Intra-domain Source Address Validation (SAVNET) Architecture

D. Li, J. Wu, M. Huang, L. Chen, **N. Geng**, L. Qin, F. Gao

July 2023

Update History

- About the draft: The document presents the high-level designs for future intra-domain SAV mechanisms.

- IETF 115
  - draft-li-savnet-intra-domain-architecture-00
- IETF 116
  - draft-li-savnet-intra-domain-architecture-01
  - draft-li-savnet-intra-domain-architecture-02
- IETF 117
  - draft-li-savnet-intra-domain-architecture-03

Comments on Version-01 in IETF 116

- **Joel**: We don’ t standardize component level.
- **Xueyan Song**: The SAV protocol extension is out of the scope of the WG. Suggest to focus on the framework and requirements.
- **Rüdiger Volk**: What is the security consideration, such as authentication of the speaker in the mechanism.
- **Jeff Haas**: Strongly suggest that as part of your in scope discussion about eventually using routing protocols talk about the security characteristics of the information carried. You don't necessarily want routers receiving information that is, for example, crypto signed. A solution that wants to carry the information safely in routing means that you have a solution that potentially has difficulties being deployed. Similar to the obstacles brought by crypto-based solutions.

- **IETF 116 Minutes**: https://datatracker.ietf.org/doc/minutes-116-savnet-202303290030/

Main Updates to Version-01

- Clearly define SAV-related Information and SAV-specific Information
- Remove solution-related content and more focus on communication instead of components
  - Response to Joel and Xueyan
- Add use cases to show why the architecture works
  - Follow the charter
- Add more descriptions on convergence and partial/incremental considerations
- Add more descriptions on security, manageability, and privacy considerations
  - Response to Rüdiger and Jeff

Table of Contents

Table of Contents

1. Introduction 2
2. Terminology 3
3. Design Goals 3
4. Intra-domain SAVNET Architecture 5
4.1. SAV Information Base Manager 6
4.2. RPDP and RPDP Speaker 7
5. Partial Deployment 8
6. Security Considerations 9
7. Privacy Considerations 9
8. IANA Considerations 9
9. References 9
9.1. Normative References 9
9.2. Informative References 9
Authors' Addresses 10

Version-01

Table of Contents

1. Introduction 3
1.1. Terminology 4
1.2. Requirements Language 5
2. Design Goals 5
3. SAV-Specific Information 6
4. Intra-domain SAVNET Architecture
4.1. Communication Channel . . . .
4.2. SAV-Specific Protocol . . . .
4.3. SAV Agent . . . . . .
5. Use Cases 11
5.1. Use Case 1: Validating Packets from a Multi-homed Subnet at Edge Routers 11
5.2. Use Case 2: Validating Packets from Other Networks at Border Routers 12
6. Connectivity Models 13
6.1. Example 1: Multiple Source Entities to One Validation Entity 13
6.2. Example 2: One Source Entity to Multiple Validation Entities 13
6.3. Example 3: One Acting as both Source and Validation Entity 14
7. Convergence Considerations 14
8. Incremental/Partial Deployment Considerations 15
9. Security Considerations . . . . . .
10. Manageability Considerations . . .
11. Privacy Considerations . . . . . .
12. IANA Considerations 18
13. Acknowledgements 18
14. References 18
14.1. Normative References 18
14.2. Informative References 19
Authors' Addresses 19

Focus on communication instead of components

More detailed considerations

Version-03

Design Goals

- Goal 1: Automatic Update
  - Adapt to dynamic routing changes automatically; the not much operational overhead
- Goal 2: Accurate Validation
  - Real incoming interfaces of source prefixes; Avoid false positive, reduce false negative
- Goal 3: Working in Incremental/Partial Deployment
  - Generate SAV rules when part of routers support the mechanism

- How to achieve the goals:
  - Goal2: Routing information is not enough. The information specific to SAV is needed.
  - Goal1 and Goal3: Follow and combine with uRPF-like mechanisms.

SAV-specific Information

- **SAV-specific information**: Explicitly or implicitly **indicate the accurate incoming direction of source addresses**, which helps routers generate accurate SAV rules.

- Examples of SAV-specific information
  - Topology information, e.g., hidden prefixes
  - Forwarding information, e.g., real forwarding paths
  - SAV rule, e.g., <prefix, valid interfaces>

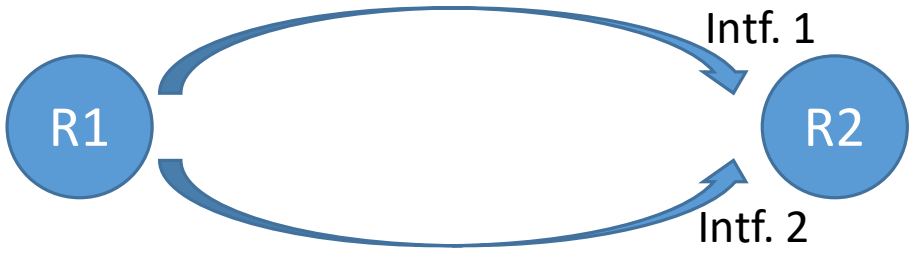
- SAV-specific information can replace or supplement routing information when routers generate SAV rules.

Main Idea of Intra-domain Architecture

Main idea:

- Besides routing information, routers automatically advertise SAV-specific information (Goal 1) for generating accurate SAV rules (Goal 2).
- Under incremental/partial deployment, combining routing and SAV-specific information (Goal 3).

Routing information: Prefix P1 has next-hop Intf. 1



SAV- specific information: Prefix P1 will arrive at Intf. 2

A simple example for Goal 1 and 2

Existing: Generate SAV rule primarily based on routing information

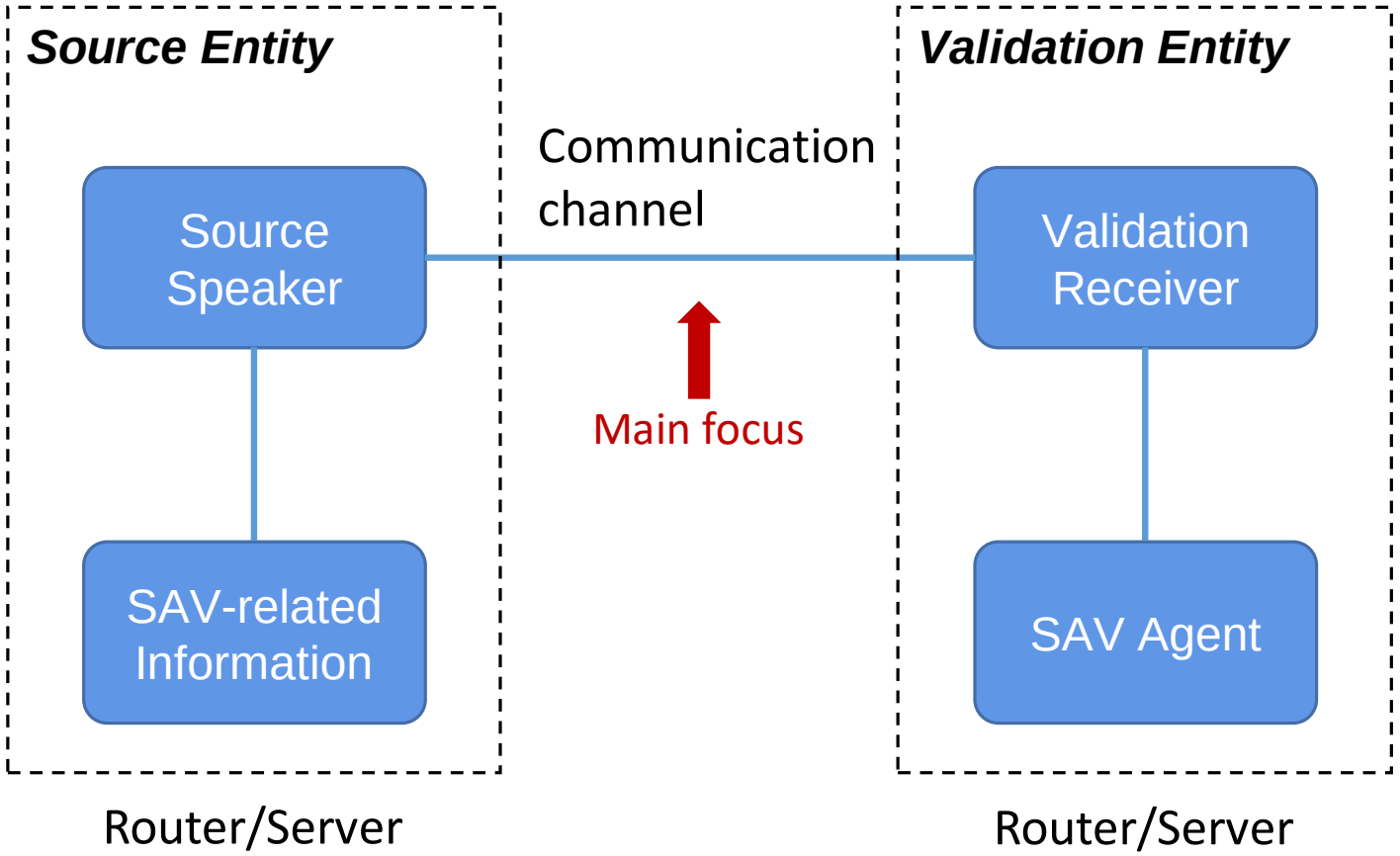
- Automatic but not accurate

New: Generate SAV rules based on SAV- specific information

- Automatic and accurate

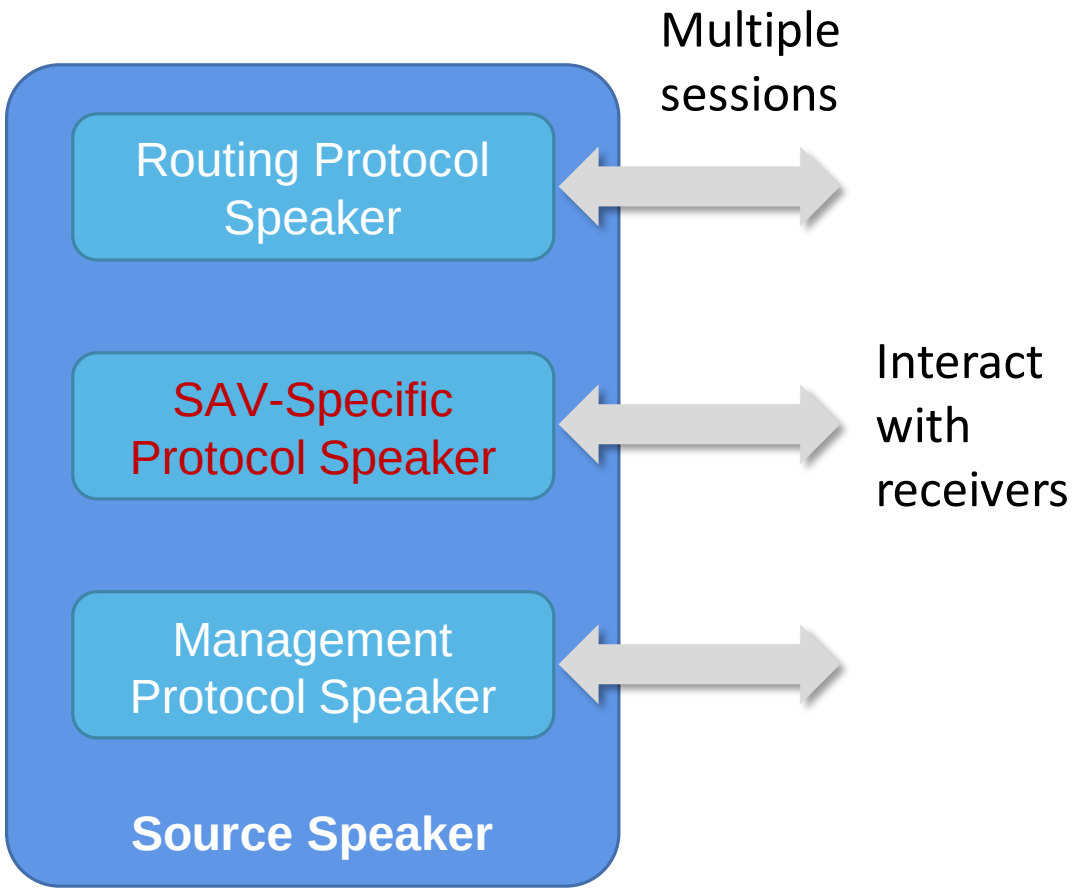
Intra-domain Architecture

- **Source Entity**: Advertise SAV-related information
- **Validation Entity**: Generate SAV rules and/or conduct validation
- **Communication channel**: Connect two entities for transmitting SAV-related information
- A device can act as a Source Entity, a Validation Entity, or both of them.



How to Advertise Information

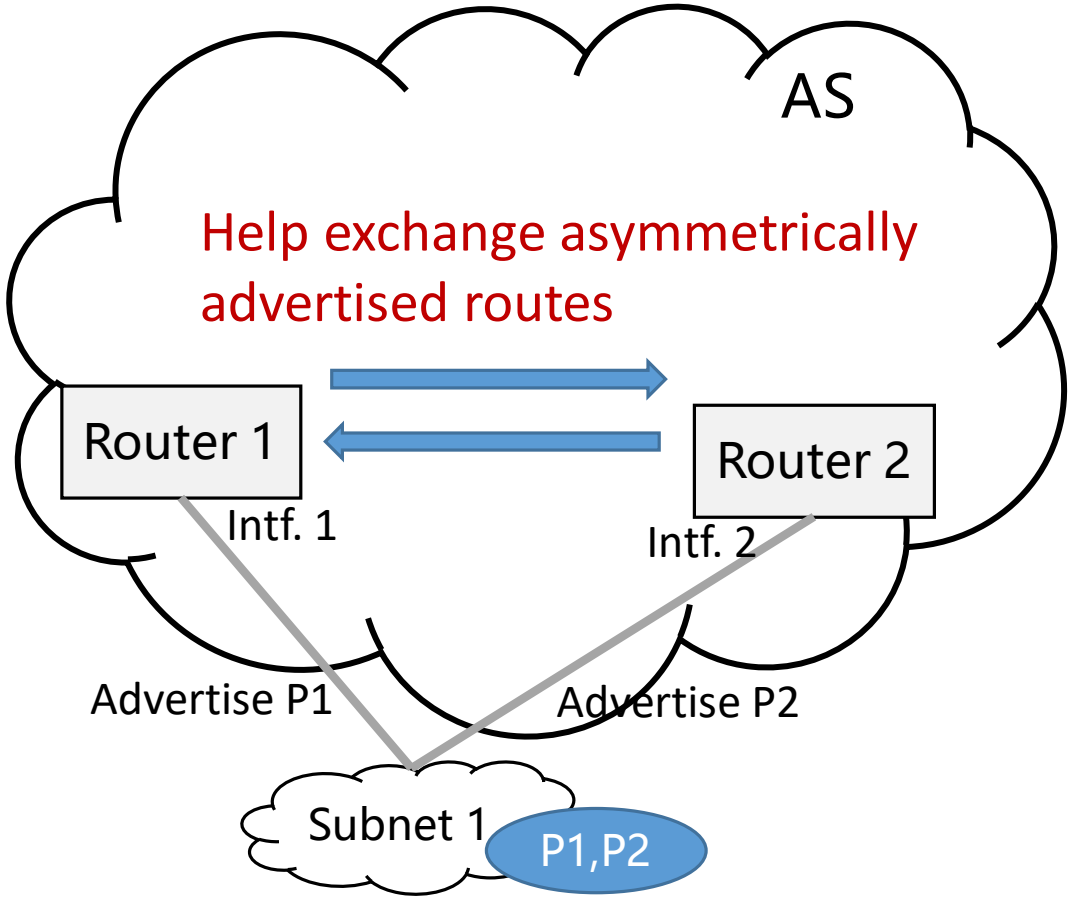
- Routing protocol
  - OSPF, IS-IS, BGP, etc.
- **SAV-specific protocol (new)**
  - Used to advertise SAV-specific information
- Management protocol
  - YANG, FlowSpec, and any other protocols for SAV



SAV-Specific Protocol

- Used for propagating SAV-specific information
- A general concept, not a specific protocol design
- For an implementation of SAV-specific protocol:
  - **SAV-specific information definitions** to be communicated
  - The **data structure or format** of the information
  - **Operations and timing** for originating, processing, propagating, and terminating messages
  - Sufficient assurance of **transmission reliability and timeliness**
  - **Authentication** can be conducted before session establishment
  - No particular limitations to connectivity models
- Concrete protocol designs or implementations are **not the focus** of this document.

Use Case 1: Validating Packets from a Multi-homed Subnet at Edge Routers



Asymmetric routing in the Multi-homed Subnet Scenario

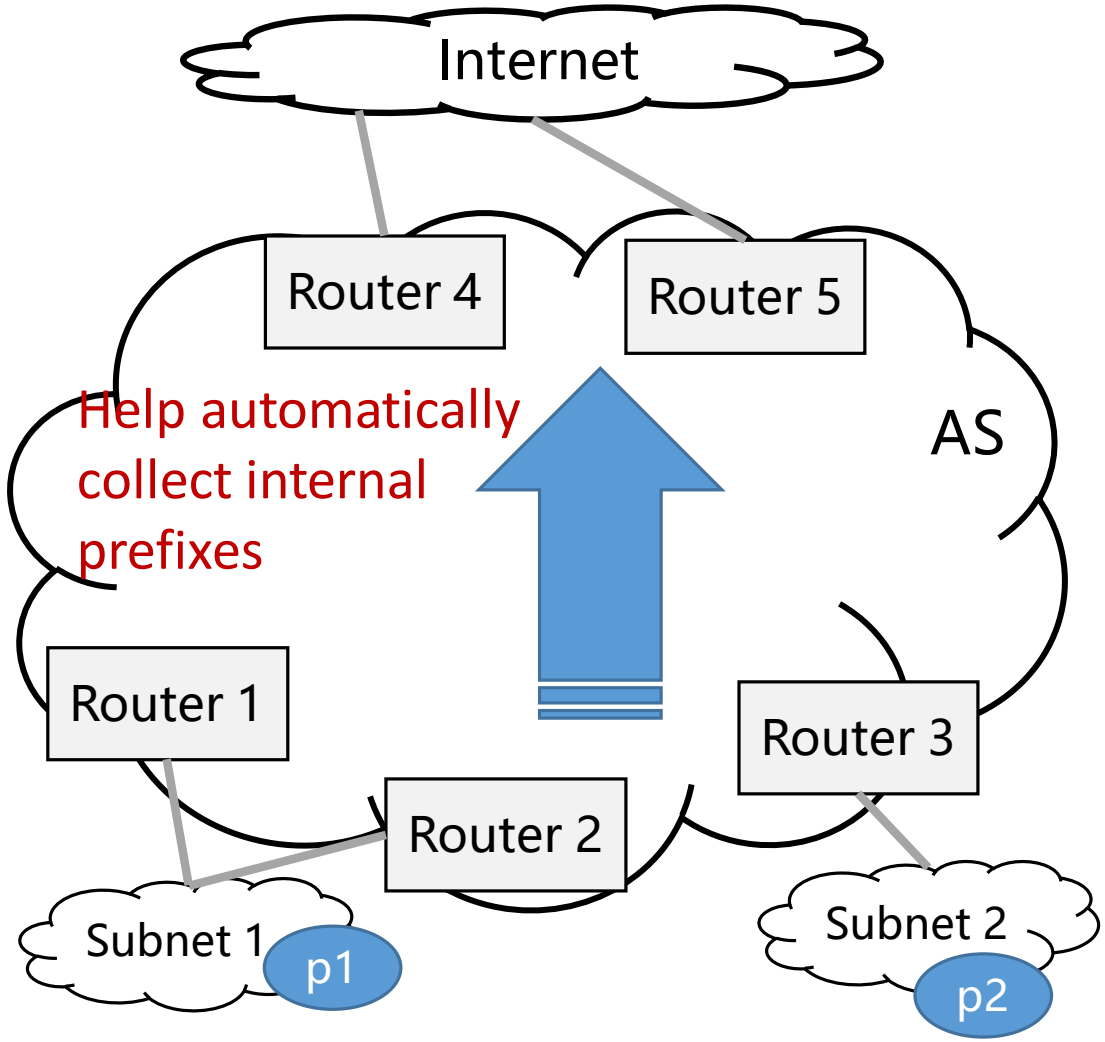
Existing: False positive (or improper block)

- Router 1 only permits P1 at Intf. 1
- Router 2 only permits P2 at Intf. 2

New: No false positive

- Router 1 and Router 2 exchange the routes advertised by Subnet 1
- Router 1 also permits P2 at Intf. 1
- Router 2 also permits P1 at Intf. 2
- Notes: The exchanging and rule generating manner should be defined in future mechanisms

Use Case 2: Validating Packets from Other Networks at Border Routers



Blocking Internal Prefixes at Internet Interfaces

Existing: Manual configurations may be required

- Configure rules to block P1 and P2 at external interfaces of Router 4 and Router 5
- Challenging in dynamic networks

New: Automatically update rules

- Router 1, Router 2, and Router 3 advertise the internal routes learned from subnets
- Router 4 and Router 5 can update rules dynamically after initial configurations
- Notes: The exchanging and rule generating manner should be defined in future mechanisms

13

Convergence Considerations

- Source Entity MUST **advertise the updates** of SAV-related information to Validation Entity in time. Then, Validation Entity MUST **update local SAV rules immediately**.

- There are some potential work directions for dealing with convergence problems:

a. Taking full use of routing information

b. Advertising and processing the information first that will probably result in false positive

Incremental/Partial Deployment Considerations

- Due to phased deployment or the limitations coming from multi-vendor supplement, not all devices support advertising SAV-specific information

- **Routing information can be used** as a supplement of SAV-specific information for SAV rule generation

- Some Other Suggestions:
  - Take on the **proper validation mode** according to the deploying of Source Entities
  - **Take appropriate actions** (drop/rate-limit/sample) on the validated data packets

Security Considerations

- **In many cases, an intra-domain network can be considered as a trusted domain.**
- Also analyze the potential threats and solutions supposing that the devices within the domain do not trust each other.
- When implementing the architecture in an extended protocol, **the existing security mechanisms of the protocol can be taken**.

Manageability Considerations

- Protocol-independent mechanisms like **YANG** SHOULD be provided

- The **diagnosis approach** and necessary **logging information** SHOULD be provided.

- Messages carrying SAV-related information come from different protocol speakers. Each corresponding protocol SHOULD have **monitoring and troubleshooting mechanisms**, which is necessary for efficiently operating the architecture.

Privacy Considerations

- Devices under the architecture will learn more forwarding information of data packets.

- An intra-domain network is mostly operated by a single organization or company, and the advertised information is only used within the network. Therefore, the architecture **does not import privacy issues** in usual cases.

- The architecture makes the forwarding information in the network clearer, which can **be helpful for network management** such as fault diagnosis and traffic visualization.

Acknowledgements

- Many thanks to the valuable comments from:
  - Igor Lubashev
  - Alvaro Retana
  - Aijun Wang
  - Joel Halpern
  - Jared Mauch
  - Kotikalapudi Sriram
  - Rüdiger Volk
  - Jeffrey Haas
  - Xiangqing Chang
  - Changwang Lin
  - etc.

Next Steps

- Comments and feedbacks are welcome
- Revise the document accordingly

Thanks!