Inter-domain Source Address Validation (SAVNET) Architecture

Dan Li, Jianping Wu, Mingqing Huang, Li Chen,
Nan Geng, **Libin Liu**, Lancheng Qin

July 23, 2024

SAVNET WG, IETF 120

Background

- Inter-domain SAVNET architecture aims to provide a comprehensive framework for developing new inter-domain SAV mechanisms
  - Address the problems of existing inter-domain SAV mechanisms.
  - Meet the requirements proposed in [draft-ietf-savnet-inter-domain-problem-statement].
- Historical versions
  - **draft-wu-savnet-inter-domain-architecture-00, IETF 115 SAVNET WG**
  - **draft-wu-savnet-inter-domain-architecture-01, IETF 116 SAVNET WG**
  - draft-wu-savnet-inter-domain-architecture-02, June 1, 2023
  - **draft-wu-savnet-inter-domain-architecture-03, IETF 117 SAVNET WG**
  - draft-wu-savnet-inter-domain-architecture-04, September 30, 2023
  - **draft-wu-savnet-inter-domain-architecture-05, IETF 118 SAVNET WG**
  - draft-wu-savnet-inter-domain-architecture-06, February 5, 2024
  - **draft-wu-savnet-inter-domain-architecture-07, IETF 119 SAVNET WG**
  - draft-wu-savnet-inter-domain-architecture-08, May 26, 2024
  - **draft-wu-savnet-inter-domain-architecture-09, IETF 120 SAVNET WG**

Quick Review of Version 07

- Summarizing the incentive of inter-domain SAVNET architecture
- Introducing the inter-domain SAVNET architecture
  - Overview figure of inter-domain SAVNET architecture.
  - SAV-specific information, general information, and their differences in terms of accuracy, timeliness, and trustworthiness.
  - SAV rule generation based on various SAV information sources.
- Describing the SAVNET communication mechanisms
  - SAV-specific information communication mechanism.
  - General information communication mechanism.
  - Management information communication mechanism.
- Illustrating the use cases of inter-domain SAVNET architecture

Summary of Comments on Version 07

- Comments on the details for acquisition of SAV-specific information
  - How does the source AS obtain its own SAV-specific information for the validation AS, especially in the partial deployment? (Alvaro)
  - In some cases, the path information would be derived from BGP, and you do not need a solution for these cases. For this document all you need is to recognize that some cases may not work as expected until a wider deployment is achieved. (Alvaro)
  - How would the source AS be aware of failures and update SAV-specific messages? (Alvaro)
- Comments on using RPKI ROA and ASPA objects as SAV information source
  - Raise the same issue like BAR-SAV, which uses RPKI-based objects and is similar but not the same. If SAV using RPKI is deployed, it will jeopardize the use of RPKI in routing security. This is a big problem but not addressed. We need new signed objects. I am happy to help but no one proposes it. (Ben Maddison)
- Comments on priority-based scheme for using SAV information sources
  - It may not generate accurate SAV rules when the high-priority SAV information sources are lacking and the information from low-priority sources is not accurate. (Olaf)

Summary of Comments on Version 07

- Comments on security considerations
  - Does this cover a man-in-the-middle attack who can generate a prefix inside BGP with the right AS origin, but can hijack the path? (Keyur)
  - Follow the concern raised by Keyur, I do not think we have a way of solving that using outbound signaling. We need source signing in band in packet header. (Ben Maddison)
  - **Quick response: We do have considered the security issues on version 07 of the draft**.
- Minor Comments on draft writing
  - **Quick response: We have revised the draft accordingly to improve the writing**.

Response #1: Illustrating the detailed process for acquisition of SAV-specific information and some specific scenarios

- In Section 7.1, we have revised the following contents to illustrate the process for acquisition of SAV-specific information and further clarify the specific scenarios for wider deployment of SAVNET agent.
  - We have updated Figure 9, which shows a detailed example to explain how the source AS (AS 1 in Figure 9(b)) obtains its SAV-specific information and communicates it to the validation AS (AS 4 in Figure 9(b)).
  - We have added a new sixth paragraph to illustrate the scenarios explicitly, where static route exists, which need to rely on the wider deployment of SAVNET agent to obtain the accurate SAV-specific information.
  - We have further illustrated how inter-domain SAVNET deals with network failures and a wider deployment of SAVNET agent can make network failure sensing more sensitive.

We discussed the updates of Section 7.1 and required comments in the mailing list.

Response #2: Describing the requirements for accurate SAV information and avoiding jeopardizing the use of RPKI

- In Section 6, we have described the requirements for obtaining accurate SAV information and avoiding jeopardizing the use of RPKI
  - We have added a new third paragraph to further explain the recommendations for different SAV information sources, especially for low-priority SAV information sources.
  - We have added the requirement that the new inter-domain SAVNET mechanism should avoid jeopardizing the use of RPKI in routing security, when using RPKI ROA objects and ASPA objects as the SAV information source.
  - We have discussed that SAV rules generated using accurate low-priority SAV information sources can avoid improper blocks but have higher degrees of improper permits compared to the SAV-specific information.


[savnet] Re: The Updated Inter-domain SAVNET Architecture Draft

Libin Liu <liulb@zgclab.edu.cn> | Sun, 09 June 2024 07:15 UTC | Show header

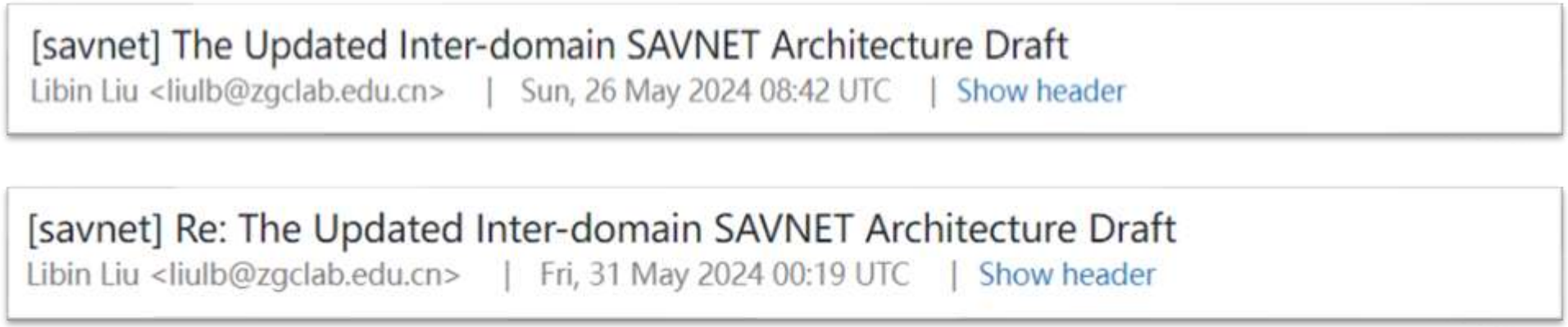
Hi Siyuan,

Thank you for the careful review. No, they are not equivalent. SAV rules generated using SAV-specific information can avoid improper blocks and minimize improper permits, while the ones generated using SAV-related information from low-priority sources avoid improper blocks but have different degrees of improper permits. The accuracy requirement for information from low-priority sources is going to avoid improper blocks.

We discussed the requirement for guaranteeing the accuracy of low-priority SAV information sources and avoiding jeopardizing the use of RPKI in the mailing list.

Response #3: Improving the draft writing and discussing how to meet the design requirements of inter-domain SAVNET

- We have added a new Section 9 to illustrate how inter-domain SAVNET meets the requirements defined in the inter-domain SAVNET problem statement draft [draft-ietf-savnet-inter-domain-problem-statement].
  - In Section 9.2, we have revised the writing of the first and second paragraphs to enhance their clarity.



We discussed the overall updates of the inter-domain SAVNET architecture and required comments in the mailing list.

Main Updates Compared to Version 07

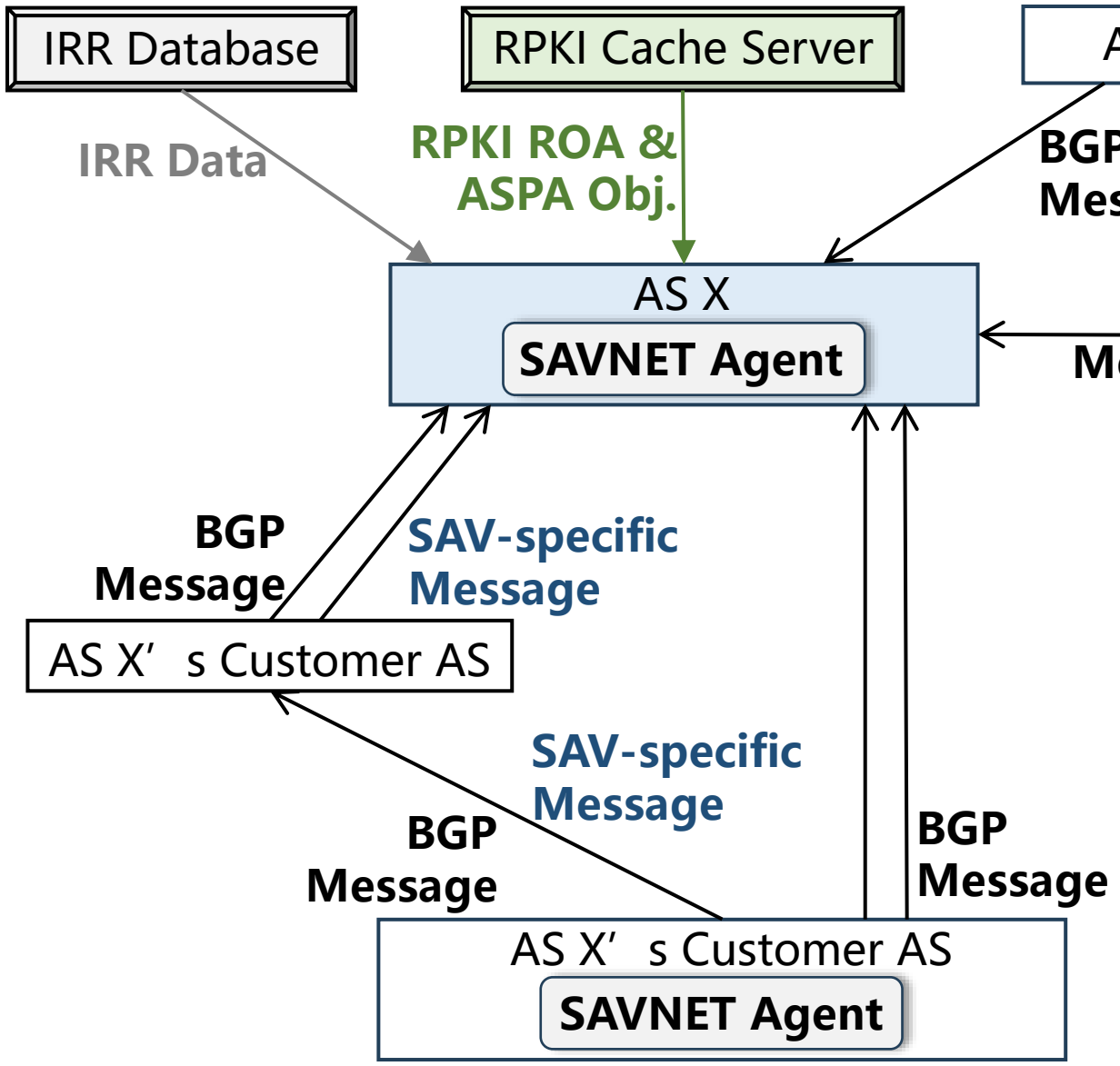
- Revise the SAV Information Base Section (Section 6)
  - Add a new third paragraph to further explain the recommendations for different SAV information sources.
- Revise the SAVNET Communication Mechanism Section (Section 7)
  - Update Figure 8 to show that SAVNET agent obtains different SAV-related information from different sources.
  - Revise SAV-specific Information Communication Mechanism Section (Section 7.1)
    - Update Figure 9 and its corresponding descriptions to explain how the source AS obtains the SAV-specific information and communicates it to the validation AS.
    - Add a new paragraph to illustrate the deployment scenarios where static route exists.
    - Revise the last paragraph to illustrate the scenarios where inter-domain SAVNET cannot be aware of the network failures and a wider deployment of SAVNET agent can help in these scenarios.
- Add a Meeting the Design Requirements of Inter-domain SAVNET Section (Section 9)

Main Updates Compared to Version 07

- Revise the SAV Information Base Section (Section 6)
  - Add a new third paragraph to further explain the recommendations for different SAV information sources.
- Revise the SAVNET Communication Mechanism Section (Section 7)
  - Update Figure 8 to show that SAVNET agent obtains different SAV-related information
  - Update Figure 9 and its corresponding descriptions to explain how the source AS obtains the SAV-specific information and communicates it to the validation AS.
  - Add a new paragraph to illustrate the deployment scenarios where static route exists.
  - Revise the last paragraph to illustrate the scenarios where inter-domain SAVNET cannot be aware of the network failures and a wider deployment of SAVNET agent can help in these scenarios.
- Add a Meeting the Design Requirements of Inter-domain SAVNET Section (Section 9)

All the updates have been discussed and illustrated in the SAVNET mailing list.

Review of Inter-domain SAVNET Architecture



- SAV-specific Information
- General Information
  - RPKI ROA objects and ASPA objects
  - Local routing information from BGP messages
  - IRR Data
- AS X and its customer AS which has deployed the SAVNET agent can exchange the SAV-specific information with each other.

Main Updates Compared to Version 07

- **Revise the SAV Information Base Section (Section 6)**
  - **Add a new third paragraph to further explain the recommendations for different SAV information sources.**
- Revise the SAVNET Communication Mechanism Section (Section 7)
  - Update Figure 8 to show that SAVNET agent obtains different SAV-related information from different sources.
  - Revise SAV-specific Information Communication Mechanism Section (Section 7.1)
    - Update Figure 9 and its corresponding descriptions to explain how the source AS obtains the SAV-specific information and communicates it to the validation AS.
    - Add a new paragraph to illustrate the deployment scenarios where static route exists.
    - Revise the last paragraph to illustrate the scenarios where inter-domain SAVNET cannot be aware of the network failures and a wider deployment of SAVNET agent can help in these scenarios.
- Add a Meeting the Design Requirements of Inter-domain SAVNET Section (Section 9)

SAV Rule Generation

- Generating SAV rules based on the priorities of SAV information sources
  - Inter-domain SAVNET architecture assigns priorities to different SAV information sources and preferentially uses higher-priority information to generate SAV rules.
  - The priorities of SAV information sources are recommended rather than mandated.
  - When SAV-specific information is not available, a new SAV mechanism can use low-priority information source and should ensure the correct information is obtained and adopts appropriate SAV actions on the data plane.
  - When using RPKI ROA objects and ASPA objects as the SAV information source, the new inter-domain SAV mechanism should avoid jeopardizing the use of RPKI in routing security.

Priority Ranking for the SAV Information Sources		
SAV Information Sources		**Priorities**
SAV-specific Information		1
General Information	ROA and ASPA Obj.	2
	RIB	3
	FIB	4
	IRR Data	5

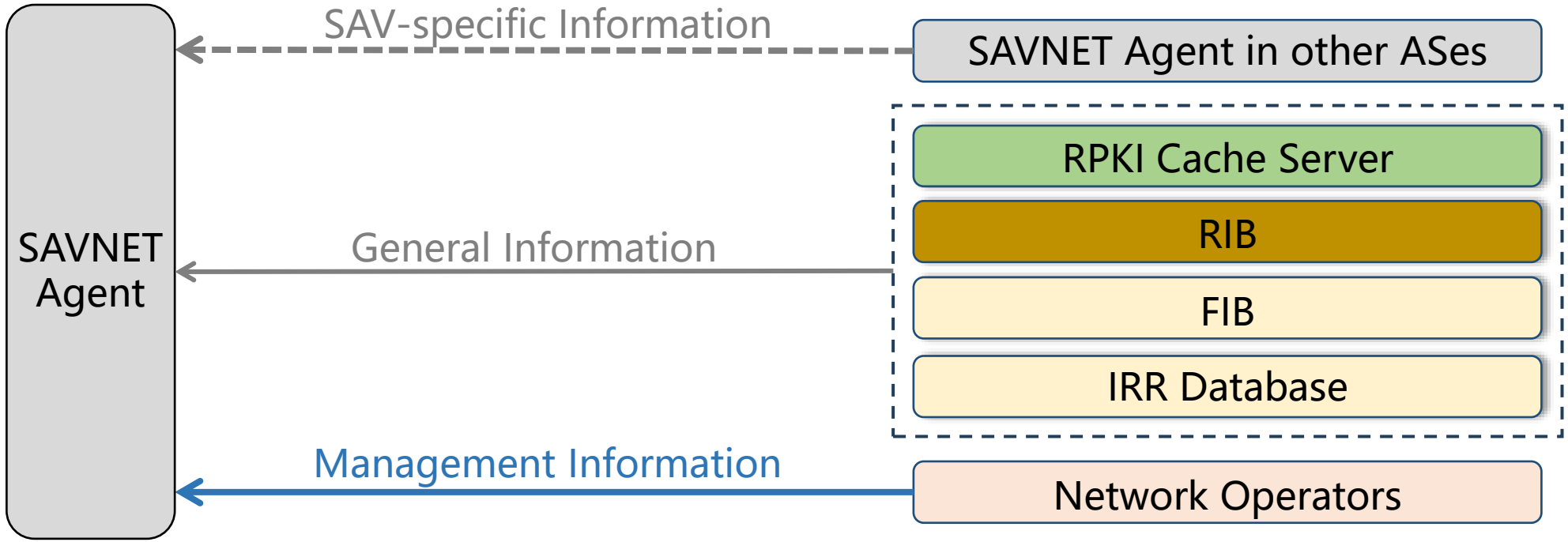
Example of the SAV Information Base				
Index	**Prefix**	**Incoming Direction**	**Relation**	**SAV Information Source**
0	**P1**	**AS 2**	**Customer**	**SAV-specific Information**
1	P1	AS 1	Customer	General Information
2	P2	AS 2	Customer	General Information
3	P3	AS 3	Provider	General Information
4	P5	AS 3	Provider	General Information
5	P5	AS 5	Customer	General Information
6	P6	AS 2	Customer	General Information SAV-specific Information

Main Updates Compared to Version 07

- Revise the SAV Information Base Section (Section 6)
  - Add a new third paragraph to further explain the recommendations for different SAV information sources.
- **Revise the SAVNET Communication Mechanism Section (Section 7)**
  - **Update Figure 8 to show that SAVNET agent obtains different SAV-related information from different sources.**
  - Revise SAV-specific Information Communication Mechanism Section (Section 7.1)
    - Update Figure 9 and its corresponding descriptions to explain how the source AS obtains the SAV-specific information and communicates it to the validation AS.
    - Add a new paragraph to illustrate the deployment scenarios where static route exists.
    - Revise the last paragraph to illustrate the scenarios where inter-domain SAVNET cannot be aware of the network failures and a wider deployment of SAVNET agent can help in these scenarios.
- Add a Meeting the Design Requirements of Inter-domain SAVNET Section (Section 9)

SAVNET Communication Mechanisms

- We have renamed the mechanism for communicating management information from "Management mechanism" to "management information communication mechanism".

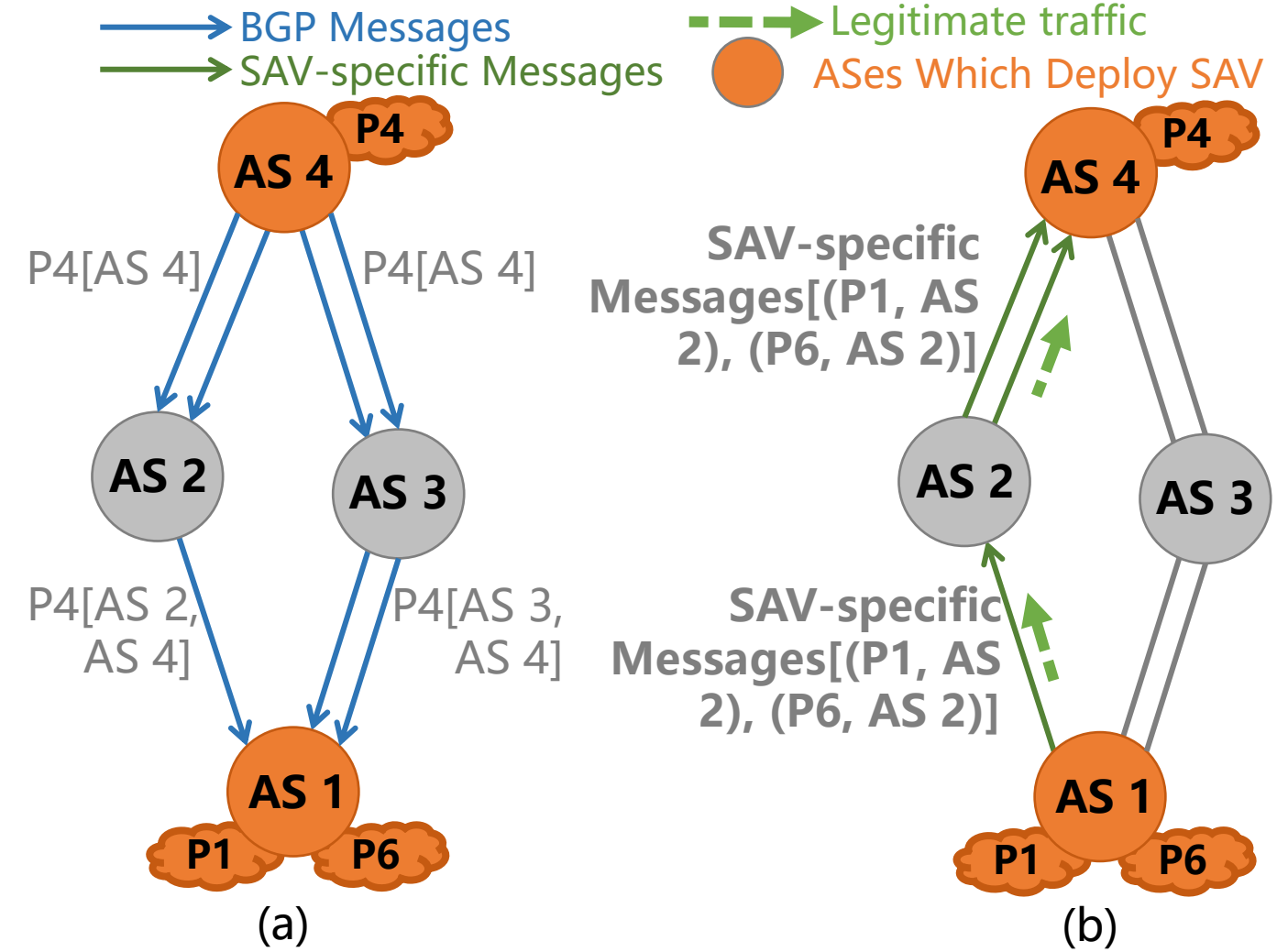


Main Updates Compared to Version 07

- Revise the SAV Information Base Section (Section 6)
  - Add a new third paragraph to further explain the recommendations for different SAV information sources.
- Revise the SAVNET Communication Mechanism Section (Section 7)
  - Update Figure 8 to show that SAVNET agent obtains different SAV-related information from different sources.
  - **Revise SAV-specific Information Communication Mechanism Section (Section 7.1)**
    - **Update Figure 9 and its corresponding descriptions to explain how the source AS obtains the SAV-specific information and communicates it to the validation AS.**
    - **Add a new paragraph to illustrate the deployment scenarios where static route exists.**
    - **Revise the last paragraph to illustrate the scenarios where inter-domain SAVNET cannot be aware of the network failures and a wider deployment of SAVNET agent can help in these scenarios.**
- Add a Meeting the Design Requirements of Inter-domain SAVNET Section (Section 9)

Acquisition of SAV-specific Information

We have used an example in Section 7.1 to display the detailed process about how the SAVNET agent of the source AS (AS 1) obtains its own SAV-specific information.



- **BGP Messages**: As shown in Figure (a), AS 4 advertises its prefix P4 along the paths [AS 4, AS 2, AS 1] and [AS 4, AS 3, AS 1].
- **Legitimate Traffic**: As shown in Figure (b), AS 1 selects the path [AS 1, AS 2, AS 4] as the best path for the legitimate traffic with source addresses in P1 or P6 and destination addresses in P4.
- **SAV-specific Messages**: AS 1 knows that its legitimate traffic whose source prefixes are P1 or P6 will enter AS 4 from the direction of AS 2. As a result, AS 1 obtains its SAV-specific information and assembles it into the SAV-specific messages.

Scenarios Needing the Wider Deployment of SAVNET Agent

We have further supplemented the descriptions for the scenarios of static route and network failures in Section 7.1.

Scenarios of static route

- In some scenarios, operators may override the default BGP decision by using static route.
- For these scenarios, the wider deployment of SAVNET agent is required to obtain the accurate SAV-specific information.

Scenarios of network failures

- The preferred AS paths of a source AS may change over time due to route changes caused by network failures.
- The SAVNET agent should be aware of the network failures by detecting the route changes and launch SAV-specific messages to update SAV-specific information in a timely manner.
- A wider deployment of SAVNET agent can make network failure sensing more sensitive.

Main Updates Compared to Version 07

- Revise the SAV Information Base Section (Section 6)
  - Add a new third paragraph to further explain the recommendations for different SAV information sources.
- Revise the SAVNET Communication Mechanism Section (Section 7)
  - Update Figure 8 to show that SAVNET agent obtains different SAV-related information from different sources.
  - Revise SAV-specific Information Communication Mechanism Section (Section 7.1)
    - Update Figure 9 and its corresponding descriptions to explain how the source AS obtains the SAV-specific information and communicates it to the validation AS.
    - Add a new paragraph to illustrate the deployment scenarios where static route exists.
    - Revise the last paragraph to illustrate the scenarios where inter-domain SAVNET cannot be aware of the network failures and a wider deployment of SAVNET agent can help in these scenarios.
- **Add a Meeting the Design Requirements of Inter-domain SAVNET Section (Section 9)**

Meeting the Design Requirements

Inter-domain SAVNET architecture proposes the guidelines for the design of new inter-domain SAV mechanisms to meet the requirements proposed in [draft-ieft-savnet-inter-domain-problem-statement].

- Requirement #1: Improving validation accuracy over existing mechanisms
  - SAV-specific information can generate more accurate SAV rules than general information.
- Requirement #2: Working in incremental/partial deployment
  - SAVNET agent can be deployed incrementally, and when SAV-specific information is not available, general information can be used to generate SAV rules.
- Requirement #3: Reducing operational overhead
  - SAVNET agent can collect SAV-specific information through SAV-specific information communication mechanism and generate SAV rules automatically.
- Requirement #4: Guaranteeing convergence
  - SAVNET agent should launch the SAV-specific messages to adapt to the route changes in a timely manner.
- Requirement #5: Providing necessary security guarantee
  - Existing security mechanisms can be used or a new security mechanism can be designed.

Summary

- Comments received from IETF 115 to 119 were discussed and addressed through the mailing list, and this document had been updated accordingly
  - draft-wu-savnet-inter-domain-architecture-00, IETF 115 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-01, IETF 116 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-02, June 1, 2023
  - draft-wu-savnet-inter-domain-architecture-03, IETF 117 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-04, September 30, 2023
  - draft-wu-savnet-inter-domain-architecture-05, IETF 118 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-06, February 5, 2024
  - draft-wu-savnet-inter-domain-architecture-07, IETF 119 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-08, May 26, 2024
  - **draft-wu-savnet-inter-domain-architecture-09, IETF 120 SAVNET WG**
- Following this architecture, the new inter-domain SAV solutions can meet the design requirements proposed in [draft-ietf-savnet-inter-domain-problem-statement]

Acknowledgements

Many thanks to Alvaro Retana, Kotikalapudi Sriram, Rüdiger Volk, Xueyan Song, Ben Maddison, Jared Mauch, Joel Halpern, Aijun Wang, Jeffrey Haas, Xiangqing Chang, Changwang Lin, Mingxing Liu, Zhen Tan, Yuanyuan Zhang, Yangyang Wang, Antoin Verschuren, Olaf Struck, Siyuan Teng etc. for their valuable comments and feedback on this document.

Next Step

- Request WG adoption

Thanks! ☺

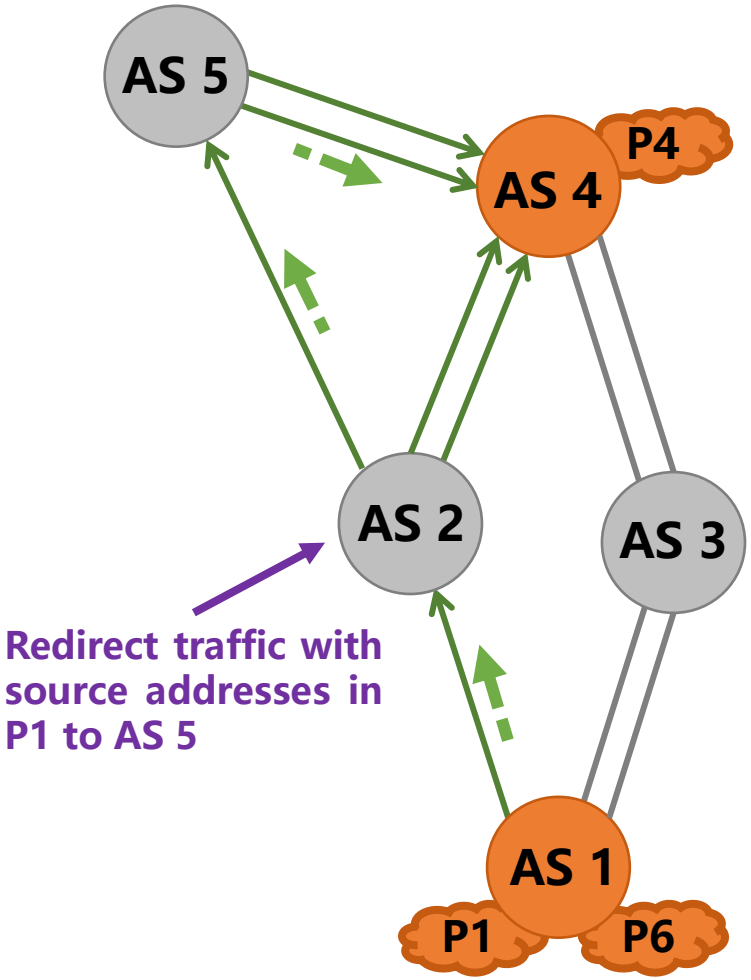
Backup

Review of General Information and SAV-specific Information

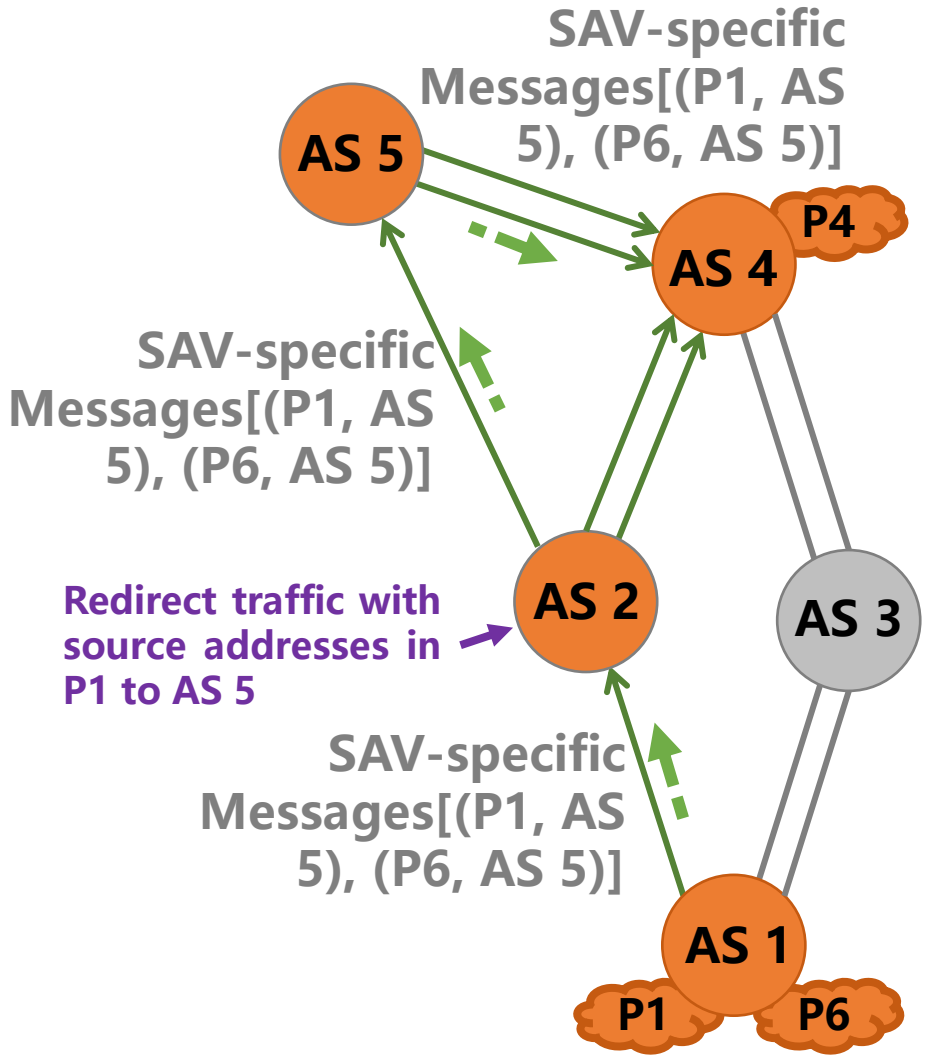
SAV-related Information		SAV Accuracy	Timeliness	Trustworthiness
General Information	IRR Data	Improper Block & Improper Permit	No	No
	Local Routing Information		Yes	No
	RPKI ROA Obj. & ASPA Obj.		No	Yes
SAV-specific Information		Functioning as Expected	Yes	Yes

- General Information
  - IRR data: IRR data may not be accurate and are updated in a slow manner.
  - Local routing information: SAV based on local routing information may lead to improper blocks or improper permits in may scenarios as analyzed in [draft-ieft-savnet-inter-domain-problem-statement].
  - RPKI ROA objects and ASPA objects: In some partial deployment scenarios, they will lead to improper blocks or improper permits. They are stable but not updated in a timely manner when network change.
- SAV-specific Information
  - SAV-specific information includes prefixes and their incoming directions for accurate SAV, and can be updated automatically in a timely manner, and SAVNET agent validates the authenticity of the connections for communicating SAV-specific information.

Scenarios of Static Route



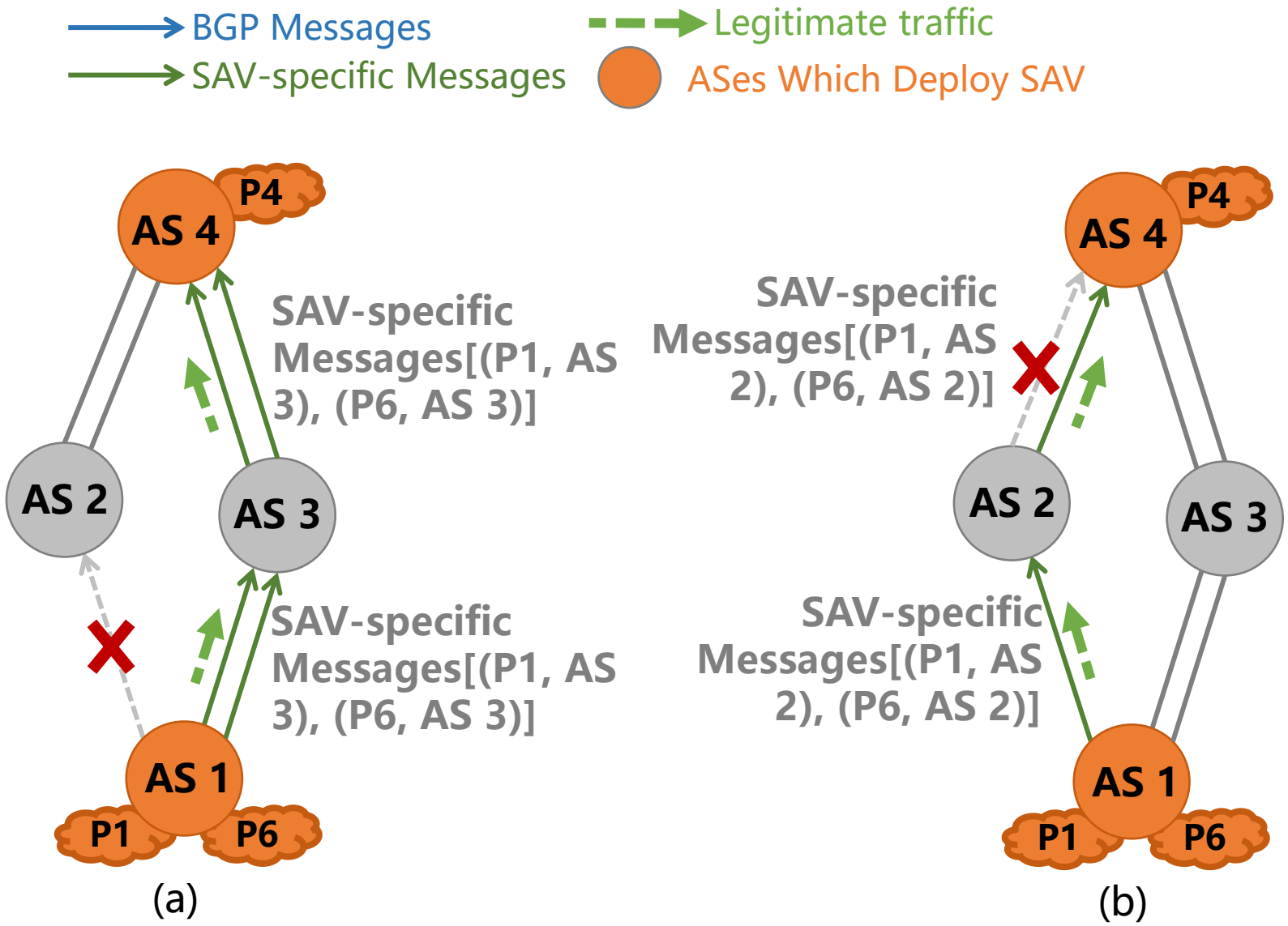
(a)



(b)

- In some scenarios, operators may override the default BGP decision by using static route.
- As shown in Figure (a), AS 2 uses AS 5 which does not appear in the AS path [AS 1, AS 2, AS 4] to transmit the legitimate traffic.
- As shown in Figure (b), for such scenarios, inter-domain SAVNET requires wider deployment (AS 2 and AS 5) to obtain the accurate SAV-specific information.

Scenarios of Network Failures



- The preferred AS path may change due to network failures, as shown in Figure (a) and (b).
- The SAVNET agent should be aware of route changes and launch SAV-specific messages to adapt to the route changes in a timely manner.
- A wider deployment of SAVNET agent can make network failure detection more sensitive.
- The SAVNET agent should deal with the route changes carefully to avoid improper blocks.

Security Considerations

- The security threats faced by SAV-specific communication mechanism in inter-domain networks can be categorized into two main aspects:
  - Session security threats
    - Session identity impersonation and session integrity destruction.
  - Content security threats
    - Message alteration, message injection, and path deviation.
- Existing security mechanisms can be used or a new security mechanism should be designed to secure SAV-specific information
  - The detailed security design of SAV-specific communication mechanism is out of scope for this document.