SAVI for Locally generated Addresses

marcelo bagnulo

SAVI WG – IETF76
Design Consideration

• Only applies to local traffic
  – Complements ingress filtering
• Aimed for SLLAC configured addresses
• No new protocols
• Address ownership based on the FCFS principle
  – Based on either first data or control packet claiming ownership of that address
SAVI enforcement perimeter
SAVI enforcement perimeter
SAVI enforcement perimeter implications

• Perimetrical security: some interfaces of a SAVI device will connect to the internal (trusted) part of the topology and other interfaces will connect to the external (untrusted) part of the topology.

• A SAVI device only verifies packets coming though one interface connected to the untrusted part of the topology.

• A SAVI device only stores binding information for the source addresses that are bound to layer-2 anchors that correspond to interfaces that connect to the untrusted part of the topology.

• SAVI uses the NSOL and NADV messages to preserve the coherency of the SAVI binding state distributed among the SAVI devices within a realm.
Types of ports

• Validating ports (VPs): when a packet is received through one of the validating ports, the SAVI processing and filtering will be executed.

• Trusted ports (TPs): packets received through trusted ports are not validated and no SAVI processing is performed in them.
Do we need other port types?

• Have been suggested:
  – Learning ports: The switch learns the address and creates bindings based on the info from that ports, but does not filter
    • Useful for routers??
  – Direct ports: ports where hosts are directly connected

• Note well that more port types implies more complexity
  – More complex _manual_ configuration of savi devices
  – much more complex state machine
Port configuration guidelines

• Ports configured as VPs:
  – Ports connected to hosts
  – Ports connected to non-SAVI switches that attach hosts

• Ports configured as TPs:
  – Ports between SAVI devices
  – Ports connected to routers
  – Ports connected to non-SAVI switches that don’t attach hosts (i.e. Only attach other SAVI devices or routers)
Main processing

• Data packets for which binding exists and matches L2 anchor
  – Forward

• Data packets for which binding does not exist or L2 binding does not match the L2 binding
  – Generate DAD-NSOL (2x) to verify who owns the address

• Control packets: DAD-NSOL for which a binding does not exist or does not match the L2 binding
  – Forward DAD-NSOL (2x) to verify who owns the address
• State info
  – IP
  – Port
  – Lifetime

• Inputs
  – VP DAD NSOL
  – VP DAD NADV
  – VP DATA PKT
  – VP’ DAD NSOL
  – VP’ DAD NADV
  – VP’ DATA PKT
  – TP DAD NSOL
  – TP DAD NADV
  – TP DATA PKT