MIP6 Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2007

R. Wakikawa (Editor)
Keio University
March 5, 2007

Home Agent Reliability Protocol
draft-ietf-mip6-hareliability-01.txt

Status of this Memo

Copyright Notice

Abstract

The home agent can be a single point of failure when Mobile IPv6 is used in a system. It is critical to provide home agent reliability in the event of a home agent crashing or becoming unavailable. This would allow another home agent to take over and continue providing service to the mobile nodes. This document describes the problem scope briefly and provides a mechanism of home agent failure detection, home agent state transfer, and home agent switching for home agent redundancy and reliability.

Table of Contents

1. Introduction

In Mobile IPv6 [1] and NEMO Basic Support[2], mobile nodes may use a bi-directional tunnel with their home agents for all traffic with correspondent nodes. A home agent on the home link maintains a binding cache entry for each mobile node and uses the binding cache entry to route any traffic meant for the mobile node or the mobile network. If the mobile node is not on the home link and does not have a binding cache entry at the home agent, it is neither reachable at its home address nor able to setup new sessions with its home address. If a home agent loses the binding cache state, due to failure or some other reason, it results in a loss of service for the mobile nodes.

It is beneficial to provide high availability and redundancy for a home agent so that mobile nodes can avail of uninterrupted service even when one home agent crashes or loses state.

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 [3].

In this document, the term mobile node refers to both a mobile node [1] and a mobile router [2].

Some of the mobility related terms used in this document are defined in [1] and [10]. In addition or in replacement of these, the following terms are defined or redefined:

Active Home Agent

A home agent that is currently serving the mobile nodes.

Standby Home Agent

A home agent which will serve the mobile nodes when the active home agent fails.

Failed Home Agent

A home agent that is not available due to hardware or software failure, system maintenance, etc.

Redundant Home Agent Set

A group of active and standby home agent(s). The Group Identifier is used to identify a redundant home agent set. The Group ID is exchanged by Hello messages.

Binding Synchronization

Synchronization of binding cache entries within the redundant home agent set.

Home Agent Preference

This preference value is defined for Duplicate Home Agent Address Discovery (DHAAD) in RFC3775. This protocol uses this preference value for home agent selection when an active home agent has failed. However, an operator can also define an independent value used only for the home agent reliability protocol if the operator wants to have different preference values for DHAAD and the home agent reliability protocol. A home agent SHOULD NOT use the same preference value as other home agents for this protocol.

3. Problem Statement and Requirements

In Mobile IPv6 [1], a mobile node registers and establishes a binding with only one home agent. Thus the home agent represents the possibility of a single point of failure for Mobile IPv6. A home agent may be responsible for multiple mobile nodes on the home link. The failure of the home agent may then result in the loss of connectivity for numerous mobile nodes located throughout the Internet. To overcome this problem, Mobile IPv6 allows deployment of multiple home agents on the home link so that upon the failure of a home agent, a mobile node can re-establish its connection through a new home agent. However, the base Mobile IPv6 specification does not address home agent failover and dynamic transfer of service from one home agent to another. This transfer of service from the failed home agent to a new working home agent requires coordination or pre-configuration among the home agents regarding security associations, transfer of mobile node bindings, and other service information for reliable Mobile IPv6 service in a deployment scenario.

For the home agent reliability solution, we define the following requirements:

Reliable Home agent service

Multiple home agents are available for a home prefix and one of them actively serves the mobile nodes. A standby home agent takes over when the active home agent becomes unavailable. The transfer of the MN-HA association should be transparent to applications and should not take longer than the care-of-addresses update procedure described in Mobile IPv6 [1].

Availability of a redundant home agent set

Availability of an active home agent address and a standby home agent address at the bootstrapping period for the mobile node is assumed.

State Synchronization

The information for mobile nodes must be able to be synchronized between an active home agent and standby home agents. This includes the Binding Cache, AAA information, other Mobile IPv6 and NEMO related information.

Consideration of IPsec/IKE transfer

An active home agent maintains several IPsec and IKE states for mobile nodes. These states are synchronized within the redundant home agent set. The details are described in Section 9.

Secured Message Exchanges

The messages used between the home agents to transfer binding cache information MAY be authenticated and encrypted.

Failure Detection

Redundant home agents must actively check for possible failure of an active home agent. If a home agent supports an existing failure detection mechanism such as VRRP[4] or HSRP[5], it can re-use that mechanism to detect the home agent failure. On the other hand, periodic Hello messages are introduced to detect active home agent's service availability in this document.

Failure Notification

If necessary, a mobile node is notified about the active home agent failure by the standby home agent.

4. Protocol Design

Mobile IPv6 depends on IPsec and IKE for home binding registration as described in [6]. A mobile node must encrypt a Binding Update sent to a home agent. In addition, the mobile node exchanges HoTI and HoT messages through the home agent by using IPsec tunnel mode. Therefore, before home agent failure, these IPsec states should be synchronized among home agents of a redundant home agent set. A mobile node may also encrypt particular data traffic sent to nodes in the Internet. IPsec information required by Mobile IPv6 is listed below.

- o Security Policy Database (SPD) and Selector Information
- o Security Association (SA) for Binding Registration (SA1 and SA2)
- o SA for HoTI/HoT Exchange (SA3 and SA4)
- o SA for Mobile Prefix Discovery (SA5 and SA6)
- o SA for data packets if any (SA7 and SA8)

There are various ways this can be achieved. One is to setup multiple IPsec security associations between the mobile node and the home agent sets. Another is to have the home agents periodically check-point IPsec session state, including the per packet sequence numbers, for the mobile node. Thus, we define two possible home agent redundancy modes as follows:

Home Agent Virtual Switch

Each mobile node negotiates just one SA with an active home agent in a redundant home agent set. The IPsec state will be shared within the redundant home agent set in the background. The active and the redundant home agents are addressed by the same home agent address, although only tje active home agent is accessible by the home agent address all of the time. IPsec/IKE states must be synchronized between the active and standby home agents. The mechanism used to synchronize IPsec state is considered out of scope for this document. In case there is a failure of the active home agent, the standby home agent takes over without the mobile node being aware of the change in the home agent.

In a redundant home agent set, a single home agent address is used by the active home agent. Thus, all the mobile nodes served by a redundant home agent set MUST associate with the same home agent (the active home agent) all the time.

Home Agent Hard Switch

The home agents are addressed by different IP addresses and the mobile node is aware of the change of home agent. A Mobile node and all home agents in a redundant home agent set negotiate independent IPsec SAs. This mode is especially useful when the IPsec/IKE states cannot be synchronized. However, the home agent change is not transparent to the mobile node. When an active home agent fails, a mobile node will receive a notification (a Home Agent Switch message [11]) from a standby home agent, and send a Binding Update to the standby home agent. In order to exchange the Home Agent Switch message securely between the standby home agent and a mobile node, the mobile node needs to establish an IPsec SA with both the active and the standby home agents in the redundant home agent set beforehand.

Since each home agent has a different address, an active home agent can be defined for each mobile node. When a mobile node boots, it will discover home agents and create IPsec SAs with them. It will then decide which one of the home agents is its active home agent. For example, when two home agents serve a home network, half of the mobile nodes might register with one home agent and the rest of mobile nodes with another home agent. When one of the home agents fails, a standby home agent, whose preference value is next highest than the failed home agent, can trigger a home agent switch by sending a Home Agent Switch message to the mobile nodes that were registered with the failed home agent.

In both the cases, the mobile node maintains only one home binding at any given time. In the Home Agent Hard Switch mode, the mobile node needs to switch its binding from the active to standby home agent upon failover. The bindings are synchronized among home agents in the redundant home agent set in the background when the Home Agent Virtual Switch mode is used.

All new messages defined in this document are defined as Mobility Header messages so that the Home Agent Reliability protocol can be extended to provide home link redundancy.

Finally, the reasons why we defined a new Hello message instead of using VRRP is described in Section 7.3 and Section 7.4. We also give instructions on how operators can run both VRRP and the Home Agent Reliability protocol at the same time in Section 7.10.

5. Protocol Overview

5.1. Home Agent Network Configuration

The Home Agent Reliability protocol supports two different configurations for standby home agents. Standby home agents can be placed on the same home link as the active home agent, or on a different link. The Global Recovery described below is not included in this document, although the Home Agent Reliability protocol can support this with slight modifications to home agent operations.

```
               HA1    HA2    HA3    HA4 .... HAn
                |      |      |      |        |
        --------+------+------+------+--------+---------
                            Home Link
```

Figure 1: Local Recovery Configuration

Figure 1 depicts the configuration where home agents serving the same home network are located on the same link. For example, HA2, HA3 and HA4 are standby home agents of HA1. This is the same as what Mobile IPv6 defines for home agent configuration.

```
         ---------IGP------>|<---BGP--->|<-----IGP---------

               HA1    HA2                      HA3    HA4
                |      |                        |      |
        --------+------+-----+ R---R---R +-----+------+-------
              Home Link          Routers     Recovery Link
```

Figure 2: Global Recovery Configuration

Figure 2 illustrates when standby home agents are located on a different link (named the recovery link in Figure 2). HA3 and HA4 are standby home agents of HA1 and HA2. In this case, HA3 and HA4 cannot receive packets meant for the home network until the route on the Routers is changed. The advantage of this configuration is that standby home agents can recover from a failure of the home link. This configuration can achieve home agent recovery even if the entire home link fails. In this configuration, the routing must be also updated to direct the packets meant for the home link to the recovery link.

This geographic redundancy is not a requirement by any SDO (Standards Development Organization), but is required by operators. Most large operators have a very stringent requirement on network availability even in the worst type of disaster or outage. For example, critical nodes in region-1 are backed up by nodes in region-2. These two regions are geographically separated. If region-1 suffers a downtime due to any reason, all the sessions will be seamlessly taken over by the nodes in region-2. This is called geographic redundancy. This is a well-known configuration for Telecommunications operators.

5.2. Home Agent Virtual Switch

A mobile node remains unaware about the change in the active home agent since the home agents have replicated all session state including the IPsec/IKE/ESP states. The IPsec/IKE/ESP state transfer is out of scope of this document.

```
  MN      HA1(active)    HA2(Standby)
   |           |           .
   |<--------->|           | 1. IKE exchange (with HoA assignment)
   |---------->|           . 2. Binding Update
   |<----------|           . 3. Binding Acknowledgment
   |           |           .
   |           |<--------->. 4. State exchanges (binding cache/IPsec)
   |           |           .
   |           X           .  HA1 FAILURE
   |           X           .
   |           X<----------. 5. Failure Detection
   |           X           | 6. HA2 takes over the HA1
   |           X           |
   |           X           |    RECOVERY COMPLETE
```

Figure 3: Overview of Home Agent Virtual Switch

The operations of the Home Agent Virtual Switch mode are shown in Figure 3. The mobile node first attempts the IKE exchange for Security Association (SA) setup and home address assignment (1). After binding registration is done (2, 3), the active home agent pushes all the states of its mobile nodes with a state synchronization message (4). The standby home agent(s) is not active unless it takes over from a failed home Agent.

When the active home agent's failure is detected (5), the standby home agent activates the IP address of the failed home agent on it and takes over for the failed home agent. All the home agents in the redundant home agent set share a virtual home agent address and the

routing will ensure only the active home agent will be reachable using that virtual home agent address. The standby home agent can serve all the mobile nodes for which the states are synchronized, without any further message exchange, because it has all the necessary information which it obtained from the failed home agent.

5.3. Home Agent Hard Switch

The overview of the Home Agent Hard Switch is shown in Figure 4. This mode is not transparent to the mobile node when the active home agent failure occurs.

```
  MN      HA1(active)    HA2(Standby)
   |           |           |
   |<--------->|           | 1. IKE exchange (with HoA assignment)
   |---------->|           | 2. Binding Update
   |<----------|           | 3. Binding Acknowledgment
   |<--------------------->| 4. IKE exchange (without HoA assignment)
   |           |           |
   |           |<--------->. 5. State exchanges (binding cache)
   |           |           |
   |           X           |  HA1 FAILURE
   |           X           |
   |           X<----------| 6. Failure Detection
   |<----------------------| 7. Sending Home Agent
   |           X           |          Switch message
   |<--------------------->| 8. Binding Registration
   |           X           |
   |           X           |    RECOVERY COMPLETE
```

Figure 4: Overview of Home Agent Hard Switch

The mobile node establishes IPsec/IKE state with all the home agents in the redundant home agent set beforehand (1 and 4), however it registers its binding only with the active home agent (2 and 3). When an active home agent fails, a standby home agent uses a pre-existing IPsec SA to notify the mobile node about the failure by securely sending a Home Agent Switch message. In order to discover home agent addresses, two different mechanisms are defined, as described in Section 8.1. The active home agent synchronizes the required states of the mobile nodes, such as Binding Cache and AAA information, with other standby home agents periodically (5). The mobile node MUST NOT request a home address(es) assignment through the IKE exchange to the standby home agent when it establishes an SA with it (4).

When the standby home agent detects the failure of the active home agent (6), it sends a Home Agent Switch message to all the mobile nodes that were registered with the failed home agent (7). The Home Agent Switch message must be encrypted by a pre-established IPsec SA. After the switch message, the mobile node MUST send a binding update to the new active home agent in order to update the Mobile IPv6 tunnel end points (8).

5.4. Active Home Agent Management

```
HA1(active)  HA2    HA3 .. HAn
    |        |      |      |
    |------->|      |      | 1. HA1 sends SwitchBack Request
    |<-------|      |      | 2. HA2 sends SwitchBack Reply
    |        |      |      |
(standby) (active)  |      | HA2 BECOMES ACTIVE HA
    |        |      |      |
       SYSTEM MAINTENANCE, ETC.
    |        |      |      |
    |------->|      |      | 3. HA1 sends SwitchOver Request
    |<-------|      |      | 4. HA2 sends SwitchOver Reply
    |        |      |      |
(active) (standby)  |      | 5. HA1 returns to active HA
    |        |      |      | HA1 BECOMES ACTIVE AGAIN
```

Figure 5: Manual Home Agent Change

In some scenarios the active home agent may need to stop serving mobile nodes for system maintenance. This specification provides for a manual home agent switch by using SwitchBack Request and Reply messages. As shown in Figure 5, the active home agent (HA1) sends a SwitchBack Request message to a standby home agent (HA2). As soon as HA2 receives the message, it becomes the active home agent. HA2 will acknowledge the message by sending a SwitchBack Reply message to HA1. HA1 becomes a standby home agent when it receives the SwitchBack Reply. After the downtime, HA1 sends a SwitchOver Request to HA2 in order to become the active home agent again.

6. Messages

6.1. New Mobility Header Messages

6.1.1. State Synchronization Message

This message is used to exchange state corresponding to a particular mobile node. It MUST be unicasted and MUST be authenticated by IPsec ESP. The State Synchronization message has the MH Type value TBD. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
 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      |    Reserved   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identifier            |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
.                                                               .
.                        Mobility Options                       .
.                                                               .
.                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: State Synchronization Message

Type

8-bit unsigned integer. It can be assigned one of the following values:

0: Request

This message is called State Synchronization Request and used to request state corresponding to a particular mobile node. The State Synchronization Request is used to solicit the active state corresponding to a particular mobile node.

1: Reply

The message is called State Synchronization Reply and is used between the home agents in the redundant home agent set to exchange binding cache information and any other information related to providing mobility service to the mobile nodes. The State Synchronization Reply can be sent by an active home agent

either periodically or in response to a State Synchronization Request.

Reserved

8-bit unsigned integer. It must be initialized to zero by the sender and must be ignored by the receiver.

Identifier

A 16-bit identifier to aid in matching state synchronization messages. The identifier should never be set to 0. It should always be more than 1.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in [1]. The receiver MUST ignore and skip any options which it does not understand.

One of the following options is mandatory in State Synchronization Request message. :

* IP Address Option (Sub-type: Home Address)[12]. If a home agent wants the Binding Cache information for a particular mobile node, it includes an IPv6 Address Option.

* Mobile Network Prefix Option. If a home agent wants to know the forwarding state setup for a particular Mobile Network Prefix, it includes a Mobile Network Prefix Option as defined in [2].

* Vendor Specific Mobility Option. If a home agent wants vendor specific information, it can solicit with this option as defined in [7].

One of the following options is mandatory in State Synchronization Reply. :

* Binding Cache Information Option

* AAA Information Option

* Vendor Specific Mobility Option

This message requires at least one mobility option, therefore, there

is no default length for this message.

6.1.2. Home Agent Control Message

This message is used to control the status of a home agent to either active or standby. This message MUST be unicasted between home agents and MUST be authenticated and encrypted by IPsec ESP. The Home Agent Control message has the MH Type value TBD. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
 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      |   Status      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                        Mobility Options                       .
.                                                               .
.                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: Home Agent Control Message

Type

8-bit unsigned integer. It can be assigned one of the following values:

0: SwitchOver Request

This message is called SwitchOver Request. It is unicasted by a standby home agent that desires to become the active home agent. The receiver of the message MUST transition to standby state as soon as the message is received and validated successfully.

1: SwitchOver Reply

This message is called SwitchOver Reply. It is used to acknowledge the receipt of the corresponding SwitchOver Request.

2: SwitchBack Request

This message is called SwitchBack Request. It is unicasted by an active home agent that desires to become the a standby home agent. The receiver of this message SHOULD transition to active state as soon as the message is received and validated successfully.

3: SwitchBack Reply

This message is called SwitchBack Reply. It is used to acknowledge the receipt of the corresponding SwitchBack Request.

Status

8-bit unsigned integer indicating the disposition of a Switchover Request or SwitchBack Request message. This field is only valid in SwitchOver Reply and SwitchBack Reply messages. The following Status values are defined:

0: Success

128: Reason unspecified

129: Administratively prohibited

130: Not active home agent (The receiver of the SwitchOver Request message is not the active home agent)

131: Not standby home agent (The receiver of the SwitchBack Request is already the active home agent)

132: Not in same redundant home agent set

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in [1]. The receiver MUST ignore and skip any options which it does not understand. No options are defined in this specification

If no options are present in this message, no padding is necessary and the Header Len field will be set to 1.

6.1.3. Home Agent Hello Message

This messages can be replaced by other protocols as described in Section 7.10. If this message is used, it MUST be either unicasted or multicasted to carry home agent information among the redundant home agent set. The Hello message is defined for two purpose: 1) an alive check and 2) home agent information exchange. A home agent Hello message SHOULD be authenticated and encrypted by IPsec ESP when it is unicasted. If a Hello message is multicasted, IPsec ESP cannot be applied. In this case the redundant home agent set should be located in a secure network. Alternatively, all the home agents MUST have a secure channel with each other. The Hello message has the MH Type value TBD. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
 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
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |          Sequence #           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Home Agent Preference    |      Home Agent Lifetime      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Hello Interval         |   Group ID    |A|R|  Reserved |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                        Mobility Options                       .
.                                                               .
.                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 8: Home Agent Hello Message

Sequence #

16-bit unsigned integer. The Sequence number of the Hello message can be used to verify whether this Hello message is the latest one or not.

Home Agent Preference

16-bit unsigned integer. The preference for the home agent sending this Hello message. This preference is the same as the Home Agent Preference value of the Home Agent Information option as defined in [1]. However, operators MAY use a different

preference value for this operation.

Home Agent Lifetime

16-bit unsigned integer. The lifetime for the home agent sending this Hello message. This lifetime is the same as the Home Agent Lifetime value of the Home Agent Information option as defined in [1].

Hello Interval

16-bit unsigned integer. The interval for the home agent sending this Hello message.

Group Identifier

8-bit unsigned integer. This value is used to identify a particular redundant home agent set.

A flag

If this flag is set, the sender of this Hello message is an active home agent. Otherwise, the sender is standby home agent

R flag

If this flag is set, the receiver of this Hello message must send back a Hello message to the sender.

Reserved

6-bit unsigned integer. It must be initialized to zero by the sender and must be ignored by the receiver.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in [1]. The receiver MUST ignore and skip any options which it does not understand. No valid options are defined in this specification.

If no options are present in this message, 0 octets of padding are necessary and the Header Len field will be set to 2.

6.1.4. Home Agent Switch Message

This message is defined in Section 8.3. The Home Agent Reliability protocol extends this message for the Home Agent Hard Switch.

```
 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
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |# of Addresses |I|  Reserved   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
.                       Home Agent Addresses                    .
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                         Mobility options                      .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9: Home Agent Switch Message

IPsec Re-key (I)

The IPsec rekey (I) bit is set to indicate that the mobile node SHOULD start an IPsec re-key with the home agent specified in the Home Agent Addresses field. This flag is used when a failed home agent recovers and needs to re-establish IPsec SA/IKE state with a mobile node.

Reserved

The reserve field is reduced from 8 to 7 bits

6.2. New Mobility Options

6.2.1. IP address Option

This option is already defined in the Fast Handovers for Mobile IPv6 (FMIP) specification [12]. This document introduces new Sub-Type values for home agent address and Home Address.

Option-Code

* 4: Home Agent Address

* 5: Home Address

6.2.2. Binding Cache Information Option

The binding cache information option has an alignment requirement of 8n+2. Its format is as follows:

```
 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 = TBD  | Length = 40   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Flags                |       Sequence Number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Lifetime             |          Reserved             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                        Home Address                           |
+                                                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                        Care-of Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                                                               .
.                 Mobile Network Prefix Option                  .
.                                                               .
.                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 10: Binding Cache Information Option

The Binding Cache Information option is only valid in a State Synchronization message.

The fields of Home Address, Care-of Address, Flags, Sequence Number, and Lifetime are copied from the registered binding of a particular

mobile node or mobile router. The 8-bit Reserved field MUST be set to zero. If the R-flag is set to indicate this binding cache entry is for a mobile router, then this option will be immediately followed by one or more Mobile Network Prefix options.

6.2.3. AAA Information Option

The AAA option is used to carry the AAA state of the mobile node's Mobile IPv6 sessions. The AAA state information can be conveyed in RADIUS or Diameter AVP formats including the user and session info. This information option is only valid in a State Synchronization message.

```
 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 = TBD  |   Length      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                                                               .
.                        AAA AVPs                               .
.                                                               .
.                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 11: Vendor Specific Inforamtion Option

Type

8-bit Type value. The value is TBD.

Length

8-bit length value.

AAA AVPs

Series of TLV encoded AAA AVPs (including vendor specific AVPs) carrying AAA-related information for each Mobile IPv6 and IPsec/IKE session.

7. Home Agent Operation

7.1. Home Agent Address Configuration

Each standby home agent obtains its individual IPv6 address from its attached link. This IPv6 address is used by the home agent reliability protocol to exchange information with the associated home agents. The link between home agents should be secured.

When the Home Agent Virtual Switch mode is used, the virtual home agent IPv6 address which is known by the mobile node is shared with the standby home agents. When a home agent fails, the standby home agent activates the IPv6 address of the failed home agent and becomes the active home agent. The standby home agent should not activate the IPv6 address until it knows the active home agent is no longer reachable at the address, otherwise address duplication will occur. To guarantee transparency of the home agent virtual switch to mobile nodes located on the home link, the neighbor cache of the home agent IP address MUST be carefully operated. See Section 7.2 in detail.

When the Home Agent Hard Switch mode is used, each home agent configures itself with a different IPv6 address from the same home prefix. This IPv6 address can be used for the Home Agent Reliability protocol if the standby home agents are located at the same link of the active home agent (Figure 1). In case of Figure 2, the router must carefully route packets to the standby home agents as described in Section 7.2. Once a mobile node registers its binding with the active home agent, it may solicit an IPsec/IKE exchange with standby home agents. These packets must be routed to the recovery link. This can be achieved by installing host routes for the standby home agents on the recovery link of the router.

7.2. Consideration of Routing and Neighbor Discovery Protocol

This section gives a brief explanation of how a home agent interacts with routing and Neighbor Discovery Protocol (NDP) when the Home Agent Virtual Switch mode is used.

When a standby home agent becomes active in the Home Agent Virtual Switch mode, it MUST start to advertise the home agent address and the home prefix of the home addresses serviced by the redundant home agent set into the routing infrastructure. This operation is normally done using a route selector such as BGP or an OSPF modifier. For example, we can use the AS_Path prepend operation for BGP, and the Metric field in OSPF for route selection.

For instance, home agents should run OSPF with the appropriate cost so that the active home agent whose preference is highest can receive

the packets from the other routers on the home link. When the active home agent is down, OSPF detects the failure and can dynamically switch the route to the standby home Agent based on the OSPF cost value. If this cost conflicts with the home agent preference value due to misconfiguration, the routers on the home link may not route packets to the desired standby home agent. Therefore, the home agent MAY dynamically change the OSPF cost based on the home agent preference value. Most of router vendors have a private MIB to set the cost via SNMP, though this is a vendor-specific function. The operator can consider other existing approaches to update routes on the routers at the home link.

When an active home agent activates a home agent address, it SHOULD use a virtual MAC address as introduced in [4]. When the active home agent is changed, the neighbor cache of the active home agent is not necessarily updated on mobile nodes located on the home link. Otherwise, the new home agent MUST update the neighbor cache entry for the home agent address on all the mobile nodes located on the home link. In addition, Mobile IPv6 uses proxy NDP to intercept packets meant for mobile nodes which are away from the home link. However, it is unnecessary for the new active home agent to overwrite the existing proxy neighbor entries of the mobile nodes.

7.3. Home Agent List Management

In Mobile IPv6 [1], each home agent periodically sends router advertisements with a Home Address Information option [1] for exchanging home agent information when there are multiple home agents present on a link. This information is managed in a home agent list introduced in [1]. When the Home Agent Reliability Protocol is used, Hello messages are used to update the home agent list. There are several reasons to use Hello message instead of Router Advertisement on the Home Agent Reliability protocol:

1. Router Advertisements are sent among home agents and also to mobile nodes. When the Home Agent Virtual Switch is used, standby home agents MUST NOT generate unsolicited Router Advertisements. The standby home agents MUST be transparent to all mobile nodes. Hello messages are exchanged only with other home agents.

2. Router Solicitation and Advertisement messages [8] cannot be used due to link-local limitations. However, as shown in Section 5.1, standby home agents are not always configured on the same link. Router Advertisements cannot be used in this case.

3. The Home Agent Reliability protocol is required to exchange additional information such as Group ID and Active/Standby Status

of the home agents.

When Hello messages are used, the Home Agent Information Option [1] MAY NOT be used in Router Advertisements on the home link, because all necessary information will be present in the Hello messages. However, mobile nodes located on the home link require this information for home agent discovery. In addition, if operators want to use different parameters such as Preference value for home agents and mobile nodes, they can utilize both Router Advertisements and Hello messages. Router Advertisements are used to carry the home agent information for mobile nodes, and Hello message are used to carry information for Home Agent Reliability operation. If an operator decides not to use the Hello messages, Router Advertisements MUST be used to update the home agent list.

Since Hello messages carry all the necessary information filled-in from the home agent list, the management of the home agent list is unchanged. If a standby home agent removes an active home agent from the list because it's lifetime has become zero, it can start recovery according to this document. < xref target="subsec:failuredetection"/> describes failure detection in detail.

7.4. Detecting Home Agent Failure

The active and standby home agents can monitor each other's status in multiple ways. One method is to reuse other failure detection mechanisms such as VRRP[4] and HSRP[5] described in Section 7.10. This document also defines its own method by using periodic exchanges of Hello messages to monitor status. The reasons to specify Hello messages are:

1. Hello messages can be sent off-link for global recovery is required by an operator. Router Advertisements cannot be used in this scenario since their scope is link-local. Thus, Hello messages are necessary to exchange home agent information among home agents in a globally redundant home agent set.

2. If Router Advertisements and VRRP are used for periodic messages, they may not detect the case where the system is running but the Mobile IPv6 stack is not operational. Mobile IPv6 may be implemented as a userland daemon, so if Hello messages are used, the failure of a home agent can be easily detected, assuming Hello message functionality is implemented in the same home agent daemon.

3. Hello messages can be frequently exchanged to detect failure, while there is a restriction on how often Router Advertisements can be sent, and on how they are processed by routers that

receive them. Router Advertisements are also not sent frequently enough to rely on their absence to detect a home agent failure.

A Hello request message (R-flag set) may be used by any home agent to request state information from any other home agent in the redundant home agent set. If a Hello message is not received from a home agent peer within a configurable amount of time, then that home agent peer is considered to have failed. The detail of the Hello message is described in Section 7.6. Failure events used in the Home Agent Reliability protocol are listed below.

Loss of Communication with the Active Peer Home Agent

In the event that a standby home agent does not receive any Hello message from its peer which is currently the active home agent for a configurable duration, the standby home agent may decide to become the active home agent.

Monitored Server Failure by the Active Home Agent

There may be number of critical servers in the network that are essential for the ongoing Mobile IPv6 sessions at the home agent. One such server may be the AAA server which is receiving the accounting information for the session. The operator may have a policy in place that requires the home agent to initiate a switch-over procedure upon detecting that the link to such a server has failed.

Routing Peer/Link Failure

In some cases, an operator may require the home agent to detect a next-hop routing peer failure. If the next-hop routing peer fails, the operator may want the home agent to initiate a switch-over procedure if the failure is fatal in nature, or due to some other routing policies.

7.5. Home Agent Switch Over

After detecting the active home agent has failed, a standby home agent whose preference value is the highest MUST take over for the failed home agent.

In the Home Agent Virtual Switch mode, the standby home agent MUST activate the virtual home agent address. If a virtual MAC address as introduced in [4] is used, the standby home agent MUST start using the virtual MAC address as well. Since all the necessary state has already been transferred to this standby home agent before the active home agent failed, it can immediately start acting as the active home

agent.

In the Home Agent Hard Switch mode, the standby home agent MUST send a Home Agent Switch message to all the mobile nodes that were registered at the failed home agent as described in Section 7.9, using the pre-established IPsec SA. The home agent switch-over is complete when it receives binding updates from all the mobile nodes.

7.6. Processing Hello Messages

Hello messages can be unicasted or multicasted. A new multicast address will be assigned by the IANA. When all home agents in a redundant home agent set are configured on a same home link, they MUST join a new multicast address (TBA) and multicast Hello. On the other hand, if a home link is separated as described in Figure 2, each home agent MUST unicast Hello messages.

7.6.1. Requesting Hello Message

A home agent can solicit a Hello message from a particular home agent in the same redundant home agent set by unicasting or multicasting a Hello message with the R-flag set. The sender MUST fill the fields of the Hello message with it's home agent information. When a Hello message is unicasted, only the destination of the Hello message will answer it. On the other hand, if a Hello message is multicasted, all the home agents in the multicast group will reply to the Hello message. This Hello request message SHOULD be generated when:

- o A new home agent needs to collect information of the other home agents in the same redundant home agent set. In this case it SHOULD multicast a Hello message in which the R-flag is set.

- o A home agent entry in the redundant home agent list is about to be removed due to home agent lifetime expiration.

- o A Hello message has not been received during the specified hello interval.

7.6.2. Sending Hello Message

The Hello message MUST be sent when a home agent receives a Hello message with the R-flag set, indicating a request is required, otherwise Hello messages are periodically sent according to the pre-configured Hello interval. In addition, a home agent SHOULD send a Hello message to the home agents of the redundant home agent set when it boots up and its local information, such as home agent preference, home agent lifetime, and registration status, etc., change. When a new home agent boots up, it SHOULD solicit Hello messages by

multicasting a Hello message with the R-flag set in parallel with sending own Hello message.

Whenever a home agent generates Hello message, it MUST increment in the Sequence Number by 1. It MUST also specify its own Group ID in the Group ID field of the Hello message. If a home agent is the active home agent, it MUST set the A-flag in it's Hello Messages. In the Home Agent Hard Switch mode, the source address of Hello messages MUST be the configured home agent address. In the Home Agent Virtual Switch mode, the individual IPv6 addresses of each home agent MUST be used.

7.6.3. Receiving Hello Message

When a home agent receives a Hello message, it SHOULD verify IPsec ESP protection. If the message is not protected, it SHOULD be silently discarded. However, if the Hello messages is sent on a dedicated link between the home agents, IPsec protection is not required. If a Hello message is sent from an IPv6 address whose scope is not global, the message MUST be silently discarded.

If the sending home agent is not in the same redundant home agent set, the message MUST be silently ignored. This can be done by comparing the Group ID field of the received Hello message with the own Group ID value. Hello messages MUST NOT be sent to a home agent whose Group ID is different from the sender. If the Sequence Number value in the Hello message is equal to or less than the Sequence Number value stored in the home agent list entry, the Hello message MUST be discarded.

Any Hello message satisfying all of these tests MUST be processed to update the redundant home agent list. The receiver copies home agent information in the Hello message to the corresponding redundant home agent list entry. The home agent address of the sender is retrieved from the Source Address field of the IPv6 header of the Hello message. If the home agent lifetime field in the Hello message is set to 0, the receiver removes the sender from the redundant home agents list.

If the R-flag is set in the received Hello message, the receiver MUST reply with a Hello message to the originator as described in Section 7.6.2.

7.7. Processing State Synchronization Messages

It is necessary for standby home agents to synchronize the state information of each mobile node registered with the active home agent. In the Home Agent Virtual Switch mode, the synchronized state

information is used by a standby home agent when it takes over for the failed home agent. In the Home Agent Hard Switch mode, the standby home agent starts the switch-over of all the mobile nodes registered to the failed home agent when the home agent failure is detected. Thus, the Binding Cache entry MUST be modified to keep the active home agent address of each mobile node.

7.7.1. Soliciting State of a Particular Mobile Node or Subset of Mobile Nodes

When a standby home agent wants state information for a particular mobile node or a subset of mobile nodes, such as Binding Cache, AAA, etc., it MAY solicit this state by sending a State Synchronization message constructed as follows:

- It MUST set the Type field to 0 (Request).

- It MUST set a random value in the Identifier field.

- It MUST include either a Home Address mobility option indicating the mobile node, or a Mobile Network Prefix mobility option indicating the mobile router. The standby home agent can send multiple home address and mobile network prefix mobility options to request state information for multiple mobile nodes in a single State Synchronization request message.

When a home agent receives the State Synchronization message with the Type field set to 0 (Request), it MUST verify the message as follows:

- The state synchronization message MUST be protected by IPsec ESP.

- The sending home agent MUST belong to the same redundant home agent set

- The receiver MUST be the active home agent for the requested home address or mobile network prefix.

Any packet carrying a State Synchronization message which fails to satisfy all of these tests MUST be silently ignored.

Otherwise, the receiver MUST reply with a State Synchronization message including state information for the requested mobile node(s) and/or mobile network prefix(es) as described in Section Section 7.7.2.

7.7.2. Synchronizing State of Mobile Nodes

A state synchronization message can be sent either:

- o When an active home agent receives a state synchronization message in which the Type field is set to 0 (Request).

- o When an active home agent creates a binding cache entry for a particular mobile node.

- o When an active home agent deletes a binding cache entry for a particular mobile node.

- o When an active home agent updates a binding cache entry for a particular mobile node, only when operating in the Home Agent Virtual Switch mode. In the Home Agent Hard Switch mode, standby home agents only use this binding cache information to send a Home Agent Switch message, so only need a home address of all the mobile nodes registered to the active home agent of the same redundant home agent set.

- o In a periodic interval to update the state information for all sessions that changed since the last update.

If an active home agent sends a State Synchronization message whenever the local state information changes, such as a binding cache change, the number of the State Synchronization messages sent can be quite large.

The binding cache information of the requested mobile nodes is stored in the State Synchronization message. The active home agent MUST copy the binding cache information of the requested mobile nodes into Binding Cache Information options. If the State Synchronization message is sent in response to a State Synchronization request message, the active home agent MUST copy the Identifier field of the State Synchronization request message to the Identifier field in the State Synchronization reply message. Otherwise, it MUST set the Identifier field to 0.

When the active home agent stores the state of multiple mobile nodes in a state synchronization message, a Binding Cache Information option is used as a separator. For each mobile node, a Binding Cache Information option is placed first, followed by any other options. When the next Binding Cache Information option is reached in the State Synchronization message, it indicates the information of a different mobile node.

A State Synchronization message MUST be authenticated and encrypted

by IPsec ESP mode, otherwise the message MUST be ignored. When a home agent receives a State Synchronization message, it MUST verify the Source address field of the IPv6 header. If the source address does not belong to any home agent in the redundant home agent set, the message MUST be silently discarded. After successfully verifying the message, the receiving home agent MUST update its binding cache and all other necessary information such as AAA and vendor specific information in the particular database. In the Home Agent Hard Switch mode, the receiver MUST also record the IPv6 address of the sender (the active home agent).

7.8. Processing Home Agent Control Messages

7.8.1. Standby Home Agent becomes an Active Home Agent

When a standby home agent decides to become an active home agent, the standby home agent sends a SwitchOver Request message (a Home Agent Control message in which the Type field is set to 0) to the active home agent. This message MUST be unicasted to the active home agent and MUST be encrypted and authenticated by IPsec ESP. The active home Agent MUST NOT generate this message.

When an active home agent receives a SwitchOver Request, it first verifies the received Home Agent Control message. If the request message is not protected by IPsec, it MUST be silently discarded. If the home agent is not an active home agent, it MUST send a SwitchOver Reply message (a Home Agent Control message in which the Type field is set to 1) with the Status field set to 130 (Not active home agent). If the receiver is an active home agent and does not want this standby home agent to become the active home agent, it MUST reply a SwitchOver reply with the Status field set to 129 (Administratively prohibited). In addition, if the sending home agent does not belong to the same redundant home agent set, a SwitchOver Reply message MUST be sent to the sender with the Status field set to 132 (Not in same redundant home agent set). Otherwise, the active home agent MUST become a standby home agent and reply with a SwitchOver Reply message with the Status field set to 0 (Success).

If a home agent receives a SwitchOver Reply message, it MUST be protected by IPsec ESP. Otherwise, the message MUST be silently discarded. If the receiving home agent did not send a SwitchOver Request message, the message MUST be silently ignored. If the Status field of the SwitchOver Reply message is 0 (Success), the receiving standby home agent immediately becomes an active home agent. If the value in the Status field is greater than 128 an error has occurred. In this case, the receiver MUST NOT become an active home agent.

7.8.2. Active Home Agent becomes in-active

When an active home agent decides to become an in-active home agent, it sends a SwitchBack Request message (i.e. a Home Agent Control message with Type field set to 3) to a standby home agent. The reason for the active home agent to send this message can be administrative intervention, and events like Monitored Server Failure by the active home agent or Routing Peer/Link Failure. This message MUST be unicasted to one of the standby home agents and MUST be encrypted and authenticated by IPsec ESP. A standby home agent MUST NOT generate this message.

A SwitchBack Reply is sent in reply to a SwitchBack Request message. When a home agent receives a SwitchBack Request message, it first verifies the message. If the SwitchBack Request message is not protected by IPsec ESP, it MUST be silently discarded. If the sending home agent of the SwitchBack Request message is not an active home agent, the receiver MUST reply with a SwitchBack Reply (a Home Agent Control message in which the Type field is set to 4) in which the Status field is set to 130 (Not active home agent). If the sending home agent does not belong to the same redundant home agent set, a SwitchBack Reply message MUST be sent in which the Status field set to 132 (Not in same redundant home agent set). Otherwise, the receiving home agent MUST send a SwitchBack Reply message in which the Status field is set to 0 (Success). After sending the SwitchBack reply, it MUST NOT become an active home agent immediately. This is because the active home agent is still active until it receives the SwitchBack Reply message acknowledging the SwitchBack Request. The standby home agent SHOULD change to active at least after LINK_TRAVERSAL_TIME.

If a home agent receives a SwitchBack Reply message, it MUST be protected by IPsec ESP, otherwise the message MUST be silently discarded. If the receiving home agent did not send a SwitchBack Request message beforehand, the message MUST be silently discarded. If the Status field of the SwitchBack Reply message is 0 (Success), the receiving home agent immediately becomes an in-active home agent. If the value in the Status field is greater than 128, an error has occurred. In this case, the receiver cannot become an in-active home agent and MUST continue to be an active home agent.

7.9. Sending Home Agent Switch Messages

This operation is valid only for the Home Agent Hard Switch mode. The standby home agent MUST send a Home Agent Switch message as defined in [11] to all the mobile nodes that were being served by the failed home agent. Since the active home agent address is recorded in each synchronized binding cache, the standby home agent knows

which mobile nodes were served by the failed home agent. The Home Agent Switch message must be encrypted with a pre-established SA. The standby home agent should include its own IPv6 address in the Home Agent Switch message. Note that a Home Agent Switch message is sent to each mobile node served by the home agent. If there is a large number of mobile nodes, sending Home Agent Switch messages will cause a lot of signaling overhead on the network.

When a failed home agent recovers, it MUST re-establish an IPsec SA with each mobile node served by its redundant home agent set. Otherwise, it cannot be either a standby or active home agent for the mobile nodes. Therefore, it sends a Home Agent Switch message with the I-flag set to all the mobile nodes serving by other home agents in the same redundant home agent set, and includes its own home agent address in the Home Agent Addresses field.

7.10. Interworking with VRRP

VRRP and HSRP specify an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. This operation is similar to the Home Agent Virtual Switch operation. For example, the VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail over in the forwarding responsibility should the Master become unavailable. Although VRRP is used to guarantee home agent address reachability, it cannot be used for state synchronization and explicit switching of Master and Backup. Thus, the Home Agent Reliability protocol cannot be replaced by VRRP. This section explains how VRRP can interwork with the Home Agent Reliability protocol.

When VRRP is available, VRRP can replace the Hello message described in Section 6.1.3. However, some of information is missed by using VRRP. After receiving a VRRP message, each home agent SHOULD process the message and store the information as if it receives Home Agent Hello messages Section 7.6.3. The Home Agents SHOULD still perform binding cache synchronization as described in Section 7.7 and SHOULD support the Home Agent Switch message as described in Section 7.9.

In addition to this, VRRP is useful only if all home agents are located on the same link. If the home agents are topologically separated, the Home Agent Reliability protocol MUST be used.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Type  | Virtual Rtr ID|   Priority    |Count IPv6 Addr|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|(rsvd) |       Adver Int       |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                       IPv6 Address(es)                        |
+                                                               +
+                                                               +
+                                                               +
+                                                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 12: VRRP Packet Format

The message format of VRRP is described in Figure 12. Each field is mapped as follows:

Virtual Rtr ID

Group ID is stored in the Virtual Rtr ID field.

Priority

Home Agent Preference is stored in the Priority field. Note that VRRP only has 8 bits for the Priority field. Therefore, values larger than 255 MUST NOT be assigned to the preference value.

Count IPv6 IPv6 Addr

This field MUST be always be 1.

Advert Int

This field MUST be mapped to the Hello Interval field of the Home Agent Hello message, though it only has 12 bytes.

IPv6 address

A home agent address is stored in this field.

Home Agent Lifetime, Sequence Number and Flags field are missing in the VRRP packet format. Therefore, operators SHOULD use the same statically configured value for Home Agent Lifetime. Each home agent does not check freshness of received VRRP message because of no sequence number. If VRRP is used, a home agent cannot determine the active home agent from the VRRP message due to lack of A flag, and cannot request a VRRP advertisement to other home agents.

7.11. Retransmissions and Rate Limiting

Standby and active home agents are responsible for retransmissions and rate limiting of a State Synchronization Request, Switchover Request, SwitchBack Request messages for which they expect a response. The home agent MUST determine a value for the initial transmission timer:

- If the home agent sends a State Synchronization Request message, it SHOULD use an initial retransmission interval of INITIAL_STATE_SYNC_REQ_TIMER.

- If a standby home agent sends a Switchover Request message, it SHOULD use an initial retransmission interval of INITIAL_SWICHOVER_REQ_TIMER.

- If an active home agent sends a SwitchBack Request message, it SHOULD use an initial retransmission interval of INITIAL_SWICHBACK_REQ_TIMER .

If the sending home agent fails to receive a valid matching response within the selected initial retransmission interval, it SHOULD retransmit the message until a response is received. All of the above constants are specified in Section 10.

The retransmission MUST use an exponential backoff process as described in [1] until either the home agent receives a response, or the timeout period reaches the value MAC_HARELIABILITY_TIMEOUT (16sec). The home agent SHOULD use a separate back-off process for different message types and different destinations. The rate limiting of Mobility Header messages is the same as one in [1]. A home agent MUST NOT send Mobility Header Messages to a particular home agent more than MAX_UPDATE_RATE (3) times a second, which is specified in [1].

8. Mobile Node Operation

Operations described in this section are valid only for the Home Agent Hard Switch mode. When the Home Agent Virtual Switch is used, all these operations can be skipped.

8.1. Home Agent Addresses Discovery

To provide home agent reliability with the Home Agent Hard Switch mode, a mobile node authenticates itself to two or more home agents and creates IPsec SAs with them during bootstrapping. When one home agent fails, another home agent can use the pre-existing SA to notify the mobile node about the failure.

Multiple home agent addresses are available in a home network. In order to discover these home agent addresses, two different mechanisms are defined in the bootstrapping solution in the split scenario [13]. One is DNS lookup by home agent Name, the other is DNS lookup by Service Name. DHCPv6 can also be used in the integrated scenario [14] to provide home agent provisioning to mobile nodes.

In the split scenario, a mobile node can use DNS lookup by Service Name to discover the home agents, as defined in [13]. For example, if home agent reliability is required by a mobile node, DNS lookup by Service Name method is recommended for the mobile node to discover multiple home agents addresses. Therefore, mobile nodes will query the DNS SRV records with a service name of mip6 and protocol name of ipv6. The DNS SRV records includes multiple home agent addresses and different preference values and weights. The mobile node SHOULD choose two or more home agents from the home agents list according to their preference value. Then the mobile node should authenticate itself to these home agents via an IKEv2 exchange.

In the integrated scenario, a mobile node can use DHCPv6 to get home agent provisioning from an MSP or ASP, as already defined in [14]. The only requirement is that the DHCPv6 response must include multiple home agents' information in order to support home agent reliability.

8.2. IKE/IPsec pre-establishment to Home Agents

After a mobile node gets multiple home agent addresses, it needs to trigger multiple IKE exchanges with theh multiple home agents selected from the home agent list. Since both IKEv1 and IKEv2 can be used to bootstrap Mobile IPv6, this solution does not introduce any new operations to co-operate with IKEv1 or IKEv2. It should initiate IKE for home agents as soon as home registration is complete.

The mobile node MUST follow the standard IKEv2 exchange in the bootstrapping solution of the split scenario [13], or the IKEv1 bootstrapping solution [15]. Home Address configuration maybe also be included, if necessary, for the first IKE exchange. After its Home Address is assigned or approved by the first home agent, mobile node SHOULD register itself with the second home agent with IKE using the same Home Address. Therefore, no home address configuration should be used in the second IKEv2 procedure. Note that the mobile node only sends a Binding Update message to the first home agent.

8.3. Receiving Home Agent Switch message

A mobile node must follow the operation specified in [11] when it receives a Home Agent Switch message.

If the I-flag is set in the received Home Agent Switch message, the mobile node MUST re-key the SA with the home agent addresses stored in the Home Agent Addresses field. The mobile node MUST NOT change its active home agent when the I-flag is set. If the home agent address is not known from the bootstrapping described in Section 8.1, the mobile node MUST NOT start an IKE session with the unknown home agent. Instead, it SHOULD re-start home agent discovery again to update its home agent address information.

When the mobile node receives a Home Agent Switch message without I-flag set, and if the message contains the IPv6 address of a standby home agent, it SHOULD pick the standby home agent in the switch message as the active home agent and send a Binding Update message to it. The mobile node already has a pre-established SA with the home agent and should use that SA to send the Binding Update.

9. Security Considerations

Since Mobile IPv6 operation requires ESP in transport mode between the mobile node and the home agent, we will discuss the ESP field synchronization issues between the mobile node and the redundant set of home agents. This synchronization is required only for Home Agent Virtual Switch mode. Most of fields should be synchronized based on RFC4301 [9]. The ESP header has the following fields:

SPI

This field identifies the SAD at the receiver.

The mobile node negotiates only one IPsec SA. Hence, the SPI value will remain unchanged upon home agent failover.

Sequence Number

This field is used for "anti-replay" feature of ESP. The transmitter must include this monotonically increasing number. The receiver may process the sequence number based on local policy.

The mobile node and the redundant home agent set will have the same set of sequence numbers for transmit and receive. Hence, synchronization of the sequence number field is mandatory in this mode of operation.

As described in Section 4, the SA1, SA2, SA3, SA4 could be synchronized between the home agents as these messages are not sent continuously. Moreover for the Binding Update case, if the mobile node is in the middle of sending a Binding Update to an active home agent for a binding refresh, and the active home agent is not available at that moment, the mobile node will not get any response from the active home agent. After a standby home agent becomes active, the mobile node will retry and it will receive the Binding Update from the mobile node with a sequence number that is +n from its last known sequence number for SA1. For the Binding Acknowledgement case (SA2), the standby home agent SHOULD add a random number to the last known sequence number over and above the replay window to ensure that the packet passes the replay check at the mobile node. The same applies to HoTi and HoT messages with SA3 and SA4. Note that this windowing of the sequence numbers for Mobile IPv6 signaling is only needed to cover the corner cases when Binding Update or HoTi is in-flight and the active home agent fails.

The technique explained above should work for user data packets if ESP is used to encrypt user data traffic as well. The actual switchover time and the routing infrastructure convergence time is the only latency that the user may perceive.

Initialization Vector

Since the Initialization Vector will be delivered in each exchange between a mobile node and home agent, this field is not necessarily synchronized between home agents.

Others

Other fields should be synchronized based on RFC4301[9]

In the Home Agent Hard Switch mode, the standby home agent needs to send a Home Agent Switch message using IPsec encryption. Since the mobile node has pre-established an IPsec SA with both the active and standby home agents, the standby home agent can send the message to the mobile node with the pre-established IPsec SA.

10. Protocol Constants

INITIAL_STATE_SYNC_REQ_TIMER: 3sec

INITIAL_SWICHOVER_REQ_TIMER: 1sec

INITIAL_SWICHBACK_REQ_TIMER 1sec

LINK_TRAVERSAL_TIME 150msec

11. Contributors

This document is a result of discussions in the Mobile IPv6 Home Agent Reliability Design Team. The members of the design team that are listed below are authors that have contributed to this document:

Samita Chakrabarti

samita.chakrabarti@azairenet.com

Kuntal Chowdhury

kchowdhury@starentnetworks.com

Hui Deng

hdeng@hitachi.cn

Vijay Devarapalli

vijay.devarapalli@azairenet.com

Sri Gundavelli

sgundave@cisco.com

Brian Haley

brian.haley@hp.com

Behcet Sarikaya

bsarikaya@huawei.com

Ryuji Wakikawa

ryuji@sfc.wide.ad.jp

12. Acknowledgements

This document includes a lot of text from [16] and [17]. Therefore the authors of these two documents are acknowledged. We would also like to thank the authors of the home agent reliability problem statement [18] for describing the problem succinctly and Alice Qin for her work on the hello protocol.

13. References

13.1. Normative References

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

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

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

[4] Hinden, R., "Virtual Router Redundancy Protocol (VRRP)", RFC 3768, April 2004.

[5] Li, T., Cole, B., Morton, P., and D. Li, "Cisco Hot Standby Router Protocol (HSRP)", RFC 2281, March 1998.

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

[7] Devarapalli, V., "Mobile IPv6 Vendor Specific Option", draft-ietf-mip6-vsm-00 (work in progress), December 2006.

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

[9] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

13.2. Informative References

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

[11] Haley, B., "Mobility Header Home Agent Switch Message", draft-ietf-mip6-ha-switch-01 (work in progress), June 2006.

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

[13] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-02 (work in progress), March 2006.

[14] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping via DHCPv6 for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-00 (work in progress), October 2005.

[15] Devarapalli, V. and M. Parthasarathy, "Mobile IPv6 Bootstrapping with IKEv1", draft-devarapalli-mip6-ikev1-bootstrap-01 (work in progress), March 2006.

[16] Wakikawa, R., "Inter Home Agents Protocol Specification", draft-wakikawa-mip6-nemo-haha-spec-01 (work in progress), March 2006.

[17] Devarapalli, V., "Local HA to HA protocol", draft-devarapalli-mip6-nemo-local-haha-01 (work in progress), March 2006.

[18] Faizan, J., "Problem Statement: Home Agent Reliability", draft-jfaizan-mipv6-ha-reliability-01 (work in progress), February 2004.

Appendix A. Change Log From Previous Versions

Changes from draft-ietf-mip6-hareliability-00

- o Combining State Synchronization Request message and State Synchronization message

- o Combining home agent SwitchOver Request & Reply and SwitchBack Request & Reply messages.

- o Many Editorial Changes

Author's Address

Ryuji Wakikawa
Keio University
Department of Environmental Information, Keio University
5322 Endo, Fujisawa, Kanagawa 252-8520
Japan

Email: ryuji@sfc.wide.ad.jp

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).