Network Working Group
Request for Comments: 5177
Category: Standards Track

K. Leung
G. Dommety
Cisco Systems
V. Narayanan
Qualcomm, Inc.
A. Petrescu
Motorola

April 2008

Network Mobility (NEMO) Extensions for Mobile IPv4

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document describes a protocol for supporting Mobile Networks between a Mobile Router and a Home Agent by extending the Mobile IPv4 protocol. A Mobile Router is responsible for the mobility of one or more network segments or subnets moving together. The Mobile Router hides its mobility from the nodes on the Mobile Network. The nodes on the Mobile Network may be fixed in relationship to the Mobile Router and may not have any mobility function.

Extensions to Mobile IPv4 are introduced to support Mobile Networks.

Table of Contents

1. Introduction 3
1.1. Examples of Mobile Networks 3
1.2. Overview of Protocol 5
2. Terminology 6
3. Requirements 7
4. Mobile Network Extensions 8
4.1. Mobile Network Request Extension 8
4.2. Mobile Network Acknowledgement Extension 9
5. Mobile Router Operation 11
5.1. Error Processing 12
5.2. Mobile Router Management 12
6. Home Agent Operation 13
6.1. Summary 13
6.2. Data Structures 14
6.2.1. Registration Table 14
6.2.2. Prefix Table 14
6.3. Mobile Network Prefix Registration 14
6.4. Advertising Mobile Network Reachability 16
6.5. Establishment of Bi-directional Tunnel 16
6.6. Sending Registration Replies 17
6.7. Mobile Network Prefix Deregistration 17
7. Data Forwarding Operation 17
8. Nested Mobile Networks 18
9. Routing Protocol between Mobile Router and Home Agent 18
10. Security Considerations 19
10.1. Security when Dynamic Routing Protocol Is Used 20
11. IANA Considerations 20
12. Acknowledgements 22
13. References 23
13.1. Normative References 23
13.2. Informative References 24

1. Introduction

This document describes network mobility extensions to the Mobile IPv4 protocol. The goal of introducing these extensions is to accommodate mobility scenarios where groups of hosts and routers move homogeneously (as a whole). It is required that all hosts and routers in a Mobile Network be able to run applications connecting to the Internet, and be reachable from the Internet.

For details regarding terminology related to network mobility (NEMO), a quick read of RFC 4885 [RFC4885] is suggested.

1.1. Examples of Mobile Networks

A Mobile Network links together a set of hosts and routers. Connecting this Mobile Network to the Internet is ensured at two levels: first, a Mobile Router is connected on one side to the Mobile Network and on another side to a wireless access system; second, a Home Agent placed on the home link manages traffic between the Correspondent Node and a Local Fixed Node (LFN, a node in the Mobile Network) by means of encapsulating traffic.

A scenario of applicability for this Mobile Network is described next. A Mobile Network is formed by a wireless-enabled Personal Digital Assistant (PDA) and a portable photographic camera, linked together by Bluetooth wireless link-layer technology. This is sometimes referred to as a Personal Area Network (PAN). In the illustration below, one can notice the PDA playing the role of a Mobile Router and the camera the role of Local Fixed Node.

```
                      ----
                     | HA |
                      ----        --------
                       |        /          \          ----
                      -+--------| Internet |---------| CN |
                                 \          /          ----
                                   --------
                                 /          \
                                /            \
                               /              \
                             ----             ----
                            | AR |           | AR |
                             ----             ----
                               |cellular       |cellular



                       /      |cellular
                       |    ----        ----
                Mobile |   | MR |      |LFN |   ---movement-->
               Network <    ----        ----
                       |      |           |
                       |     -+-----------+-
                       \       Bluetooth
```

The camera (Local Fixed Node) uploads photographic content to a Correspondent Node (CN) server. When the Mobile Network moves away, the Mobile Router serving the Mobile Network changes its point of attachment from one cellular access (Access Router) to another, obtaining a new Care-of Address. The Home Agent (HA) encapsulates application traffic for the CN and LFN.

Whereas the illustration above is a very simple instantiation of the applicability of Mobile IP-based Mobile Networks, more complex Mobile Networks are easily accommodated by the Mobile IPv4 extensions presented in this document (NEMOv4). For example, laptop computers used by passengers in a bus, train, ship, or plane should all be considered as forming Mobile Networks, as long as they move together (homogeneously).

1.2. Overview of Protocol

As introduced previously, this document presents extensions to the Mobile IPv4 protocol. The entities sending and receiving these extensions are the Mobile Router and the Home Agent. The Local Fixed Node is relieved from running Mobile IP software and, although it moves (together with the Mobile Network), its IP stack is not seeing any change in addressing.

Mobility for the entire Mobile Network is supported by the Mobile Router registering its current point of attachment (Care-of Address) to its Home Agent: the Mobile Router sends an extended Registration Request to the Home Agent, which returns an extended Registration Reply. This signaling sets up the tunnel between the two entities, as illustrated in the following figure:

```
                LFN        MR                      HA        CN
                 |         |                       |         |
                 |         | Extended Registration |         |
                 |         |----------------------->|         |
                 |         |        Request        |         |
                 |         |                       |         |
                 |         |                       |         |
                 |         | Extended Registration |         |
                 |         |<-----------------------|         |
                 |         |        Reply          |         |
                 |         |                       |         |
                 |<--------o=======================o-------->|
                 |         |     Encapsulated      |         |
                 |         |  Application Traffic  |         |
                 |         |                       |         |
```

The prefix(es) used within a Mobile Network (either implicitly configured on the Home Agent or explicitly identified by the Mobile Router in the Registration Request) is/are advertised by the Home Agent for route propagation in the home network. Traffic to and from nodes in the Mobile Network are tunneled by the Home Agent to the Mobile Router, and vice versa. Though packets from a Local Fixed Node placed in the Mobile Network can be forwarded by the Mobile Router directly without tunneling (if reverse tunneling were not used), these packets will be dropped if ingress filtering is turned on at the Access Router.

Extensively relating to Mobile IPv4 [RFC3344], this specification addresses mainly the co-located Care-of Address mode. Foreign Agent Care-of Address mode (with 'legacy' Foreign Agents [RFC3344]) is

supported but without optimization, and with double encapsulation being used. For an optimization of this mode, the gentle reader is directed to an extension document [NEMOv4-FA].

Compared to Mobile IPv4, this document specifies an additional tunnel between a Mobile Router's Home Address and the Home Agent. This tunnel is encapsulated within the normal tunnel between the Care-of Address (CoA) and Home Agent. In Foreign Agent CoA mode, the tunnel between the Mobile Router and Home Agent is needed to allow the Foreign Agent to direct the decapsulated packet to the proper visiting Mobile Router. However, in co-located CoA mode, the additional tunnel is not essential and could be eliminated because the Mobile Router is the recipient of the encapsulated packets for the Mobile Network; a proposal for this feature is in the extending document mentioned above [NEMOv4-FA].

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

A similar protocol has been documented in RFC 3963 [RFC3963] for supporting IPv6 Mobile Networks with Mobile IPv6 extensions.

Multihoming for Mobile Routers is outside the scope of this document.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Terminology for Mobile IPv4 mobility support is defined in RFC 3344 [RFC3344]. Terminology for network mobility support (NEMO), from an IPv6 perspective, is described in RFC 4885 [RFC4885]. In addition, this document defines the following terms for NEMOv4.

Mobile Router

> RFC 3344 [RFC3344] defines a Mobile Router as a mobile node that can be a router that is responsible for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak.

Mobile Network Prefix

The network prefix of the subnet delegated to a Mobile Router as the 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 the Prefix Table to determine which Mobile Network Prefixes belong to a particular Mobile Router.

Local Fixed Node

RFC 4885 [RFC4885] defines a Local Fixed Node (LFN) to be a fixed node belonging to the Mobile Network and unable to change its point of attachment. This definition should not be confused with "Long, Fat Network, LFN" of RFC 1323 [RFC1323], at least because the latter is pronounced "elephan(t)" whereas a NEMO LFN is distinctively pronounced "elefen".

3. Requirements

Although the original Mobile IPv4 specifications stated that Mobile Networks can be supported by the Mobile Router and Home Agent using static configuration or running a routing protocol (see Section 4.5 of RFC 3344 [RFC3344]), there is no solution for explicit registration of the Mobile Networks served by the Mobile Router. A solution needs to provide the Home Agent a means to ensure that a Mobile Router claiming a certain Mobile Network Prefix is authorized to do so. A solution would also expose the Mobile Network Prefixes (and potentially other subnet-relevant information) in the exchanged messages, to aid in network debugging.

The following requirements for Mobile Network support are enumerated:

- o A Mobile Router should be able to operate in explicit or implicit mode. A Mobile Router may explicitly inform the Home Agent which Mobile Network(s) need to be propagated via a routing protocol. A Mobile Router may also function in implicit mode, where the Home Agent may learn the Mobile Networks through other means, such as from the AAA server, via pre-configuration, or via a dynamic routing protocol.

- o The Mobile Network should be supported using Foreign Agents that are compliant to RFC 3344 [RFC3344] without any changes ('legacy' Foreign Agents).

- o The Mobile Network should allow Fixed Nodes, Mobile Nodes, or Mobile Routers to be on it.

- o The Local Fixed Nodes on a Mobile Network should be able to execute their sessions without running Mobile IP stacks. The Mobile Router managing the LFNs' Mobile Network is 'hiding' mobility events like the changes of the Care-of Address from the Local Fixed Nodes in that Mobile Network.

4. Mobile Network Extensions

4.1. Mobile Network Request Extension

For Explicit Mode, the Mobile Router informs the Home Agent about the Mobile Network Prefixes during registration. The Registration Request contains zero, one, or several Mobile Network Request extensions in addition to any other extensions defined by or in the context of RFC 3344 [RFC3344]. When several Mobile Networks need to be registered, each is included in a separate Mobile Network Request extension, with its own Type, Length, Sub-Type, Prefix Length, and Prefix. A Mobile Network Request extension is encoded in Type-Length-Value (TLV) format and respects the following ordering:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |   Sub-Type    | Prefix Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Prefix                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

148 Mobile Network Extension

Length:

Decimal 6.

Sub-Type:

0 (Mobile Network Request)

Prefix Length:

8-bit unsigned integer indicating the number of leftmost bits covering the network part of the address contained in the Prefix field.

Prefix:

32-bit unsigned integer in network byte-order containing an IPv4 address whose leftmost Prefix Length bits make up the Mobile Network Prefix.

4.2. Mobile Network Acknowledgement Extension

The Registration Reply contains zero, one or several Mobile Network Acknowledgement extensions in addition to any other extensions defined by or in the context of RFC 3344 [RFC3344]. For Implicit Mode, the Mobile Network Acknowledgement informs the Mobile Router the prefixes for which the Home Agent sets up forwarding with respect to this Mobile Router. Policies such as permitting only traffic from these Mobile Networks to be tunneled to the Home Agent may be applied by the Mobile Router. For Explicit Mode, when several Mobile Networks need to be acknowledged explicitly, each is included in a separate Mobile Network Acknowledgement extension, with its own Type, Sub-Type, Length, Prefix, and Prefix Length fields. At least one Mobile Network Acknowledgement extension MUST be in a successful Registration Reply to indicate to the Mobile Router that the Mobile Network Request extension was processed, and therefore was not skipped by the Home Agent.

A Registration Reply may contain any non-zero number of Explicit Mode and Implicit Mode Acknowledgements sub-types. Both sub-types can be present in a single Registration Reply. A Mobile Network Acknowledgement extension is encoded in Type-Length-Value (TLV) format. When the registration is denied with Code HA_MOBNET_ERROR (Code field in the Registration Reply), the Code field in the included Mobile Network Extension provides the reason for the failure.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |   Sub-Type    |      Code     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Prefix Length |    Reserved   |            Prefix...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
             ...Prefix          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

148 Mobile Network Extension

Length:

Decimal 8.

Sub-Type:

1 (Explicit Mode Acknowledgement)

2 (Implicit Mode Acknowledgement)

Code:

Value indicating success or failure:

0 Success

1 Invalid prefix (MOBNET_INVALID_PREFIX_LEN)

2 Mobile Router is not authorized for prefix (MOBNET_UNAUTHORIZED)

3 Forwarding setup failed (MOBNET_FWDING_SETUP_FAILED)

Prefix Length:

8-bit unsigned integer indicating the number of leftmost bits covering the network part of the address contained in the Prefix field.

Reserved:

Sent as zero; ignored on reception.

Prefix:

32-bit unsigned integer in network byte-order containing an IPv4 address whose leftmost Prefix Length bits make up the Mobile Network Prefix.

5. Mobile Router Operation

A Mobile Router's operation is generally derived from the behavior of a Mobile Node, as set in RFC 3344 [RFC3344]. In addition to maintaining mobility bindings for its Home Address, the Mobile Router, together with the Home Agent, maintains forwarding information for the Mobile Network Prefix(es) assigned to the Mobile Router.

A Mobile Router SHOULD set the 'T' bit to 1 in all Registration Request messages it sends to indicate the need for reverse tunnels for all traffic. Without reverse tunnels, all the traffic from the Mobile Network will be subject to ingress filtering in the visited networks. Upon reception of a successful Registration Reply, the Mobile Router processes the registration in accordance to RFC 3344 [RFC3344]. In addition, the following steps are taken:

- o Check for Mobile Network Acknowledgement extension(s) in Registration Reply.

- o Create tunnel to the Home Agent if the Mobile Router is registered in reverse tunneling mode.

- o Set up default route via this tunnel or egress interface when the Mobile Router is registered with or without reverse tunneling, respectively.

In accordance with this specification, a Mobile Router may operate in one of the following two modes: explicit and implicit. In explicit mode, the Mobile Router includes Mobile Network Prefix information in all Registration Requests (as Mobile Network Request extensions), while in implicit mode it does not include this information in any Registration Request. In the latter case, the Home Agent obtains the Mobile Network Prefixes by other means than Mobile IP. One example of obtaining the Mobile Network Prefix is through static configuration on the Home Agent.

A Mobile Router can obtain a co-located or Foreign Agent Care-of Address while operating in explicit or implicit modes.

For deregistration, the Mobile Router sends a registration request with lifetime set to zero without any Mobile Network Request extensions.

5.1. Error Processing

In a Mobile IP Registration Reply message, there may be two Code fields: one proper to the Registration Reply header (the 'proper' Code) and one within the Mobile Network Acknowledgement Extension (simply the 'Code'). A Mobile Router interprets the values of the Code field in the Mobile Network Acknowledgement Extension of the Registration Reply in order to identify any error related to managing the Mobile Network Prefixes by the Home Agent. It also interprets the values of the Code field in the Registration Reply header (the proper Code).

If the value of the Code field in the Registration Reply (the proper) is set to HA_MOBNET_DISALLOWED, then the Mobile Router MUST stop sending Registration Requests with any Mobile Network Prefix extensions to that Home Agent.

If the value of the Code field in the Registration Reply (the proper) is set to HA_MOBNET_ERROR, then the Mobile Router MUST stop sending Registration Requests that contain any of the Mobile Network Prefixes that are defined by the values of the fields Prefix and Prefix Length in the Mobile Network Acknowledgement extension. Note that the registration is denied in this case, and no forwarding for any Mobile Network Prefixes would be set up by the Home Agent for the Mobile Router.

It is possible that the Mobile Router receives a Registration Reply with no Mobile Network extensions if the registration was processed by a Mobile IPv4 Home Agent that does not support this specification at all. In that case, the absence of Mobile Network extensions must be interpreted by the Mobile Router as the case where the Home Agent does not support Mobile Networks.

All the error code values have been assigned by IANA; see Section 11.

5.2. Mobile Router Management

Operating a Mobile Router in a Mobile IPv4 environment has certain requirements on the management of the necessary initial configuration and supervision of the ongoing status information. Mobile Router maintenance indicators may need to be exposed in a manner consistent with other Mobile IPv4 indicators.

The objects for the Management Information Base (MIB) for Mobile IPv4 are defined in RFC 2006 [RFC2006]. The structure of the basic model of Mobile IP protocol describes three entities: Mobile Node, Home Agent, and Foreign Agent. In addition to these entities, this document proposes a functional entity to be the Mobile Router.

The necessary initial configuration at a NEMOv4-enabled Home Agent includes, but is not limited to, the contents of the Prefix Table. The Mobile Router MAY need to store the Mobile Network Prefixes as the initial configuration.

The definition of MIB objects related to the Mobile Router and to a NEMOv4-enabled Home Agent is outside the scope of this document.

6. Home Agent Operation

6.1. Summary

A Home Agent MUST support all the operations specified in RFC 3344 [RFC3344] for Mobile Node support. The Home Agent MUST support both implicit and explicit modes of operation for a Mobile Router.

The Home Agent processes the registration in accordance to RFC 3344 [RFC3344], which includes route setup to the Mobile Router's Home Address via the tunnel to the Care-of Address. In addition, for a Mobile Router registering in explicit mode, the following steps are taken:

1. Check that the Mobile Network Prefix information is valid.

2. Ensure the Mobile Network Prefix(es) is/are authorized to be on the Mobile Router.

3. Create a tunnel to the Mobile Router if it does not already exist.

4. Set up route for the Mobile Network Prefix via this tunnel.

5. Propagate Mobile Network Prefix routes via routing protocol if necessary.

6. Send the Registration Reply with the Mobile Network Acknowledgement extension(s).

If there are any subnet routes via the tunnel to the Mobile Router that are not specified in the Mobile Network extensions, these routes are removed.

In the case where the Mobile Node is not permitted to act as a Mobile Router, the Home Agent sends a Registration Reply message whose Code field is HA_MOBNET_DISALLOWED (the proper Code field of the Registration Reply).

For a Mobile Router registering in implicit mode, the Home Agent performs steps 3-6 above, once the registration request is processed successfully.

For deregistration, the Home Agent removes the tunnel to the Mobile Router and all routes using this tunnel. The Mobile Network extensions are ignored.

6.2. Data Structures

6.2.1. Registration Table

The Registration Table in the Home Agent, in accordance with RFC 3344 [RFC3344], contains binding information for every Mobile Node registered with it. RFC 3344 [RFC3344] defines the format of a Registration Table. In addition to all the parameters specified by RFC 3344 [RFC3344], the Home Agent MUST store the Mobile Network Prefixes associated with the Mobile Router in the corresponding registration entry, when the corresponding registration was performed in explicit mode. When the Home Agent is advertising reachability to Mobile Network Prefixes served by a Mobile Router, the information stored in the Registration Table can be used.

6.2.2. Prefix Table

The Home Agent must be able to authorize a Mobile Router for use of Mobile Network Prefixes when the Mobile Router is operating in explicit mode. Also, when the Mobile Router operates in implicit mode, the Home Agent must be able to locate the Mobile Network Prefixes associated with that Mobile Router. The Home Agent may store the Home Address of the Mobile Router along with the Mobile Network prefixes associated with that Mobile Router. If the Mobile Router does not have a Home Address assigned, this table may store the Network Access Identifier (NAI) [RFC2794] of the Mobile Router that will be used in dynamic Home Address assignment.

6.3. Mobile Network Prefix Registration

The Home Agent must process Registration Requests coming from Mobile Routers in accordance with this section. RFC 3344 [RFC3344] specifies that the Home Address of a mobile node registering with a Home Agent must belong to a prefix advertised on the home network. In accordance with this specification, however, the Home Address must be configured from a prefix that is served by the Home Agent, not necessarily the one on the home network.

If the Registration Request is valid, the Home Agent checks to see if there are any Mobile Network Prefix extensions included in the Registration Request.

If so, the Mobile Network Prefix information is obtained from the included extensions, and the Home Address from the Home Address field of the Registration Request. For every Mobile Network Prefix extension included in the registration request, the Home Agent MUST perform a check against the Prefix Table. If the Prefix Table does not contain at least one entry pairing that Home Address to that Mobile Network Prefix, then the check fails; otherwise, it succeeds.

Following this check against the Prefix Table, the Home Agent MUST construct a Registration Reply containing Mobile Network Acknowledgement extensions. For a Mobile Network Prefix for which the check was unsuccessful, the Code field in the corresponding Mobile Network Acknowledgement extension should be set to MOBNET_UNAUTHORIZED.

For a Mobile Network Prefix for which the check was successful, the Code field in the respective Mobile Network Acknowledgement extensions should be set to 0.

The Home Agent MUST attempt to set up forwarding for each Mobile Network Prefix extension for which the Prefix Table check was successful. If the forwarding setup fails for a particular Mobile Network Prefix (for reasons such as not enough memory available or not enough devices available), the Code field in the respective Mobile Network Acknowledgement extension should be set to MOBNET_FWDING_SETUP_FAILED.

If forwarding and setup was successful for at least one Mobile Network Prefix, then the Code field (the proper) of the Registration Reply message should be set to 0. Otherwise, when forwarding and setup was unsuccessful for each and every Mobile Network Prefixes, that Code (the proper) should be HA_MOBNET_ERROR.

If the Registration Request is sent in implicit mode, i.e., without any Mobile Network Request extension, the Home Agent may use pre-configured Mobile Network prefix information for the Mobile Router to set up forwarding.

If the Home Agent is updating an existing binding entry for the Mobile Router, it MUST check all the prefixes in the Registration Table against the prefixes included in the Registration Request. If one or more Mobile Network prefixes are missing from the included

information in the registration request, the Home Agent MUST delete those prefixes from the registration table. Also, the Home Agent MUST disable forwarding for those prefixes.

If all checks are successful, the Home Agent either creates a new entry for the Mobile Router or updates an existing binding entry for it and returns a successful registration reply back to the Mobile Router or the Foreign Agent (if the Registration Request was received from a Foreign Agent).

In accordance with RFC 3344 [RFC3344], the Home Agent does proxy Address Resolution Protocol (ARP) for the Mobile Router Home Address when the Mobile Router Home Address is derived from the home network.

If the 'T' bit is set, the Home Agent creates a bi-directional tunnel for the corresponding Mobile Network prefixes or updates the existing bi-directional tunnel. This tunnel is maintained independent of the reverse tunnel for the Mobile Router home address itself.

6.4. Advertising Mobile Network Reachability

If the Mobile Network prefixes served by the Home Agent are aggregated with the home network prefix and if the Home Agent is the default router on the home network, the Home Agent does not have to advertise the Mobile Network Prefixes. The routes for the Mobile Network Prefix are automatically aggregated into the home network prefix (it is assumed that the Mobile Network Prefixes are automatically aggregated into the home network prefix). If the Mobile Router updates the Mobile Network prefix routes via a dynamic routing protocol, the Home Agent SHOULD propagate the routes on the appropriate networks.

6.5. Establishment of Bi-directional Tunnel

The Home Agent creates and maintains a bi-directional tunnel for the Mobile Network prefixes of a Mobile Router registered with it. A Home Agent supporting IPv4 Mobile Router operation MUST be able to forward packets destined to the Mobile Network prefixes served by the Mobile Router to its Care-of Address. Also, the Home Agent MUST be able to accept packets tunneled by the Mobile Router with the source address of the outer header set to the Care-of Address of the Mobile Router and that of the inner header set to the Mobile Router's Home Address or an address from one of the registered Mobile Network prefixes.

6.6. Sending Registration Replies

The Home Agent MUST set the status code in the registration reply to 0 to indicate successful processing of the Registration Request and successful setup of forwarding for at least one Mobile Network prefix served by the Mobile Router. The Registration Reply MUST contain at least one Mobile Network Acknowledgement extension.

If the Home Agent is unable to set up forwarding for one or more Mobile Network prefixes served by the Mobile Router, it MUST set the Mobile Network Acknowledgement Extension status Code in the Registration Reply to MOBNET_FWDING_SETUP_FAILED. When the prefix length is zero or greater than decimal 32, the status Code MUST be set to MOBNET_INVALID_PREFIX_LEN.

If the Mobile Router is not authorized to forward packets to a Mobile Network prefix included in the request, the Home Agent MUST set the Code to MOBNET_UNAUTHORIZED.

6.7. Mobile Network Prefix Deregistration

If the received Registration Request is for deregistration of the Care-of Address, the Home Agent, upon successful processing of it, MUST delete the entry (or entries) from its Registration Table. The Home Agent tears down the bi-directional tunnel and stops forwarding any packets to/from the Mobile Router. The Home Agent MUST ignore any included Mobile Network Request extension in a deregistration request.

7. Data Forwarding Operation

For traffic to the nodes in the Mobile Network, the Home Agent MUST perform double tunneling of the packet, if the Mobile Router had registered with a Foreign Agent Care-of Address. In this case, the Home Agent MUST encapsulate the packet with the tunnel header (source IP address set to Home Agent, and destination IP address set to Mobile Router’s Home Address) and then encapsulate one more time with the tunnel header (source IP address set to Home Agent, and destination IP address set to CoA).

For optimization, the Home Agent SHOULD only encapsulate the packet with the tunnel header (source IP address set to Home Agent, and destination IP address set to CoA) for co-located CoA mode.

When a Home Agent receives a packet from the Mobile Network prefix in the bi-directional tunnel, it MUST de-encapsulate the packet and route it as a normal IP packet. It MUST verify that the incoming

packet has the source IP address set to the Care-of Address of the Mobile Router. The packet MUST be dropped if the source address is not set to the Care-of Address of the Mobile Router.

For traffic from the nodes in the Mobile Network, the Mobile Router encapsulates the packet with a tunnel header (source IP address set to Mobile Router's Home Address, and destination IP address set to Home Agent) if reverse tunnel is enabled. Otherwise, the packet is routed directly to the Foreign Agent or access router.

In co-located CoA mode, the Mobile Router MAY encapsulate one more time with a tunnel header (source IP address set to the CoA and destination IP address set to Home Agent).

8. Nested Mobile Networks

Nested Network Mobility is 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. Two issues should be noted though. First, whenever physical loops occur in a nested aggregation of Mobile Networks, this protocol neither detects nor solves them -- datagram forwarding may be blocked. Second, Mobile Routers in a deep nested aggregation of Mobile Networks might introduce significant overhead on the data packets as each level of nesting introduces another tunnel header encapsulation. Applications that do not support MTU discovery are adversely affected by the additional header encapsulations because the usable MTU is reduced with each level of nesting.

9. Routing Protocol between Mobile Router and Home Agent

There are several benefits of running a dynamic routing protocol between the Mobile Router and the Home Agent. If the Mobile Network is relatively large, including several wireless subnets, then the topology changes within the moving network can be exposed from the Mobile Router to the Home Agent by using a dynamic routing protocol. The purpose of the NEMOv4 protocol extensions to Mobile IPv4, as defined in previous sections, is not to inform the Home Agent about these topology changes, but to manage the mobility of the Mobile Router.

Similarly, topology changes in the home network can be exposed to the Mobile Router by using a dynamic routing protocol. This may be necessary when new fixed networks are added in the home network.

Here too, the purpose of NEMOv4 extensions is not to inform the Mobile Router about topology changes at home.

Examples of dynamic routing protocols include, but are not limited to, OSPF Version 2 [RFC2328], BGP [RFC4271], and RIP [RFC2453].

The recommendations are related to how the routing protocol and the Mobile IPv4 implementation work in tandem on the Mobile Router and on the Home Agent (1) without creating incoherent states in the forwarding information bases at home and on the Mobile Router, (2) without introducing topologically incorrect addressing information in the visited domain, and (3) without duplicating sent data or over-provisioning security.

The information exchanged between the Mobile Router and the Home Agent is sent over the bi-directional tunnel established by the Mobile IPv4 exchange Registration Request - Registration Reply (see Section 6.5). If a network address and prefix of a subnet in the moving network is sent by the Mobile Router within a routing protocol message, then they SHOULD NOT be sent in the Mobile IPv4 Registration Request too. This avoids incoherencies in the forwarding information bases. The Mobile Router SHOULD use NEMOv4 implicit mode in this case (see Section 3).

The Mobile Router SHOULD NOT send routing protocol information updates in the foreign network. The subnet addresses and prefixes valid in the moving network are topologically incorrect in the visited network.

If the Mobile Router and the Home Agent use a dynamic routing protocol over the tunnel interface, and if that protocol offers security mechanisms to protect that protocol’s messages, then the security recommendations in Section 10.1 apply.

10. Security Considerations

The Mobile Network extension is protected by the same rules as for Mobile IP extensions in registration messages. See the Security Considerations section in RFC 3344 [RFC3344].

The Home Agent MUST be able to verify that the Mobile Router is authorized to provide mobility service for the Mobile Networks in the Registration Request, before anchoring these Mobile Network Prefixes on behalf of the Mobile Router. Forwarding for prefixes MUST NOT be set up without successful authorization of the Mobile Router for those prefixes. The Mobile Router MUST be notified when there is a registration failure because it cannot be successfully authorized for prefixes it requested.

All Registration Requests and replies MUST be authenticated by the MN-HA Authentication Extension as specified in RFC 3344 [RFC3344]. When the registration request is sent in explicit mode, i.e., with one or more Mobile Network Prefix extensions, all the Mobile Network Prefix extensions MUST be included before the MN-HA Authentication extension. Also, these extensions MUST be included in the calculation of the MN-HA authenticator value.

The Mobile Router should perform ingress filtering on all the packets received on the Mobile Network prior to reverse tunneling them to the Home Agent. The Mobile Router MUST drop any packets that do not have a source address belonging to the Mobile Network.

The Mobile Router MUST also ensure that the source address of packets arriving on the Mobile Network is not the same as the Mobile Router's IP address on any interface. These checks will protect against nodes attempting to launch IP spoofing attacks through the bi-directional tunnel.

The Home Agent, upon receiving packets through the bi-directional tunnel, MUST verify that the source addresses of the outer IP header of the packets are set to the Mobile Router's Care-of Address. Also, it MUST ensure that the source address of the inner IP header is a topologically correct address on the Mobile Network. This will prevent nodes from using the Home Agent to launch attacks inside the protected network.

10.1. Security when Dynamic Routing Protocol Is Used

If a dynamic routing protocol is used between the Mobile Router and the Home Agent to propagate the Mobile Network information into the home network, the routing updates SHOULD be protected with IPsec ESP confidentiality between the Mobile Router and Home Agent, to prevent information about home network topology from being visible to eavesdroppers.

11. IANA Considerations

IANA has assigned rules for the existing registry "Mobile IPv4 numbers - per RFC 3344". The numbering space for Extensions that may appear in Mobile IP control messages (those sent to and from UDP port number 434) should be modified.

The new Values and Names for the Type for Extensions appearing in Mobile IP control messages are the following:

Value	Name
148	Mobile Network Extension

Table 1: New Values and Names for Extensions in Mobile IP Control Messages

A new number space has been created for the Values and Names for the Sub-Type for Mobile Network Extensions. This number space is initially defined to hold the following entries, allocated by this document:

Value	Name
0	Mobile Network Request Extension
1	Explicit Mode Acknowledgement Extension
2	Implicit Mode Acknowledgement Extension

Table 2: New Values and Names for the Sub-Type for Mobile Network Extensions

The policy of future assignments to this number space is following Standards Action or IESG Approval (see [RFC2434]).

The new Code Values for Mobile IP Registration Reply messages are the following (for a registration denied by the Home Agent):

Value	Name
147	Mobile Network Prefix operation error (HA_MOBNET_ERROR)
148	Mobile Router operation is not permitted (HA_MOBNET_DISALLOWED)

Table 3: New Code Values for Mobile IP Registration Reply

A new number space has been created for the Code Values for the Mobile Network Acknowledgement Extension. This number space is initially defined to hold the following entries, allocated by this document (result of registration, as sent by the Home Agent):

0	Success
1	Invalid prefix length (MOBNET_INVALID_PREFIX_LEN)
2	Mobile Router is not authorized for prefix (MOBNET_UNAUTHORIZED)
3	Forwarding setup failed (MOBNET_FWDING_SETUP_FAILED)

Table 4: New Code Values for Mobile Network Acknowledgement Extension

The policy of future assignments to this number space is following Standards Action or IESG Approval (see [RFC2434]).

12. Acknowledgements

The authors would like to thank Christophe Janneteau, George Popovich, Ty Bekiares, Ganesh Srinivasan, Alpesh Patel, Ryuji Wakikawa, George Tsirtsis, and Henrik Levkowetz for their helpful discussions, reviews, and comments. Vijay Devarapalli extensively reviewed one of the later versions of the document. Hans Sjostrand identified the last clarifications with respect to Foreign Agent mode treatment. Pete McCann contributed necessary refinements of many statements.

Mobile IPv4 versions as early as 1996 (RFC 2002 by Charles Perkins) described Mobile Networks and Mobile Routers support.

Fred Templin indicated the potential confusion for the term "LFN".

Amanda Baber of IANA agreed on the principles of allocating numbers for this specification and suggested improvements on the IANA section.

Tim Polk of the IESG identified a deeply entrenched error on managing the Code fields.

Lars Eggert of the IESG suggested the accommodation of the otherwise legal non-contiguous netmask fields, instead of simply prefix lengths.

Dan Romascanu of the IESG indicated the necessity of manageability of Mobile Routers and NEMOv4-enabled Home Agents and their deployability in MIP4 environments.

David Borman of TSV-DIR reviewed this document as part of the transport area directorate's ongoing effort to review key IETF documents. The implications of the growth of usable MTU adversely affecting applications deep in a Mobile Network were suggested.

Gonzalo Camarillo provided a generalist review by an additional set of eyes for documents as they are being considered for publication (General Area Review Team).

Jari Arkko of the IESG reviewed, suggested necessary improvements to, and diligently shepherded this document through IESG.

13. References

13.1. Normative References

[RFC1323] Jacobson, V., Braden, B., and D. Borman, "TCP Extensions for High Performance", RFC 1323, May 1992.

[RFC2006] Cong, D., Hamlen, M., and C. Perkins, "The Definitions of Managed Objects for IP Mobility Support using SMIv2", RFC 2006, October 1996.

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

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998.

[RFC2794] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

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

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

13.2. Informative References

[NEMOv4-FA] Tsirtsis, G., Park, V., Narayanan, V., and K. Leung, "FA extensions to NEMOv4 Base", Work in Progress, February 2008.

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

[RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, July 2007.

Authors' Addresses

Kent Leung
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

Phone: +1 408-526-5030
EMail: kleung@cisco.com

Gopal Dommety
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

Phone: +1 408-525-1404
EMail: gdommety@cisco.com

Vidya Narayanan
QUALCOMM, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-2483
EMail: vidyan@qualcomm.com

Alexandru Petrescu
Motorola
Parc les Algorithmes Saint Aubin
Gif-sur-Yvette, Essonne 91140
France

Phone: +33 169354827
EMail: alexandru.petrescu@motorola.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.