cases, alternative approaches are discussed.

8.1 Considerations in the Use of Mutable Router Alert Option

8.1.1 Overview of Router Alert Option

The ARO Solution described in this memo is designed so that it will work in a nested NEMO where some mobile routers are ARO-enabled and some are not. Thus, some form of indications on a packet is necessary to inform upstream mobile routers to attempt to use the ARO Solution. Since the indication is meant for intermediate routers, a hop-by-hop option is needed.

The Router Alert Option [6] lends itself readily for use. By assigning a value in RAO, a ARO-enabled mobile router can request its access router to attempt to forward the packet directly to the destination without using reverse tunnel. However, further analysis

reveals that there is a need for a mobile router that is not attached to a ARO-enabled access router to disable this behavior.

8.1.2 Example where an Immutable RAO is Used

To understand why a MR that is not attached to a ARO- enabled access router should disable the NEMO-Fwd RAO, consider the following scenario, where MR1, MR2, and MR4 are ARO-enabled mobile routers, LFR3 is a non-ARO-enabled local fixed router attached to MR4, and HA1 is the home agent of MR1.

```
MR1---MR2---LFR3---MR4---[Internet]---HA1
```

Suppose both MR1 and MR2 have performed binding updates successfully with HA1, thus the state of the Binding Cache of HA1 will be:

Home-Address	Care-of-Address	Access Router
MR1.HoA	MR1.CoA	MR2.HoA
MR2.HoA	MR2.CoA	<invalid>

When MR1 encapsulates a packet to be tunneled to HA1, MR1 adds a NEMO-Fwd RAO in the outer packet (since MR2, the access router of MR1, is ARO-enabled). Thus the packet from MR1 to MR2 will contains the following contents:


```
IPv6 Hdr (src=MR1.CoA, dst=HA1)
Hop-by-Hop Opt
      RAO (NEMO-Fwd)
Dest Opt
      HAO (MR1.HoA)
```

Since MR2 has already performed a binding update with HA1, it changes the source address and forwards the packet to LFR3. LFR3 is a fixed router, thus it simply forwards the packet to MR4. At MR4, the packet contents is then:

```
IPv6 Hdr (src=MR2.CoA, dst=HA1)
Hop-by-Hop Opt
      RAO (NEMO-Fwd)
```

```
          Dest Opt
                HAO (MR1.HoA)
```

When MR4 intercepts this packet, the presence of the NEMO-Fwd RAO will cause MR4 to start a binding update with HA1, and tunnels the packet to its home agent. From the home agent of MR4, the packet is forwarded to HA1.

Suppose now HA1 accepts the binding update with MR4, and its Binding Cache is thus as follows:

Home-Address	Care-of-Address	Access Router
MR1.HoA	MR1.CoA	MR2.HoA
MR2.HoA	MR2.CoA	<invalid>
MR4.HoA	MR4.HoA	<invalid>

Now, when MR1 sends a tunnel packet to HA1 again, the packet will arrive at MR4 with the following contents:

```
          IPv6 Hdr (src=MR2.CoA, dst=HA1)
          Hop-by-Hop Opt
                RAO (NEMO-Fwd)
          Dest Opt
                HAO (MR1.HoA)
```

This time, MR4 checks that HA1 is on its Binding Update List, thus it will change the source address of the packet to its CoA and forward the packet to HA1 through the Internet. When HA1 receives the packet, the contents will be:

```
          IPv6 Hdr (src=MR4.CoA, dst=HA1)
          Hop-by-Hop Opt
                RAO (NEMO-Fwd)
```



```
          Dest Opt
                HAO (MR1.HoA)
```

Because the Access Router field of the BCE for MR2 is marked invalid, the algorithm for checking the validity of the source address as shown in Figure 9 of Section 5.2 will fail. Thus the packet will be discarded at HA1.

8.1.3 The Need for Mutable RAO

The example in the previous section shows that the presence of a local fixed router (LFR) that is not ARO-enabled may cause an unintentional denial-of-service to mobile routers that are attached to the LFR.

To avoid this problem, MR4 must somehow realize that it should ignore the NEMO-Fwd RAO in a packet forwarded by MR2. One method is to check that the source address is a valid source address in the ingress interface of MR4. However, MR2 might obtain a CoA that contains a prefix that is valid in the ingress interface of MR4. Thus checking source address does not completely eliminate the problem.

If MR2 can somehow invalidate the NEMO-Fwd RAO, the problem can be eliminated. But the Router Alert Option as defined in [6] is an immutable hop-by-hop option, so what is needed here is a mutable router alert option.

8.1.4 Alternatives to the Mutable Router Alert Option

There are other alternatives to the mutable Router Alert Option. These include using the Flow label in IPv6 header, and defining a new routing header type. These are briefly described below.

- IPv6 Flow Label

  It is possible to use the IPv6 Flow label to achieve the same effects as the mutable Router Alert Option. A specific, universal Flow label can be reserved to indicate to NEMO-enabled routers that they should try to forward the packets directly to their destination (instead of using a reverse tunnel with home agents).

  This approach eliminates the need of defining a new hop-by-hop header option. However, this means that a specific flow label has to be reserved, which may be in contention with currently deployed IPv6 nodes. In addition, this will mean that NEMO-enabled mobile routers are unable to use Flow label for other purposes.

- New Routing Header Type

  A new routing header type can be defined to store the address of the final destination. When such a routing header is used, the originator will place the address of the final destination in the routing header, and place the home-address of the access router of the originator in the destination (when the access router is NEMO-enabled). When a NEMO-enabled mobile router that is not attached to a NEMO-enabled access router receives a packet with this type of routing header, it will overwrite the destination address of the packet with the final destination specified in the routing header, and decrement the Segments Left field. When a NEMO-enabled mobile router that is attached to a NEMO-enabled access router receives a packet with this type of routing header, it will overwrite the destination address of this packet with the home-address of its access router and the leave the contents of the routing header untouched.

  There remain issues that are unclear when this new type of routing header is used with other routing headers. Also, the security implication of defining a new type of routing header is yet to be explored.

- Discarding Immutable RAO

  Another possibility is to use the normal immutable RAO and instead allow routers en-route to simply discard the RAO (instead of changing it to a NEMO-NoFwd RAO). This will work exactly the same, and is both applicable to NEMO-Fwd and NEMO-BU RAO. It will in fact reduce processing delay when the RAO is only option in the hop-by-hop header. Since this will cause the hop-by-hop header to be removed, and en-route router need not process the hop-by-hop header and only to find that it contains a NEMO-NoFwd RAO which requires no processing.

8.2 Change of Source Address

This memo proposed to allow intermediate routers to change the source address of a packet en-route. It is expected that this will cause some disturbances, as it is generally not allowed for routers to change the source address. We hope to justify our design decision in this section, and discuss some alternatives.

8.2.1 Justifications

The main factor in consideration to changing the source address en-route is to overcome ingress filtering. In order for a packet to be

able to pass through an ingress filter, the source address must be topologically compatible with where the packet is originated. Thus, to overcome ingress filtering, the source address must somehow be changed. We view the change of source address as somewhat akin to the use of a CoA as the packet source address in MIPv6.

For the case of MIPv6, mobile nodes use the CoA to overcome ingress filtering, and use the BU mechanism and Home Address Destination Option to allow receivers to establish a relationship between the source address (i.e. CoA) and the HoA. In the ARO Solution, receivers can use the algorithm depicted in Figure 9 of Section 5.2 to establish a similar relationship between the source address (in this case, the CoA/HoA of an upstream access router) and the HoA.

8.2.2 Alternatives

There are alternatives to changing source address for the purpose of overcoming ingress filters. One method is to use packet encapsulation to achieve the same effect as changing of source address (since the outer packet has a different source address). Currently, evaluating such a scheme is in progress.

9. Security Considerations

This proposal introduces several modifications to existing protocols. In this section, we will discuss additional security issues that arise due to these modifications.

9.1 Addition of Access Router Option

Access Router Option is introduced so that a recipient can establish a credible link between the global address of the access router specified, and the HoA of the mobile node that sends the Access Router Option.

When a mobile node sends BU to its HA, current MIPv6 draft specifies that the BU should be secured (either by ESP or AH). For this case, the introduction of Access Router Option does not introduce new security threats.

When sending BU to CN, the mobile node inserts the Access Router Option only when sending the actual BU message. The BU message is protected using a key generated after obtaining the Care-of-Test (CoT) and Home-Test (HoT) messages, so the Access Router Option should be relatively secure. However, there exist the slight possibility of an attacker snooping on both the CoT and HoT messages, thus allowing the attacker to generate the key independently. The attacker can then proceed to change the values in the Access Router Option and change the Authenticator value of the BU message using the generated key, thus leading the correspondent node to believe that the mobile node is attached to another access router.

To overcome this, the mobile node may insert the Access Router Option when sending the CoT Init Message. The ARO-enabled CN, should then generate the care-of cookie using

```
Care-of cookie = First64(MAC_Kcn(CoA | access router address |
                                 nonce))
```

instead of using only the CoA and nonce. In this way, the global address of the access router in the Access Router Option is protected the same way the CoA is protected.

Note that if the CN does not recognize the Access Router Option, it will not use the access router address to generate the care-of-cookie. However, we do not require the mobile node to change the way the Authenticator value is generated, i.e. the value is generated using the method as specified in MIPv6 [1]:

Kbu = Hash(home cookie | care-of cookie)

Authenticator = MAC_Kbu(CoA | CN address | BU)

So, the BU will be verified to be authentic by the CN regardless of how the care-of cookie is generated, provided the generation of care-of cookie is consistent. The mobile node must still request for BA so that it if the CN has accepted the Access Router Option.

9.2 Router Global Address Option

The introduction of global address of the access router in the BU message is the crux of the ARO Solution, since this is the link which allows HA and CN to set up the RH2 and to accept packets from otherwise unknown sources. From previous discussion, the global address of the access router is fairly secure since

- BU sent by an away node to its home agent that contains the access router's global address is secure, and
- BU sent to CN are reasonably protected using the Return Routability Procedure.

The weakest link is now the method in which the mobile node learns the global address of the access router it attaches to. The method proposed in this memo is to use the Router Advertisement. Two possible security threats are identified here:

1. a malicious access router advertising false global address in the RA messages it broadcasts, and

2. an attacker replays a RA message from a legitimate access router, but changes the global address contained in the Router Global Address Option to a false entry.

The severity of the two threats is yet to be fully analyzed. We do provide our initial analysis here to invite further discussion. For the first case, advertising a false global address is believed to be one of least harm a malicious access router could do. There are other far more potent threats faced by the mobile router when it attaches itself to a malicious access router. For the second case where an attacker replays a modified RA, we believed that the threat existed in IPv6 Neighbor Discovery [11]. In [11], security issues pertaining to RA are discussed. This discussion should be able to shed some light on how to advert such an attack.

9.3 Accepting Tunnel with a Source Address not Directly Bound to the Home Address

MIPv6 forbids home agent from accepting tunnels with a source address

that is not bound to the HoA specified in a Home Address Option. This proposal relaxed this security measure. The home agent should now admit tunnels from a source address that is "indirectly" bound (through the linkage of access router field in the binding cache) to the home-address specified in the Home Address Option. The algorithm presented in Figure 9 of Section 5.2 can be used to verify if the source address is "indirectly" bound to the HoA specified in the Home Address Option.

As considered above in Section 8.2, the Access Router Option is secured by the fact that a BU to the HA is always secure. In addition, the Access Router Option is fairly secured with the Return Routability Procedure. Thus the relaxation of the security measure of source address verification of a tunnel does not significantly increase the HA's vulnerability to attacks. It is also recommended that the tunnel between the mobile node and the home agent to be secured by ESP or AH. In addition, we also recommend that all implementations to allow the support of this ARO Solution to be administratively disabled or enabled. The default should be enabled.

9.4 Use of Extended Routing Header Type 2

The extension of the RH2 exposes this solution to additional security threats in that attackers can change the entries in the RH2 to be routed to another entity. However, we note that this extension is designed so that the extended RH2 is now very similar to the Type 0 Routing Header. Thus, the security threats faced by RH2 is not a new threat introduced by this solution itself. In any case, the harm an attacker can do by changing the entries in the routing header is limited to:

- causing the packet to be routed to another entity for snooping into the contents of the payloads;
- denial-of-service attack causing the packet to be discarded by intermediate routers; and
- using the RH2 to reflect packets off a mobile network.

In the first two cases, given that the attacker has the ability to change the contents in the routing header, it can perform the same attack even if a RH2 is not used. For the threat where attacker construct a RH2 to reflect packets off a mobile network, we recommend that all routers supporting the RH2 to perform the following security measures:

- When the mobile node receives a packet with the destination field set to its HoA or CoA, it should check for the existence of a RH2. Any packet that is sent to the mobile node's CoA without a RH2 should be discarded.
- If the Segment Left field has a value of 1, the last address in the routing header must contain the HoA of the mobile node.
- If the Segment Left field has a value greater than 1, the new destination address must contain a valid address in one of the mobile router's ingress links. If the mobile node is a mobile host, the packet should be discarded.

Effectively, the above security checks ensure the mobile node will discard any packets it received with a RH2 that requires it to forward the packet through an egress link. This should reduce, if not eliminate, the possibility of using the extended RH2 for

reflection attacks.

In addition, it must be noted that the extended RH2 is mutable but predictable. Thus, it can be protected using AH.

9.5 Mutable Router Alert Option

The mutable Router Alert Option is used in this memo to request/stop subsequent routers to attempt to forward the packet directly to its destination. Possible security threats identified are:

The attacker can add a NEMO-Fwd RAO to a packet. This will cause subsequent mobile routers to perform BU with the destination. When BU is successful, subsequent mobile routers will forward the packets directly to the destination, causing the packet to be discarded (due to failure of algorithm in Figure 9).

The attacker can add a NEMO-NoFwd RAO to a packet. This has no effect, since the default behavior of processing a packet with NEMO-NoFwd RAO at a mobile router is the same as the default behavior of processing a packet without any RAO.

The attacker can change the value of the NEMO-Fwd RAO to a NEMO-NoFwd RAO. The effect of this form of attack is to cause the packet to be delivered sub-optimally (i.e. nested tunnels).

The attacker can change the value of the NEMO-NoFwd RAO to a NEMO-Fwd RAO. The effect of this form of attack is to cause subsequent mobile routers to perform BU with the destination. When BU is successful, subsequent mobile routers will forward the packets directly to the destination, causing the packet to be discarded (due to failure of algorithm in Figure 9).

All the security threats described above require the attacker to be on the path of the packet route. In addition, the most severe effect the attacker can achieve is causing packets to be discarded at the receiver. Since the attacker must be on the path of the packet

route, the attacker can achieve the same effect by simply discarding the intercepted packet. Thus, the use of mutable router alert option described in this memo does not introduce any new security threats.

9.6 IPSec Processing

9.6.1 Processing of Extended Routing Header Type 2

As covered in Section 5.4.2, the extended RH2 is a mutable but predictable header, thus the sender must ordered the fields in the RH2 (and the destination address of the IPv6 header) as they will appear at the final destination when generating the AH authentication header.

9.6.2 Processing of Home Address Destination Option

As specified in MIPv6, the originator should use its HoA as the IPv6 source address in the IPv6 header, and place its CoA in the Home Address field of the Home Address destination option, when generating the AH authentication data.

The ARO Solution allows mobile routers to modify the source address of the IPv6 Header, thus when the source address field may no longer contain the CoA of the sender at the final destination.

All home agents MUST use the algorithm shown in Figure 9 of Section 5.2 to establish the authenticity of the source address. Once the source address is verified, the source address field will be replaced by the HoA specified in the Home Address destination option, and the Home Address field of the Home Address destination option will be replaced with the CoA of the sender. This CoA is obtained from the receiver's BCE.

The above processing MUST be carried out before AH processing.

9.6.3 Processing of Mutable Router Alert Option

As described in Section 4.3.2, when the sender of a packet inserts a NEMO-Fwd RAO or NEMO-BU RAO to the packet, the receiver always

received the RAO modified to NEMO-NoFwd. Thus the mutable NEMO-Fwd RAO is predictable. It is thus possible for the originator to use

NEMO-NoFwd RAO to generate the AH authentication data. However, it is recommended that the RAO simply be left out of any IPSec processing.

10 References

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

[2] Devarapalli, V., "Network Mobility (NEMO) Basic Support Protocol", draft-ietf-nemo-basic-support-03 (work in progress), June 2004.

[3] Ernst, T., "Network Mobility Support Goals and Requirements", draft-ietf-nemo-requirements-02 (work in progress), February 2004.

[4] Thubert, P., Molteni, M. and C. Ng, "Taxonomy of Route Optimization models in the Nemo Context", draft-thubert-nemo-ro-taxonomy-02 (work in progress), February 2004.

[5] Ernst, T. and H. Lach, "Network Mobility Support Terminology", draft-ietf-nemo-terminology-01 (work in progress), February 2004.

[6] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, October 1999.

[7] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[8] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[9] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[10] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[11] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[12] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[13] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

Authors' Addresses

Chan-Wah Ng
Panasonic Singapore Laboratories Pte Ltd
Blk 1022 Tai Seng Ave #06-3530
Tai Seng Industrial Estate
Singapore 534415
SG

Phone: +65 65505420
EMail: cwng@psl.com.sg

Jun Hirano
Matsushita Electric Industrial Co., Ltd. (Panasonic)
5-3 Hikarino-oka
Yokosuka, Kanagawa 239-0847
JP

Phone: +81 46 840 5123
EMail: hirano.jun@jp.panasonic.com

Appendix A. Acknowledgement

The authors would like to express our sincere gratitude to Takeshi Tanaka for his contribution to the initial version of this draft. In addition, appreciation is also extended to Thierry Ernst, Pascal Thubert, and various people in the NEMO WG who have given us valuable comments.

Intellectual Property Statement

Disclaimer of Validity

WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.