NEMO Working Group
Internet Draft
Expires: May 1, 2003

T. J. Kniveton
Jari T. Malinen
Vijay Devarapalli
Charles E. Perkins
Nokia
November 1, 2002

Mobile Router Tunneling Protocol
draft-kniveton-mobrtr-03.txt

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at:
http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at:
http://www.ietf.org/shadow.html.

This document is a submission by the NEMO Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the nemo@nal.motlabs.com mailing list.

Distribution of this memo is unlimited.

Abstract

This document describes how to support mobile networks with Mobile IP or Mobile IPv6 using reverse tunneling. It provides this support capability with no modifications to Mobile IP or routing protocol signaling, but also defines new extensions to ease in the implementation of network mobility. There are two described scenarios of mobile router support, consumer mode, and fully enabled mode. In the former, the mobile router is not allowed to use routing protocol signaling with the home agent, but performs routing for subnet(s) assigned to it. In the latter mode, both the home agent and the mobile router use a routing protocol in the same manner as fixed routers.

Contents

1. Introduction

This document describes the problem of mobile router support and requirements for solving this problem. It then shows how to solve this problem and support mobile networks with Mobile IP [9] or Mobile IPv6 [5]. The document describes two categorical scenarios, static (``consumer'') and dynamic (``fully enabled'') mobile routers, and

outlines how these scenarios are possible using unmodified Mobile IP or Mobile IPv6, with or without a dynamic routing protocol.

Within the context of this document, a Mobile Router is defined as a node which operates as a Mobile Node as detailed in Mobile IP or Mobile IPv6, but has the additional capability of routing between its point of attachment (Care-of Address), and a network fragment (subnet) which moves with the mobile router.

An architecture to enable mobile routers is required to:

1 support unmodified Mobile IP or Mobile IPv6 signaling.

2 support communication to or from nodes on subnetwork(s) connected to and moving with the mobile router.

3 support both fixed and mobile nodes in the network moving with the mobile router. Fixed nodes are unmodified IP or IPv6 hosts or routers which do not necessarily have any mobility support nor any knowledge of the mechanisms described in this document. Mobile nodes are nodes supporting Mobile IP or Mobile IPv6 with no knowledge of the mechanisms described in this document.

4 support arbitrary nesting level of mobile routers; i.e., support connection (into the mobile router's moving network) of another mobile router and its associated network.

5 support static configuration; that is, the mobile router need not have a dynamic routing protocol running on it.

6 support dynamic configuration; that is, the mobile router may run a dynamic routing protocol and communicate with such a routing protocol to signal its home agent.

7 allow routing entities such as the home agent and mobile router to be able to run these dynamic routing protocols with no modifications to their signaling.

8 support an end-to-end security model for mobility where no intermediate node or router alters mobility state in mobile nodes, routers, or their respective home agents and correspondent nodes.

Mobile router support described here is NOT assumed to:

- solve the problems resulting from excessively fast relative topology changes. The outcome of implementing a mobile network as described here will inherit the characteristics of Mobile IP and the routing protocol chosen, and thus be able to support

movement and topology changes to the same extent as those protocols. Hence, any routing protocol which would be used to support mobile routers is assumed to be suitable for the rate of change to topology in anticipated usage scenarios.

- solve the problem of scalability resulting from fixed network connectivity of a cascaded mesh of routers (and their subnetworks) that contain non-aggregable, host-based routes.

2. Terms

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 [1].

In addition, this document uses the following terms:

Fixed Node
: A host not capable moving from its home link to other links. A fixed node is capable of sending and receiving packets, that is, being a source or destination of traffic, but not a forwarder of it.

Fixed Router
: A router not capable of moving from its home link to other links. A fixed router is capable of forwarding packets between two or more interfaces, and possibly running a dynamic routing protocol modifying the state by which to do packet forwarding.

Mobile Node
: A host moving from its home link to other links. A mobile node is capable of sending and receiving packets, that is, being a source or destination of traffic, but not a forwarder of it.

Mobile Router
: A router moving from its home link to other links. A mobile router is capable of forwarding packets between two or more interfaces, and possibly running a dynamic routing protocol modifying the state by which to do packet forwarding.

This terminology is intended to conform to those that have been used in IPv6, Mobile IPv6, and other Internet protocols [3, 5].

3. Solution Overview

This document outlines a solution which satisfies the above requirements. The one-digit prefixes are assumed to be legal prefixes for globally routable links, e.g,. with prefix length 64.

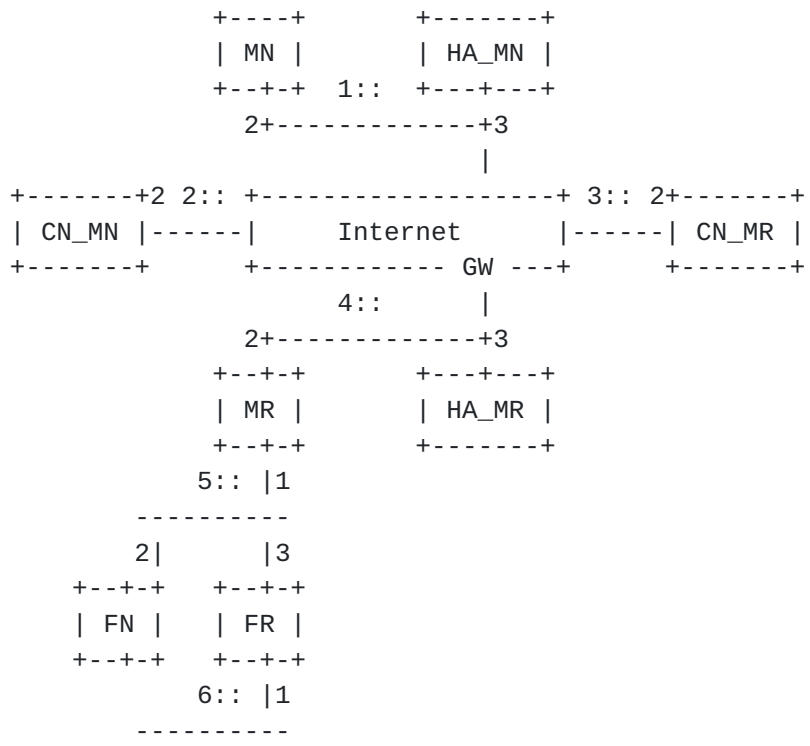


Figure 1: Mobile node and mobile router at home.

In Figure 1, a mobile node (MN) 1::2 is at home on its home link where we have its home agent 1::3 (HA_MN). A mobile router (MR) 4::2 is at its home. It also provides routing for an access link 5::, on which there is a fixed node (FN). MR also provides access for access link 6::, which is behind a fixed fouter (FR). MR, GW, and HA are supposed to be routers, so that they at least forward packets. They may also run the same dynamic routing protocol.

In Figure 2 we see the bindings when MN moves away from its home to link 6::, after MN has signaled its home agent (HA_MN) and its correspondent node (CN_MN), assuming mobile nodes or routers get the same host number as in their home addresses.

In Figure 3 we see the bindings when MR moves away from its home link, to link 7::, and it has updated its home agent (HA_MR), and its correspondent node (CN_MR) on its new location.

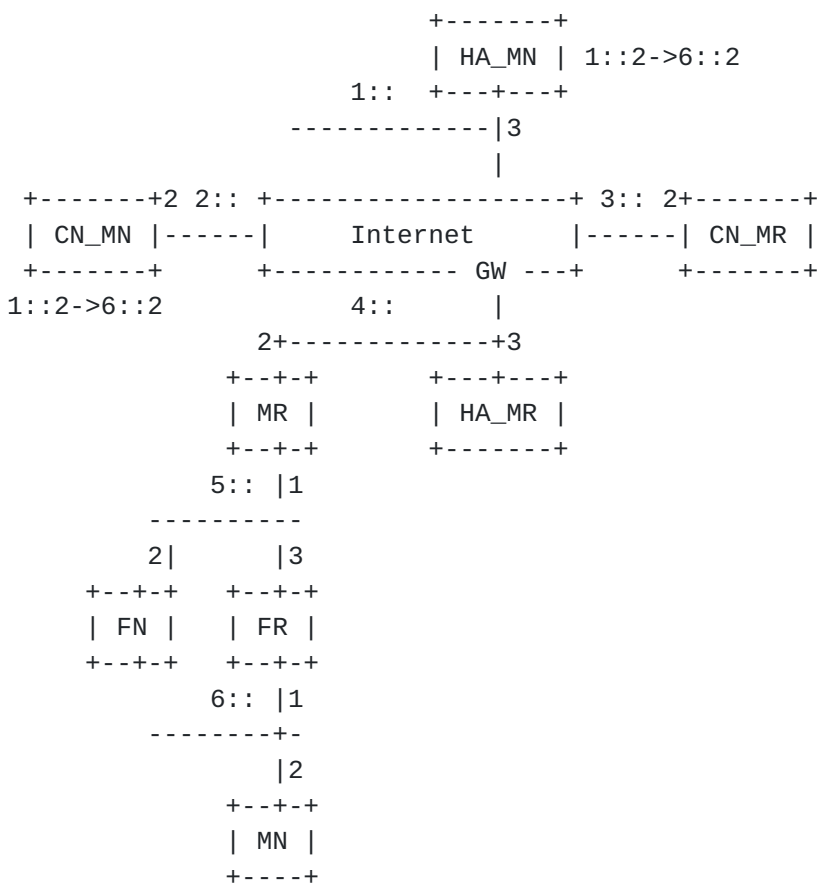


Figure 2: Mobile node not at home.

Both MN and MR hence use unmodified Mobile IPv6, except that there are minor implications to the packet forwarding implementation of MR and HA_MR. Basically, MR and HA_MR have a bidirectional tunnel between them. These rules are simply that

- MR locally knows it is a mobile router and when not at home it installs an encapsulation interface towards its home agent. Through this interface, MR forwards (reverse-tunnels) all packets not originated from MR towards its HA. For packets originated from MR the behavior is as if MR were a normal MN; they get forwarded on the visited link, except if the packets are targeted to the home link; then they get reverse-tunneled to HA. Hence, when arriving at a visited link, MR injects a default route and a network route of its home link, towards the reverse tunnel it creates pointing to its home agent, in addition to a default route to MR's default router on the visited link.

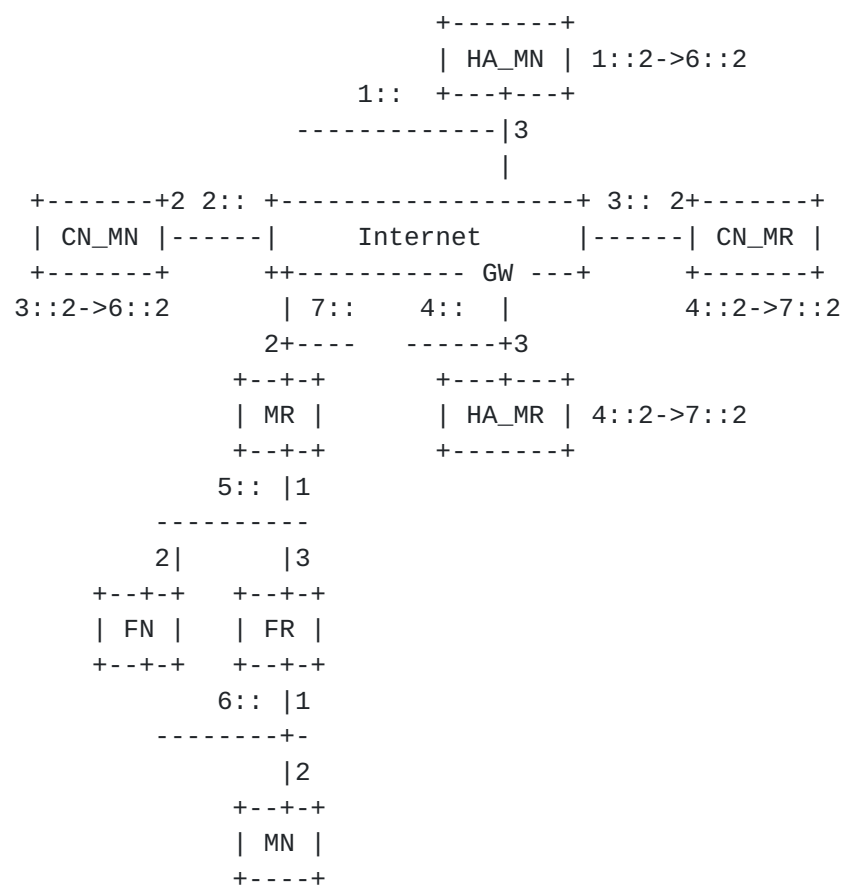


Figure 3: Mobile node and mobile router both on a visited link.

- If MR, HA_MR, and GW were running a dynamic routing protocol, MR redirects control traffic of this protocol towards HA_MR, tunneling these packets through the reverse tunnel pointing to HA_MR. The dynamic routing protocol updates the routing state between GW, HA_MR, and MR, so that next hops between GW and MR now go through intermediate router HA_MR. There MAY be expedition of routing state update, triggered by registration of MR with its home agent.

- If it is not desired that MR runs a dynamic routing protocol, HA_MR MUST inject routing entries for all mobile links behind MR, using MR's home address as the next hop. That is, in our example, HA_MR would inject network routes for 5:: and 6:: with next hop 4::2.

- When HA_MR captures a data packet forwarded towards MR, its forwarding engine then does a route lookup for this packet. If

the returned route has MR's home address as the next hop, it then

does a binding cache lookup for this next hop, and tunnels the packet to the registered care-of-address of MR.

3.1. Application Scenarios

There are two application scenarios for this proposal, one for restricted ``consumer'' mobile router support, and one for ``fully enabled'' mobile router support. In the former, HA_MR injects static routes for a restricted set of links behind each MR, when MR registers with its HA. These are statically configured for each MR in its HA. In this mode, MR cannot run dynamic routing protocol and arbitrarily modify provider's routing cloud state. In the latter scenario, MR is a genuine router running dynamic routing protocol. This provides support e.g. for the case when provider's router moves to a visited link, or there is exterior routing protocol running between MR and its GW, that is, when the mobile router support is ``fully enabled''.

3.2. Mapping to requirements

With the simple scenario presented above, we can support the requirements stated above. The solution

1 supports unmodified Mobile IP or Mobile IPv6 signaling.

2 supports communication to or from nodes on subnetwork(s) connected to and moving with the mobile router.

3 supports both fixed and mobile nodes in the network moving with the mobile router. Since links moving with MR do not change as a result of movement, and their traffic get forwarded via MR's home address, these nodes do not need separate binding updates to any nodes. Binding-triggered route updates, as stated above, keep them connected in a timely manner as a result of standard routing.

4 supports arbitrary nesting level of mobile routers. MR support provides transparency where second-level MR only sets up a tunnel to its HA, this tunnel going inside tunnel set up by first-level MR. This can then applied to subsequent levels, inductively.

5 supports static configuration; that is, the mobile router need not have a dynamic routing protocol running on it. This is provided by the ``consumer'' scenario.

6 supports dynamic configuration; This is provided by the ``fully-enabled'' scenario.

7 allows routing entities to run the dynamic routing protocols with no modifications to their signaling. Routing protocols are not affected, though there can be route injections triggered by binding updates from MR.

8 supports the end-to-end security model for mobility. No intermediate node or router alters mobility state in mobile nodes, routers, or their respective home agents and correspondent nodes, since nodes do not send any additional binding updates on behalf of other nodes.

However, this solution has one drawback: it has less than full route optimization for the packets as they get forwarded through two-way tunneling via MR's home agent. Route optimization is available for MN in that it can let its CNs know its CoA. However, these packets pass through the tunnel between MR and HA_MR. Route optimization is, however, fully available for communication between MR and its CNs. With this restriction, however, we can support arbitrary links behind MRs, nested MNs, MRs, stub- and transit networks.

4. Protocol Messages and Signaling

This Mobile Router solution requires support in Home Agents and Mobile Routers, since both entities must understand that a tunnel is to be established, and packets for the mobile network must be routed through that tunnel. Part of the support includes signaling, which can be implicit (meaning that no changes to Mobile IP are necessary), or explicit (allowing greater communication of status conditions and specificity of prefix mappings).

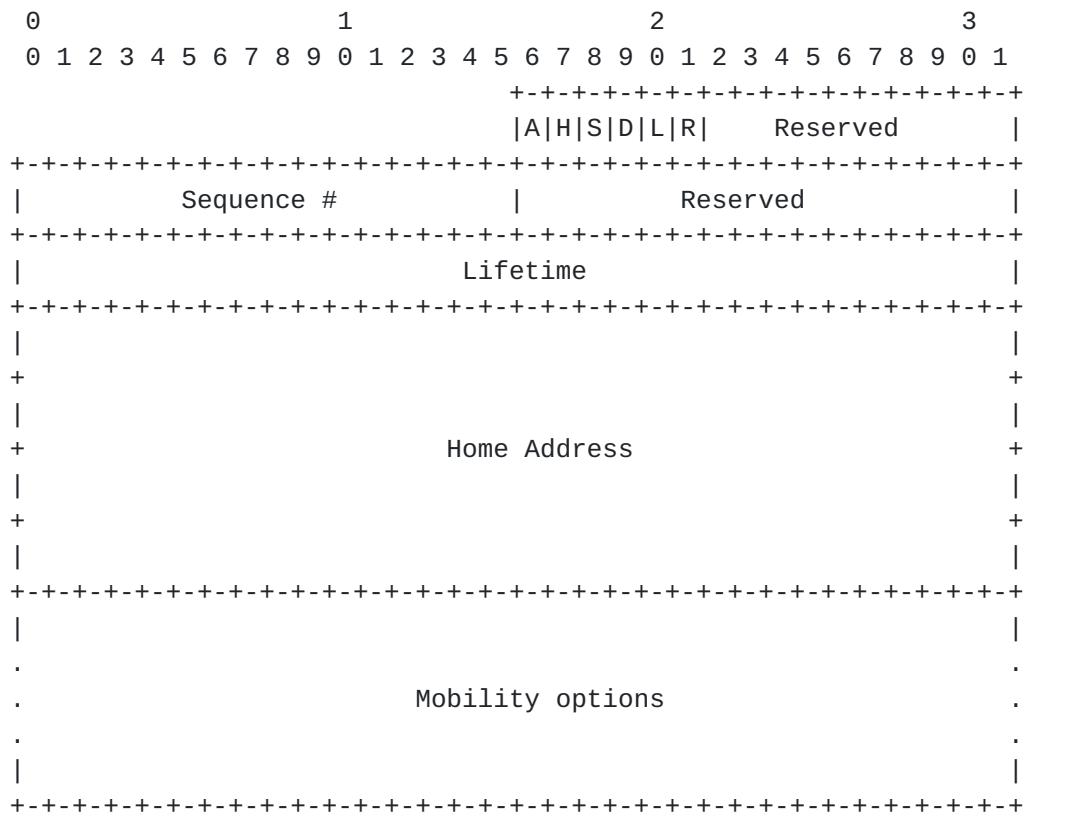
In general, it is preferable to explicitly signal the intention to change location of mobile network route segments. However, it may not always be possible to specify changes to other protocols. Therefore, both modes of signaling will be included. It is possible to support both modes on a home agent and mobile router.

4.1. Explicit Signaling for IPv6 nodes

For IPv6 implementations, the following messages are suggested to be used in signaling the intention to establish a Mobile Tunnel. These messages are new protocol messages that are included in Mobile IPv6 Binding Updates and Binding Acknowledgements.

4.1.1. R-bit

This draft extends Mobile IPv6 to include a Mobile Router bit (R) in the Binding Update message.



R-bit The R-bit is located at the 21st bit of the binding update as depicted. It should be set to 1 only in BUs sent to the HA.

The R-bit indicates that the home agent should create a route to tunnel the mobile network packets to the CoA included in the Binding Update.

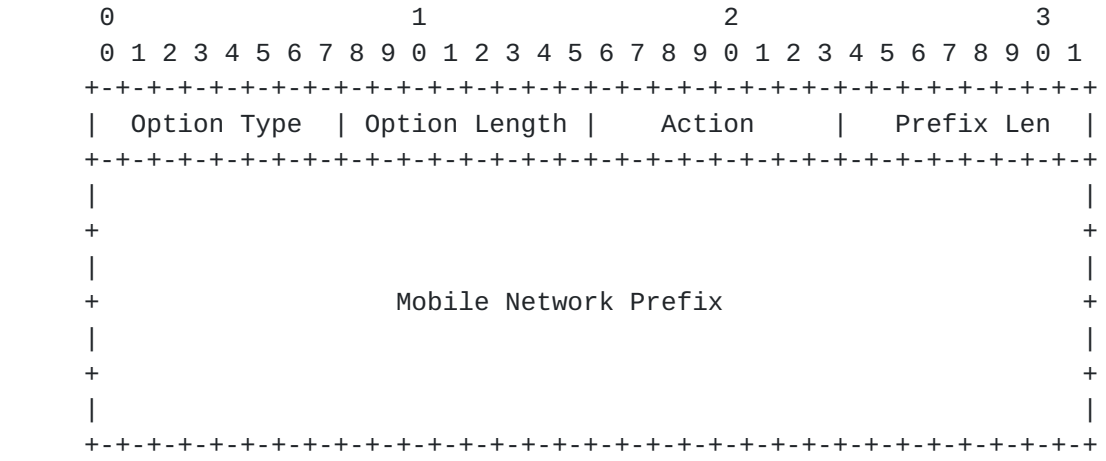
If the R-bit is set to 0 and a previous static route existed, the HA should delete it and cease forwarding packets to the mobile network. The MR can use R=0 to cease routing functionality and, in effect, become a MN.

4.1.2. Mobile Network Option

The Mobile Network Option is a mobility option included in the mobile router's Binding Update message to specify the prefix(es) associated with the MR. The Mobile Network Option is also used as a mobility option in Binding Acknowledgement messages returned by the home agent to

specify the prefix(es) which have routing established. Mobile Network Options are only used in Binding Update messages with R=1 from a mobile router to its home agent, and Binding Acknowledgements from the home agent to the mobile router. These two messages are distinguished by the value of the Action field.

The mobile router may request specific prefixes for which the HA to establish tunnel routes. Alternatively, if the HA is configured with a list of MRs and their mobile network prefixes, the MR may omit the Mobile Network Options and ``all prefixes'' is implied -- the HA will start forwarding packets for all appropriate mobile network prefixes as if Mobile Network Options for all usable prefixes were included in the BU.



Option Type 6 (TBD by IANA)

Option Length 18

Action (in BU) 0 = No Action (remove routes)

1 = Forward (route through tunnel)

2 = Verify (Send ACK if this prefix is mine)

Action (in BA) 100 = OK (Route successfully created)

101 = Mobile Network Option sent from non-MR

102 = Invalid prefix (not part of valid address space)

103 = Prefix not owned by this domain/link

104 = Prefix not owned by MR which sent this MNO

105 = Could not create route / insufficient resources

Prefix Length Length of prefix, in bits (valid range is 1..128)

Mobile Network Prefix Prefix to route. Any bits after <prefixlen> should be set to 0.

Alignment requirement: This message must be aligned to 8n + 4.

Mobile Network Options should be sent by the home agent in response to a binding update which establishes a binding for the first time. It is not necessary to send them when the MR is updating a binding with a new CoA, or when deregistering a binding / removing a route.

4.2. Implicit Signaling

In general, implicit signaling means that signaling is not necessary because of the implication of other factors. When a mobile router sends a binding update to its home agent, the home agent knows which prefixes are assigned to the router, and it sets up the static route and begins forwarding traffic to the mobile network. The mobile router can test that the tunnel is properly established by sending an echo request from its CoA to its address on the mobile network.

With implicit signaling, the home agent keeps a list of mobile routers and their associated prefixes. When a mobile router establishes a binding, the home agent goes through all the same steps as in explicit signaling (static route setup, and rules for packet forwarding), but does not relay any status information to the mobile router. Thus, the effects of routing changes must be learned using existing protocol messages, i.e. ICMP echo request/reply.

5. Alternate Solutions

Another solution [4] was previously proposed, and follows a slightly different set of requirements. It includes support for route optimization, and requires changes to Mobile IP signaling. Providing a generic scalable solution for the address ownership problem may prove to be complicated. A problem is, how can a mobile router or an intermediate agent efficiently authorize multiple fixed and mobile

nodes
to communicate with their peers, when all these may be from multiple different domains, and the mobile router is not and end node for their communication. However, if this issue can be solved, or if a controlled
security environment is feasible, this alternate may provide additional
benefits when compared to this proposal.

Other solutions using inter-domain routing protocols may be possible, depend on the willingness of the routing infrastructure to trust mobile routers.

6. Support for Dynamic Routing Protocol

In the fully enabled mode, the mobile router (MR) runs a dynamic routing protocol with its home agent (assumed to be a router) to exchange up-to-date routing information. The mobile router continues running this intra-domain routing protocol even when it moves away from home and attaches to a visited domain. One of the requirements listed in section 1 is to avoid any modifications to the routing protocol. This can be done by dynamically modifying the list of interfaces on which the routing protocol is active. For example, let us assume a mobile router used interface 'A' when it was connected to its home network and was exchanging routing updates through that interface. When the mobile router moves and attaches to a visited network with the same interface, the routing protocol is turned off for that interface. This is to prevent the mobile router from advertising the routes in its mobile subnet to the visited network. The mobile router then sets up a encapsulating tunnel to its home agent (HA_MR). This encapsulating tunnel is then added as a virtual interface to the list of interfaces on which the routing protocol is active. The mobile router then starts sending routing information through this tunnel to the HA_MR. Most IPv6 intra-domain routing protocols assume link local address to appear as the source address for routing information messages. The encapsulating tunnel takes care of this, by encapsulating the routing messages in a IP header whose source address is the mobile router's CoA and the destination address is HA_MR's address. When HA_MR receives the tunneled routing message, it decapsulates it and processes the inner routing message. The inner routing message appears as if the packet was sent from a node on the link.

The HA_MR also sets up a similar tunnel to the MR and adds the tunnel to the list of interfaces on which the routing protocol is active. HA_MR then tunnels the routing information it has towards the mobile router. The mobile router now learns about HA_MR's routing information.

The tunneled packets are sent through a secured channel between the mobile router and HA_MR. This secured channel is made possible by a static or a pre-negotiated security association between the mobile router and its HA_MR. The tunneled routing messages MUST be protected by Authentication Header [6]. If data confidentiality is required, ESP [7] SHOULD be used.

Certain routing protocols like OSPFv2 [8]or OSPF for IPv6 [2] exchange periodic HELLO messages between adjacent routers. In our case these

periodic messages from the mobile router are sent through this tunnel to its HA_MR.

6.1. Processing the Tunneled Routing Messages

When the HA_MR receives the routing information from the mobile router through the bidirectional tunnel, it adds the corresponding routes to its routing table with the next hop set to the mobile router's address, in case of IPv6 MR's link local address. This next hop address is obtained from the source address of the inner packet. The HA_MR in turn propagates this information when it sends routing updates to other routers on the mobile router's home link.

The HA_MR also needs a binding cache entry for that address which is the next hop address for the MR's subnet. In the case of IPv4 this is created when the MR sends a registration request [?] for its home address when it moves away from its home link. In the case of IPv6 HA_MR needs a binding cache entry to the mobile router's link local address. This is because the next hop address in the routing table entry returns the mobile router's link local address. And to forward packets to the mobile router's link local address, a binding cache entry is needed. A binding cache entry is not created unless HA_MR receives a binding update from the mobile router. Therefore the mobile router MUST send a binding update for its link local address in addition to its home address. This is optional in the current Mobile IPv6 [5] specification.

6.2. Forwarding Packets to MR's subnet

Since HA_MR advertised routing reachability information for MR's subnet, it receives the packets meant for the nodes in the MR's subnet. Route lookup on HA_MR returns the address of the mobile router as the next hop address. By making use of the binding cache entry for the mobile router's address (link local address in case of IPv6) and the bi-directional tunnel with the mobile router, HA_MR starts forwarding packets throught the tunnel to the mobile router. The mobile router in turn decapsulates the packet and fowards it on its subnet.

7. Security Considerations

The mechanism described in this draft requires routing messages exchanged between a mobile router and its home agent to be secured when the mobile router is not on its home link. This is done by creaating a static security association between the mobile router and its home agent. This document does not require changes to either Mobile IP or any routing protocol. Therefore, it does not introduce any additional security requirements.

8. IANA Considerations

The following protocol numbers may require allocation from IANA:

- The Mobile Network Option is a mobility option in the Mobile IPv6 mobility header. The Option Type should be allocated within this namespace.

9. Intellectual Property Right Considerations

On IPR related issues, Nokia refers to its statement on patent licensing. Please see http://www.ietf.org/ietf/IPR/NOKIA.

10. Acknowledgements

The authors would like to thank the following individuals who have made suggestions to improve the text of this draft which were incorporated:

Marco Molteni (Cisco) Tapio Suihko (Technical Research Centre of Finland)

References

[1] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. Request for Comments (Best Current Practice) 2119, Internet Engineering Task Force, March 1997.

[2] R. Coltun, D. Ferguson, and J. Moy. OSPF for IPv6. Request for comments (proposed standard), Internet Engineering Task Force, December 1999.

[3] S. Deering and R. Hinden. Internet Protocol, Version 6 (ipv6) Specification. Request for Comments (Draft Standard) 2460, Internet Engineering Task Force, December 1998.

[4] et al. Ernst, T. Mobile networks support in mobile ipv6. Internet Draft, Internet Engineering Task Force, June 2001.

[5] D. Johnson and C. Perkins. Mobility support in IPv6 (work in progress). Internet Draft, Internet Engineering Task Force, November 1998.

[6] S. Kent and R. Atkinson. IP Authentication Header. Request for Comments (Proposed Standard) 2402, Internet Engineering Task Force, November 1998.

[7] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). Request for Comments (Proposed Standard) 2406, Internet Engineering Task Force, November 1998.

[8] J. Moy. OSPF Version 2. Request for Comments (Standard) 2328, Internet Engineering Task Force, April 1998.

[9] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, October 1996.

Authors' Addresses

T. J. Kniveton
Communication Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1 650 625-2025
EMail: timothy.kniveton@nokia.com
Fax: +1 650 625-2502

Vijay Devarapalli
Communication Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1 650 625-2320
EMail: vijayd@iprg.nokia.com
Fax: +1 650 625-2502

Jari T. Malinen
Communication Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1 650 625-2355
EMail: jmalinen@iprg.nokia.com
Fax: +1 650 625-2502

Charles Perkins
Communication Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1 650 625-2986
EMail: charliep@iprg.nokia.com
Fax: +1 650 625-2502

Full Copyright Statement

Acknowledgement

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