Abstract

This document identifies one type of the denial of service attack which can be possible in Mobile IPv6 and tries to propose a solution for same.

Currently in MIPv6 each Home Agent is required to maintain a home agent list. This home agent list is generated by receiving RA.
messages on the home link and the addresses learned are sent to Mobile node when it does Home Agent discovery. On learning this list MN tries to register with addresses in this list one by one in order of preference. Now if the home network is flooded with spurious RA packets having high preference value the home agent list is populated with non reachable addresses and no mobile node is able to register from that home network

This document proposes to first carry out reachability confirmation for each home agent entry before adding to Home Agent list

Conventions used in this document

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].

Table of Contents

1. Introduction...................................................2
2. Problem........................................................3
3. Solution.......................................................3
   3.1 Receiving RA messages....................................3
   3.2 Success of Neighbor reachability detection.............4
   3.3 Failure of Neighbor reachability detection.............4
   3.4 Receiving Dynamic Home Agent Discovery Request Message....4
   3.5 Interface seize to act as a Home Agent Interface........5
4. Changes required in MIP6.....................................5
5. Formal Syntax................................................5
6. Security Considerations.......................................5
7. References....................................................5
8. Acknowledgments................................................5
9. Author’s Addresses.............................................6

1. Introduction

In Mobile IPv6 each home agent is required to maintain a Home Agent List, which contain the list of all Home Agents in the network along with the global addresses

In dynamic home agent discovery mechanism Home Agent replies to Home Agent discovery request with the addresses present in this home Agent list. This Home Agent list is populated on receiving RA messages on the home link.
This document identifies the Denial of service attack due to spurious RAs and also proposes solution for the same.
2. Problem

The on-link home Agent list is maintained by each home agent by getting the information from RA messages.

If some malicious node is flooding RA messages on behalf of non-existent nodes, the Home Agent list will be populated with incorrect entries.

This is because no verification of RA is done by Home Agent before updating its home agent list. On receiving the spurious packet, Home Agent list is updated with these addresses. When any mobile node goes in foreign network and start the dynamic home agent discovery process, the Home Agent will return the list of address that it has learnt through the above mentioned process.

Mobile node will start registering with each of these addresses with minimum interval of initialBindackTimeoutFirstReg (1.5 Seconds) since these addresses do not belong to any node, they may not be reachable.

If the first valid address in the list follows after a number of invalid addresses, the mobile node will get service after a very long time. If there are no valid addresses in the list, then Mobile Node will never get the service at all.

3. Solution

In order to control the spurious Home Agent addresses in the list, we can deploy a mechanism that shall ensure that Addresses learnt are reachable belonging to on link Home Agent.

A state needs to be associated for each entry in Home Agent list. The state can either be in STALE or REACHABLE state. The transition of these states is mentioned in subsequent sub-sections.

3.1 Receiving RA messages

Whenever RA is received on the Home Agent interface with H bit set, Home Agent SHOULD do the following processing:

- If entry already exists with same Link Local address and its state is REACHABLE then directly update the existing entry.

- If entry is not present in Home Agent List then...
Add the entry in Home Agent list and make the state of that entry as STALE (same as ND, when entry is added in Neighbor cache through RA, it is added in STALE state).

After adding the entry start the neighbor reachability detection as per RFC-2461 [2] for that link local address

If the entry exists and it state is STALE then simply ignore this RA message.

Apart from doing existing checks as mentioned by RFC 3775 [4] following addition check SHOULD be done

- If in the RA H bit is set but it does not contain any global address then this RA MUST be discarded (i.e. R flag is not set in any of the prefix options received)
- If the preference value in received RA is out of range as mentioned by RFC 3775 [4] then this received RA SHOULD be discarded

3.2

Success of Neighbor reachability detection

Processing NA messages: Whenever NA is received and home agent functionality is enabled then Home Agent SHOULD do the following processing

- ON receiving NA after checking neighbor cache, Home Agent list is also queried and if the entry exist in Home Agent list and the state is STALE, it state is changed to REACHABLE state

3.3

Failure of Neighbor reachability detection

If no reply is received for Link layer address and neighbor reachability detection fails then the corresponding Stale entry MUST be deleted Home Agent List.

3.4

Receiving Dynamic Home Agent Discovery Request Message

Whenever DHAAD message HA will prepare the DHAAD reply message adhering to following rules

- HA SHOULD only send back the global addresses from Home Agent list whose state is REACHABLE
- In case the DHAAD reply message becomes more then PMTU then HA must include self Home Agent address. This will ensure at least one valid reachable home agent address
3.5 Interface cease to act as a Home Agent Interface

As the home agent functionality is configurable so by configuration or otherwise if the interface seize to act as a Home Agent interface then Home Agent SHOULD send a final RA message with H bit set as 0 to indicate the other home agents on the link to update there home agent list and delete the entry corresponding to this home agent.

4. Changes required in MIP6

   o Additional Flag is required in Home Agent list entry to maintain the state of Entry

5. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC-2234.

Security Considerations

This draft enhances the security of RA packets by confirming the Link Layer address of sender.

Further improvement to this solution can be to carry out NUD for each of this global address received in RA and maintain the state corresponding to each of those global addresses

References


All references are normative.

Acknowledgments

Our sincere thanks to Saurabh Rastogi for his constant encouragement and Keshava A.K. for his guidance and review during the development of this specification.

Author’s Addresses

Sachin Dutta
Huawei Technologies India Pvt. Ltd.
Level-3, Leela Galleria
The Leela Palace, Airport Road
Bangalore-India
Phone: +91-080-25217152
Email: sachind@huawei.com

Deshbandhu Sinha
Huawei Technologies India Pvt, Ltd.
Level-3, Leela Galleria
The Leela Palace, Airport Road
Bangalore-India
Phone: +91-080-25217152
Email: deshbandhus@huawei.com

Suraj Shetty
Huawei Technologies India Pvt, Ltd.
Level-3, Leela Galleria
The Leela Palace, Airport Road
Bangalore-India
Phone: +91-080-25217152
Email: surajs@huawei.com

Mao Shanxiang
Huawei Technologies Co., Ltd.
Shenzhen, China
Email: maoshx@huawei.com

Disclaimer of Validity

“This document and the information contained herein are provided on
APPENDIX A: Home Agent State Machine

<table>
<thead>
<tr>
<th>State</th>
<th>Event</th>
<th>Action</th>
<th>New state</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>RA and H bit set</td>
<td>Create entry.</td>
<td>STALE</td>
</tr>
<tr>
<td>-</td>
<td>Any other message then RA</td>
<td>No relationship</td>
<td>-</td>
</tr>
<tr>
<td>STALE</td>
<td>Reachability Timeout</td>
<td>Delete the corresponding - Home Agent Entry</td>
<td></td>
</tr>
<tr>
<td>STALE</td>
<td>RA and H bit set for that local address</td>
<td>Discard RA</td>
<td>STALE</td>
</tr>
<tr>
<td>STALE</td>
<td>NA for that link local address</td>
<td>Update the state</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>REACHABLE</td>
<td>RA and H bit set for that local address</td>
<td>Update the global addresses and timers</td>
<td>REACHABLE</td>
</tr>
</tbody>
</table>