SAVI for Delegated IPv6 Prefixes

draft-kaippallimalil-savi-dhcp-pd-00.txt
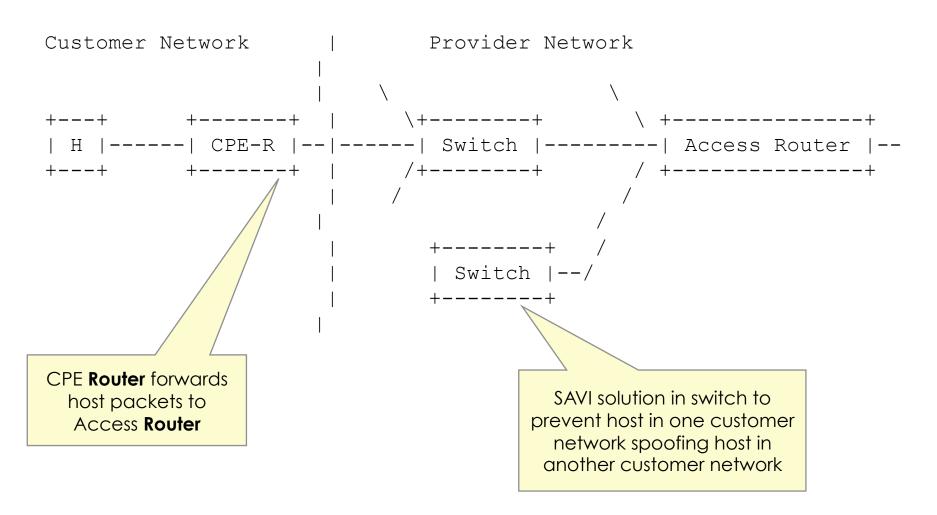
John Kaippallimalil
Frank Xia

July 2009

Problem Statement

- CPE-R obtains delegated prefix from Access Router using RFC 3633, provides individual prefixes to hosts.
  (CPE-R may also obtain other addresses using SLAAC, DHCP).

- How to validate IPv6 source address of upstream packets initiated by host, forwarded by CPE-R to Access Router (AR).

- Switch (in between CPE-R, AR) needs to ensure that IPv6 address and lower binding anchor are not spoofed.

Provider Network Architecture

```
Customer Network          |          Provider Network
                          |
                          |    \                    \
+---+        +-------+    |     \+-------+      \ +--------------+
| H |-------| CPE-R |--|------| Switch |---------| Access Router |--
+---+        +-------+    |     /+-------+      / +--------------+
                          |    /                /
                          |   /                /
                          |                   /
                          |   +--------+     /
                          |   | Switch |--/
                          |   +--------+
                          |
```

CPE **Router** forwards host packets to Access **Router**

SAVI solution in switch to prevent host in one customer network spoofing host in another customer network

3

Solution

- Solution based on snooping RFC 3633, builds binding state information
  [section 2.3]

- Determine Prefix ownership:
  Switch snoops RFC 3633 and binds an IPv6 prefix with lower level binding anchor (Line ID, MAC).
  [section 2.4 - 2.6]

- Filter Upstream Traffic:
  Switch inspects upstream traffic based on filtering rules.
  [section 3]

Solution Applicability

- Proposed solution satisfies Broadband Forum filtering for delegated prefixes:

  "..AN SHOULD inspect upstream and downstream DHCPv6 (RFC3315, RFC3633) and ND (RFC4861, 4862) per user port, discover the mapping of IPv6 prefix to MAC address and populate its IP Anti-spoofing table accordingly" (WT-177)

- Applies to access provider networks, and complies with SAVI scope:

  "…the WG is already chartered to work also on a solution for Ethernet-based broadband access networks that are used in DSL environments."

  [SAVI Charter]

- Comments?

- Interest to adopt as WG draft?

Thank you