SAVI in an EVPN network

IETF-118

E. Levy-Abegnoli (Cisco)
P. Thubert (Cisco)
Ratko Kovacina (Cisco)
Goal of the draft

• The goal of the draft is to describe interactions & integration between SAVI and EVPN

• SAVI (Source-Address-Validation a.k.a Source-Guard) is a mature technology described and standardized years ago: 6 RFCs covering framework, threat analysis and protocols, v4 and v6, DHCP, SLAAC and static addresses

• SAVI scales by distributing the host database among access switches

• SAVI has two strategies for validating:
  1. Rely on DHCP assignment “authority” to allow Source address on interface
  2. First Come First Serve (FCFS)

• SAVI provides very generic 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, worth explaining.

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

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

- draft-sajassi-bess-evpn-first-hop-security addresses point 3
Next steps

- READ THE DRAFT
- QUESTIONS, COMMENTS ON ML

THANK YOU!