draft-levyabegnoli-bess-evpn-savi-03

SAVI in EVPN network

IETF-120

Eric Levy-Abegnoli

Pascal Thubert

Ratko Kovacina

Goal of the draft

- The goal of the draft to describe interactions and integration between SAVI and EVPN
- SAVI (Source-Address-Validation a.k.a Source-Guard) is a mature technology described and standardized years ago, focusing on address validation at Layer 2
- SAVI has two strategies for validating source addresses:
  1. Rely on DHCP assignment “authority” to allow Source address on interface
  2. First Come First Serve (FCFS)
- SAVI provides very generic and scalable security solution, applicable equally to IPv6 & IPv4, covering DHCP, SLAAC & Static addresses, Link-Locals & Globals

Why a draft?

- Any extended layer-2 network, like EVPN, which requires Source Address validation is a use-case for SAVI, is worth explaining

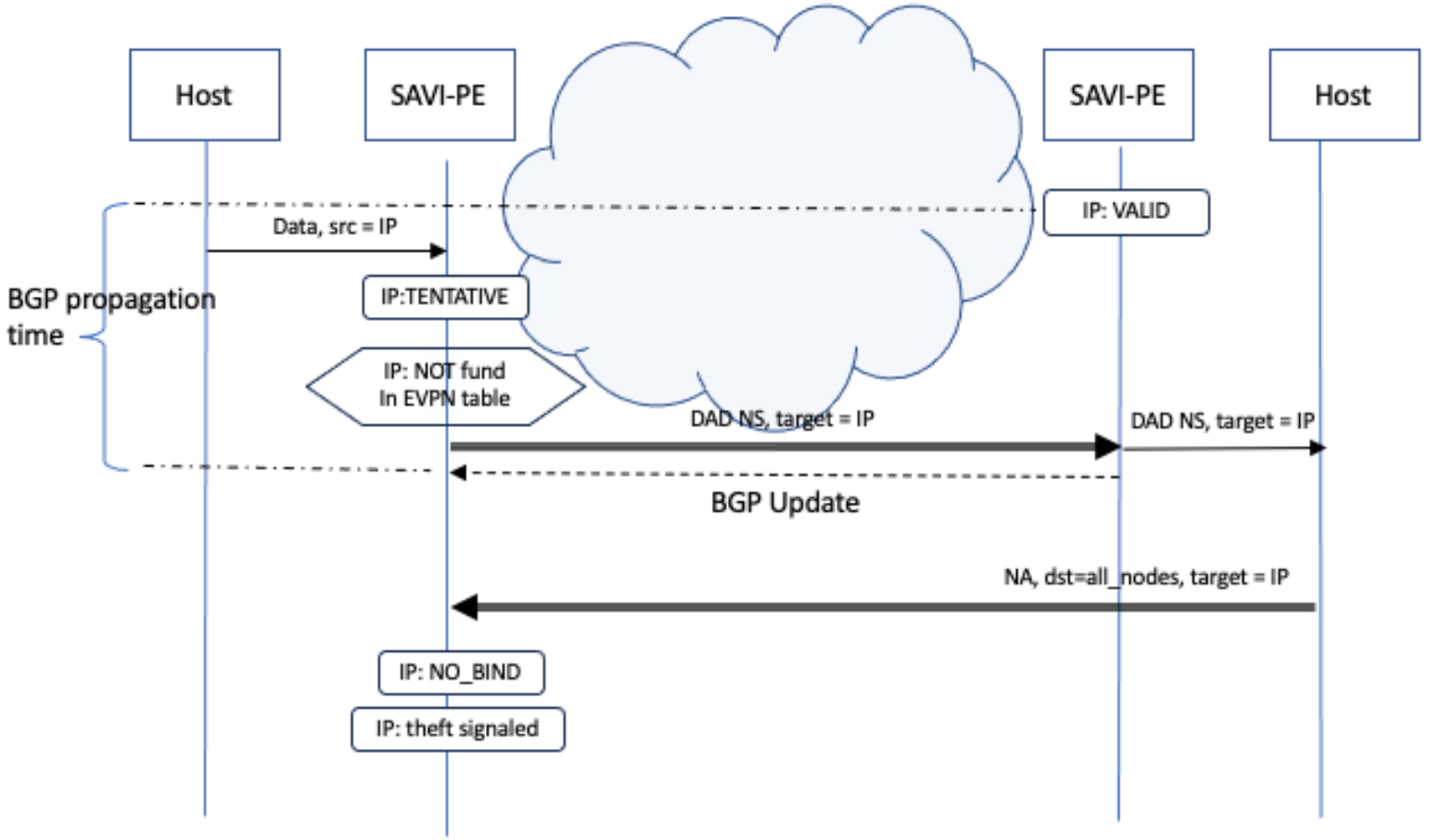
- SAVI can come without integration, however, there is a price to pay:
  - FCFS Validation rely on Link-Layer multicast over the core
  - FCFS come with a (default) 500ms delay to authorize move
  - DHCP validation requires DHCP snooping and DHCP LeaseQuery

- The integration (described in the draft) addresses points 1&2

- Another draft: draft-sajassi-bess-evpn-first-hop-security-02 addresses point 3

Summary of the updates

- Clarified section 6.2 – SAVI and EVPN integration use cases
  - Section 6.2.1 - IP address is not found in EVPN table
    - BGP propagation delay considerations



Summary of the updates

- Interaction with Duplicate IP Detection Subfunction described in RFC 9161
  - When SAVI function is implemented, the ARP/NP Proxy Subfunction - Duplicate IP Detection - as described in RFC 9161 will never kick in.
- Added a section on interaction with SAVNET
- Some naming convention updates

Next Steps

- Request feedback / comments from WG members
- Consider WG adoption

THANK YOU