Network Working Group
Internet Draft
Document: draft-mohan-nflm-proto-00.txt
Expires: April 2006

M.Parthasarathy
Basavaraj Patil
Rajeev Koodli
Nokia

October 2005

Network-based Fast Handovers for Local Mobility (NFLM)

Status of this Memo

Copyright Notice

Abstract

Local Mobility is IP mobility over a restricted geographical and administrative domain. This document describes a network based localized mobility management protocol which does not require host involvement while moving within such a local mobility domain.

Network-based Fast Handovers for local mobility October 2005

Table of Contents

1.0 Introduction

Localized mobility management has been addressed by various protocols like HMIPv6 [3]. These protocols involve the host to manage the mobility on their own when moving within the local domain. This document describes a protocol where the mobility is managed by the network without the involvement of the host. The protocol is based on FMIPv6 [2] message exchanges. In FMIPv6 [2], the handoff is either

initiated by the network or the mobile node. In either case, the host sends a fast binding update (FBU) to setup a tunnel with the access router on the previous link. By establishing such a tunnel, the mobile node ensures that the packets can keep flowing as it updates the home agent and the correspondent node using the Mobile IPv6 [10] signaling over the Internet, including the Return Routability

procedure. The protocol described in this document does not involve the host to send the FBU; instead the Access router sends the FBU to a Mobility Anchor Point (MAP) on behalf of the mobile node. This ensures that the packets can continue to flow from the MAP towards the new access router while the mobile node does not even know that it has changed access routers. We refer to this protocol as Network-based Fast Handovers for Local Mobility (NFLM).

This document is organized as follows. First, it discusses the requirements of the localized mobility management protocol(LMM). Next, it discusses the IP address configuration mechanism followed by the protocol description. All the messages defined in this document are taken from [2]. There are no new messages defined here. There are a few extra options needed by NFLM which are defined in Section 8.0.

2.0 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 [1].

The following terminology and abbreviations are taken from [2] and modified for NFLM.

Mobile Node (MN)

A Mobile IPv6 host.

Access Point (AP)

A Layer 2 device connected to an IP subnet that offers wireless connectivity to an MN. An Access Point Identifier (AP-ID) refers to the AP's L2 address. Sometimes, AP-ID is also referred to as a Base Station Subsystem ID (BSSID).

Access Router (AR)

The MN's default router.

Previous Access Router (PAR)

The MN's default router prior to its handover.

New Access Router (NAR)

The MN's default router subsequent to its handover.

Previous CoA (PCoA)

The MN's Care of Address valid on PAR's subnet.

Handover

The process by which a mobile node moves from one point of attachment to another point of attachment, resulting in the MN terminating existing connectivity and establishing new IP connectivity.

Fast Binding Update (FBU)

A message from the NAR instructing the MAP to redirect traffic (toward NAR).

Fast Binding Acknowledgment (FBack)

A message from the MAP in response to an FBU.

Handover Initiate (HI)

A message from the PAR to the NAR regarding an MN's handover.

Handover Acknowledge (HAck)

A message from the NAR to the PAR as a response to HI.

MN identifier

An identifier to uniquely identify a mobile node in the local domain. This can be a link-layer address or some other identifier depending on the access technology.

MAP

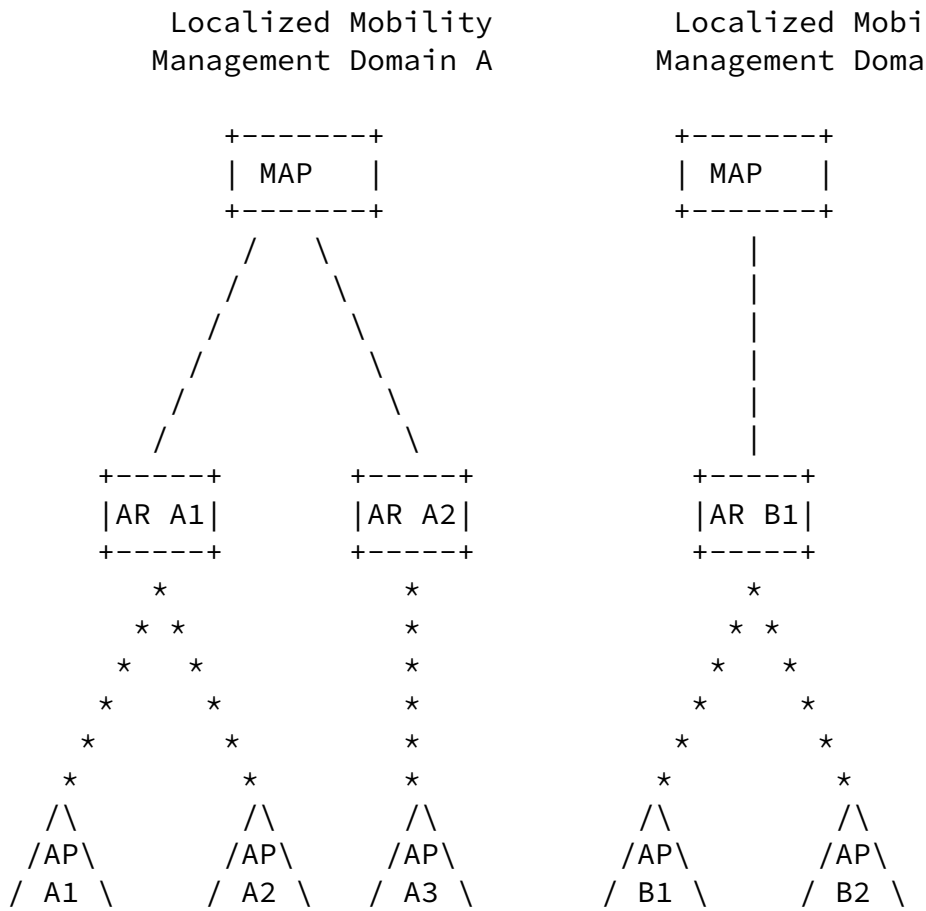
Mobility Anchor Point. The router that maintains reachability for hosts in the local domain using host routes.

3.0 Requirements for LMM

The requirements for a localized mobility management protocol can be considered as follows.

1) The protocol should address mobility within the local domain as shown in Figure 1 without the involvement of the host. To be more specific, the protocol is used when the MN moves between AP 2 and AP 3.

2) The host should be able to maintain the same IP address when moving within the local mobility domain.



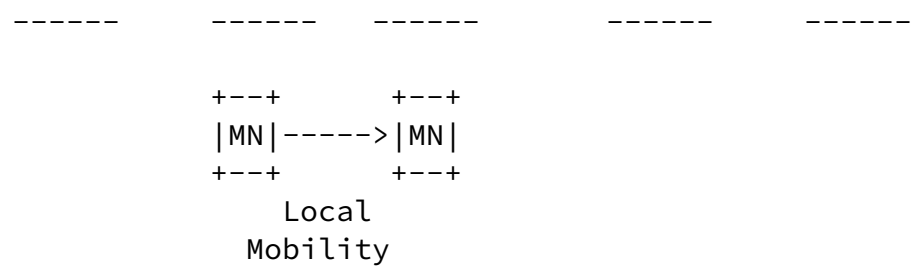


Figure 1) Localized Mobility Management Domain

3) The host should not have any involvement in its mobility management (except for advertising its presence on the new link), when moving within the local mobility domain.

4) Access Routers should be able to discover MAPs and prefixes dynamically without the need for manual configuration.

4.0 IP Address Configuration

The mobile node configures the IP address when it enters the local domain for the first time. The mobile node configures the IP address as it would do when it moves to a new IP link i.e., there is nothing special required from the mobile node. Once it has configured the IP

address as described below, the MN does not have to configure a new IP address as long as it stays within the local domain. This implies that when the mobile node connects to a new access router, it should not determine that it has moved to a new IP link. Otherwise, it will configure a new IP address which should be avoided. This influences the address configuration method. Following sections describe the address configuration options.

4.1 DHCPv6

DHCPv6 [4] may be used for address configuration in the local domain. This can be enabled in different ways.

. As specified in stateless autoconfiguration [6], the host attempts to use stateful autoconfiguration if no routers are present on the link. This can be achieved by turning of the router advertisements on the Access Routers.

. Routers can be configured to send router advertisements without including any prefixes but setting the Managed address configuration flag (M bit) in the router advertisement. This will trigger the host to invoke DHCPv6 for address configuration.

Since mobile hosts are expected to send router solicitation to detect whether they moved links or not, the latter option SHOULD be used.

As specified in [4], the client MUST include the client identifier option in the DHCP request message. Any valid DHCP unique identifier specified in [4] can be used. When the client may have moved to a new link (e.g. switching wireless access point), the client should use the CONFIRM message along with the client Identifier option that was sent with the DHCP request message. The client performs DAD and declines the address if the address is used already on the link.

The DHCP server SHOULD be located centrally so that it is able to assign the same address to the client as long as it remains in the local domain. The DHCP relay agent will be present on the Access routers, forwarding the DHCP messages towards the DHCP server. When the server receives the DHCP message from the relay agent, either the link-address or the interface ID option will be present.

The link-address field is assigned from the interface on which the message is received from the client. If there is more than one prefix on the interface from which the packet was received, the DHCP relay agent may not be able to pick the right prefix to insert in the link-address field. The link-address field should match the prefix of the client's address in the CONFIRM request. As the server uses the link-address field to select an appropriate address for the client,

inserting a wrong link-address value can lead the server to reject the request and return NotOnLink status in its reply. Hence, this option should not be used by the relay agent unless it can insert the prefix matching the address in the CONFIRM request.

The DHCPv6 relay agent may use the Interface-ID field to influence the address assignment policy on the server. As this is considered to be opaque, the agent may copy the prefix of the requested address in the CONFIRM request to the Interface-ID. Then the server may be configured to use the Interface-ID for policy assignment i.e the interface-ID SHOULD match the prefix of the requested address.

4.2 Stateless Address Autoconfiguration

The client may also autoconfigure the address using the prefix information in the Router advertisements (RA) sent by the Access Router. As the client needs to keep the same address across all the links that moves in the NELMM domain, all the access routers in the local mobility domain SHOULD advertise the same set of client prefixes so that the clients believe that they have not moved at layer 3.

The router advertisement normally contains prefixes that are valid for the link. The prefix information option contained in the RA has two bits for each prefix. The A bit indicates whether the prefix can be used to auto-configure an address. This bit MUST be set on at least one prefix so that the mobile nodes can autoconfigure an address. There is another bit in the RA namely the L bit which is used to determine the on-link status. As the mobile nodes roam around in the local domain keeping the same address, it is not possible to use the prefix information to determine the current point of attachment of a given node. Both the Access router and the MAP use the host routes to learn about the current Point of Attachment of the clients. Hence, the on-link flag MUST NOT be set on any prefixes.

When the client configures the address for the first time, it would send a router solicitation with unspecified source address. The router advertisement MUST contain the same set of prefixes that will be advertised by all Access routers in the local mobility domain. The mobile node follows the procedure described in [5] and [6] for configuring the address. When the MN believes that it may have moved to a new link, it should send a router solicitation with the address configured earlier. This is used by the new access router to set up any tunnel if needed.

4.3 Duplicate Address Detection

Duplicate Address Detection MUST be performed on all unicast addresses prior to assigning them to an interface, regardless of

whether they are obtained through stateless address autoconfiguration or DHCPv6 [6]. This procedure verifies that another node on the link is not using the same address. But the LMM requirements require that the node maintains the same address in the local domain. This implies that one has to make sure that no two nodes on any link has the same address.

NFLM achieves this by MAP verifying that there is only one binding for a given MN address. But as the node moves to a different link, the binding needs to be updated. If the MAP would check whether a binding exists already, the update would fail as the binding was created when the node was on a previous link. Hence, the MAP uses a unique client identifier to verify that it is the same client that moved to a new link. The security issues related to this are discussed later.

5.0 Local Domain Configuration

The local domain configuration consists of two parts.

1. Discovery of MAP by Access Routers.

2. Discovery of the prefixes that needs to be advertised to the clients by Access Routers.

RFC 2782 [8] defines the service resource record (SRV RR), that allows a client to locate the address of a particular service/protocol. This can be used by the Access Routers to discover MAP in the local domain. A new service name ("netlmm-aflm") for NFLM needs to be defined and the protocol name is 'ipv6'.

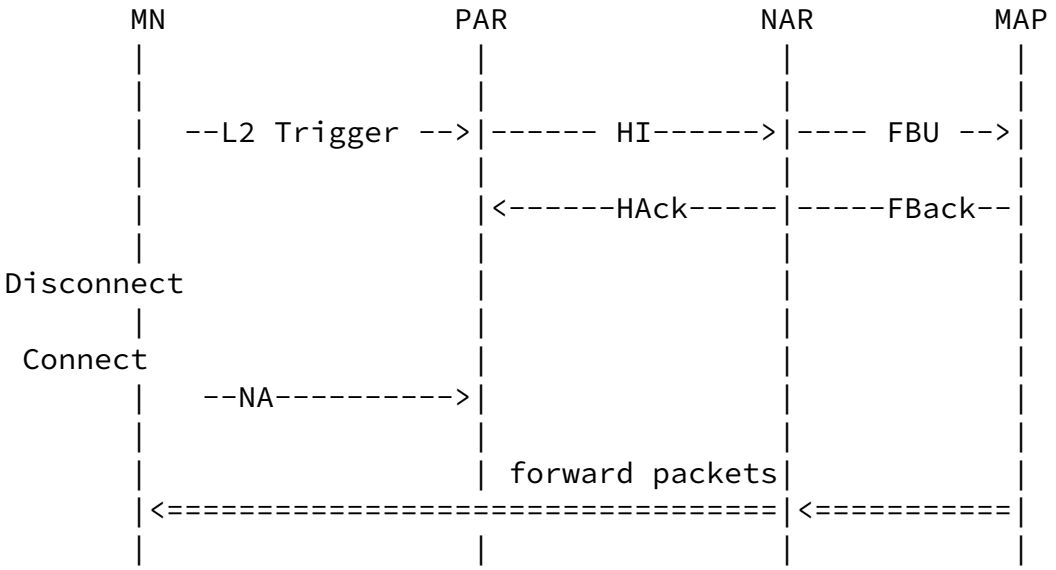
All the Access routers advertise prefixes for clients to configure an address that is valid in the local domain. These prefixes can be learnt from the MAP using Mobile Prefix discovery as defined in RFC 3775 [8].

6.0 Protocol Details

The NFLM protocol begins when the mobile node is handing over to a new Access Router. In some wireless technologies, the handover control may reside in the network (Access Router). NFLM supports both Predictive handoff and Reactive handoff. MN does not do anything special in the NFLM protocol. It does what a node would do when it receives a L2 trigger. The next two sections discuss the Predictive and reactive handoff.

6.1 Predictive handoff

The Predictive handoff happens when the MN is already connected to the local domain and the Access Router receives a L2 trigger informing it of a certain MN's upcoming movement to a new Access Router. The trigger provides enough information from which the IP address of the new access router (NAR) and IP address of the MN can be obtained.



When the PAR receives the L2 trigger, PAR sends a Handoff Initiate message to the NAR. The Handoff Initiate message contains the MN's IP address (PCoA) and MN's identifier. When NAR receives the HI message, it SHOULD check whether a tunnel to the MAP exists for PCoA or not. If the tunnel already exists, it could mean one of two things. The HI message from PAR is spurious and NAR already had setup a tunnel with MAP when it saw the L2 trigger earlier. It could also mean that there is already a node with the same PCoA address on the link. The NAR could verify the MN's identifier to see whether it is the same node or a different node. If it is the same node, then it continues processing the HI message. Otherwise, it returns failure indicating Duplicate Address. When PAR receives such a message, it SHOULD fail the handover process if possible. If the handover has already happened, then the MN would figure out that it has a duplicate address when it does DAD on the new link.

If NAR successfully processes the HI message, it sends a Fast Binding Update message to the MAP to redirect the tunnel from the old Access Router to itself. The FBU message contains PCoA as the home address, NAR's address as the Care-of address and an option to carry the MN's unique identifier. When MAP receives the FBU message, it does the following checks.

. It checks to see if there is a binding for the PCoA. If it does not exist, it creates a new binding entry.

. If a binding already exists, it checks to see if the MN's identifier in the FBU matches with the identifier in the binding. If it does not match, it fails the request. If it matches, then it updates the binding information.

Once the MAP successfully processes the FBU, it sets (or updates) the tunnel to NAR for sending and receiving packets from PCoA. Normally a host route will be added for PCoA pointing to the tunnel. When the NAR receives a successful FBack message, it checks to see if the FBU was processed successfully. If there is a failure, the same is indicated in the HAck message. If FBack indicates success, it creates a tunnel to the MAP and sets up the forwarding in such a way that packets with source address as PCoA gets forwarded into the tunnel. It also maintains state (similar to the binding state) which can be used to verify duplicates or spurious indications from PAR or MN. It also creates a host route for forwarding packets to the MN. NAR sends a HAck message back to the PAR indicating that it successfully processed the Handoff procedure. When PAR receives the HAck message, it removes the PAR-MAP tunnel and host routes for PCoA.

When the MN connects to the new link, it sends out a Neighbor advertisement. The NAR can use this indication to start forwarding packets to the PCoA. It will also forward the buffered packets (if any) when the NA indication is received.

6.2 Reactive handoff

This handoff procedure happens when the MN connects to the local domain for the first time or it connects to a new Access Router as a result of L2 change. This is explained separately depending on how the address is configured.

6.2.1 Autoconfiguration

When the MN connects to the local domain for the first time, following things could happen.

. MN sends a router solicitation with unspecified address

. MN sends a router solicitation with an address configured from a previous network probing to see if it is still connected to the

same network.

In either case, NAR just sends a Router advertisement.

If the MN receives the RA, it assigns the IP address if there any valid prefixes present and then it SHOULD send a unsolicited NA to indicate its presence.

When the NAR receives the unsolicited NA, it sends the FBU message to the MAP and the rest of the processing is the same as the previous section. The unsolicited NA should contain the MN's identifier in the SLLA option [5].

If there is a failure in the FBU processing, the MAP and NAR does not forward packets to the MN. The NAR SHOULD send an RA with NAACK indicating failure [2].

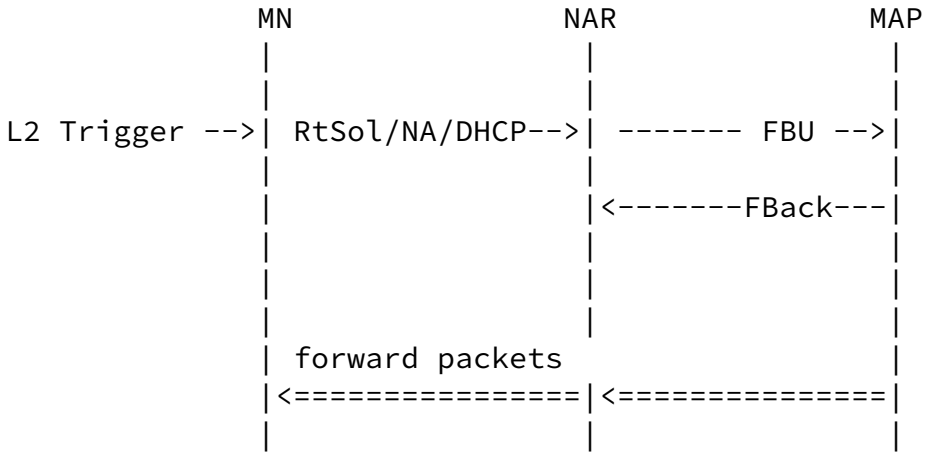
If the MN has already configured an address in the local domain and just handing over to a new Access Router, it would send a router solicitation and/or a neighbor solicitation to verify whether it is still connected to the same access router or not. If the old Access Router receives this message, it does not do any NFLM specific operation. If it handed off to a new Access Router, the NS/RS message is an indication that a new MN is possibly trying to get access. The NAR checks to see if a tunnel/binding already exists for the PCoA. If it exists, it checks to see if the MN's identifier matches with the binding state. If there is a mismatch, router advertisement is sent with NAACK option indicating failure. If it is successful, then the NAR sends FBU to the MAP. The MAP also SHOULD add the IP address of the PAR in the FBack option. This enables the NAR to send an unsolicited HAck to PAR for cleaning up the host routes. Rest of the processing by MAP and NAR is similar to the previous section.

6.2.2 DHCP Configuration

If the client is booting up for the first time, then it would send a REQUEST [4] message to acquire the IP address. When the server sends a successful DHCPv6 reply message to the client, the client assigns the address normally and sends an unsolicited NA. This can be used as an indication to setup the tunnel with the MAP as described in the previous section.

If the client is handing off to a new Access Router, it SHOULD send a CONFIRM [4] message. A successful reply to the CONFIRM can be taken as an indication to send the FBU to the MAP.

DISCUSS: The DHCP server does not seem to check the client identifier option in the CONFIRM request to match with the client identifier option that was sent earlier during the REQUEST.



7.0 Packet Forwarding in local domain

The communication between a mobile node in the local domain and a node in the external domain happens through MAP. MAP intercepts packets from the external network and forwards it to the Access Router (via the tunnel) to where the node is attached currently. MAP always knows the correct point of attachment of the mobile node.

The communication between two nodes in the local domain can happen through multiple ways. As the on-link (L bit) prefix is not set in the RA, all packets from the MN are sent to the Access Router. If the attached node is connected to the same Access Router, then the router may forward the packets directly to the attached node without going through MAP. It may also send a redirect to the mobile node so that it can directly reach the peer node. If the peer node is not connected to the same Access Router, then it forwards to the MAP which in turn forwards to the right Access Router where the node is located.

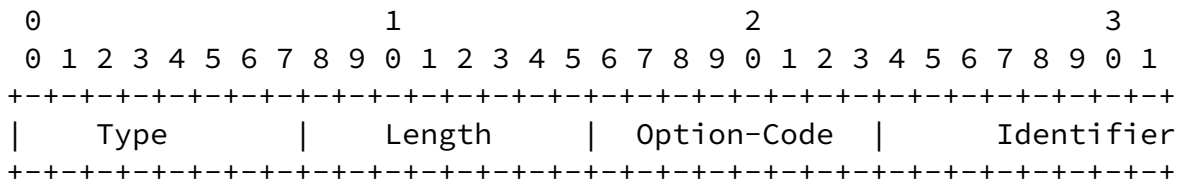
8.0 Message Formats

The messages defined in [2] will be used by NFLM. Instead of Link-layer option, this document defines a new MN identifier option which will be used by the network to identify a mobile node.

The messages used by NFLM are Handover Initiate message, Handover Acknowledgement message, Fast Binding Update and Fast Binding Acknowledgement. Following sections describe the differences between NFLM and FMIPv6 [2].

8.1 MN identifier option

This is a new option defined by NFLM. Though this has resemblance to the Link Layer address option, this subsumes the functionality of the link-layer address option.



Type TBD

Length

The size of this option in 8 octets including Type, Option-code, and Length fields.

Option-code TBD

Identifier

A unique identifier for the MN in the local domain. It MAY be a link-layer address of the MN or any other unique identifier that can be used to uniquely identify a given node in the local domain.

Appropriate padding MUST be used to ensure that the option size is a multiple of 8 octets.

8.2 Handover Initiate message

The Handover Initiate message is an ICMPv6 message sent by an Access Router (PAR) to another Access Router (AR) to initiate the process of a MN's handover.

The message format is identical to [2] except for the options. Following options MUST be included.

MN-identifier option

The unique value to identify the MN in the local network

Previous care-of Address

The IP address used by the MN while attached to the router where this message is originating. It is the same as the MN's address that is configured in the local domain.

8.3 Handover Acknowledgement message

The Handover Acknowledgement message is an ICMPv6 message sent by an Access Router (NAR) to another Access Router (PAR) to acknowledge the MN's handover. NAR also sends an unsolicited HAck to flush the host routes in PAR for the reactive handoff case.

MN-identifier option

This SHOULD be included to help PAR locate any state if needed.

A new code value should be defined to indicate that PCoA is not valid.

8.4 Fast Binding Update

The Fast Binding Update message is sent by the Access router to the Mobility anchor point to update the current binding of the MN. The

Home Address is PCoA and care-of address is the IP address of the router originating this message (NAR).

The MN-identifier option SHOULD also be included in the message.

8.5 Fast Binding Acknowledgement

The Fast Binding Acknowledgement message is sent by the MAP to the Access Router to acknowledge the Binding Update.

The MN-identifier option MAY be included in the message. The Alt-coa option defined in [2] is not needed.

The MAP SHOULD also include the IP address of the PAR in its response. This is used by NAR to send an unsolicited message to PAR to clean up the host routes.

9.0 IANA Considerations

This document specifies the following messages which require new Type assignment from IANA.

1. Fast Binding Update: Section 8.4
2. Fast Binding Acknowledgment: Section 8.5
3. Handover Initiate: Section 8.2
4. Handover Acknowledgment: Section 8.3

The Handover Acknowledgment message needs an additional Type assignment to support unsolicited transmission mode.

This document specifies the following new option which requires Type assignment from IANA.

1. Mobile Node Identifier Option: Section 8.1

This document specifies a new code value for the HAck message.

1. PCoA Not valid, Duplicate Address

The future versions of this document may specify additional IANA assignments.

10.0 Security considerations

As the MAP and AR is under the same trusted domain, the communication between them (MAP-AR and AR-AR) can be secured using IPsec [10].

Fast Binding Updates are sent by the Access Router to redirect traffic destined to a particular address (PCoA) to itself. Fast Binding Updates are triggered by unsolicited NA, Router Solicitation, L2 trigger, DHCPv6 reply and DHCPv6 confirm messages. An attacker may be able to send false messages to trigger the FBU and hence redirecting the traffic to either itself or the victim. The victim will be located on the link because the care-of address would be NAR.

Access Router check to see if a binding already exists by checking both the IP address and the MN-identifier. This prevents an attacker on the link to redirect traffic to itself. But the attacker can move to a new link and cause the same attack by spoofing the MN-identifier and the IP address. This is limited in the Predictive handoff case because only L2 triggers can cause the access router to send the FBU. If L2 triggers cannot be spoofed, such attacks can be avoided.

If neighbor discovery messages are secured using SEND [7], then the attacker cannot spoof IP addresses within the local domain. A legitimate owner of the IP address can still spoof MAC address as it is not protected by SEND. But this attack is not specific to NFLM.

Even if DHCP messages are secured, the attacker can still trigger false FBU by sending a CONFIRM message. SEND does not apply to addresses configured using DHCP.

Attacker can pre-create a binding if it knows the IP address that will be assigned to the MN. If SEND is used, then the attacker cannot spoof the IP address.

11.0 Normative References

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

[2] R. Koodli et al., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005

12.0 Informative References

[3] H. Soliman et al., "Hierarchical Mobile IPv6 Mobility Management", RFC 4140, August 2005

[4] R. Droms et. al, "Dynamic Host Configuration Protocol for IPv6", RFC 3315, July 2003

[5] T. Narten et al., "Neighbor Discovery for IP version 6 (IPv6)", draft-ietf-ipv6-2461bis-04.txt, work in progress

[6] S. Thomson et. al, "IPv6 Stateless Address Autoconfiguration", draft-ietf-ipv6-rfc2462bis-08.txt, work in progress

[7] J. Arkko et al., "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005

[8] A. Gulbrandsen et. al, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000

[9] D. Johnson et. al, "Mobility support in IPv6", RFC 3775, June 2004

[10] S. Kent et. al, "Security Architecture for the Internet Protocol", draft-ipsec-rfc2401bis-06.txt, work in progress

13.0 Acknowledgments

The authors would like to thank Charles Perkins for providing a very good feedback on this document.

14.0 Author's Addresses

Mohan Parthasarathy
NOKIA
313 Fairchild Drive
Mountain View CA-94043

Email: mohan.parthasarathy@nokia.com

Rajeev Koodli
NOKIA
313 Fairchild Drive
Mountain View CA-94043

Email: Rajeev.Koodli@nokia.com

Basavaraj Patil
Nokia
6000 Connection drive,
Irving, TX 75039

Email: basavaraj.patil@nokia.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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