Source Address Validation Enhanced by Network Controller

draft-tong-savnet-sav-enhanced-by-controller-01

Tian Tong (China Unicom)

Changwang Lin (New H3C Technologies)

Nan Wang (China Unicom)

IETF-121

Quick Review of Version 00 （IETF-120）

Motivation：

Many newly proposed Source Address Validation (SAV) mechanisms such as IGP-based and BGP-based SAVNET solutions take a distributed manner to generate SAV rules.

Distributed SAVNET solutions acquire source prefix information of other subnets within intra-domain networks or inter-domain networks utilizing BGP/IGP protocols extensions.

All devices are required to support SAVNET mechanism in order to ensure accurate validation.

There are accuracy and manageability challenges in incremental/partial deployment scenarios.

Aim：

This document proposes a network controller-based solution for enhancing SAVNET capability in intra-domain and inter-domain networks, which supports accurate verification, automated configuration, threat analysis, traceability and visualization.

clarification：

Not replacement but an enhancement of distributed SAVNET solutions.

Quick Review of Version 00
Scenarios and Requirements for Centralized SAVNET

1. Challenges and Limitations of Distributed SAVNET in Incremental/Partial deployment Scenarios.

Routers can only gather partial prefix to generate SAV rules， could not generate accurate enough SAV rules.

2. Challenges and Limitations of Distributed SAVNET with Special IP addresses, such as Anycast Prefix.

Distributed SAVNET solutions have to manually identify and manage special addresses, such as advertising anycast prefix with a special flag to indicate its anycast nature.

It significantly increases management and configuration burden.

3. Other Requirements for Centralized SAVNET：

① SAVNET routers need to be automatic configured and management.

② Threat analysis and traceability requirements.

③ Obtain information from external systems.

Such as subnet ID 、 access type 、 prefix type 、 verification mode 、 disposal strategies, etc.

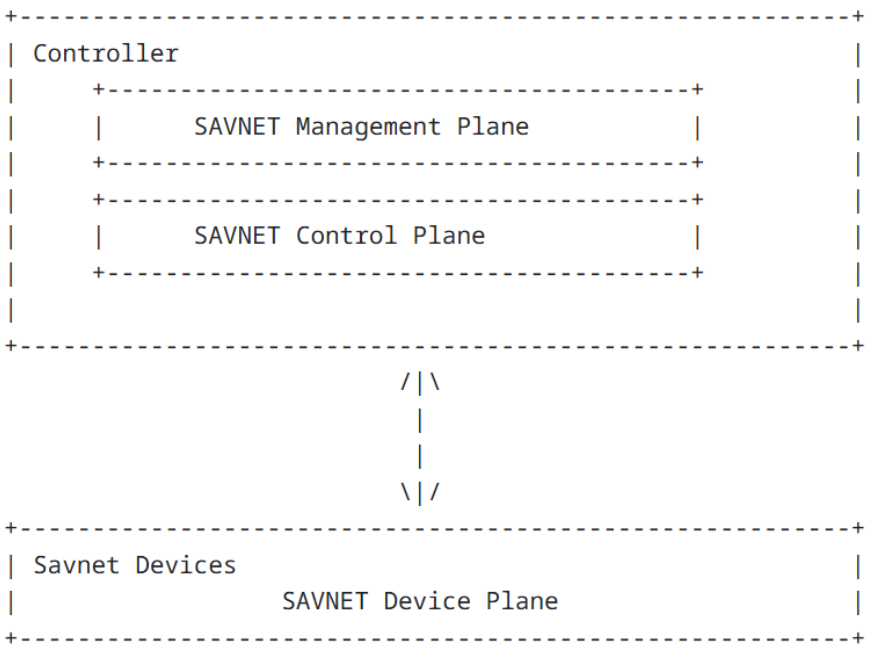
Changes in version 01

1. Centralized SAVNET capability enhancement solution:

- Overal framework.
- Function of each plane.
- Interfaces between SAVNET controller and devices.

2. Intra-domain and Inter-domain SAVNET centralised framework.

Centralized SAVNET capability enhancement solution



Centralized SAVNET framework

SAVNET Management Plane：

Monitor, configure and maintain SAVNET and Non-SAVNET devices: Devices configuration, manage and check source address prefixes and SAV rules on devices.

SAVNET Control Plane:

Generate SAV rules. The incoming interfaces of source address prefixes are calculated based on topology informations, source address prefixes, roles of devices.

Finally, SAV entries/rules are generated and sent to corresponding network devices.

SAVNET devices data plane:

1. Maintain and update SAVNET entries from different sources.
2. Source address verification and forwarde packets.

The SAVNET entries can have multiple sources:

①. From intra-domain or inter-domain device control plane protocols, see [I-D. draft-ietf-savnet-intra-domain-architecture] and [I-D.draft-wu-savnet-inter-domain-architecture] for detail.

②. From controller as well.

Interfaces in Centralized SAVNET

Report the network topology：
Basic BGP-LS in [RFC9552] applies to this document to advertise the network information to the controller.

Report source address (prefix) and SAVNET capabilities of network devices:
Extend BGP-LS or YANG model.
For BGP-LS extensions, see [I-D.draft-cheng-lsr-adv-savnet-capbility].

Report SAV rules:
Monitor and manage SAV rules through a centralized controller.
Extend BGP Link-State to collect SAV rules generated by different protocols/mechanisms in [I-D. tong-idr-bgp-ls-sav-rule] can facilitate multi-sourced SAV rule monitoring and management.

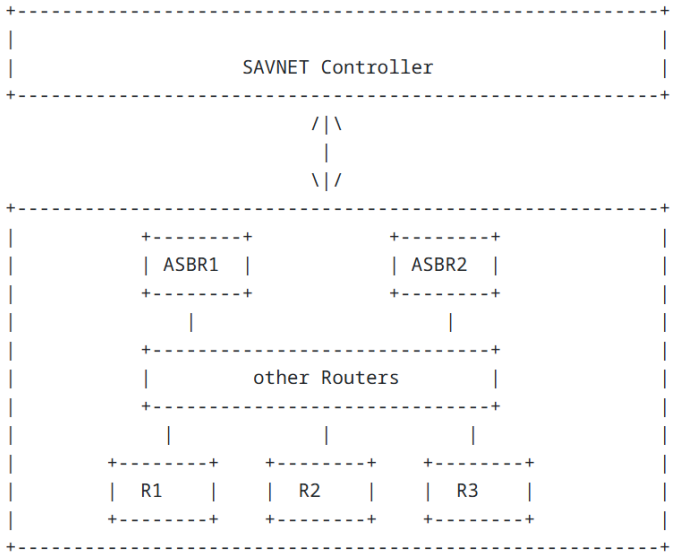
Deliver SAV rules:
SAV rules can be delivered through YANG [I-D.Li-savnet-sav-yang], BGP-LS[I-D.haas-savnet-bgp-sav-distribution] and BGP-FS [I-D.geng-idr-flowspec-sav].
When some network devices do not support SAVNET, the controller can deliver other protection policies, such as ACL rules, to the corresponding network devices.

Other interfaces:
Deliver SAV-related configuration, threat information collection,etc.

Intra-domain SAVNET Centralised Framework

Controller can implement different control policies based on roles of devices.

- Centralized SAVNET capability enhancement architecture in an intra-domain network



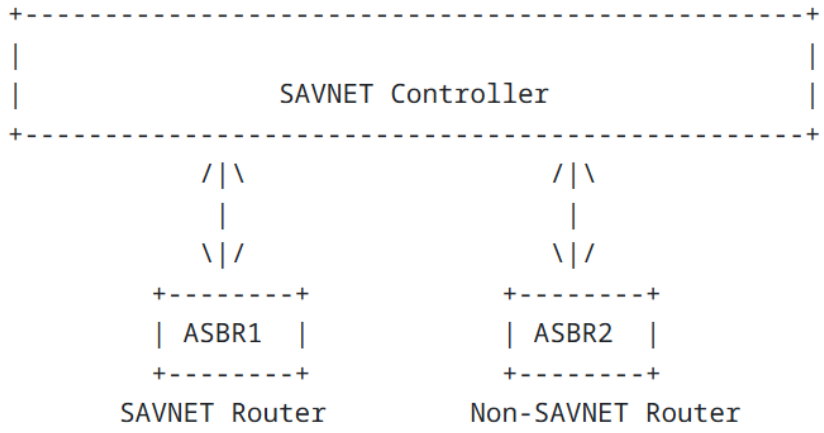
■ **AS boundary Router (ASBR):**

Blacklist policy is adopted.

① Controller collects source address (prefix) of all subnets in AS,

② Removes special IP address or prefix, such as anycast IP address,

③ Generates the SAV rule/policy in blacklist mode and sends to ASBR.

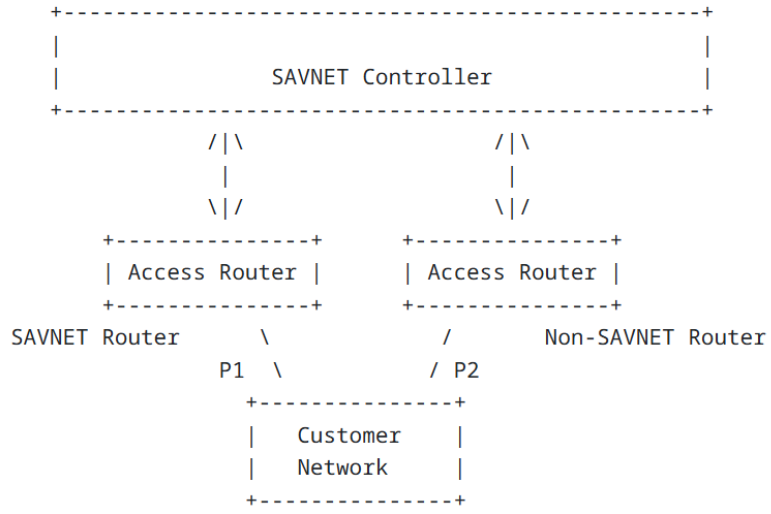


- Deliver SAV rule/policy to ASBR

■ **Access Router:**

For multi-homing access scenario, If only one router supports SAVNET and another does not, controller can generate the SAV entry of P2 and send it to R1.

Prefix-interface whitelist includes P1 and P2 to avoid false blocking in R1.



- Deliver SAV rules to access routers

■ SAVNET routers: SAV rules.

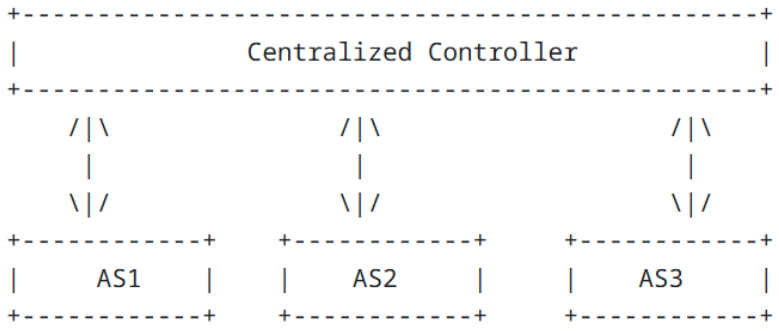
■ Non-SAVNET routers: other defense policy, such as ACL.

Inter-domain SAVNET Centralised Framework

Scenario 1: Centralized controller in single management domain with multiple ASes

If an unified controller manages multiple ASes, controller can deliver SAV rules to the devices of each AS as required.

Based on prefixes of entire AS, relationship between ASes, and third-party authentication information such as ROA objects and ASPA objects, controller can calculate the SAV rules of the entire management domain and deliver SAV rules to the corresponding devices.

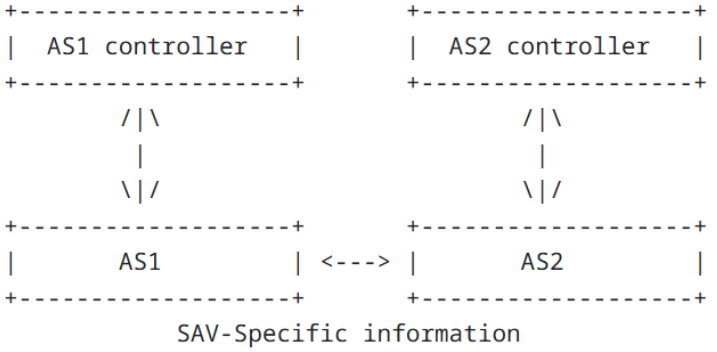


- Centralized controller with one controller within multiple ASes

Scenario 2: Different ASes has different controllers:

Each controller collects complete prefixes of its AS and sends to its ASBRs. ASBRs generate inter-domain SAV-Specific information and advertise to ASBRs of neighboring AS.

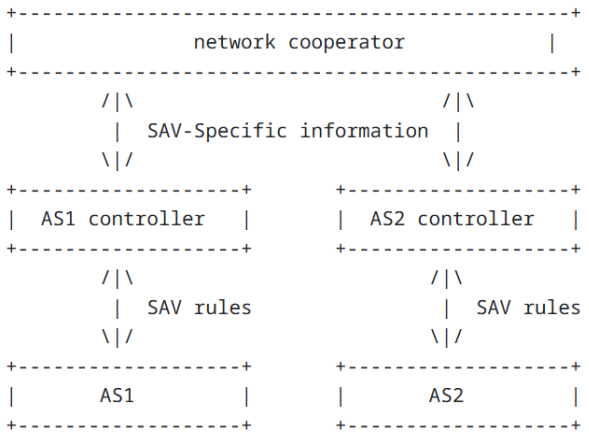
Controllers can also deliver synchronization key to ASBRs to ensure the reliability and flexibility of inter-domain SAV-Specific information transmission.



- Different ASes has different controllers

Scenario 3: ASBR can not generate inter-domain SAV-Specific information

If ASBR do not support SAVNET and can not generate inter-domain SAV-Specific information, information can be advertised through network cooperator for rapid deployment. Each controller can generate SAV rules and advertise to ASBR to achieve SAV.



- generate SAV-Specific information by network cooperator

Next Step

- **Request to adopt this document.**

Now that we have seen there are several centralized interface extensions and YANG model：

① [I-D.cheng-lsr-adv-savnet-capbility] Signal SAVNET capablity and source prefix used for SAV to controller using IGP and BGP-LS.

② [I-D. tong-idr-bgp-ls-sav-rule] Report multi-sourced SAV rules using BGP-LS extension.

③ [I-D.Li-savnet-sav-yang] Allow operators to manage SAV configuration and deliver SAV rules in a heterogeneous environment with routers supplied by multiple vendors.

④ [I-D.haas-savnet-bgp-sav-distribution] Deliver SAV rules using BGP.

⑤ [I-D.geng-idr-flowspec-sav] Deliver SAV rules using BGP-Flowspect.

⑥ [draft-cheng-savnet-intra-domain-oam] OAM using Controller for intra-domain SAVNET

So, the centralized SAVNET framework document is general and really necessary.

- **What we're going to refine next?**

We will add several usecases:

Case 1: More accurate intra-domain edge protection.

Case 2: More accurate intra-domain border protection.

Case 3: More accurate Inter-domain protection.

Case 4: More accurate protection with anycast IP address.

- **More review...**

Thank You

Appendix: Challenges and Limitations of Distributed SAVNET in Incremental/Partial deployment Scenarios

Devices are upgraded gradually due to various limitations such as device performance, version and vendor.

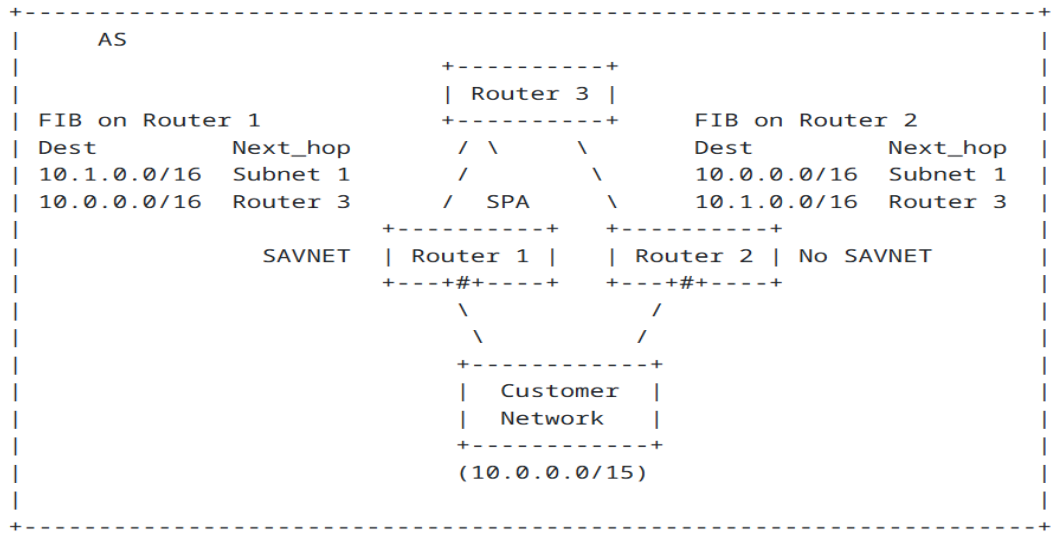


Figure 1: Asymmetric multi-homing scenario in incremental deployment of intra- domain

R1 is a SAVNET router while R2 is a non-SAVNET router.
R1 can only gather partial prefix to generate SAV rules.
R2 uses FIB for SAV:

- R2 deploy Strict URPF: Improper block.
- R2 deploy Loose URPF: Improper pass.

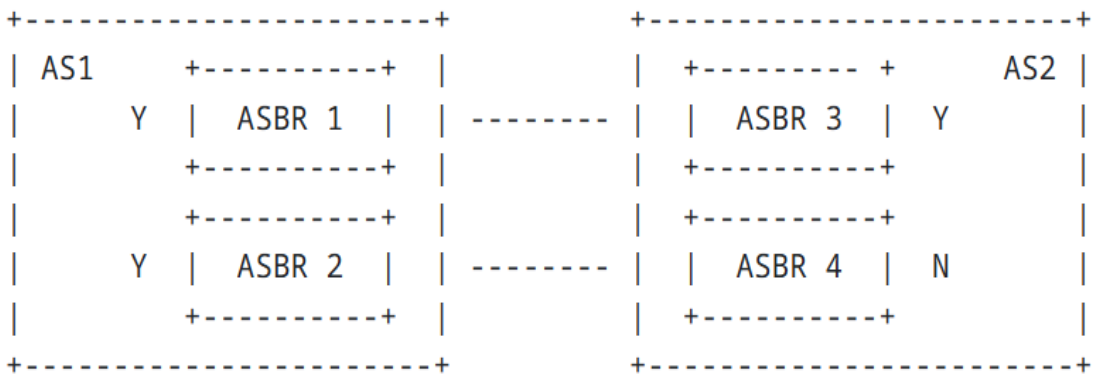


Figure 2: Partial deployment of Savnet for inter-domain

ASBR1/2/3 are SAVNET routers while ASBR4 is a non-SAVNET router, so ASBR4 cannot generate accurate SAV rules without obtaining SAV-specific information from other routers in its AS and other AS.

Routers with distributed SAVNET could not generate accurate SAV rules in incremental/partial deployment scenario.
Furthermore, enhancing the protective effectiveness and incentives of SAVNET in this scenario is necessary, too.

Appendix: Challenges and Limitations of Distributed SAVNET with special IP addresses

P1~P4 are common prefixes, while P5 is an anycast prefix that has multiple legitimate origins. If R1could not recognize P5 as anycast address:

- Interfaces a, b, and c: SAVNET whitelist.
- Interfaces d and e: blacklist with P5. Improper block.

To prevent anycast prefix from being inadvertently added to a blacklist,

Router1 must advertise P5 with a special flag to indicate its anycast nature.

Distributed SAVNET solutions have to manually identify and manage special addresses, such as anycast addresses scenario.

It significantly increases management and configuration burden.

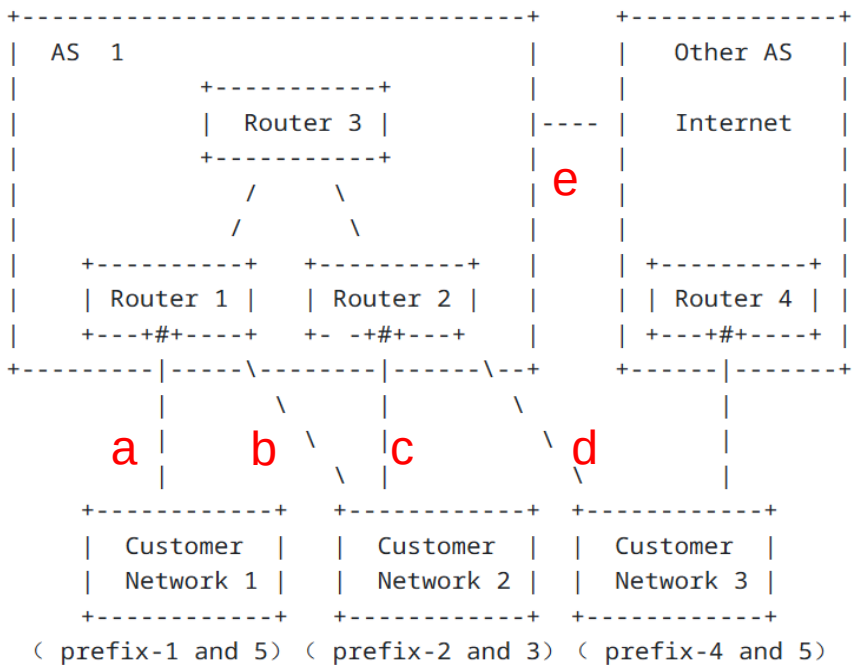


Figure 3: Impact of anycast prefix

In centralized SAVNET, the prefix type can be ascertained and configured on the edge router via a controller.

Appendix: Other Requirements for Centralized SAVNET

SAVNET routers need to be configured

- Disposal strategies should be configured on SAVNET routers. such as drop, rate-limit or permit for forged packets.
- Subnet ID and access type 、 prefix type.
- Verification Modes such as whitelist and blacklist.

Automatic configuration

Centralized network controller can deliver subnet and prefix information, dynamically adjust the authentication modes, disposal strategies for SAVNET routers by configuration delivery, offering greater flexibility in network management.

Obtain information from external systems

To ensure network security, ASBRs need gather RPKI ROA objects and ASPA objects from RPKI cache server.

Centralized controller is more suitable for establishing information exchange channel with RPKI cache server than routers.

Analysis and traceability requirements

Distributed SAVNET does not have the capability of threat packet analysis and threat source tracing.

Centralized controller can gather source address forgery packets from SAVNET routers, enable centralized analysis and tracing, visualizing the attack's source and target. Enhanced effectiveness of SAV significantly.

Avoid IP addresses and IP prefix conflicts. Avoid disrupt standard SAVNET operations.