A SAVI Solution for DHCP

Draf-ietf-savi-dhcp-06

J. Bi, J. Wu, G. Yao, F. Baker

IETF79, Beijing

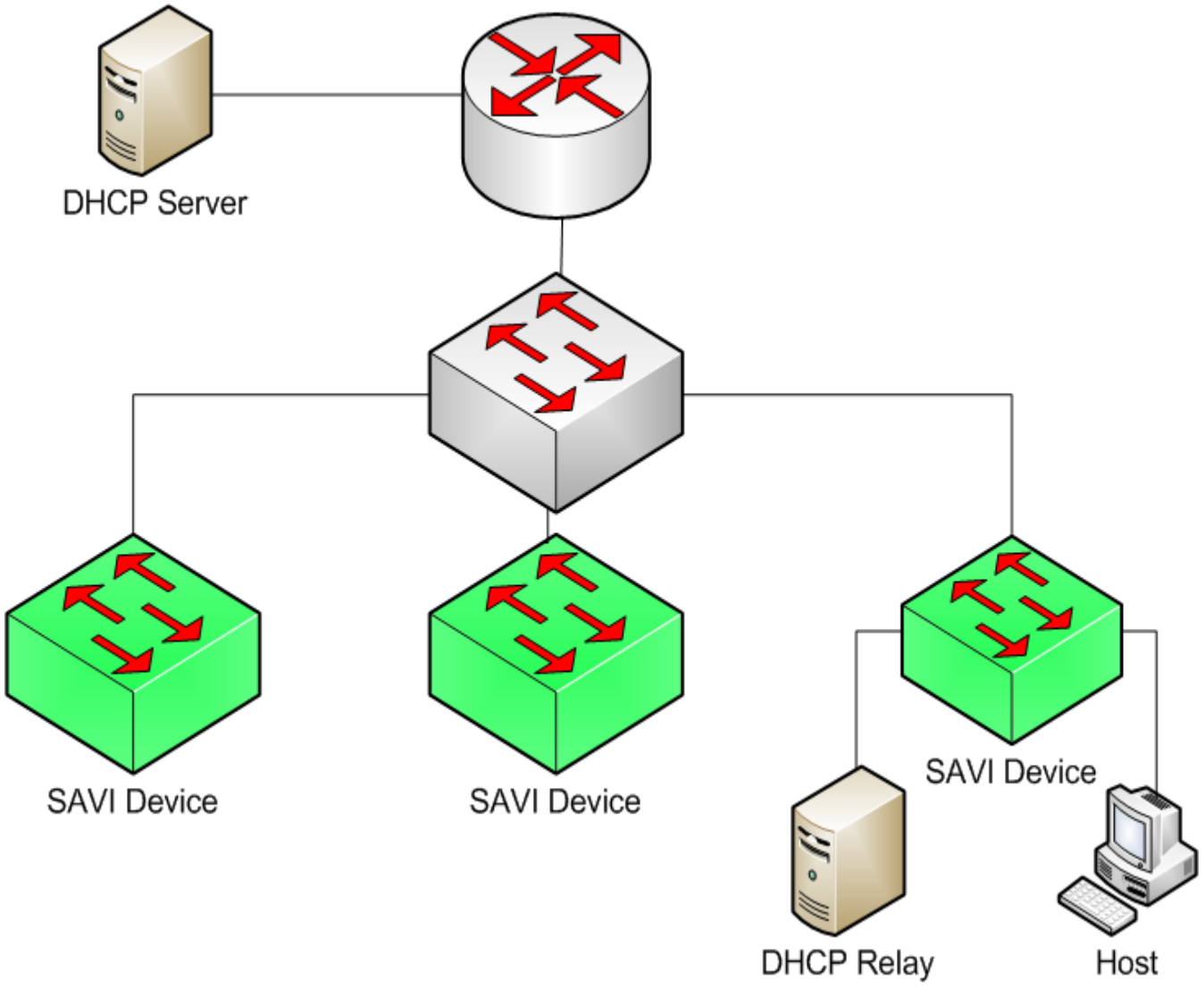
Nov. 9, 2010

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.

Attribute	Action
No attribute(by default)	Default droping DHCP server type message
SAVI-Validation	Snooping & Filtering
SAVI-SAVI	No binding and no filtering
SAVI-DHCP-Trust	Trust DHCP server type message
SAVI-BindingRecovery	Recovery binding triggered by data packet (not MUST)
SAVI-ExtSnooping	Recovery binding triggered by other control packets

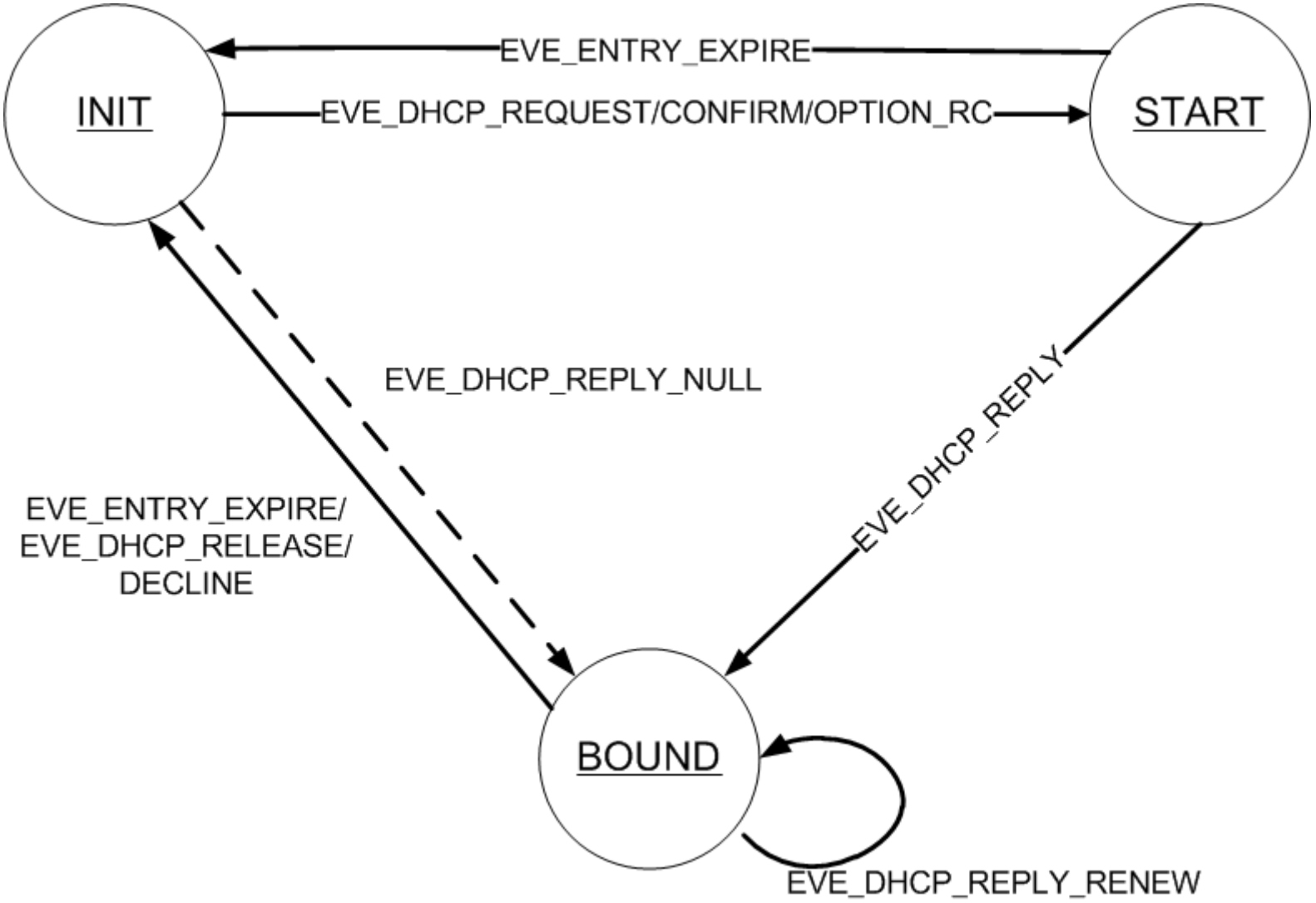
States

- 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

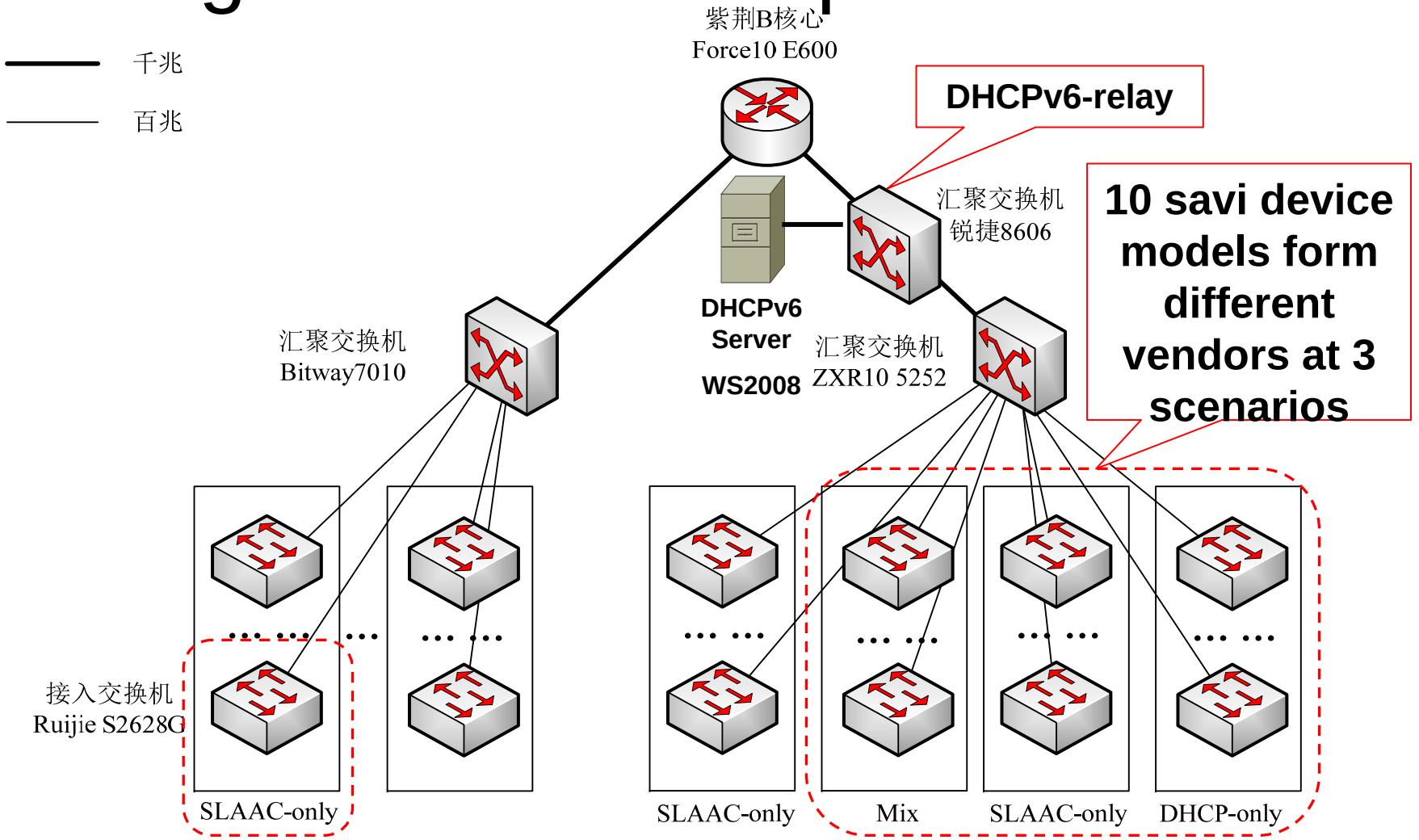
State Transit Diagram



Implemented, tested, and deployed

- It become 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



高机房，共4组，每组10台组成1个子网

低机房，共4组，每组10台组成1个子网

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

```
[ZJ14-L01-F-01]display ip check source ipv6
Total entries found: 5
 MAC Address     IP Address                          VLAN  Interface      Type
 001c-b3ab-6162  FE80::21C:B3FF:FEAB:6162             1     GE1/0/5        ND-SNP
 940c-6d74-c244  FE80::960C:6DFF:FE74:C244            1     GE1/0/7        ND-SNP
 0022-156c-ba34  FE80::222:15FF:FE6C:BA34             1     GE1/0/9        ND-SNP
 0011-2517-fe6b  2402:F000:5:C801:3463:B3D8:E63      1     GE1/0/14       DHCPv6-SNP
                 C:8FC8
 001f-d0a1-45ed  FE80::AD55:DE48:DDC9:2EDB           1     GE1/0/17       ND-SNP
```

```
ZJ14-L05-F-05#show savi ipv6 check source binding

Static binding count: 0
Dynamic binding count: 8
Binding count: 8

MAC               IP                                      VLAN Port          Type    State     Expires
-------------------------------------------------------------------------------------------------------
90-e6-ba-78-f2-06  2402:f000:5:ca01:d999:3fae:bf36:4178    1    Ethernet1/14  dhcp    BOUND     1012389
90-e6-ba-78-f2-06  fe80::14df:55e9:2639:43ba             1    Ethernet1/14  slaac   BOUND     4374
90-e6-ba-78-f2-06  2402:f000:5:ca01:14df:55e9:2639:43ba  1    Ethernet1/14  slaac   BOUND     14276
90-e6-ba-78-f2-06  2402:f000:5:ca01:2840:a378:d686:fc0b  1    Ethernet1/14  slaac   BOUND     14276
c8-0a-a9-41-b5-a1  2402:f000:5:ca01:639b:f7c8:7999:13c8  1    Ethernet1/21  dhcp    BOUND     1036459
c8-0a-a9-41-b5-a1  fe80::d1d8:1aa5:45b2:b883             1    Ethernet1/21  slaac   BOUND     14058
c8-0a-a9-41-b5-a1  2402:f000:5:ca01:d1d8:1aa5:45b2:b883  1    Ethernet1/21  slaac   BOUND     14058
c8-0a-a9-41-b5-a1  2402:f000:5:ca01:8c12:15a3:553e:f8a5  1    Ethernet1/21  slaac   BOUND     14058
```

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