Intra-domain Source Address Validation (SAVNET) Architecture

Dan Li, Jianping Wu, **Lancheng Qin,** Nan Geng, Li Chen,

Mingqing Huang, Fang Gao

March 19, 2024

Background

- Intra-domain SAVNET architecture aims to achieve accurate SAV in an intra-domain network by an automatic way
  - Address the problems of existing intra-domain SAV mechanisms
  - Meet the requirements proposed in [draft-ietf-savnet-intra-domain-problem-statement]
- Historical versions
  - draft-li-savnet-intra-domain-architecture-00, IETF 115 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-01, IETF 116 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-02, June 2023
  - draft-li-savnet-intra-domain-architecture-03, IETF 117 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-04, Oct 2023
  - **draft-li-savnet-intra-domain-architecture-05, IETF 118 SAVNET WG**
  - draft-li-savnet-intra-domain-architecture-06, Jan 2024
  - **draft-li-savnet-intra-domain-architecture-07, IETF 119 SAVNET WG**

Quick Review of Version-05

- Introduce intra-domain SAVNET architecture
  - SAV-related information: SAV specific information and local routing information
  - Roles of SAVNET router: source entity and validation entity
  - SAV-specific information communication mechanism
  - SAV rule generation
- Use two use cases to illustrate that intra-domain SAVNET can achieve more accurate and efficient SAV than existing intra-domain SAV mechanisms
- Describe how intra-domain SAVNET meets the five design requirements proposed in [draft-ietf-savnet-intra-domain-problem-statement]

Comments on Version-05

- Architecture improvements
  - Use **a figure to overview the overall architecture** by displaying SAV information flow in an intra-domain network (from Joel and Aijun)
  - Intra-domain architecture should **add data-plane considerations** (from Xueyan and Krishnaswamy)
- Improper or ambiguous words
  - **No need of communication channel**. You can just distribute information by using IGP (from Huaimo)
  - Clarify the **description of SAV-specific information communication mechanism** (from Xueyan)
  - **Terms** such as subnet, edge router, and border router can be **ambiguous** (from Joel)
  - Clarify that **SAV-specific information** helps generate **more accurate SAV** rules (from Joel)

Response on the Mailing List #1

[savnet] Clarification of the communication channel in intra-domain SAVNET architecture
Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Mon, 04 December 2023 08:06 UTC | Show header

[savnet] Clarification of the communication channel in intra-domain SAVNET architecture
Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Mon, 04 December 2023 08:06 UTC | Show header

Hi all,

The terminology “communication channel” in intra-domain SAVNET architecture has caused some misunderstandings, leading some to think that this is a request to establish a new channel between intra-domain routers (see https://github.com/SAVNET-ProblemStatement-Architecture/Intra-domain-SAVNET-Architecture/issues/4).

In intra-domain SAVNET architecture draft, we have clarified that the communication channel can be implemented by either a new protocol or an extension to an existing protocol. If the SAV solution uses an existing protocol, it can of course use the channel of that protocol to communicate SAV-specific information without establishing a new communication channel.

I wonder if such a clarification would avoid misunderstanding. If it's still confusing, I'll consider modifying the terminology.

Response: remove the terminology of communication channel and refine description

Response on the Mailing List #2

[savnet] Data-plane considerations in the architecture draft
Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Mon, 18 December 2023 05:40 UTC | Show header

[savnet] Data-plane considerations in the architecture draft
Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Mon, 18 December 2023 05:.. UTC | Show header

Hi all,

In IETF118 SAVNET WG meeting, Xueyan suggested that the architecture draft should add some data-plane considerations [1]. We received similar comments from Krishnaswamy after the meeting.

To address this issue, we are planning to refine the architecture draft accordingly. Since draft-huang-savnet-sav-table [2] has introduced the general SAV capabilities from data plane perspective, we plan to cite this draft and add some data-plane considerations at a high level in the updated architecture draft.

[savnet] Data-plane considerations in the archite… Lancheng Qin
Re: [savnet] Data-plane considerations in the arc… song.xueyan2
Re: [savnet] Data-plane considerations in the arc… Libin Liu
Re: [savnet] Data-plane considerations in the arc… song.xueyan2
Re: [savnet] Data-plane considerations in the arc… Lancheng Qin
Re: [savnet] Data-plane considerations in the arc… song.xueyan2
Re: [savnet] Data-plane considerations in the arc… Libin Liu
Re: [savnet] Data-plane considerations in the arc… song.xueyan2
Re: [savnet] Data-plane considerations in the arc… Libin Liu
Re: [savnet] Data-plane considerations in the arc… song.xueyan2
Re: [savnet] Data-plane considerations in the arc… Libin Liu

Response: add high-level data-plane considerations and cite [draft-huang-savnet-sav-table]

Response on the Mailing List #3

[savnet] Planned updates of intra-domain SAVNET architecture
Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Fri, 05 January 2024 08:05 UTC | Show header

[savnet] Planned updates of intra-domain SAVNET architecture
Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Fri, 05 January 2024 08:05 UTC | Show header

Hi all,

Over the past few weeks, we have been discussing how to address the issues [1] of intra-domain SAVNET architecture and refine the document. Based on the results discussed in the mailing list, we are planning to update the draft now. Here is a list of planned updates:

1. Clarify the definition of SAV-specific information communication mechanism and remove the term of communication channel.

2. Add high-level data-plane considerations about intra-domain SAV and cite draft-huang-savnet-sav-table [2]

3. Add a topology diagram to show the overall architecture of intra-domain SAVNET and explain the SAV function of different kinds of intra-domain routers.

We will revise the draft gradually and ask for comments in the mailing list. The draft will also be updated in github [3].

[savnet] Planned updates of intra-domain SAVNET a… Lancheng Qin
[savnet] Updates on Intra-domain SAVNET Architect… Lancheng Qin

Invite comments on the planned updates

Response on the Mailing List #4

[savnet] Updates on Intra-domain SAVNET Architecture

Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Sun, 21 January 2024 08:47 UTC | Show header

[savnet] Updates on Intra-domain SAVNET Architecture

Lancheng Qin <qlc19@mails.tsinghua.edu.cn> | Sun, 21 January 2024 08:47 UTC | Show heade

Hi all,

We have updated intra-domain SAVNET architecture[1] according to discussions on the mailing list.

- We remove the term of communication channel in the updated version. In addition, we replace ambiguous terms such as subnet, edge router, and border router by using clearer terms such as host network, customer network, host-facing router, customer-facing router, and AS border router.

- We add a new Section 3.5 to introduce high-level data-plane considerations about intra-domain SAVNET.

- We add a new Section 3.1. In this section, we use a figure to overview intra-domain SAVNET architecture in an intra-domain network.

Revise this document according to the comments

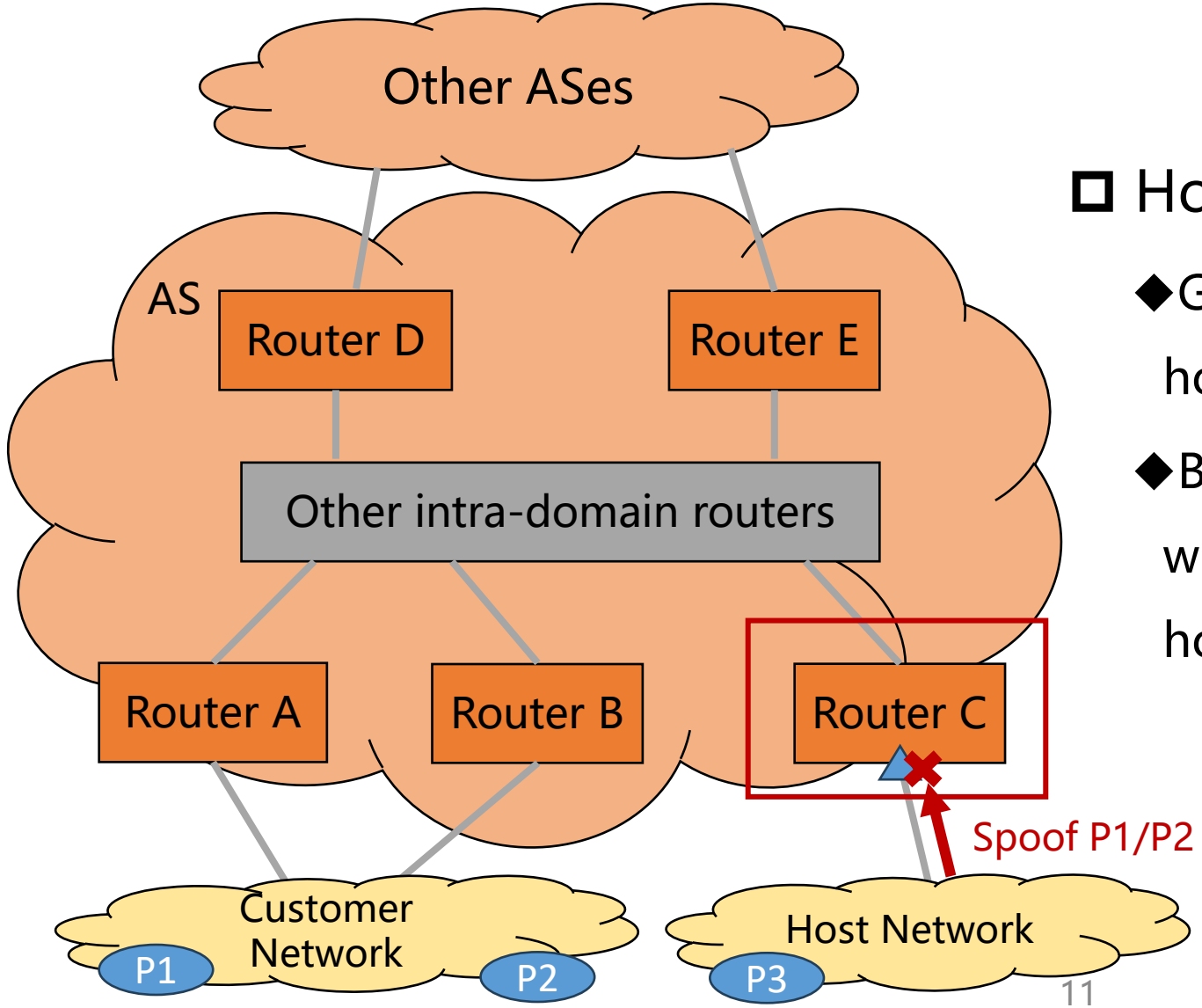
Main Updates Compared to Version-05

- Updates in Introduction section
  - Clarify that **SAV-specific information** helps generate **more accurate SAV** rules
- Updates in Terminology section
  - Add the definition of **host-facing router, customer-facing router, and AS border router**
- Updates in Intra-domain SAVNET Architecture section
  - Add **a figure to overview the overall architecture** in an intra-domain network
  - Remove the term of communication channel and **clarify the description of SAV-specific information communication mechanism**
  - Revise **Figure 3** and introduce the process of **SAV rule generation for host-facing router, customer-facing router, and AS border router**, respectively
  - Add **high-level data-plane considerations** about intra-domain SAVNET
- Updates in Use Cases section
  - Revise **Figure 4 and Figure 5** to illustrate that intra-domain SAVNET can achieve more accurate and efficient SAV on host-facing routers, customer-facing routers, and AS border routers

New Terminologies

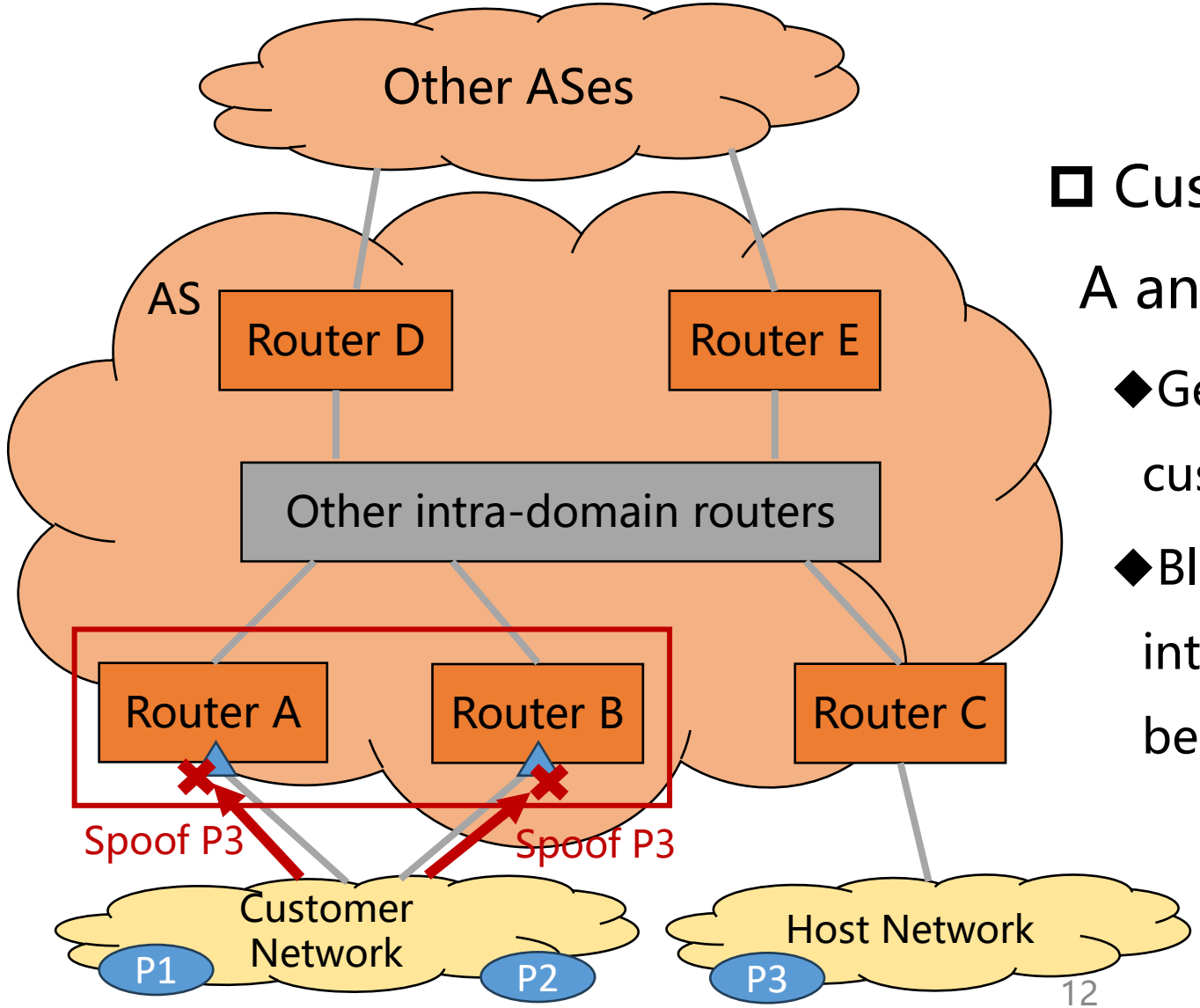
- Host-facing router
  - An intra-domain router of an AS which is connected to a host network (i.e., a layer-2 network)
- Customer-facing router
  - An intra-domain router of an AS which is connected to an intra-domain customer network running the routing protocol (i.e., a layer-3 network)
- AS border router
  - An intra-domain router of an AS which is connected to other ASes

Overview of Intra-domain SAVNET Architecture



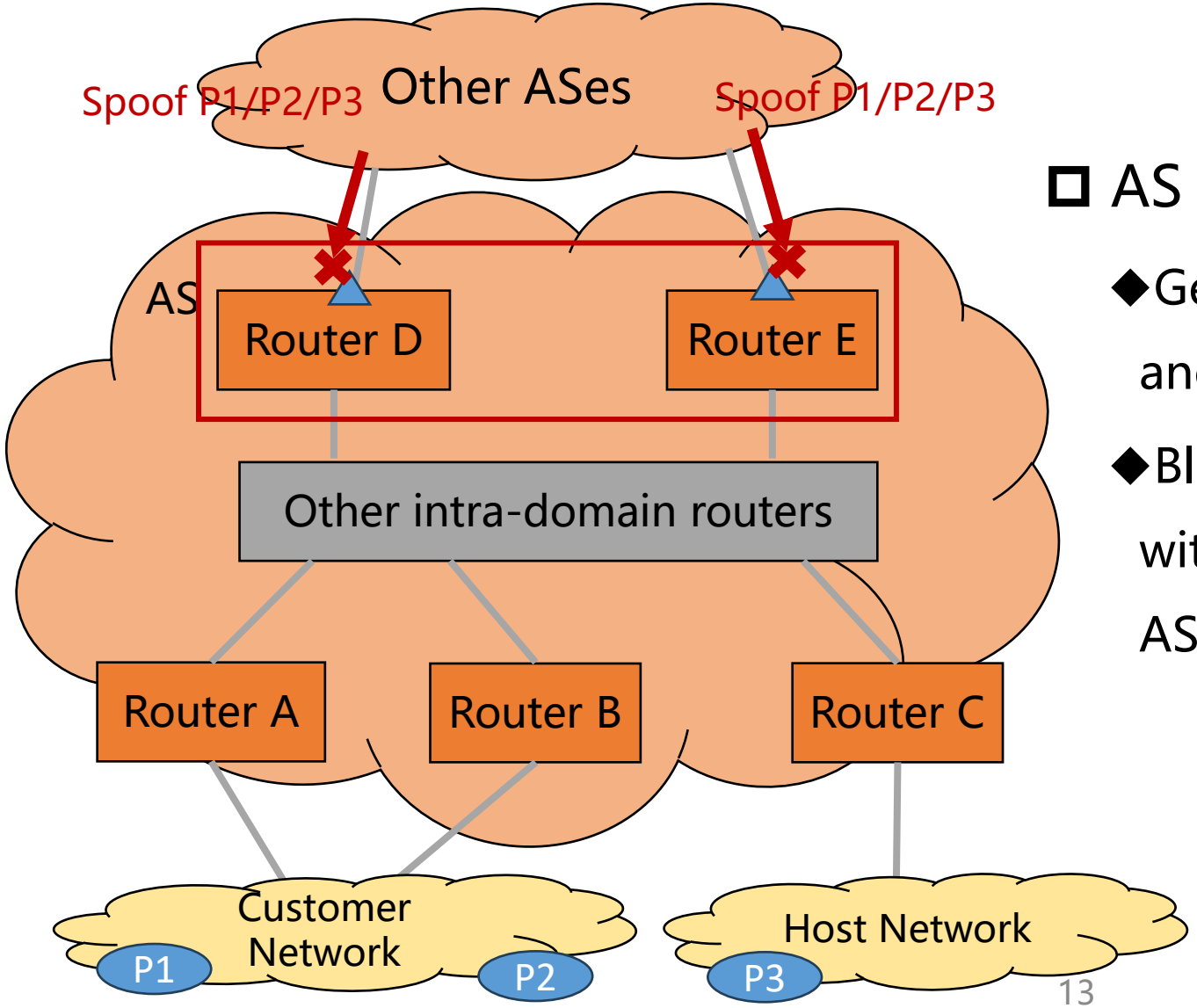
- Host-facing router (e.g., Router C)
  - Generate SAV rules on interfaces facing the host network
  - Block data packets received at those interfaces with source addresses not belonging to the host network

Overview of Intra-domain SAVNET Architecture



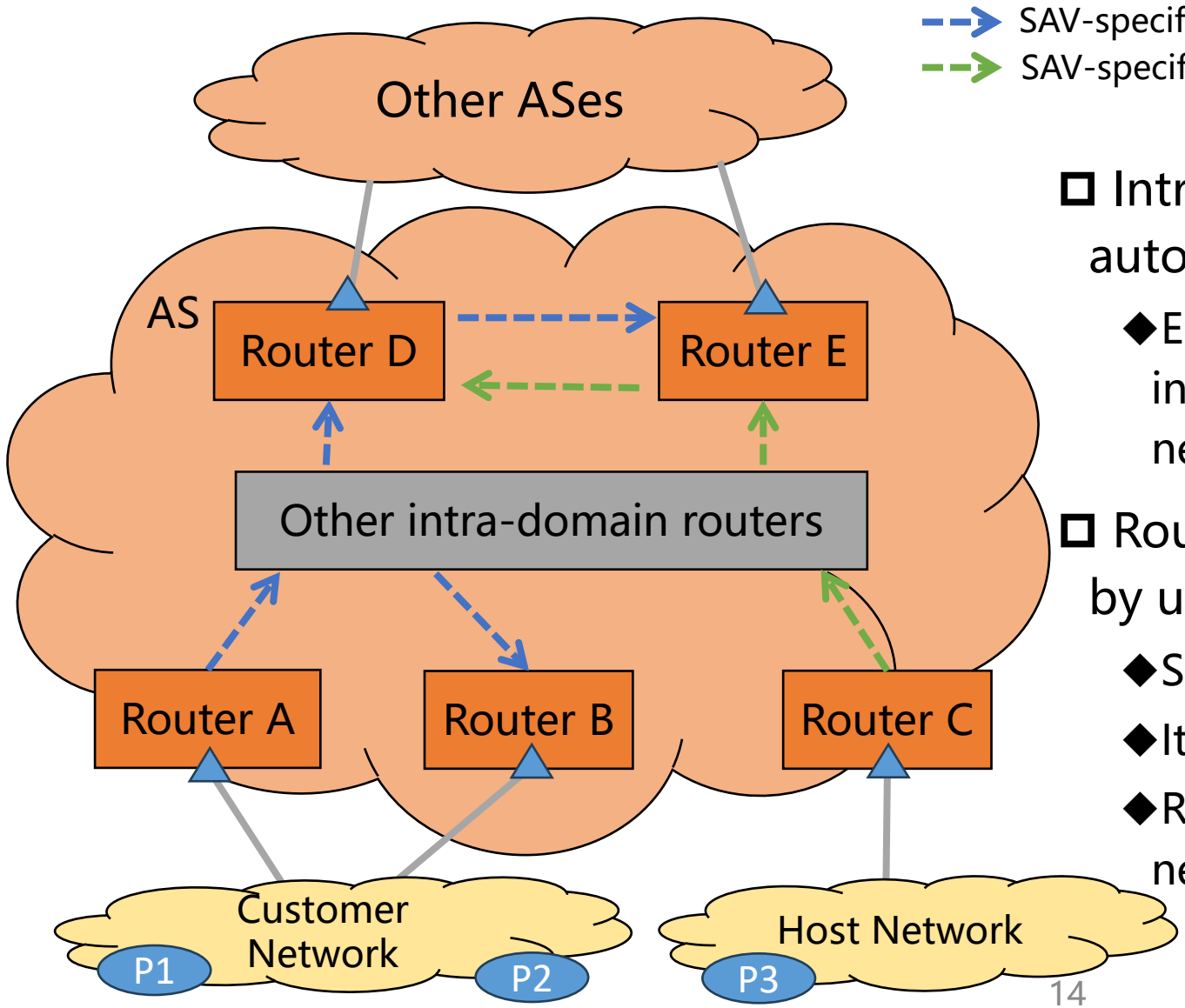
- Customer-facing router (e.g., Routers A and B)
  - Generate SAV rules on interfaces facing the customer network
  - Block data packets received at those interfaces with source addresses not belonging to the customer network

Overview of Intra-domain SAVNET Architecture



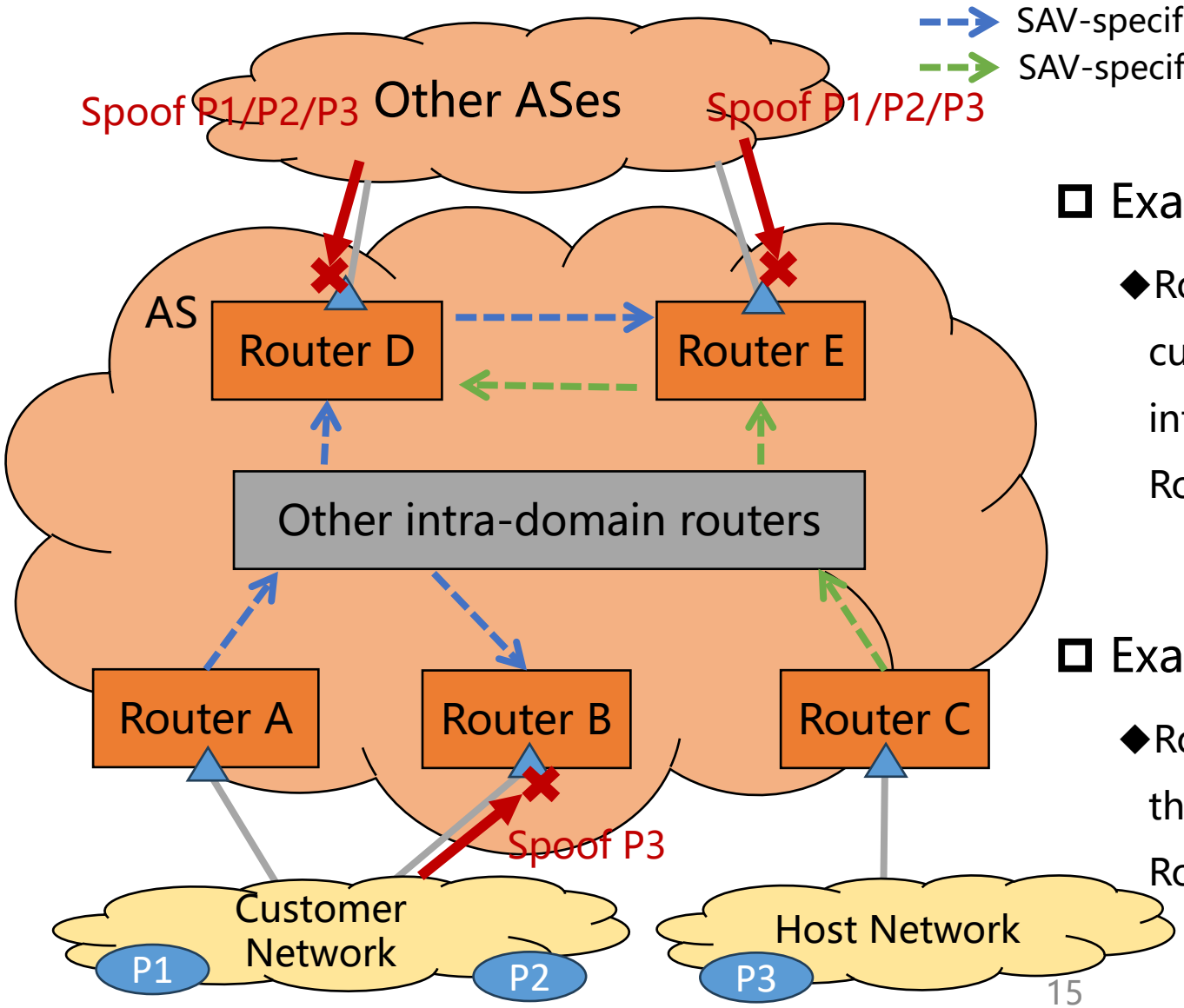
- AS border router (e.g., Routers D and E)
  - Generate SAV rules on interfaces facing another AS
  - Block data packets received at those interfaces with source addresses belonging to the local AS

Overview of Intra-domain SAVNET Architecture



- Intra-domain SAVNET requires routers to automatically exchange SAV-specific information
  - Each router can choose to provide its SAV-specific information to any router in the intra-domain network
- Routers can generate more accurate SAV rules by using
  - SAV-specific information provided by other routers
  - Its own SAV-specific information
  - Routing information in the local FIB/RIB (if necessary)

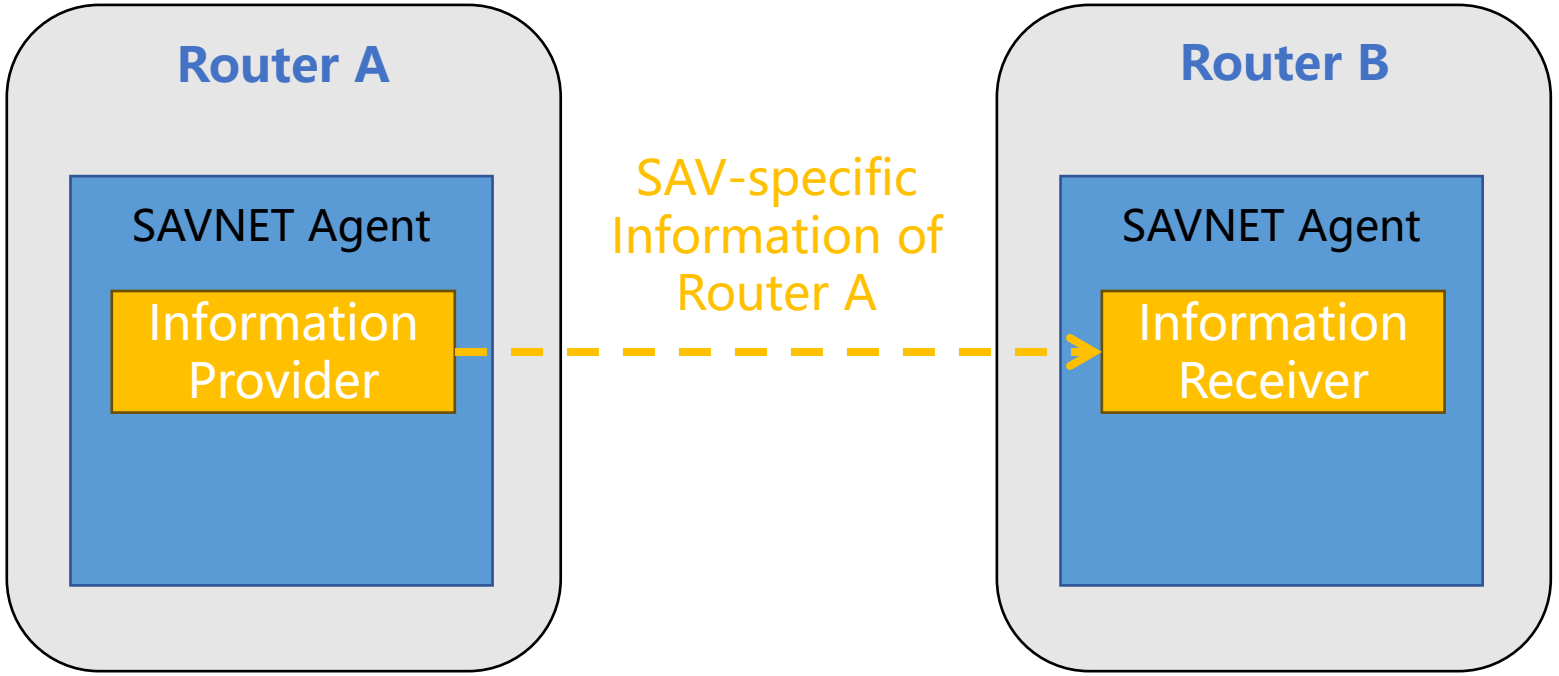
Overview of Intra-domain SAVNET Architecture



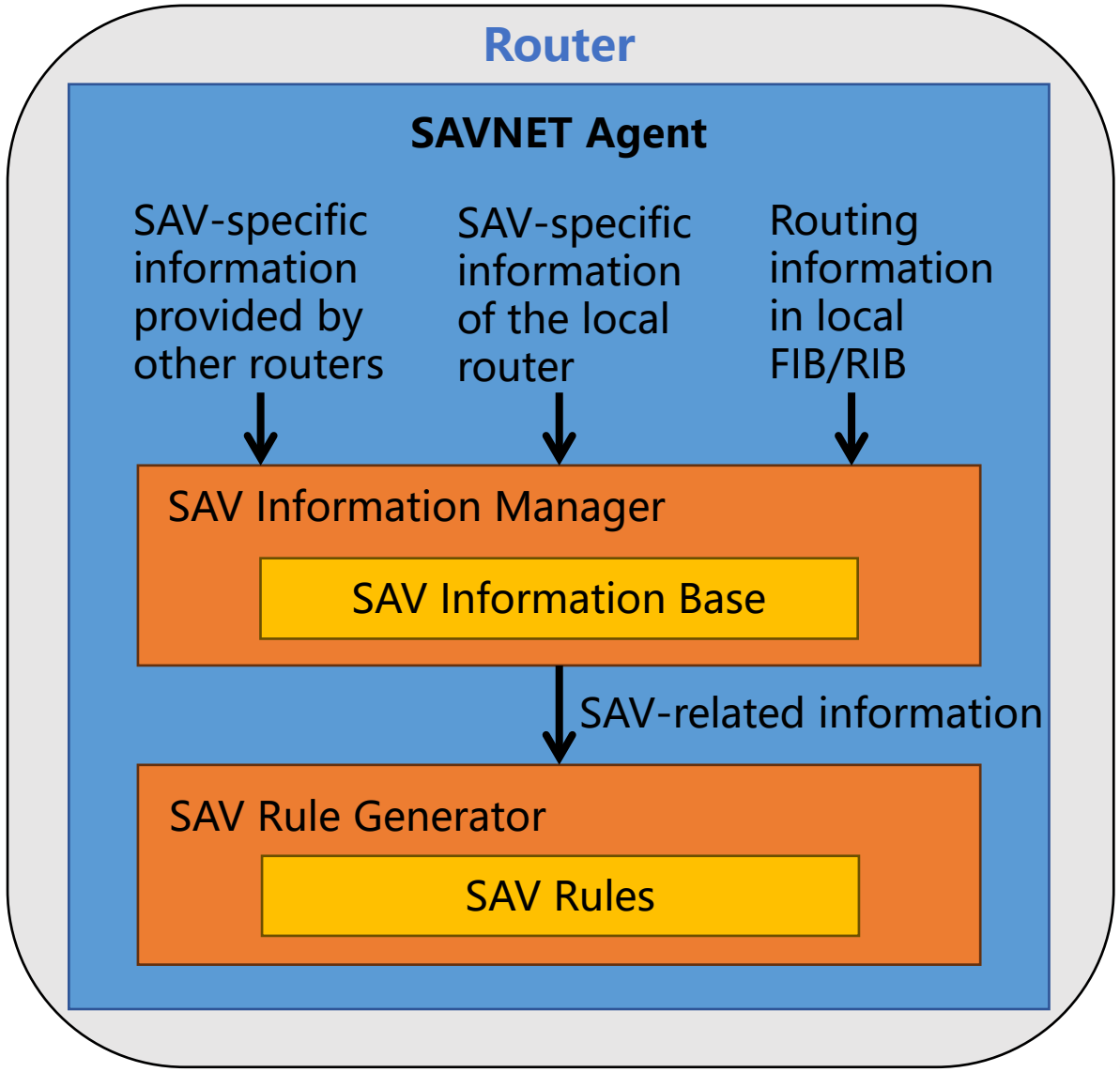
- Example #1
  - Router B can identify all prefixes belonging to the customer network by using its own SAV-specific information and SAV specific information provided by Router A
- Example #2
  - Routers D and E can identify all prefixes belonging to the AS by using SAV specific information provided by Routers A, B, and C

SAV-specific Information Communication

- A SAV-specific information communication mechanism should be designed to propagate SAV-specific information between routers
  - ◆Support automatic update and session authentication
- It can be either a new protocol or an extension to an existing protocol



Workflow of SAV Rule Generation



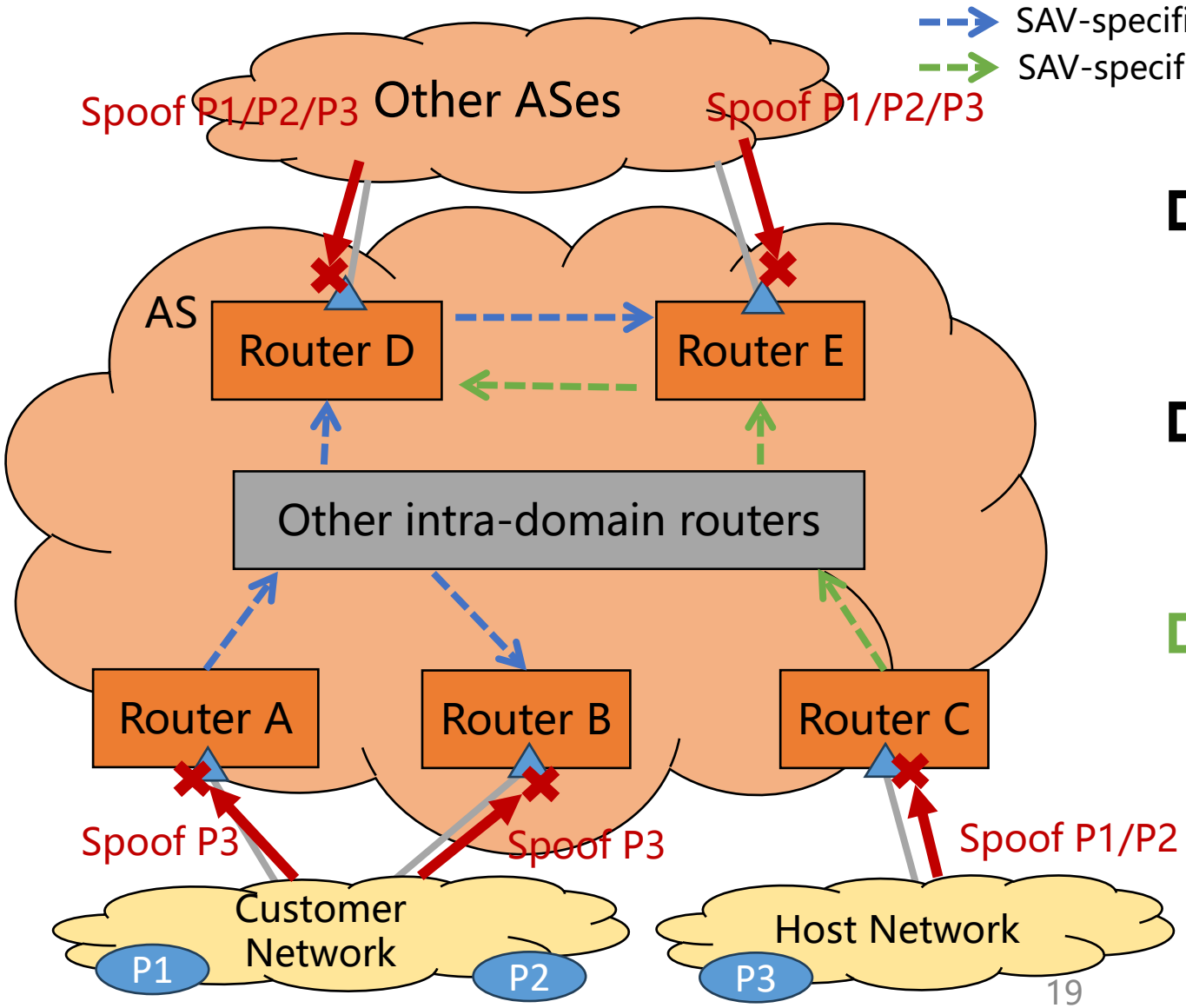
- Routers preferentially use SAV-specific information to generate SAV rules
  - ◆SAV-specific information helps generate more accurate SAV rules than local routing information
- If some SAV-specific information is unavailable in the incremental or partial deployment scenario
  - ◆Local routing information can be also used to generate SAV rules
    - ➢Must avoiding improper block

Data-Plane Considerations

- High-level data-plane considerations
  - SAVNET routers check source addresses of incoming data packets against local SAV rules and drop those that are identified as using spoofing source addresses

- More data-plane details can be found in [draft-huang-savnet-sav-table]

Use Cases



- ACL-based Ingress filtering
  - Manual update
- Strict uRPF
  - Improper block
- **Intra-domain SAVNET**
  - **Automatic update**
  - **Accurate validation**

Summary

- Comments received in IETF 115, 116, 117, and 118 are discussed and addressed through SAVNET mailing list, and this document has been updated accordingly
  - draft-li-savnet-intra-domain-architecture-00, IETF 115 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-01, IETF 116 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-02, June 2023
  - draft-li-savnet-intra-domain-architecture-03, IETF 117 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-04, Oct 2023
  - draft-li-savnet-intra-domain-architecture-05, IETF 118 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-06, Jan 2024
  - **draft-li-savnet-intra-domain-architecture-07, IETF 119 SAVNET WG**
- Following this architecture, the new intra-domain SAV solution can meet the design requirements proposed in [draft-ietf-savnet-intra-domain-problem-statement]

Next Step

- Call for WG adoption

Thanks!