Network Working Group
Request for Comments: 3963
Category: Standards Track

V. Devarapalli
Nokia
R. Wakikawa
Keio University
A. Petrescu
Motorola
P. Thubert
Cisco Systems

January 2005

Network Mobility (NEMO) Basic Support Protocol

Status of This Memo

Copyright Notice

Abstract

This document describes the Network Mobility (NEMO) Basic Support protocol that enables Mobile Networks to attach to different points in the Internet. The protocol is an extension of Mobile IPv6 and allows session continuity for every node in the Mobile Network as the network moves. It also allows every node in the Mobile Network to be reachable while moving around. The Mobile Router, which connects the network to the Internet, runs the NEMO Basic Support protocol with its Home Agent. The protocol is designed so that network mobility is transparent to the nodes inside the Mobile Network.

Table of Contents

1. Introduction

This document describes protocol extensions to Mobile IPv6 (MIPv6) [1] to enable support for network mobility. The extensions are backward compatible with Mobile IPv6. In particular, a NEMO-compliant Home Agent can operate as a Mobile IPv6 Home Agent. The solution described here satisfies the goals and requirements identified in [11] for network mobility.

The NEMO Basic Support ensures session continuity for all the nodes in the Mobile Network, even as the Mobile Router changes its point of attachment to the Internet. It also provides connectivity and reachability for all nodes in the Mobile Network as it moves. The solution supports both mobile nodes and hosts that do not support mobility in the Mobile Network.

Within the context of this document, the definition of a Mobile Router extends that of a Mobile IPv6 [1] Mobile Node, by adding routing capability routing between its point of attachment (Care-of Address) and a subnet that moves with the Mobile Router.

The solution described in this document proposes a bi-directional tunnel between the Mobile Router and its Home Agent. This tunnel is set up when the Mobile Router sends a successful Binding Update to its Home Agent, informing the Home Agent of its current point of attachment.

All traffic between the nodes in the Mobile Network and Correspondent Nodes passes through the Home Agent. This document does not describe route optimization of this traffic.

The terminology document [10] describes Nested Mobility as a scenario where a Mobile Router allows another Mobile Router to attach to its Mobile Network. There could be arbitrary levels of nested mobility. The operation of each Mobile Router remains the same whether the Mobile Router attaches to another Mobile Router or to a fixed Access Router on the Internet. The solution described here does not place any restriction on the number of levels for nested mobility. But note that this might introduce significant overhead on the data packets as each level of nesting introduces another IPv6 header encapsulation.

This document does not discuss multihoming for Mobile Routers.

2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [7].

Network Mobility - related terminology is defined in [9] and [10]. This document in addition defines the following terms.

Mobile Network Prefix

An IPv6 prefix delegated to a Mobile Router and advertised in the Mobile Network. More than one Mobile Network Prefix could be advertised in a Mobile Network.

Prefix Table

A list of Mobile Network Prefixes indexed by the Home Address of a Mobile Router. The Home Agent manages and uses Prefix Table to determine which Mobile Network Prefixes belong to a particular Mobile Router.

3. Overview of the NEMO Protocol

A Mobile Network is a network segment or subnet that can move and attach to arbitrary points in the routing infrastructure. A Mobile Network can only be accessed via specific gateways called Mobile Routers that manage its movement. Mobile Networks have at least one Mobile Router serving them. A Mobile Router does not distribute the Mobile Network routes to the infrastructure at its point of attachment (i.e., in the visited network). Instead, it maintains a bi-directional tunnel to a Home Agent that advertises an aggregation of Mobile Networks to the infrastructure. The Mobile Router is also the default gateway for the Mobile Network.

A Mobile Network can also comprise of multiple and nested subnets. A router without mobility support may be permanently attached to a Mobile Network for local distribution. Also, Mobile Routers may be attached to Mobile Networks owned by different Mobile Routers and may form a graph. In particular, with Basic NEMO Support, each Mobile Router is attached to another Mobile Network by a single interface. If loops are avoided, the graph is a tree.

A Mobile Router has a unique Home Address through which it is reachable when it is registered with its Home Agent. The Home Address is configured from a prefix aggregated and advertised by its Home Agent. The prefix could be either the prefix advertised on the home link or the prefix delegated to the Mobile Router. The Mobile

Router can have more than one Home Address if there are multiple prefixes in the home link. The Mobile Router also advertises one or more prefixes in the Mobile Network attached to it. The actual mechanism for assigning these prefixes to a given Mobile Router is outside the scope of this specification.

When the Mobile Router moves away from the home link and attaches to a new access router, it acquires a Care-of Address from the visited link. The Mobile Router can at any time act either as a Mobile Host or as a Mobile Router. It acts as a Mobile Host as defined in [1] for sessions it originates and provides connectivity to the Mobile Network. As soon as the Mobile Router acquires a Care-of Address, it immediately sends a Binding Update to its Home Agent as described in [1]. When the Home Agent receives this Binding Update, it creates a cache entry binding the Mobile Router's Home Address to its Care-of Address at the current point of attachment.

If the Mobile Router seeks to act as a Mobile Router and provide connectivity to nodes in the Mobile Network, it indicates this to the Home Agent by setting a flag (R) in the Binding Update. It MAY also include information about the Mobile Network Prefix in the Binding Update by using one of the modes described in section 5.2, so that the Home Agent can forward packets meant for nodes in the Mobile Network to the Mobile Router. A new Mobility Header Option for carrying prefix information is described in section 4.3. If the Mobile Network has more than one IPv6 prefix and wants the Home Agent to setup forwarding for all of these prefixes, it includes multiple prefix information options in a single Binding Update. The Home Agent sets up forwarding for each of these prefixes to the Mobile Router's Care-of Address. In some scenarios the Home Agent would already know which prefixes belong to a Mobile Router by an alternate mechanism such as static configuration. In these scenarios, the Mobile Router does not include any prefix information in the Binding Update. The Home Agent sets up forwarding for all prefixes owned by the Mobile Router when it receives a Binding Update from the Mobile Router with the Mobile Router Flag (R) set.

The Home Agent acknowledges the Binding Update by sending a Binding Acknowledgement to the Mobile Router. A positive acknowledgement with the Mobile Router Flag (R) set means that the Home Agent has set up forwarding for the Mobile Network. Once the binding process finishes, a bi-directional tunnel is established between the Home Agent and the Mobile Router. The tunnel end points are the Mobile Router's Care-of Address and the Home Agent's address. If a packet with a source address belonging to the Mobile Network Prefix is received from the Mobile Network, the Mobile Router reverse-tunnels the packet to the Home Agent through this tunnel. This reverse-tunneling is done by using IP-in-IP encapsulation [3]. The Home

Agent decapsulates this packet and forwards it to the Correspondent Node. For traffic originated by itself, the Mobile Router can use either reverse tunneling or route optimization, as specified in [1].

When a Correspondent Node sends a data packet to a node in the Mobile Network, the packet is routed to the Home Agent that currently has the binding for the Mobile Router. The Mobile Router's network prefix would be aggregated at the Home Agent, which would advertise the resulting aggregation. Alternatively, the Home Agent may receive the data packets destined to the Mobile Network by advertising routes to the Mobile Network Prefix. The actual mechanism by which these routes are advertised is outside the scope of this document. When the Home Agent receives a data packet meant for a node in the Mobile Network, it tunnels the packet to the Mobile Router's current Care-of Address. The Mobile Router decapsulates the packet and forwards it onto the interface where the Mobile Network is connected. Before decapsulating the tunneled packet, the Mobile Router has to check whether the Source address on the outer IPv6 header is the Home Agent's address. This check is not necessary if the packet is protected by IPsec in tunnel mode. The Mobile Router also has to make sure that the destination address on the inner IPv6 header belongs to a prefix used in the Mobile Network before forwarding the packet to the Mobile Network. If it does not, the Mobile Router should drop the packet.

The Mobile Network could include nodes that do not support mobility and nodes that do. A node in the Mobile Network can also be a fixed or a Mobile Router. The protocol described here ensures complete transparency of network mobility to the nodes in the Mobile Network. Mobile Nodes that attach to the Mobile Network treat it as a normal IPv6 access network and run the Mobile IPv6 protocol.

The Mobile Router and the Home Agent can run a routing protocol through the bi-directional tunnel. In this case, the Mobile Router need not include prefix information in the Binding Update. Instead, the Home Agent uses the routing protocol updates to set up forwarding for the Mobile Network. When the routing protocol is running, the bi-directional tunnel must be treated as a tunnel interface. The tunnel interface is included in the list of interfaces on which routing protocol is active. The Mobile Router should be configured not to send any routing protocol messages on its egress interface when it is away from the home link and connected to a visited link.

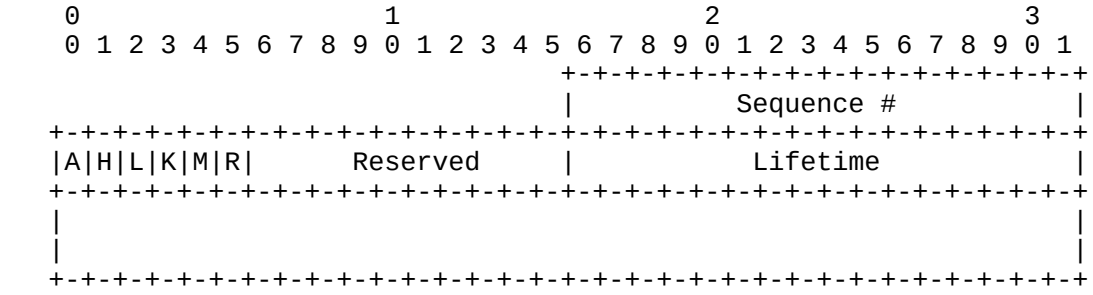
Finally, the Home Agent may be configured with static routes to the Mobile Network Prefix via the Mobile Router's Home Address. In this case, the routes are set independently of the binding flows and the returning home of a Mobile Router. The benefit is that such movement does not induce additional signalling in the form of routing updates

in the home network. The drawback is that the routes are present even if the related Mobile Routers are not reachable (at home or bound) at a given point of time.

4. Message Formats

4.1. Binding Update

A new flag (R) is included in the Binding Update to indicate to the Home Agent whether the Binding Update is coming from a Mobile Router and not from a mobile node. The rest of the Binding Update format remains the same as defined in [1].



Mobile Router Flag (R)

The Mobile Router Flag is set to indicate to the Home Agent that the Binding Update is from a Mobile Router. If the flag is set to 0, the Home Agent assumes that the Mobile Router is behaving as a Mobile Node, and it MUST NOT forward packets destined for the Mobile Network to the Mobile Router.

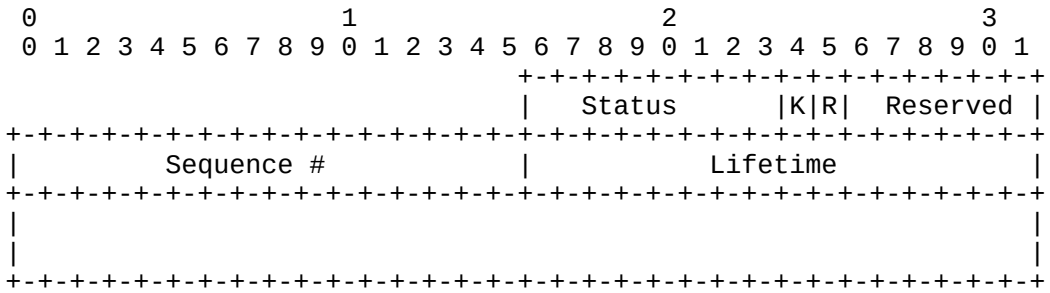
Mobility Options

A variable length field that can include zero or more mobility options. This document defines a new mobility option in addition to what is defined in [1].

For descriptions of the other fields in the message, see [1].

4.2. Binding Acknowledgement

A new flag (R) is included in the Binding Acknowledgement to indicate that the Home Agent that processed the corresponding Binding Update supports Mobile Routers. The flag is set only if the corresponding Binding Update had the Mobile Router Flag (R) set to 1. The rest of the Binding Acknowledgement format remains the same, as defined in [1].



Mobile Router Flag (R)

The Mobile Router Flag is set to indicate that the Home Agent that processed the Binding Update supports Mobile Routers. It is set to 1 only if the corresponding Binding Update had the Mobile Router Flag set to 1.

For descriptions of the other fields in the message, see [1].

This document also introduces the following new Binding Acknowledgement status values. The values shown below are decimal values.

140 Mobile Router Operation not permitted

141 Invalid Prefix

142 Not Authorized for Prefix

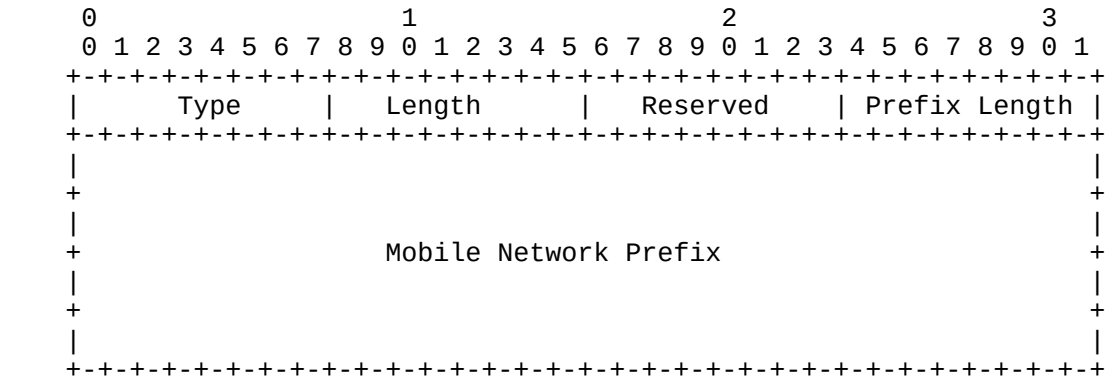
143 Forwarding Setup failed (prefixes missing)

Status values less than 128 indicate that the Binding Update was processed successfully by the receiving nodes. Values greater than 128 indicate that the Binding Update was rejected by the Home Agent.

4.3. Mobile Network Prefix Option

The Mobile Network Prefix Option is included in the Binding Update to indicate the prefix information for the Mobile Network to the Home Agent. There could be multiple Mobile Network Prefix Options if the Mobile Router has more than one IPv6 prefix in the Mobile Network and wants the Home Agent to forward packets for each of these prefixes to the Mobile Router’s current location.

The Mobile Network Prefix Option has an alignment requirement of 8n+4. Its format is as follows.



Type

6

Length

Eight-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. Set to 18.

Reserved

This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Prefix Length

Eight-bit unsigned integer indicating the prefix length of the IPv6 prefix contained in the option.

Mobile Network Prefix

A sixteen-byte field containing the Mobile Network Prefix

5. Mobile Router Operation

Mobile Router operation is derived largely from the combined behaviors of a host, of a router [5], and of a Mobile Node [1].

A Mobile Node can act in two ways: (1) as a Mobile Host, in which case the Home Agent doesn't maintain any prefix information related to the Mobile Host's Home Address but does maintain a binding cache entry related to the Mobile Host's Home Address, and (2) as a Mobile Router, in which case, in addition to maintaining the binding cache entry corresponding to the Mobile Router Home Address, the Home Agent

maintains forwarding information related to prefixes assigned to the Mobile Network. The distinction between the two modes is represented by the value of the Mobile Router Flag (R).

A Mobile Router MUST implement all requirements for IPv6 Mobile Nodes as described in section 8.5 of [1].

5.1. Data Structures

Like a Mobile Host, a Mobile Router also maintains a Binding Update List, described in section 11.1 of the Mobile IPv6 specification [1]. The Binding Update list is a conceptual data structure that records information sent in the Binding Updates. There is one entry per each destination to which the Mobile Router is currently sending Binding Updates.

This document introduces a new Prefix Information field in the Binding Update list structure. This field is used to store any prefix information that the Mobile Router includes in the Binding Update. If the Mobile Router sets the Mobile Router Flag (R) in the Binding Update but does not include any prefix information in it this field is set to null. The Mobile Router does not include prefix information in the Binding Update in the implicit mode or when it, runs a dynamic routing protocol with its Home Agent.

As does a Mobile Host, a Mobile Router stores the information regarding status of flags of the Binding Update in the corresponding Binding Update List entry. This document introduces a new Mobile Router Flag (R) for this entry. The status of this flag is stored in the Binding Update list whenever a Binding Update is sent.

A Mobile Router also maintains a Home Agent list populated according to the same procedure as a Mobile Host.

5.2. Sending Binding Updates

A Mobile Router sends Binding Updates to its Home Agent, as described in [1]. If the Mobile Router is not running a routing protocol as described in section 8, it uses one of the following modes to tell the Home Agent to determine which prefixes belong to the Mobile Router. In both modes, the Mobile Router sets the Mobile Router Flag (R).

Implicit:

In this mode, the Mobile Router does not include a Mobile Network Prefix Option in the Binding Update. The Home Agent can use any mechanism (not defined in this document) to

determine the Mobile Network Prefix(es) owned by the Mobile Router and to set up forwarding for the Mobile Network. One example would be manual configuration at the Home Agent mapping the Mobile Router's Home Address to the information required for setting up forwarding for the Mobile Network.

Explicit:

In this mode, the Mobile Router includes one or more Mobile Network Prefix Options in the Binding Update. These options contain information about the Mobile Network Prefix(es) configured on the Mobile Network.

A Mobile Router MUST implement at least one mode and MAY implement both. In the latter case, local configuration on the Mobile Router decides which mode to use. This is out of scope for this document.

If the Mobile Router Flag is set, the Home Registration Flag (H) MUST be set.

If the Mobile Router has a valid binding cache entry at the Home Agent, subsequent Binding Updates for the same Home Address should have the same value as the value in the binding cache for the Mobile Router Flag (R). In explicit mode, the Mobile Router MUST include prefix information in all Binding Updates, including those sent to refresh existing binding cache entries, if it wants forwarding enabled for the corresponding Mobile Network Prefixes.

5.3. Receiving Binding Acknowledgements

The Mobile Router receives Binding Acknowledgements from the Home Agent corresponding to the Binding Updates it sent. If the Binding Acknowledgement status is set to 0 (Binding Update accepted) and the Mobile Router Flag (R) is set to 1, the Mobile Router assumes that the Home Agent has successfully processed the Binding Update and has set up forwarding for the Mobile Network. The Mobile Router can then start using the bi-directional tunnel to reverse-tunnel traffic from the Mobile Network. If the Mobile Router Flag (R) is not set, then the Mobile Router concludes that its current Home Agent does not support Mobile Routers and it performs Dynamic Home Agent Address Discovery again to discover Home Agents that do. The Mobile Router MUST also de-register with the Home Agent that did not support it before attempting registration with another.

5.4. Error Processing

If the Binding Acknowledgement status is set to a value between 128 and 139, the Mobile Router takes necessary actions as described in the Mobile IPv6 specification [1]. For the Binding Acknowledgement status values defined in this document, the following sections explain the Mobile Router's behavior.

5.4.1. Implicit Mode

In Implicit mode, the Mobile Router interprets only error statuses 140 (Mobile Router Operation not permitted) and 143 (Forwarding Setup failed). The Mobile Router MUST treat Binding Acknowledgements with statuses '141' and '142' as fatal errors, since they should not be sent by the Home Agent in implicit mode.

If the Binding Acknowledgement from the Home Agent has the status 140, the Mobile Router SHOULD send a Binding Update to another Home Agent on the same home link. If no Home Agent replies positively, the Mobile Router MUST refrain from sending Binding Updates with the Mobile Router Flag set to any Home Agent on the home link, and it must log the information.

If the Binding Acknowledgement has the status 143, the Mobile Router SHOULD send a Binding Update to another Home Agent on the same home link. If no Home Agent replies positively, the Mobile Router SHOULD refrain from sending this Binding Update to any Home Agent on the home link, and MAY send Binding Updates in Explicit mode to a Home Agent on the same home link.

5.4.2. Explicit Mode

If the Mobile Router sent a Binding Update to the Home Agent in explicit mode, then the Mobile Router interprets only error statuses 140 (Mobile Router Operation not permitted), 141 (Invalid Prefix), and 142 (Not Authorized for Prefix). The Mobile Router MUST treat Binding Acknowledgements with status '143' as a fatal error, since it should not be sent by the Home Agent in explicit mode.

If the Binding Acknowledgement from the Home Agent has the status 140, the Mobile Router SHOULD send a Binding Update to another Home Agent on the same home link. If no Home Agent replies positively, then the Mobile Router MUST refrain from sending Binding Updates with the Mobile Router Flag set to any Home Agent on the home link, and it must log the information.

If the Binding Acknowledgement has the status 141 or 142, the Mobile Router SHOULD send a Binding Update to another Home Agent on the same

home link. If no Home Agent replies positively, then the Mobile Router SHOULD refrain from sending Binding Updates to any Home Agent on the home link. The Mobile Router MUST also stop advertising the prefix in the Mobile Network and try to obtain new IPv6 prefix information for the Mobile Network. It would do this by the same means that it initially got assigned the current Mobile Network Prefix. Alternatively, the Mobile Router MAY send Binding Updates in Implicit mode to a Home Agent on the same home link.

If by the end of this Error Processing procedure, as described in sections 5.4.1 and 5.4.2, the Mobile Router has tried every available mode and still has not received a positive Binding Acknowledgement, the Mobile Router MUST stop sending Binding Updates with the Mobile Router Flag set for this Home Address and it must log the information.

In all cases above, the Mobile Router MUST conclude that the Home Agent did not create a binding cache entry for the Mobile Router's Home Address.

5.5. Establishment of Bi-directional Tunnel

When a successful Binding Acknowledgement is received, the Mobile Router sets up its endpoint of the bi-directional tunnel.

The bi-directional tunnel between the Mobile Router and the Home Agent allows packets to flow in both directions, while the Mobile Router is connected to a visited link. The bi-directional tunnel is created by merging two unidirectional tunnels, as described in RFC 2473 [3]. The tunnel from the Mobile Router to the Home Agent has the Care-of address of the Mobile Router as the tunnel entry point and the Home Agent's address as the tunnel exit point. The tunnel from the Home Agent to the Mobile Router has the Home Agent's address and the Mobile Router's Care-of Address as the tunnel entry point and exit point, respectively. All IPv6 traffic to and from the Mobile Network is sent through this bi-directional tunnel.

A Mobile Router uses the Tunnel Hop Limit normally assigned to routers (not to hosts). Please refer to [3] for more details.

5.6. Neighbor Discovery for Mobile Router

When the Mobile Router is at home, it MAY be configured to send Router Advertisements and to reply to Router Solicitations on the interface attached to the home link. The value of the Router Lifetime field SHOULD be set to 0 to prevent other nodes from configuring the Mobile Router as the default router.

A Mobile Router SHOULD NOT send unsolicited Router Advertisements and SHOULD NOT reply to Router Solicitations on any egress interface when that interface is attached to a visited link. However, the Mobile Router SHOULD reply with Neighbor Advertisements to Neighbor Solicitations received on the egress interface, for addresses valid on the visited link.

A router typically ignores Router Advertisements sent by other routers on a link. However, a Mobile Router MUST NOT ignore Router Advertisements received on the egress interface. The received Router Advertisements MAY be used for address configuration, default router selection, or movement detection.

5.7. Multicast Groups for Mobile Router

When at home, the Mobile Router joins the multicast group All Routers Address with scopes 1 interface-local (on the home-advertising interface), and 2 link-local, on any of its egress interfaces. When in a visited network, the Mobile Router MUST NOT join the above multicast groups on the corresponding interface.

5.8. Returning Home

When the Mobile Router detects that it has returned to its home link, it MUST de-register with its Home Agent. The Mobile Router MUST implement and follow the returning-home procedures defined for a mobile node in [1]. In addition, the Mobile Router MAY start behaving as a router on its egress interface, especially as follows:

- The Mobile Router MAY send Router Advertisements on its egress interfaces, but the router lifetime SHOULD be set to 0 so that hosts on the home link do not pick the Mobile Router as the default router.

- The Mobile Router MAY join the All Routers Address multicast group on the home link.

- The Mobile Router MAY send routing protocol messages on its egress interface if it is configured to run a dynamic routing protocol.

When the Mobile Router sends a de-registration Binding Update in Explicit mode, it SHOULD NOT include any Mobile Network Prefix options in the Binding Update. When the Home Agent removes a binding cache entry, it deletes all associated Mobile Network Prefix routes.

6. Home Agent Operation

For a Mobile Router to operate correctly, the Home Agent MUST satisfy all the requirements listed in section 8.4 of [1]. The Home Agent MUST implement both modes described in section 5.2 of this document.

6.1. Data Structures

6.1.1. Binding Cache

The Home Agent maintains Binding Cache Entries for each Mobile Router currently registered with the Home Agent. The Binding Cache is a conceptual data structure described in detail in [1].

The Home Agent might need to store the Mobile Network Prefixes associated with a Mobile Router in the corresponding Binding Cache Entry. This is required if the Binding Update that created the Binding Cache Entry contained explicit prefix information. This information can be used later to clean up routes installed in explicit mode, when the Binding Cache Entry is removed, and to maintain the routing table, for instance, should the routes be removed manually.

The Home Agent also stores the status of the Mobile Router Flag (R) in the Binding Cache entry.

6.1.2. Prefix Table

The Home Agent SHOULD be able to prevent a Mobile Router from claiming Mobile Network Prefixes belonging to another Mobile Router. The Home Agent can prevent such attacks if it maintains a Prefix Table and verifies the prefix information provided by the Mobile Router against Prefix Table entries. The Prefix Table SHOULD be used by the Home Agent when it processes a Binding Update in explicit mode. It is not required when a dynamic routing protocol is run between the Mobile Router and the Home Agent.

Each entry in the Prefix Table contains the following fields:

- The Home Address of the Mobile Router. This field is used as the key for searching the pre-configured Prefix Table.

- The Mobile Network Prefix of the Mobile Router associated with the Home Address.

6.2. Mobile Network Prefix Registration

The Home Agent processes the Binding Update as described in section 10.3.1 of the Mobile IPv6 specification [1]. This section describes the processing of the Binding Update if the Mobile Router (R) Flag is set. The Home Agent performs the following check.

- The Home Registration (H) Flag MUST be set. If it is not, the Home Agent MUST reject the Binding Update and send a Binding Acknowledgement with status set to 140. Note: The basic support does not allow sending a Binding Update for a Mobile Network Prefix to correspondent nodes (for route optimization).

- Mobile IPv6 specification [1] requires that the Home Address in the Binding Update be configured from a prefix advertised on the home link. Otherwise the Binding Update is rejected with status value 132 [1]. This specification relaxes this requirement so that the Home Agent rejects the Binding Update only if the Home Address does not belong to the prefix that the Home Agent is configured to serve.

If the Home Agent has a valid binding cache entry for the Mobile Router, and if the Binding Update has the Mobile Router Flag (R) set to a value different from that in the existing binding cache entry, then the Home Agent MUST reject the Binding Update and send a Binding Acknowledgement with status set to 139 (Registration type change disallowed). However, if the Binding Update is a de-registration Binding Update, the Home Agent ignores the value of the Mobile Router Flag (R).

If the Lifetime specified in the Binding Update is 0 or the specified Care-of address matches the Home Address in the Binding Update, then this is a request to delete the cached binding for the home address and specified Mobile Network Prefixes. The Binding Update is processed as described in section 6.7.

If the Home Agent does not reject the Binding Update as invalid, and if a dynamic routing protocol is not run between the Home Agent and the Mobile Router as described in section 8, then the Home Agent retrieves the Mobile Network Prefix information as described below.

- If a Mobile Network Prefix Option is present in the Binding Update, the prefix information for the Mobile Network Prefix is retrieved from the Mobile Network Prefix field and the Prefix Length field of the option. If the Binding Update contains more than one option, the Home Agent MUST set up forwarding for all the Mobile Network Prefixes. If the Home Agent fails to set up forwarding to all the prefixes listed in the Binding Update, then

it MUST NOT forward traffic to any of the prefixes. Furthermore, it MUST reject the Binding Update and send a Binding Acknowledgement with status set to 141 (Invalid Prefix).

If the Home Agent verifies the prefix information with the Prefix Table and the check fails, the Home Agent MUST discard the Binding Update and send a Binding Acknowledgement with status set to 142 (Not Authorized for Prefix).

- If there is no option in the Binding Update carrying prefix information, the Home Agent uses manual pre-configured information to determine the prefixes assigned to the Mobile Router and to set up forwarding for the Mobile Network. If there is no information that the Home Agent can use, it MUST reject the Binding Update and send a Binding Acknowledgement with status set to 143 (Forwarding Setup failed).

If the Home Agent has a valid binding cache entry for the Mobile Router, it should compare the list of prefixes in the Binding Update against the prefixes stored in the binding cache entry. If the binding cache entry contains prefixes that do not appear in the Binding Update, the Home Agent MUST disable forwarding for these Mobile Network Prefixes.

If all checks are passed, the Home Agent creates a binding cache entry for Mobile Router's Home Address or updates the entry if it already exists. Otherwise, the Home Agent MUST NOT register the binding of the Mobile Router's Home Address.

The Home Agent defends the Mobile Router's Home Address through Proxy Neighbor Discovery by multicasting a Neighbor Advertisement message onto the home link on behalf of the Mobile Router. All fields in the Proxy Neighbor Advertisement message should be set the same way they would be by the Mobile Router if it sent this Neighbor Advertisement while at home, as described in [6]. There is an exception: If the Mobile Router (R) Flag has been set in the Binding Update, the Router (R) bit in the Advertisement MUST be set.

The Home Agent also creates a bi-directional tunnel to the Mobile Router for the requested Mobile Network Prefix or updates an existing bi-directional tunnel as described in section 6.4.

6.3. Advertising Mobile Network Reachability

To receive packets meant for the Mobile Network, the Home Agent advertises reachability to the Mobile Network. If the Home Link is configured with an aggregated prefix and the Mobile Network Prefix is aggregated under that prefix, then the routing changes related to the

Mobile Network may be restricted to the Home Link. If the Home Agent is the only default router on the Home Link, routes to the Mobile Network Prefix are aggregated naturally under the Home Agent, which does not have to do anything special.

If the Home Agent receives routing updates through a dynamic routing protocol from the Mobile Router, it can be configured to propagate those routes on the relevant interfaces.

6.4. Establishment of Bi-directional Tunnel

The implementation of the bi-directional tunnels and the mechanism for attaching them to the IP stack are outside the scope of this specification. However, all implementations MUST be capable of the following operations:

- The Home Agent can tunnel packets meant for the Mobile Network prefix to the Mobile Router's current location, the Care-of Address.

- The Home Agent can accept packets tunneled by the Mobile Router with the source address of the outer IPv6 header set to the Mobile Router's Care-of Address.

6.5. Forwarding Packets

When the Home Agent receives a data packet destined for the Mobile Network, it MUST forward the packet to the Mobile Router through the bi-directional tunnel. The Home Agent uses either the routing table, the Binding Cache, or a combination to route packets to the Mobile Network. This is implementation specific. Two examples are shown below.

1. The Home Agent maintains a route to the Mobile Network Prefix with the next hop set to the Mobile Router's Home Address. When the Home Agent tries to forward the packet to the next hop, it finds a binding cache entry for the home address. Then the Home Agent extracts the Mobile Router's Care-of address and tunnels the packet to the Care-of address.

2. The Home Agent maintains a route to the Mobile Network Prefix with the outgoing interface set to the bi-directional tunnel interface between the Home Agent and the Mobile Router. For this purpose, the Home Agent MUST treat this tunnel as a tunnel interface. When the packets are forwarded through the tunnel interface, they are encapsulated automatically, with the source address and

destination address in the outer IPv6 header set to the Home Agent's address and the Mobile Router's Care-of address, respectively.

6.6. Sending Binding Acknowledgements

A Home Agent serving a Mobile Router sends Binding Acknowledgements with the same rules it uses for sending Binding Acknowledgements to Mobile Hosts [1], with the following enhancements.

The Home Agent sets the status code in the Binding Acknowledgement to 0 (Binding Update accepted) to indicate to the Mobile Router that it successfully processed the Binding Update. It also sets the Mobile Router Flag (R) to indicate to the Mobile Router that it has set up forwarding for the Mobile Network.

If the Home Agent is not configured to support Mobile Routers, it sets the status code in the Binding Acknowledgement to 140 (Mobile Router Operation not permitted).

If one or more prefixes received in the Binding Update are invalid and the Home Agent cannot set up forwarding for the prefixes, the Home Agent sets the status code in the Binding Acknowledgement to 141 (Invalid Prefix) to indicate this to the Mobile Router.

If the Mobile Router is not authorized to use this Home Address to forward packets for one or more prefixes present in the Binding Update, the Home Agent sets the status code in the Binding Acknowledgement to 142 (Not Authorized for Prefix) to indicate this.

The Home Agent sets the status code to 143 (Forwarding Setup failed) if it is unable to determine the information needed to set up forwarding for the Mobile Network. This is used in the Implicit mode, in which the Mobile Router does not include any prefix information in the Binding Update.

6.7. Mobile Network Prefix De-registration

When the Home Agent successfully processes the de-registration BU, it deletes the Binding Cache Entry for the Mobile Router's Home Address and stops proxying the Home Address. This is described in detail in the Mobile IPv6 specification [1].

In addition, the Home Agent removes the bi-directional tunnel and stops forwarding packets to the Mobile Network. The Home Agent should keep all necessary information to clean up whichever routes it installed, whether they come from an implicit or explicit source.

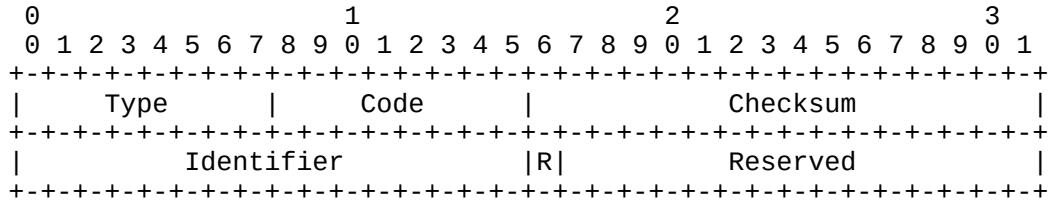
In Explicit mode, the Home Agent MUST ignore any Mobile Network Prefix Options present in the de-registration Binding Update.

7. Modifications to Dynamic Home Agent Address Discovery

This document extends the Dynamic Home Agent Address Discovery (DHAAD) defined in [1] so that Mobile Routers only attempt registration with Home Agents that support them.

7.1. Modified Dynamic Home Agent Discovery Address Request

A new flag (R) (Support for Mobile Routers) is introduced in the DHAAD Request message, defined in [1]. The Mobile Router sets this flag to indicate that it wants to discover Home Agents supporting Mobile Routers.



Mobile Router Support Flag (R)

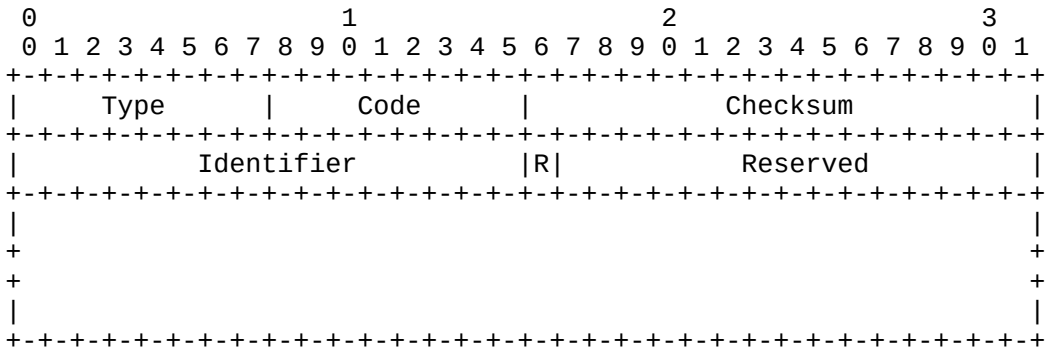
A one-bit flag that when set indicates that the Mobile Router wants to discover Home Agents supporting Mobile Routers.

For a description of the other fields in the message, see [1].

7.2. Modified Dynamic Home Agent Discovery Address Request

A new flag (R) (Support for Mobile Routers) is introduced in the DHAAD Reply message, defined in [1]. If a Home Agent receives a Dynamic Home Agent Discovery request message with the Mobile Router Support Flag set, it MUST reply with a list of Home Agents supporting Mobile Routers. The Mobile Router Support Flag MUST be set if there is at least one Home Agent supporting Mobile Routers. If none of the Home Agents support Mobile Routers, the Home Agent MAY reply with a list of Home Agents that only support Mobile IPv6 Mobile Nodes. In this case, the Mobile Router Support Flag MUST be set to 0.

The modified message format is as follows.



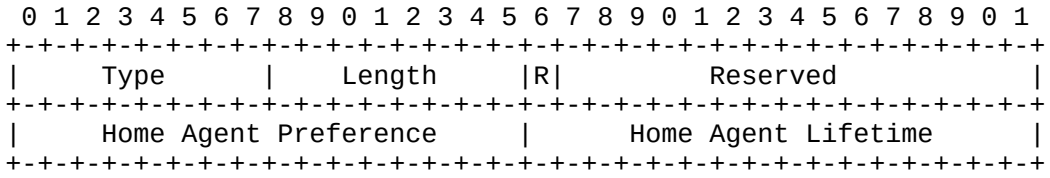
Mobile Router Support Flag (R)

A one-bit flag that when set indicates that the Home Agents listed in this message support Mobile Routers.

For a description of the other fields in the message, see [1].

7.3. Modified Home Agent Information Option

A new flag (R) (Support for Mobile Routers) is introduced in the Home Agent Information Option defined in [1]. If a Home Agent supports Mobile Routers, it SHOULD set the flag.



Mobile Router Support Flag (R)

A one-bit flag that when set indicates that the Home Agent supports Mobile Routers.

For a description of the other fields in the message, see [1].

8. Support for Dynamic Routing Protocols

In the solution described so far, forwarding to the Mobile Network at the Home Agent is set up when the Home Agent receives a Binding Update from the Mobile Router. An alternative to this is for the Home Agent and the Mobile Router to run an intra-domain routing protocol such as RIPng [12] and OSPF [13] through the bi-directional tunnel. The Mobile Router can continue running the same routing protocol that it ran when attached to the home link.

Support for running a intra-domain routing protocol is optional and is governed by the configuration on the Mobile Router and the Home Agent.

This feature is very useful when the Mobile Network is large with multiple subnets containing different IPv6 prefixes. Routing changes in the Mobile Network are quickly propagated to the Home Agent. Routing changes in the home link are quickly propagated to the Mobile Router.

When the Mobile Router is attached to the home link, it runs a routing protocol by sending routing updates through its egress interface. When the Mobile Router moves and attaches to a visited network, it should stop sending routing updates on the interface by which it attaches to the visited link. This reduces the chances that prefixes specific to the Mobile Network will be leaked to the visited network if routing protocol authentication is not enabled in the visited network and in the Mobile Network. It is expected that normal deployment practices will include proper authentication mechanisms to prevent unauthorized route announcements on both the home and visited networks. The Mobile Router then starts sending routing protocol messages through the bi-directional tunnel toward the Home Agent. Most routing protocols use link-local addresses as source addresses for the routing information messages. The Mobile Router is allowed to use link-local addresses for the inner IPv6 header of an encapsulated packet. But these MUST NOT be forwarded to another link by either the Mobile Router or the Home Agent.

When the Home Agent receives the inner packet, it processes the encapsulated routing protocol messages and updates its routing table accordingly. As part of normal routing protocol operation, the next hop information in these routing entries is filled with the Mobile Router’s link-local address, with the outgoing interface set to the bi-directional tunnel.

Similarly, the Home Agent sends routing updates through the bi-directional tunnel to the Mobile Router. The Mobile Router processes these routing protocol messages and updates its routing table. For

all routes advertised by the Home Agent, the Mobile Router sets the outgoing interface to the bi-directional tunnel to the Home Agent.

When the Mobile Router and the Home Agent exchange routes through a dynamic routing protocol, the Mobile Router SHOULD NOT include Mobile Network Prefixes in the Binding Update to the Home Agent. Depending on its configuration, the Home Agent might not add routes based on the prefix information in the Binding Updates and might use only the routing protocol updates. Moreover, including prefix information in both the Binding Updates and the routing protocol updates is redundant.

As the routing protocol messages from the Home Agent to the Mobile Router could potentially contain information about the internal routing structure of the home network, these messages require authentication and confidentiality protection. Appropriate authentication and confidentiality protection mechanisms, defined in [14], MUST be used. For protecting routing protocol messages by using IPsec ESP [4], the bi-directional tunnel between the Mobile Router and the Home Agent should be treated as the outgoing interface, with the Home Agent and Mobile Router's addresses as source and destination addresses for the inner encapsulated messages.

If a link state routing protocol such as OSPFv3 is run by the Mobile Router and the Home Agent, the recommendations in Appendix B should be followed.

9. Security Considerations

All signaling messages between the Mobile Router and the Home Agent MUST be authenticated by IPsec [8]. The use of IPsec to protect Mobile IPv6 signaling messages is described in detail in the HA-MN IPsec specification [2]. The signaling messages described in this document extend Mobile IPv6 messages and do not require any changes to what is described in [2].

The Mobile Router has to perform ingress filtering on packets received from the Mobile Network to ensure that nodes in the Mobile Network do not use the bi-directional tunnel to launch IP spoofing attacks. In particular, the Mobile Router SHOULD check that the IP source addresses in the packets received belong to the Mobile Network Prefix and are not the same as one of the addresses used by the Mobile Router. If the Mobile Router receives an IP-in-IP tunneled packet from a node in the Mobile Network and it has to forward the decapsulated packet, it SHOULD perform the above mentioned checks on the source address of the inner packet.

The Home Agent has to verify that packets received through the bi-directional tunnel belong to the Mobile Network. This check is necessary to prevent nodes from using the Home Agent to launch attacks that would have otherwise been prevented by ingress filtering. The source address of the outer IPv6 header MUST be set to the Mobile Router's current Care-of Address. The source address of the inner IPv6 header MUST be topologically correct with respect to the IPv6 prefixes used in the Mobile Network.

If the Mobile Router sends a Binding Update with a one or more Mobile Network Prefix options, the Home Agent MUST be able to verify that the Mobile Router is authorized for the prefixes before setting up forwarding for the prefixes.

When the Mobile Router runs a dynamic routing protocol as described in section 8, it injects routing update messages into the Home Link. As the routing protocol message could contain information about the internal routing structure of the home network, these messages require confidentiality protection. The Mobile Router SHOULD use confidentiality protection through IPsec ESP as described in [14]. If the bi-directional tunnel between the Mobile Router and the Home Agent is protected by ESP, in tunnel mode for all IP traffic, then no additional confidentiality protection specific to the routing protocol is required.

Home Agents and Mobile Routers may use IPsec ESP to protect payload packets tunneled between themselves. This is useful to protect communications against attackers on the path of the tunnel.

Please refer to the Mobile IPv6 specification [1] for security considerations when the Mobile Router operates as a Mobile Host.

10. IANA Considerations

This document defines a new Mobility Header Option, the Mobile Network Prefix Option as described in section 4.3. The type value for this option MUST be assigned from the same space used by the mobility options defined in [1].

This document also defines the following new Binding Acknowledgement status values. These status values are defined in section 4.2 and MUST be assigned from the same space used for Binding Acknowledgement status values in [1].

- Mobile Router Operation not permitted
- Invalid Prefix
- Not Authorized for Prefix
- Forwarding Setup failed (prefixes missing)

11. Contributors

We would like to acknowledge Ludovic Bellier, Claude Castelluccia, Thierry Ernst [15], Miguel Catalina-Gallego, Christophe Janneteau, T.J. Kniveton, Hong-Yon Lach, Jari T. Malinen, Koshiro Mitsuya, Alexis Olivereau, Charles E. Perkins, and Keisuke Uehara for their work on earlier proposals for Network Mobility. This document has inherited a lot of ideas from these proposals.

12. Acknowledgements

We thank all members of the NEMO Working Group, and of the preceding MONET BoF, for fruitful discussions on the mailing list and at IETF meetings.

Kent Leung, Marco Molteni, and Patrick Wetterwald are acknowledged for their work on Network Mobility for IPv4 and IPv6.

Tim Leinmueller is acknowledged for many insightful remarks and for section 7.

Jari Arkko, James Kempf, Chan-Wah Ng, and Erik Nordmark are acknowledged for their thorough review and comments.

Souhwan Jung, Fan Zhao, S. Felix Wu, HyunGon Kim, and SungWon Sohn are acknowledged for identifying threats related to tunneling between the Mobile Network and the Home Agent.

13. References

13.1. Normative References

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

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

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

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

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

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

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

13.2. Informative References

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

[9] Manner, J. and M. Kojo, Eds., "Mobility Related Terminology", RFC 3753, June 2004.

[10] Ernst, T., and H.-Y. Lach, "Network Mobility Support Terminology", Work in Progress, October 2004.

[11] Ernst, T., "Network Mobility Support Goals and Requirements", Work in Progress, October 2004.

[12] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[13] Coltun, R., Ferguson, D., and J. Moy, "OSPF for IPv6", RFC 2740, December 1999.

[14] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", Work in Progress, December 2004.

[15] Ernst, T., "Network Mobility Support in IPv6", PhD Thesis, University Joseph Fourier, Grenoble, France. October 2001.

[16] Moy, J., "Extending OSPF to Support Demand Circuits", RFC 1793, April 1995.

[17] Thubert, P., et al., "NEMO Home Network models", Work in Progress, October 2004.

Appendix A. Examples of NEMO Basic Support Operation

This section tries to illustrate the NEMO protocol by using a Mobile Router and a Mobile Node belonging to different administrative domains. The Mobile Router's Mobile Network consists of a Local Fixed Node (LFN) and a Local Fixed Router (LFR) [10]. The LFR has an access link to which other Mobile Nodes or Mobile Routers could attach.

Figure 1 depicts the scenario where both the Mobile Router and the Mobile Node are at home.

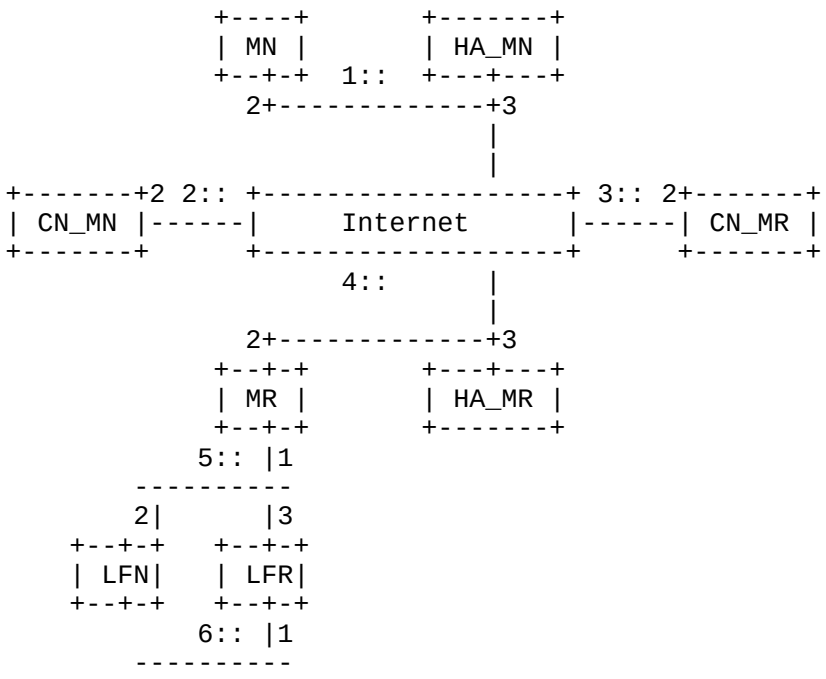


Figure 1. Mobile Router and Mobile Node at home.

The Mobile Router then moves away from the home link and attaches to a visited link. This is shown in Figure 2. The Mobile Router sends a Binding Update to HA_MR when it attaches to a visited link and configures a Care-of Address. HA_MR creates a binding cache entry for the Mobile Router's Home Address and also sets up forwarding for the prefixes on the Mobile Network.

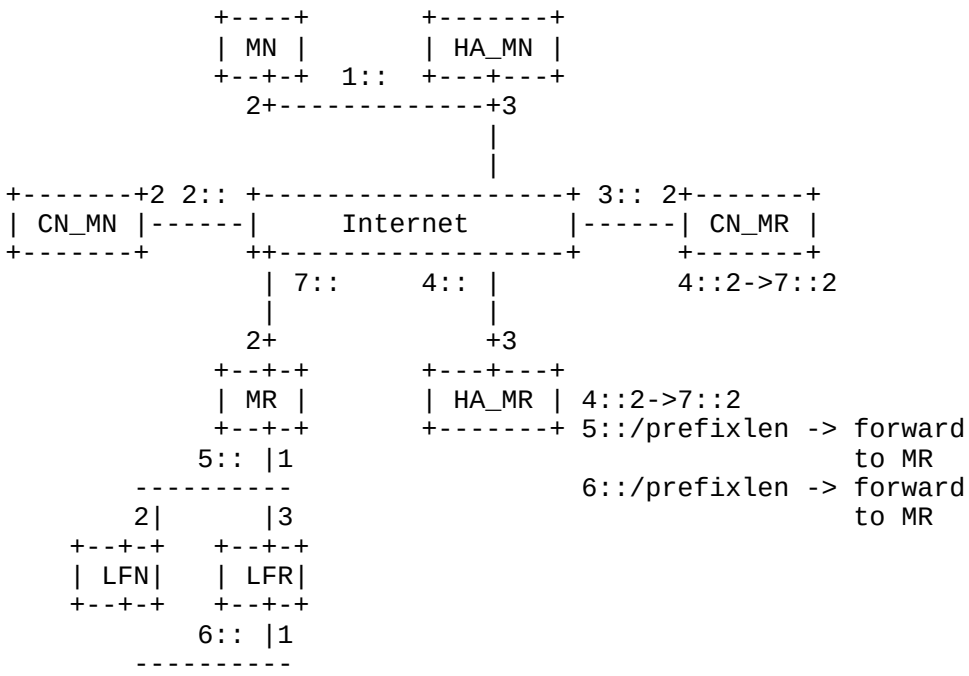


Figure 2. Mobile Router on a visited link.

Figure 3 shows the Mobile Node moving away from its home link and attaching to the Mobile Router. The Mobile Node configures a Care-of Address from the prefix advertised on the Mobile Network and sends a Binding Update to its Home Agent (HA_MN) and to its Correspondent Node (CN_MN). Both HA_MN and CN_MN create binding cache entries for the Mobile Node's Home Address.

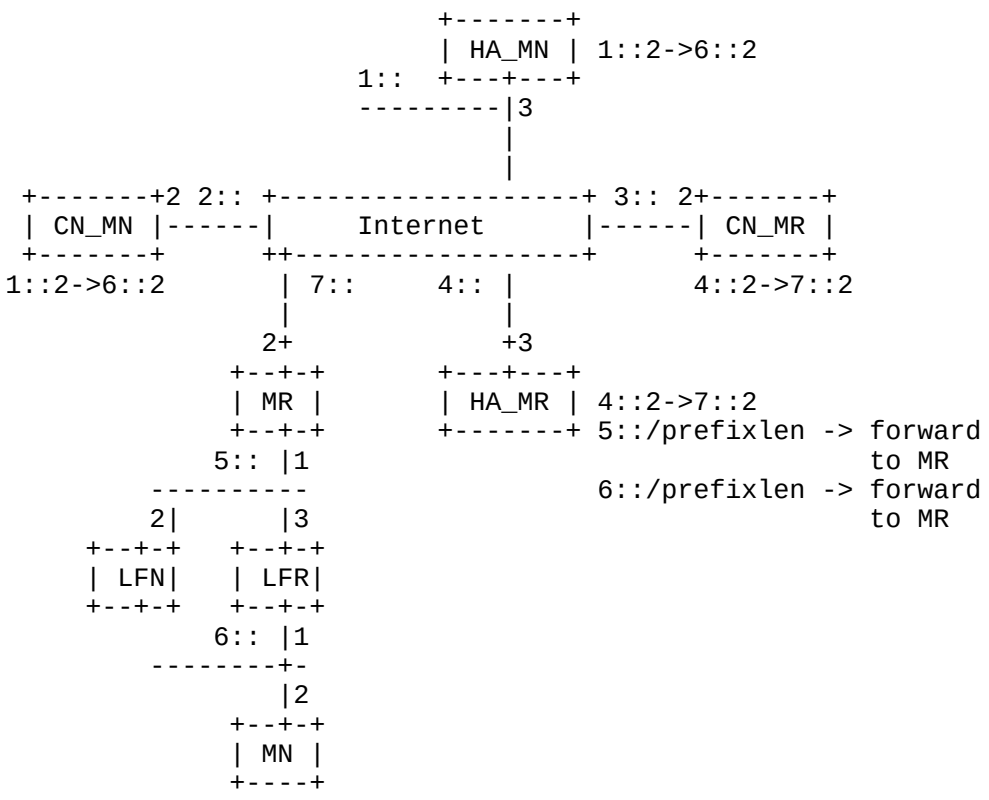


Figure 3. Mobile Node attached to Mobile Router on a visited link

Appendix B. Running Link State Routing Protocol with NEMO Basic Support

The bi-directional tunnel between the Mobile Router and the Home Agent is used as a virtual interface over which routing protocol messages are exchanged. When a link state routing protocol is run, the following recommendations should be followed.

B.1. Tunnel Interface Considerations

If the tunnel interface goes up and down every time the Mobile Router moves to a new visited network with a high level of mobility and a sufficient number of Mobile Routers, the amount of interface state changes will adversely affect the Home Agent's performance. This also introduces a high level of instability in the home network. To avoid this, the following should be considered when the bi-directional tunnel is implemented:

- A tunnel interface is consistently assigned to each Mobile Router, as long as it has a valid binding cache at the Home Agent.

- Every time the Mobile Router moves and updates the binding cache entry, the bi-directional tunnel should not be torn down and set up again. The tunnel end points should be updated dynamically with the Mobile Router's current Care-of Address.

- With a large number of interfaces, Hello packet processing may become a burden. Therefore, the tunnel interface should be treated as On-Demand circuits for OSPF [16].

B.2. OSPF Area Considerations

The following should be considered when the Home Network is configured for running OSPF:

- The entire Home domain SHOULD NOT be configured as a single area if a Home Agent supports Mobile Routers. At least the home network should be configured as a separate area.

- The bi-directional tunnel interfaces to the Mobile Routers should never be included in the same area as the backbone links.

For a more detailed discussion on configuring a home network for NEMO Basic Support, please see [17].

One disadvantage of running OSPFv3 with NEMO Basic Support is the possibility that the Mobile Networks will be told of the topology of the entire home network, including all the fixed and Mobile Routers. The only thing the Mobile Routers might really need is a default route through the Home Agent.

To reduce the amount of routing protocol messages received by a Mobile Router, one can configure each bi-directional tunnel to a Mobile Router as a separate area. But this requires that the Home Agent support a large number of OSPF areas if it supports a large number of Mobile Routers, and it might not be possible with most router implementations.

Another option is to configure multiple areas on the Home Link and group a number of Mobile Routers into each area. This reduces the number of areas that a Home Agent needs to support but also reduces the amount of routing protocol traffic that a Mobile Router receives.

Authors' Addresses

Vijay Devarapalli
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043
USA

EMail: vijay.devarapalli@nokia.com

Ryuji Wakikawa
Keio University and WIDE
5322 Endo Fujisawa Kanagawa
252-8520
Japan

EMail: ryuji@sfc.wide.ad.jp

Alexandru Petrescu
Motorola Labs
Parc les Algorithmes Saint Aubin
Gif-sur-Yvette 91193
France

EMail: Alexandru.Petrescu@motorola.com

Pascal Thubert
Cisco Systems Technology Center
Village d'Entreprises Green Side
400, Avenue Roumanille
Biot - Sophia Antipolis 06410
France

EMail: pthubert@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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