

Inter-domain Source Address Validation (SAVNET) Architecture

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

July 27, 2023

Outline

- Background
- Quick review of requirements for the new inter-domain SAV mechanism
- Inter-domain SAVNET Architecture
- Summary

Background

- Inter-domain SAVNET architecture aims to provide a high-level 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**

Comments on Version-01

□ Remove the details which may relate to a specific solution.

◆Response: We revise the draft to make inter-domain SAVNET architecture **more general**.

□ K. Sriram: The terminology of Passive Acquired Information and Active Collaboration Information may not be clearly defined.

◆Response: We **revise the names and descriptions** of different SAV-related information.

□ Actively elaborate on what diagnosis and logging you would do to allow operators to address the underlying problems.

◆Response: We revise the draft and **add management considerations**.

Comments on Version-01

□ Rüdiger Volk: Should not only address the partially deployed situation, also should consider the convergence issue, since the internet is a consistently moving system.

◆Response: We revise the draft and **add convergence considerations**.

□ Concern of delay or loss of active collaboration information, resulting in improper block.

◆Response: We **add convergence considerations** to discuss these issues

Comments on Version-01

- Igor Lubashev: Security concern of control flow messages taking same data path as the packets.
 - ◆Response: We revise draft to consider security issues of SAV-specific protocol in **the security considerations section**. The detailed design of SAV-specific protocol is out of scope for this document.

- Ben Maddison: Security issues should be considered in the Architecture.
 - ◆Response: We **add more security considerations** in the draft.

Comments on Version-01

□ Xueyan Song: What is the relationship and **difference between the intra- and inter-domain Architecture?**

◆Response: Compared to intra-domain SAVNET architecture, inter-domain SAVNET architecture uses more AS-level information (e.g., RPKI ROA and ASPA objects, AS-level forwarding paths), and has different deployment, convergence, management, and security considerations.

□ Zhen Tan: What is the relationship between the Architecture draft and the other draft about SAV table?

◆Response: This Architecture draft describes the high-level framework to generate SAV rules, while the other draft describes how to organize and use a SAV table.

Main Updates Compared to Version-01

- Updates in Inter-domain SAVNET Architecture section
 - ◆ Revise the SAV-related information and sources
 - ◆ Add the description of SAV-specific messages
 - ◆ Define the priorities of different SAV-related information sources
 - ◆ Add the description of management channel and information channel
- Revise the Partial/Incremental Deployment section
- Add a new Convergence Considerations section
- Add a new Management Considerations section
- Revise the Security Considerations section

Outline

- Background
- Quick review of requirements for the new inter-domain SAV mechanism
- Inter-domain SAVNET Architecture
- Summary

Quick Review of Requirements for the New Inter-domain SAV Mechanism

- Requirement #1: Improving Validation Accuracy over Existing Mechanisms
 - ◆ The new inter-domain SAV mechanism should improve the validation accuracy upon existing inter-domain SAV mechanisms
- Requirement #2: Working in Incremental/Partial Deployment
 - ◆ The new inter-domain SAV mechanism should provide effective protection for source addresses when it is partially deployed in the Internet
- Requirement #3: Reducing Operational Overhead
 - ◆ The new inter-domain SAV mechanism must be able to adapt to dynamic networks and asymmetric routing scenarios automatically
- Requirement #4: Communicating SAV-specific Information between ASes
 - ◆ A SAV-specific communication approach between ASes should be designed

Outline

- Background
- Quick review of requirements for the new inter-domain SAV mechanism
- Inter-domain SAVNET Architecture**
- Summary

Basic Idea of Inter-domain SAVNET Architecture

□ To meet Requirement #1, #3, and #4

- ◆ Inter-domain SAVNET architecture allows ASes to **communicate SAV-specific information through a SAV-specific protocol**
- ◆ When SAV-specific information is available, **SAV-specific information is preferentially used** to generate SAV rules
 - Because SAV-specific information can help generate more accurate SAV rules than the information (e.g., routing information) used in existing inter-domain SAV mechanisms

□ To meet Requirement #2

- ◆ When SAV-specific information for some prefixes are not available, general information (such as routing information or RPKI ROA and ASPA objects) can be used to generate SAV rules

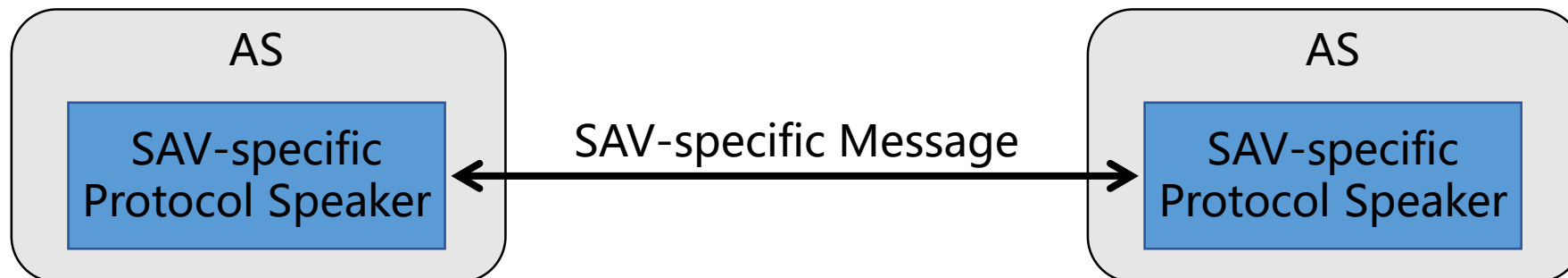
SAV-related Information and Sources

- **SAV-specific information** is the information designed specifically for SAV
 - ◆ **The real forwarding path information** from other ASes, which consists of their legitimate source prefixes and the corresponding incoming interfaces
- **General information** refers to the information that is not designed for SAV but can also be used for SAV to some extent
 - ◆ Such as routing information in RIBs or FIBs, the relationships between prefixes and ASNs in RPKI ROA Objects, and the Customer-to-Provider relationships in RPKI ASPA Objects

SAV-specific information can help generate **more accurate** SAV rules than general information

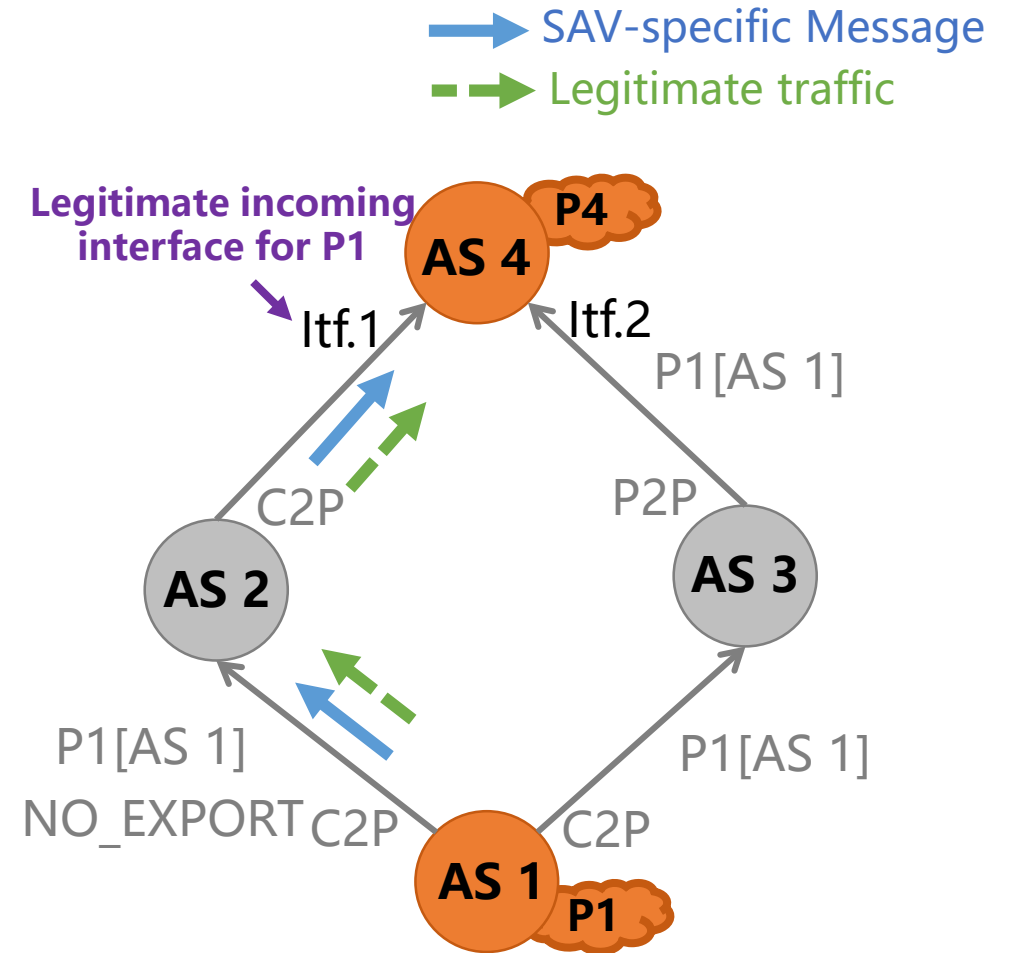
SAV-specific Messages

- The SAV-specific Messages propagate or originate SAV-specific information between the SAV-specific Protocol Speakers in different ASes
 - ◆ The SAV-specific Protocol Speaker can obtain the forwarding path information towards each destination AS based on the local RIB information, and advertise the forwarding path information through SAV-specific Messages
 - ◆ After receiving and processing the SAV-specific Messages from other ASes, the AS can obtain the legitimate incoming interfaces for the source prefixes of the origin AS



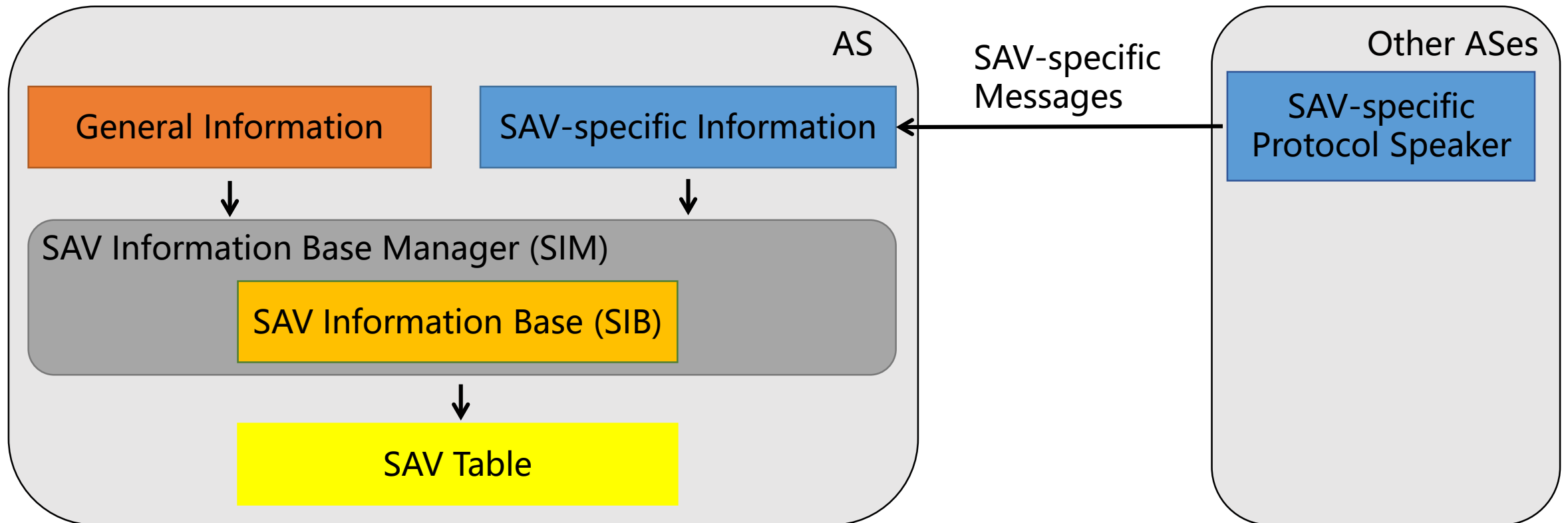
SAV-specific Messages: An Example

- ❑ Assume AS 1 selects AS 1→AS 2→AS 4 as the best forwarding path to P4
- ❑ By using the SAV-specific protocol, AS 1 advertises its forwarding path information in SAV-specific Messages
- ❑ After receiving the SAV-specific Message originated from AS 1, AS 4 identifies the legitimate incoming interface for source prefix of AS 1



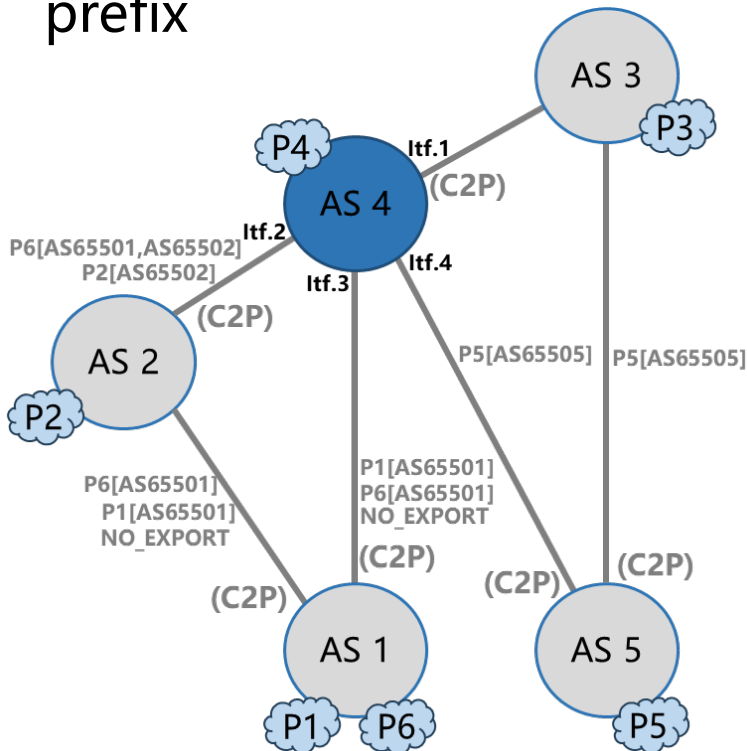
Workflow of Inter-domain SAVNET Architecture

Consolidate SAV-related information from multiple sources and generate SAV rules based on the SAV-related information



SAV Information Base (SIB)

- SIB consolidates SAV-related information from various sources
 - ◆ Each row records the index, the prefix, the prefix's valid AS-level incoming interface, the prefix's incoming direction, and the corresponding SAV information source
 - ◆ Different SAV information sources may specify different incoming interfaces for the same prefix



SAV Information Base for AS 4				
Index	Prefix	AS-level Interface	Direction	SAV Information Source
0	P3	ltof.1	Provider	General Information
1	P2	ltof.2	Customer	General Information
2	P1	ltof.2	Customer	SAV-specific Information
3	P1	ltof.3	Customer	General Information
4	P6	ltof.2	Customer	General Information
5	P6	ltof.3	Customer	SAV-specific Information, General Information
6	P5	ltof.4	Customer	General Information
7	P5	ltof.1	Provider	General Information

How to Identify the Most Accurate Incoming Interface?

□ Priorities of different SAV information sources

- ◆ Inter-domain SAVNET architecture assigns priorities to different SAV information sources and **preferentially uses higher-priority information** to generate SAV rules

Priority Ranking for the SAV Information Sources		
SAV Information Sources	Priorities	
SAV-specific Information	1	
General Information	ROA and ASPA	2
	RIB	3
	FIB	4

SAV Information Base for AS 4				
Index	Prefix	AS-level Interface	Direction	SAV Information Source
0	P3	Itf.1	Provider	General Information
1	P2	Itf.2	Customer	General Information
2	P1	Itf.2	Customer	SAV-specific Information ✓
3	P1	Itf.3	Customer	General Information
4	P6	Itf.2	Customer	General Information
5	P6	Itf.3	Customer	SAV-specific Information, General Information
6	P5	Itf.4	Customer	General Information
7	P5	Itf.1	Provider	General Information

Management Channel and Information Channel

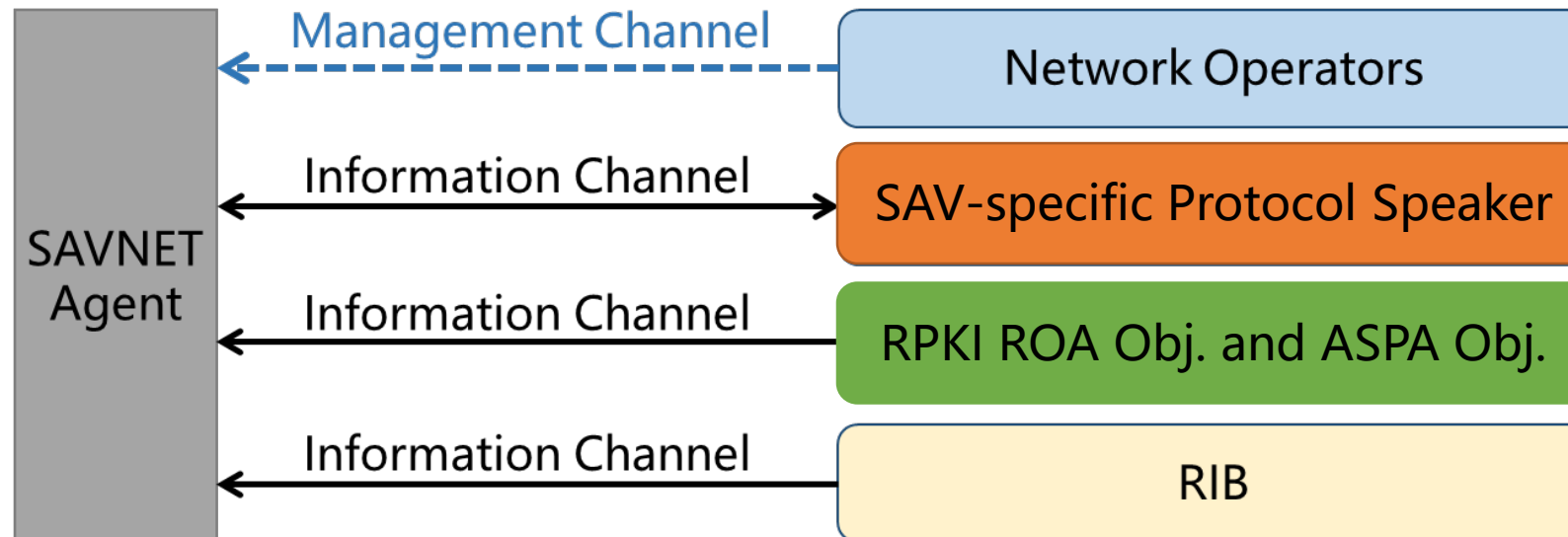
□ Management Channel

◆ Deliver manual configurations of network operators

- Such as SAV configurations using YANG, CLI, SAVNET operation and management, and inter-domain SAVNET provisioning

□ Information Channel

◆ Serve as a means to transmit SAV-related information from different sources



Partial/Incremental Deployment

- ❑ New inter-domain SAV mechanisms MUST support partial or incremental deployment
 - ◆ When SAV-specific information for some prefixes are unavailable, general information (e.g., routing information from RIB and FIB) should be used to generate SAV rules for these prefixes
- ❑ To reduce the deployment risks, network operators can enable the block action incrementally:
 - ◆ First, conduct measurement and analyze the accuracy of validation results
 - ◆ Then, limit the rate of packets with invalid validation results
 - ◆ Finally, block packets with invalid validation results after verifying the SAV accuracy, impact on forwarding performance, and operational overhead

Convergence Considerations

- ❑ Source Information Base Manager should collect SAV-related information from various SAV information sources and consolidate them in a timely manner
 - ◆ For general information (e.g., routing information, ROA objects, or ASPA objects), it relies on the convergence mechanisms in routing protocols or RPKI
 - ◆ For SAV-specific information, the SAV-specific protocol Speaker should launch SAV-specific Messages to adapt to route changes in a timely manner
- ❑ SAV-specific protocol should be designed with consideration of factors that may affect the convergence
 - ◆ Such as packet loss, unpredictable network latency, or message processing latency

Management Considerations

□ Interoperability

- ◆ Devices from different vendors or different releases of the same product can be managed through a unified data model such as YANG

□ Scalability

- ◆ Scalable operation and management methods such as NETCONF and syslog protocol should be supported

□ Implementation considerations

- ◆ Management operations (including diagnosis and logging) should be designed and implemented in existing protocols or protocol extensions

Security Considerations

- The security threats faced by SAV-specific protocol 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 (e.g., MD5, Keychain) can be used or a new security mechanism should be designed to secure SAV-specific protocol
 - ◆ The detailed security design of SAV-specific protocol is out of scope for this document

Outline

- Background
- Quick review of requirements for the new inter-domain SAV mechanism
- Inter-domain SAVNET Architecture
- Summary

Summary

Inter-domain SAVNET architecture can well **meet the requirements** proposed in [draft-ietf-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
 - ◆ When some SAV-specific information is not available, **general information** can still be used
- Requirement #3: Reducing Operational Overhead
 - ◆ SAV-related information can be **automatically collected through information channels**
- Requirement #4: Communicating SAV-specific Information between ASes
 - ◆ **SAV-specific protocol** is used to communicate SAV-specific information between ASes

Next Step

- Solicit comments and refine the draft

- ◆ Many thanks to Igor, Sriram, Rüdiger Volk, Ben Maddison, Xueyan Song, and Zhen Tan for their valuable comments

- ◆ Your comments are welcome!

Thanks!

Backup slides

SAV Table

- By checking the source address and the actual incoming interface of each packet against the SAV table, the validity state of each packet can be considered “valid”, “invalid”, or “unknown”
 - ◆ Packets with “valid ” state should be permitted
 - ◆ Packets with “invalid” state should be blocked
 - ◆ Packets with “unknown” state can be blocked or permitted according to the SAV configurations
- More details about how to use the SAV table can be found in [draft-huang-savnet-sav-table]

Three Validity States

□ “Valid” means

- ◆ There is a source prefix in SAV table covering the source address of the packet, and the valid incoming interfaces cover the actual incoming interface of the packet

□ “Invalid” means

- ◆ There is a source prefix in SAV table covering the source address of the packet, but the actual incoming interface of the packet does not match any valid incoming interface

□ “Unknown” means

- ◆ There is no source prefix in SAV table covering the source address of the packet