A SAVI Solution for DHCP

Draf-ietf-savi-dhcp-06
J. Bi, J. Wu, G. Yao, F. Baker
IETF79, Beijing
Nov. 9, 2010
Outline

• Solution Overview

• Major revision since IETF78
  – Mechanism is modified to DHCP-only scenario. Correspondingly, Detection and Live states are removed

• Next Step
Solution Overview
Typical Scenario

The Router or SAVI device may also play the role of DHCP Relay (or even DHCP server) in implementation.
## Anchor Attributes

**Attribute**: Configurable features of anchor (e.g. SAVI switch port).
- An anchor may be configured to have one or more compatible attributes, depending on the requirement of administrator.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No attribute(by default)</td>
<td>Default dropping DHCP server type message</td>
</tr>
<tr>
<td>SAVI-Validation</td>
<td>Snooping &amp; Filtering</td>
</tr>
<tr>
<td>SAVI-SAVI</td>
<td>No binding and no filtering</td>
</tr>
<tr>
<td>SAVI-DHCP-Trust</td>
<td>Trust DHCP server type message</td>
</tr>
<tr>
<td>SAVI-BindingRecovery</td>
<td>Recovery binding triggered by data packet (not MUST)</td>
</tr>
<tr>
<td>SAVI-ExtSnooping</td>
<td>Recovery binding triggered by other control packets</td>
</tr>
</tbody>
</table>
States

• INIT
  – The state before a binding has been set up.
• START
  – A DHCP request (or a DHCPv6 Confirm, or a DHCPv6 Solicitation with Rapid Commit option) has been received from host, and it may trigger a new binding.
• BOUND
  – The address has passed duplicate detection and it is bound with the binding anchor.
• Two states are removed from state machine because this document is for dhcp-only scenario
  – Detection state
  – Live state
Events

• **Timer expiration event**
  – EVE_ENTRY_EXPIRE: The lifetime of an entry expires

• **Control message arriving event**
  – EVE_DHCP_REQUEST
  – EVE_DHCP_CONFIRM
  – EVE_DHCP_OPTION_RC
  – EVE_DHCP_REPLY
  – EVE_DHCP_REPLY_NULL
  – EVE_DHCP_DECLINE
  – EVE_DHCP_RELEASE
  – EVE_DHCP_REPLY_RENEW
Implemented, tested, and deployed

- It became a feature of multiple vendors: ZTE, Huawei, H3C (3Com), Ruijie, Digital China, Bitway, Centec
- CERNET2 had formally tested those implementations: Conformance, Performance, Interoperability, and testing in production network after deployment
- China Telecom and China Mobile are also testing in their IPv6 networks
Deployment Example: Tsinghua Univ. Campus Network

10 savi device models form different vendors at 3 scenarios

DHCPv6-relay
H3C(3COM): DHCPv6-only
Digital China: DHCP-SLAAC-mix

[ZJ14-L01-F-01]display ip check source ipv6
Total entries found: 5

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Interface</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>001c-b3ab-6162</td>
<td>FE80::21C:B3FF:FEAB:6162</td>
<td>1</td>
<td>GE1/0/5</td>
<td>ND-SNP</td>
</tr>
<tr>
<td>940c-6d74-c244</td>
<td>FE80::960C:6DFF:FE74:C244</td>
<td>1</td>
<td>GE1/0/7</td>
<td>ND-SNP</td>
</tr>
<tr>
<td>0022-156c-ba34</td>
<td>FE80::222:15FF:FE6C:BA34</td>
<td>1</td>
<td>GE1/0/9</td>
<td>ND-SNP</td>
</tr>
<tr>
<td>0011-2517-fe6b</td>
<td>2402:F000:5:C801:3463:B3D8:E63</td>
<td>1</td>
<td>GE1/0/14</td>
<td>DHCPv6-SNP</td>
</tr>
<tr>
<td></td>
<td>2402:F000:5:C801:3463:B3D8:E63</td>
<td>1</td>
<td>GE1/0/17</td>
<td>ND-SNP</td>
</tr>
</tbody>
</table>

[ZJ14-L05-F-05]#show savi ipv6 check source binding
static binding count: 0
Dynamic binding count: 8
Binding count: 8

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Port</th>
<th>Type</th>
<th>State</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>90-66-0a-78-f2-06</td>
<td>2402:f000:5:ca01:d999:3fae:bf36:4178</td>
<td>1</td>
<td>Ethernet1/14</td>
<td>dhcp</td>
<td>BOUND</td>
<td>1012389</td>
</tr>
<tr>
<td>90-66-0a-78-f2-06</td>
<td>fe80::14df:55e9:2639:43ba</td>
<td>1</td>
<td>Ethernet1/14</td>
<td>sLaac</td>
<td>BOUND</td>
<td>4374</td>
</tr>
<tr>
<td>90-e6-0a-78-f2-06</td>
<td>2402:f000:5:ca01:14df:55e9:2639:43ba</td>
<td>1</td>
<td>Ethernet1/14</td>
<td>sLaac</td>
<td>BOUND</td>
<td>14276</td>
</tr>
<tr>
<td>90-e6-0a-78-f2-06</td>
<td>2402:f000:5:ca01:2840:a378:d686:fc0b</td>
<td>1</td>
<td>Ethernet1/14</td>
<td>sLaac</td>
<td>BOUND</td>
<td>14276</td>
</tr>
<tr>
<td>c8-0a-94-41-b5-a1</td>
<td>2402:f000:5:ca01:639b:f7c8:7999:13c8</td>
<td>1</td>
<td>Ethernet1/21</td>
<td>dhcp</td>
<td>BOUND</td>
<td>1036459</td>
</tr>
<tr>
<td>c8-0a-94-41-b5-a1</td>
<td>fe80::c1d8:1a95:45b2:b883</td>
<td>1</td>
<td>Ethernet1/21</td>
<td>sLaac</td>
<td>BOUND</td>
<td>14058</td>
</tr>
<tr>
<td>c8-0a-94-41-b5-a1</td>
<td>2402:f000:5:ca01:8c12:15a3:553e:f8a5</td>
<td>1</td>
<td>Ethernet1/21</td>
<td>sLaac</td>
<td>BOUND</td>
<td>14058</td>
</tr>
<tr>
<td>c8-0a-94-41-b5-a1</td>
<td>2402:f000:5:ca01:8c12:15a3:553e:f8a5</td>
<td>1</td>
<td>Ethernet1/21</td>
<td>sLaac</td>
<td>BOUND</td>
<td>14058</td>
</tr>
</tbody>
</table>
Next Step

• WG last call
Thank you very much!
Back up
Major revision since IETF77: Supplemental Binding Process
Supplemental Binding Process

• It is designed to handle the special case to avoid permanent blocking on legitimate traffic: packet is sent by host without previous DHCP procedure sensed by the SAVI device.

• Two approaches
  – Extend Control Packet Snooping
  – Data packet/Counter triggered
Extend Control Packet Snooping

• Other than DHCP initialization messages, other types of control packets received by SAVI device will trigger the device to perform a binding recovery process.
  – (1) Address Resolution Neighbor Solicitation; (2) Neighbor Advertisement; (3) Neighbor Unreachability Detection; (4) Multicast Listener Discovery; (5) Address Resolution Protocol; (6) DHCP Renew/Rebind. (7) Other ICMP messages that may be processed by intermediate device
Extended Control Packet Snooping

• Binding recovery process: probes sent from SAVI device:
  – (1) DAD
  – (2) DHCP LEASEQUERY, or DHCP Confirm in case of pure L2 device
• **MUST** be implemented
Data Packet/Counter Triggered

- Data Plan snooping/Counter triggers the SAVI switch to perform the binding recovery
  - Recovery process is same as the previous slide
- Potential issues
  - Vendors reported that the data packet snooping will be a heavy burden to the device
  - The potential DoS attacks against data packet snooping brought to the operator – refer to analysis messages from Fred Baker, etc. in SAVI mailing-list
Data Packet/Counter Triggered

• There may be multiple ways to achieve it, an example is refer to [draft-baker-savi-one-implementation-approach] to get the to-be-bound address and corresponding binding anchor

• Based on the poll asked by SAVI WG chair in mailing-list, the conclusion is “conditional SHOULD”

• If a vendor can implement it, it SHOULD be implemented unless the implementation is known to directly attached to host