General Source Address Validation Capabilities

draft-huang-savnet-sav-table-05

M. Huang, W. Cheng, D. Li, N. Geng, **M. Liu**, L. Chen, C. Lin

March 2024

IETF118

- ✓ **At the last meeting, we have introduced existing tools has many limitations, such as inaccurate verification and high operational overhead, because their SAV capabilities are derived from other functions, e.g., FIB, ACL.**

- ✓ **We summarize the general SAV capabilities from intra- and inter-domain SAV architectures and propose three SAV modes.**

  - ◆ **Mode 1-- source prefix allowlist that takes effect on a configured interface**
    - Contains all source prefixes are allowed coming into the interface
    - Source prefixes that are not in the allowlist are considered invalid.
    - It is suitable to interfaces with a small number of source prefixes, such as those connecting to a subnet, a stub AS, or a customer cone.

  - ◆ **Mode 2-- source prefix blocklist that takes effect on a configured interface**
    - Aims to block some invalid source prefixes coming into the interface
    - Source prefixes that are not in the blocklist are considered valid
    - This mode does not require the complete blocklist. It is suitable to interfaces that connect to ISP or the provider AS.

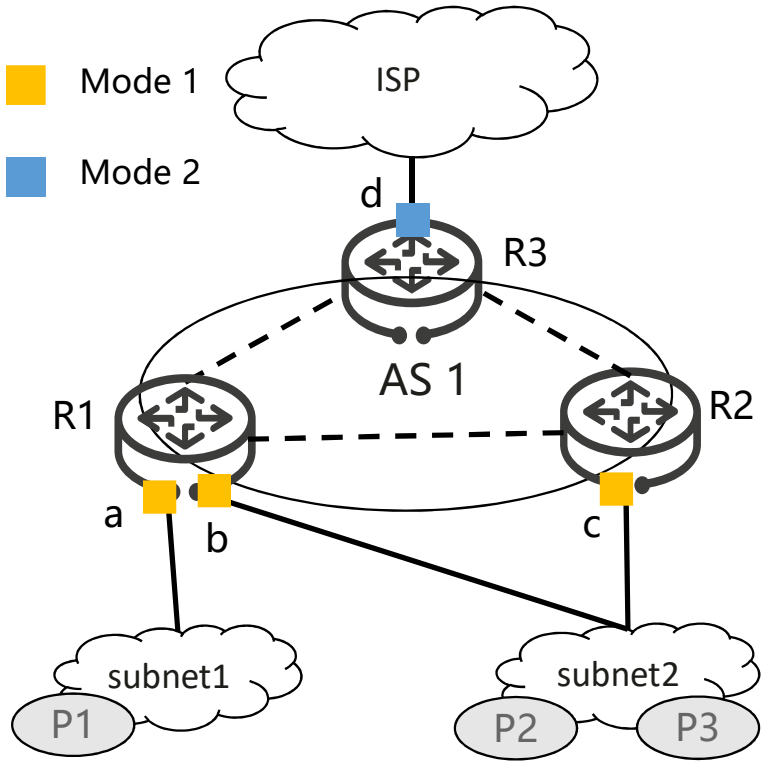
  - ◆ **Mode 3-- prefix-based interface allowlist/blocklist**
    - Mode 3 works in a router global level.
    - For a given source prefix, the traffic only be allowed coming in through the specific interface list

Main Updates

- Update the application scenario of Mode1 and Mode2
- Revise the description of Mode 3
  - Mode 3 is the prefix-based interface list. It may be an allowlist or a blocklist.
  - Mode 3 and Mode1/2 are not mutually exclusive. They have different application scopes.
- Revise the Validation Procedure section

Application Scenarios of Mode 1/2

- **Mode 1 and Mode 2 are interface-scale validation mode, aiming to filter out spoofed packets on the specific interface.**



SAV on R1	
Incoming interface	**Source prefix allowlist**
a	P1
b	P2，P3

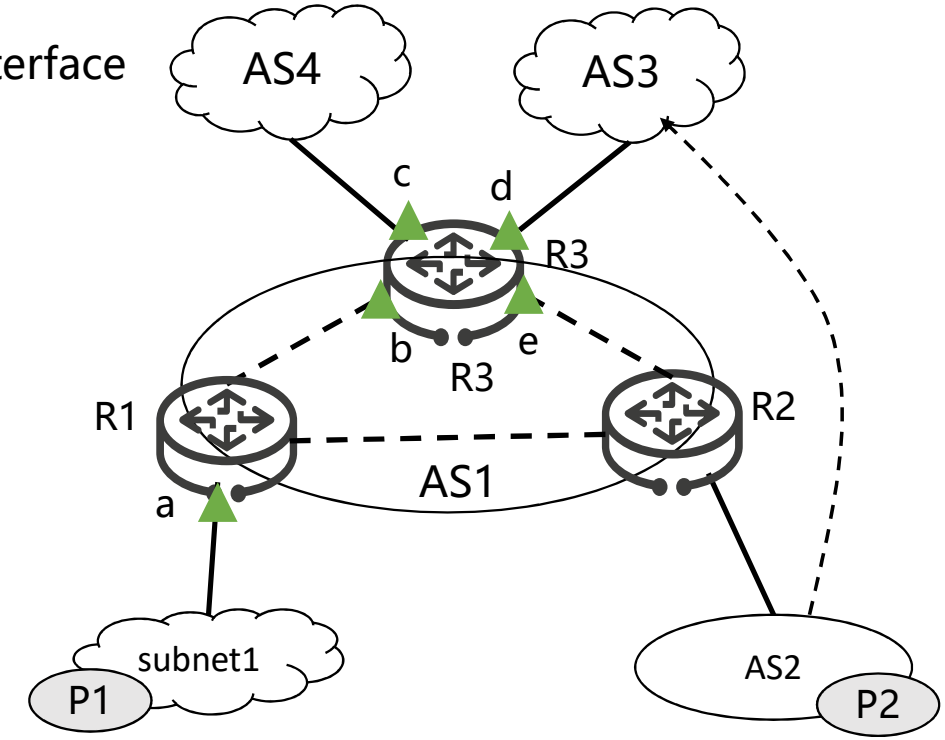
SAV on R3	
Incoming interface	**Source prefix allowlist**
c	P2, P3

SAV on R3	
Incoming interface	**Source prefix blocklist**
d	P1, P2, P3

Application Scenarios of Mode 3

- **Mode 3 is a global validation mode, aiming to filter out spoofed packets with forged specific source prefixes from all directions on a router.**
- **Mode 3 is applicable to the scenario where valid incoming interfaces of a source prefix change dynamically.**

▲ SAV-enabled interface

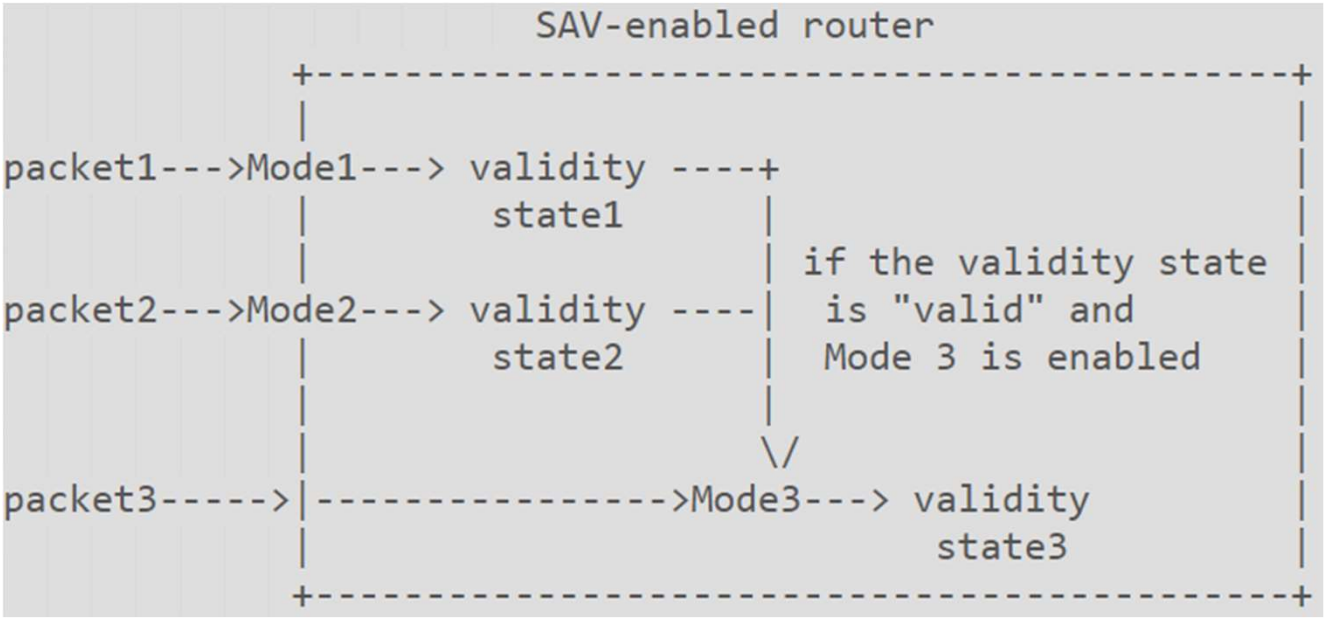


SAV on R1	
Source Prefix	**Incoming interface allowlist**
P1	a

SAV on R3	
Source Prefix	**Incoming interface blocklist**
P1	c, d
P2	Dependent on specific SAV protocol

Validation Procedure

- **When a packet arrives at the router, the router will take the source address and the incoming interface of the packet as the input and look up the SAV rules to get the validity state.**
  - Firstly, the packet is validated by the enabled interface-scale mode, i.e., Mode 1 or Mode 2. If the validity state1 or validity state2 is "invalid", the final validation state is "invalid" and the packet does not have to be validated by Mode 3.
  - If the validity state1 or validity state2 is "valid", the packet still needs to be validated by the enabled Mode 3.
  - If Mode 3 is not enabled, either the validity state1 or the validity state2 is the final validity state. If the router has only Mode 3 enable， the validity state3 is the final validity state.



Relationships with the intra- and inter-domain architecture

- The intra- and inter-domain architecture drafts
  - Focus on SAV framework and SAV rule acquisition in the control plane.
  - Do not focus on the SAV capability of the data plane
- This document
  - Focuses on general SAV capabilities of the data plane required by both intra- and inter-domain architecture.
  - Does not address the specific implementation of the data plane.
- This document summarizes the common points of the intra- and inter-domain architecture, which can guide the design and implementation of SAV solution.

Acknowledgements

- Many thanks to Joel Halpern, Aijun Wang, Fang Gao, Xiangqing Chang, Xueyan Song, etc. for their valuable comments and feedback on this document.

Next Steps

- Welcome Any questions or comments
- Ask for WG Adoption