SAVI Solution for Delegated IPv6 Prefixes
draft-kaippallimalil-savi-dhcp-pd-01.txt

Abstract

This document specifies the procedure for creating bindings between a DHCPv6 assigned source IPv6 prefix and an anchor. These bindings can be used to filter packets with forged IPv6 prefixes.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

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

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 29, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1. Introduction ........................................... 3
2. Mechanism and Architecture Context ........................ 3
   2.1. Mechanism Overview .................................... 3
   2.2. Architecture Context .................................... 3
3. Background and Related Protocols ............................ 4
4. Terminology ............................................. 4
5. Conceptual Data Structures .................................. 5
   5.1. Binding State Table (BST) ............................... 5
   5.2. Filtering Table (FT) .................................... 5
   5.3. Binding State Description ............................... 6
6. Anchor Attributes ........................................... 6
   6.1. SAVI-Validation Attribute ............................... 6
   6.2. SAVI-DHCP Trust Attribute ............................... 6
7. Binding Specification ....................................... 6
   7.1. Process of DHCP-PD Snooping ............................ 6
      7.1.1. Initialization ...................................... 6
      7.1.2. From START to BOUND ................................ 7
      7.1.3. State transition from BOUND ......................... 8
   7.2. State Machine for DHCP-PD Snooping .................... 9
8. Filtering Specification ...................................... 9
   8.1. Data Packet Filtering ................................... 9
   8.2. Control Packet Filtering ................................. 9
9. Other Events .............................................. 10
   9.1. Port Down Event ....................................... 10
   9.2. Port Up Event .......................................... 10
   9.3. Binding Number Limit ................................... 10
   9.4. SAVI Device Failure .................................... 10
10. Security Considerations .................................... 10
11. References ............................................... 10
   11.1. Normative References ................................ 10
   11.2. Informative References ................................. 10
Authors’ Addresses ........................................... 12
1. Introduction

This document specifies the procedure for creating bindings between a DHCPv6 [RFC3633] assigned source IPv6 prefix and an anchor (refer to [SAVI Framework]).

These bindings can be used to filter packets with forged IPv6 prefixes. The use of these bindings are specified in [SAVI Framework]. The definition and examples of anchor is also specified in [SAVI Framework].

This binding process is applicable to a SAVI switch in the path between a Requesting Router and Delegating Router. In a broadband access network, the CPE-R is the requesting router, access router is delegating router and there maybe SAVI switches in between.

2. Mechanism and Architecture Context

2.1. Mechanism Overview

The mechanism specified in this document is designed to provide IPv6 prefix validation as a supplement to BCP38. The broadband access network consists of CPE-R (Requesting Router), access router (Delegating Router) and SAVI access device in between. This mechanism is deployed on the access device (such as DSLAM, OLT, etc.), and performs DHCPv6 snooping of prefix delegation to setup bindings between the assigned IPv6 prefix and corresponding anchors. The bindings can be used to validate the source prefix in the packets.

2.2. Architecture Context
Figure 1: Provider Network Architecture

Figure 1 shows a network topology in which prefix delegation maybe used. The provider network consists of access Routers (AR) and switches. CPE-Rs are located at the boundary of the customer network. Hosts in the customer network are attached to the CPE-R.

The CPE-R behaves as a router for hosts attached to it (i.e. CPE-R is the router for H). A host attached to an CPE-R uses prefixes that are advertised by the CPE-R. These prefixes are in turn delegated to the CPE-R using [RFC3633]. Details of prefix delegation, and other address configuration mechanisms for CPE-R are described in [I-D.ietf-v6ops-ipv6-cpe-router].

A switch in the provider network terminates access lines and aggregates connections. A SAVI-Device may be placed in the switch. The access router is the first router in the provider network. The provider network should be able to verify if packets from the CPE-R belong to the prefix delegated by the access router.

3. Background and Related Protocols

This mechanism is an instance of a SAVI [SAVI Framework] solution specialized for IPv6 prefixes assigned using DHCPv6 prefix delegation protocol.

In IPv6, the requesting router node must still assign its link-local address through IPv6 Stateless Autoconfiguration [RFC4862]. [RFC4861] Neighbor Discovery Protocol may be used for duplicate address detection of the link local address. A DHCP client in the requesting router may use this link-local address to send a message to the DHCP server. This mechanism concerns DHCPv6 messages used for prefix delegation.

4. Terminology

Host: A network device that connects to the service provider network through a residential gateway.

User: An entity that attaches to the network using one or more hosts. The user is usually the subscriber that owns the CPE-Router.

CPE-Router: Gateway device located at the edge of the customer network and is an IP router. For a user within the customer network, the CPE-R is a gateway to the service provider network.
5. Conceptual Data Structures

This section describes a set of conceptual data structures that are necessary for this mechanism.

Two key data structures are used to record bindings and their states. The Binding State Table (BST) contains entries populated based on snooping the RFC3633 protocol. The Filtering Table (FT) contains bindings used to filter data plane traffic.

5.1. Binding State Table (BST)

This table contains the state of bindings between source IPv6 prefix and anchor. Entries are keyed on anchor and source IPv6 prefix. Each entry has length of prefix, lifetime field containing the lifetime of the entry, a field recording the state of the binding, the default Router interface MAC address and a field for other information.

```
+--------+--------+--------+-------+----------+--------+
| Anchor | Prefix | Length | State | Lifetime | Other  |
+--------+--------+--------+-------+----------+--------+
| A      | IP_1   | 56     | Bound | 65535    |        |
+--------+--------+--------+-------+----------+--------+
| A      | IP_2   | 56     | Bound | 10000    |        |
+--------+--------+--------+-------+----------+--------+
| B      | IP_3   | 60     | _Start| 1        |        |
+--------+--------+--------+-------+----------+--------+
```

Figure 2: Instance of BST

5.2. Filtering Table (FT)

This table contains the bindings between anchor and prefix/length, keyed on anchor. This table does not contain any state of the binding. It is used to filter packet.
### 5.3. Binding State Description

This section describes the binding states of this mechanism.

- **START** A DHCPv6 request with IA_PD is received from customer router.
- **BOUND** The prefix is assigned to the customer and bound to the anchor.

### 6. Anchor Attributes

This section specifies the anchor attributes involved in this mechanism.

#### 6.1. SAVI-Validation Attribute

The SAVI-Validation attribute should be set if and only if source prefix validation must be performed on traffic from this anchor.

#### 6.2. SAVI-DHCP Trust Attribute

The SAVI-DHCP Trust attribute must be set if and only if an anchor is associated with a trustable DHCP server/relay.

### 7. Binding Specification

This section specifies the procedure of setting up bindings based on snooping [RFC3633].

#### 7.1. Process of DHCP-PD Snooping

#### 7.1.1. Initialization

This procedure is not performed if an unspoofable MAC is used as anchor (802.11i, 802.1ae/af). If not, DHCPv6 MUST be snooped for prefix delegation option.
7.1.1.1. Trigger Event

A DHCPv6 REQUEST/option code OPTION_IA_PD is received on an anchor for which the SAVI-Validation attribute has been set.

7.1.1.2. Message Validation

The SAVI device checks the REQUEST message for the following:
1. Will the limitation on binding entry number of this anchor be exceeded.

7.1.1.3. Following Actions

Allow forwarding the REQUEST message if the binding entry limit is not exceeded.

Generate an entry in the Binding State Table (BST) and set the state field to START. The lifetime of this entry is set to MAX_DHCP_RESPONSE_TIME. The Transaction ID field of the request packet is also recorded in the entry.

+--------+--------+--------+-------+-----------------------+-------+
| Anchor | Prefix | Length | State | Lifetime              |Other  |
|--------+--------+--------+-------+-----------------------+-------|
| A      |        |        | START |MAX_DHCP_RESPONSE_TIME | TID   |
+--------+--------+--------+-------+-----------------------+-------+

Figure 4: Binding entry in BST on initialization

The transaction ID (TID) is kept for assurance that the response from the DHCP server can be matched to the prefix delegation requesting router.

7.1.2. From START to BOUND

7.1.2.1. Trigger Event

A DHCPv6 REPLY message is received with option code OPTION_IA_PD.

7.1.2.2. Message Validation

The SAVI device checks the REPLY message for the following:
1. Whether the message is received with an anchor which has the SAVI-DHCP-Trust attribute.
2. Whether an entry in the BST with corresponding TID is in the START state.

7.1.2.3. Following Actions

Deliver the message to the destination.

Set the state of the corresponding entry to BOUND. The lifetime of the entry is set to value of valid lifetime in OPTION_IAPREFIX. This lease time is recorded in the entry.

<table>
<thead>
<tr>
<th>Anchor</th>
<th>Prefix</th>
<th>Length</th>
<th>State</th>
<th>Lifetime</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>IP_1</td>
<td>56</td>
<td>BOUND</td>
<td>OPTION_IAPREFIX: valid-lifetime</td>
<td>Lease</td>
</tr>
</tbody>
</table>

Figure 5: Binding entry in BST on assignment

An entry is inserted into the filtering table if the assigned prefix is not bound to another anchor.

<table>
<thead>
<tr>
<th>Anchor</th>
<th>Prefix</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>IP_1</td>
<td>56</td>
</tr>
</tbody>
</table>

Figure 6: Binding Entry in FT on assignment

7.1.3. State transition from BOUND

Whenever a DHCPv6 RELEASE is received from the host, if the state of the entry is BOUND, the entry is deleted in the BST and FT.

If DHCPv6 REPLY with Renew is received from the server, set lifetime of entry in BST with the new valid lifetime in OPTION_IAPREFIX.

If the lifetime of an entry in with state BOUND expires, delete the entry in BST and FT.
7.2. State Machine for DHCP-PD Snooping

<table>
<thead>
<tr>
<th>State</th>
<th>Message/Event</th>
<th>Action</th>
<th>Next State</th>
</tr>
</thead>
<tbody>
<tr>
<td>_*</td>
<td>REQUEST/CONFIRM</td>
<td>Set up new Entry</td>
<td>START</td>
</tr>
<tr>
<td>START</td>
<td>REPLY</td>
<td>Record Lease time</td>
<td>BOUND</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enter in FT</td>
</tr>
<tr>
<td>START</td>
<td>Timeout</td>
<td>Remove Entry</td>
<td>-</td>
</tr>
<tr>
<td>BOUND</td>
<td>RELEASE</td>
<td>Remove Entry</td>
<td>-</td>
</tr>
<tr>
<td>BOUND</td>
<td>Lease timeout</td>
<td>Remove Entry</td>
<td>-</td>
</tr>
<tr>
<td>BOUND</td>
<td>RENEW (Reply)</td>
<td>Set new Lease time</td>
<td>BOUND</td>
</tr>
</tbody>
</table>

Figure 7

8. Filtering Specification

8.1. Data Packet Filtering

Data packets with an anchor which has attribute SAVI-Validation MUST be checked.

If the source prefix of a packet associated with its anchor is in the FT, this packet SHOULD be forwarded; else the packet MUST be discarded.

8.2. Control Packet Filtering

For anchors with SAVI-Validation attribute:

The source address of DHCPv6 Request/Confirm MUST be an address associated with the corresponding anchor in FT. The source address of DHCPv6 Solicit MUST be the link layer address bound to the corresponding anchor. The link layer address MAY be bound based on SAVI-SLAAC solution.

All DHCPv6 Reply packets MUST be from anchor with the SAVI-DHCP-Trust attribute.
9. Other Events

9.1. Port Down Event

When a port with attribute SAVI-Validation goes down, the bindings with the anchor MUST be kept for a short time. If the port comes back up during this period, the prefix is still active.

9.2. Port Up Event

When a port with attribute SAVI-Validation comes up after a failure, the bindings with the anchor in BST and FT are populated as in initialization.

9.3. Binding Number Limit

9.4. SAVI Device Failure

10. Security Considerations

This document does not introduce any new vulnerabilities to IPv6 specifications or operation. Source address validation of hosts attached to various access networks supported by the fixed broadband network architecture is the subject of these specifications.

11. References

11.1. Normative References


11.2. Informative References

[I-D.ietf-v6ops-ipv6-cpe-router]


Authors’ Addresses

John Kaippallimalil
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX  75075
Phone: +1 214-606-2005
Email: jkaippal@huawei.com

Frank Xia
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX  75075
Phone: +1 972-509-5599
Email: xiayangsong@huawei.com

Jun Bi
CERNET
Network Research Center, Tsinghua University
Beijing,  100084
Phone: +1 972-509-5599
Email: junbi@cernet.edu.cn