T. Tong
China Unicom
C. Lin
New H3C Technologies
N. Wang
China Unicom
Internet-Draft
Intended status: Informational
Expires: 4 September 2025
3 March 2025

Source Address Validation Enhanced by Network Controller
draft-tong-savnet-sav-enhanced-by-controller-02

Abstract

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, but they are faced with accuracy and managability challenges in incremental/partial deployment scenarios. 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.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-tong-savnet-sav-enhanced-by-controller/.

Discussion of this document takes place on the Source Address Validation in Intra-domain and Inter-domain Networks Working Group mailing list (mailto:savnet@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/savnet/. Subscribe at https://www.ietf.org/mailman/listinfo/savnet/.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

Distributed SAVNET solutions utilize protocol message exchanges among SAVNET routers to acquire source prefix information related to other subnets within intra-domain networks or inter-domain networks, such as Source Prefix Announcement (SPA) technology for intra-domain SAVNET, which can be transmitted by a new protocol or an extension to an existing protocol [I-D.li-savnet-source-prefix-advertisement]. Nonetheless, under circumstances characterized by device heterogeneity, partial upgrades, asymmetric routing, and peculiar address, these solutions face diminished accuracy in Source Address Validation (SAV). Furthermore, there are necessities for enhancement in areas such as automated configuration, threat analysis, traceability, and visualization.

In this document, on the basis of distributed intra-domain and inter-domain SAVNET architecture, we propose a controller-based and centralized SAVNET enhancement solution. The distributed SAVNET solutions rely on local routing information and SAV-specific information. In this solution, the controller can generate and deliver SAV rules based on the global information, and can also obtain ROA and other external information to generate inter-domain SAV rules, so as to achieve accurate source address verification (SAV) in both intra-domain and inter-domain in a combination of centralized and distributed ways.

In this solution, SAVNET routers and non-SAVNET routers can cooperate via the network controller. More accurate source address verification rules can be generated based on more comprehensive information in the scenario of partial/incremental deployment of SAVNET. Concurrently, the SAVNET can support accurate verification, automated configuration, threat analysis, traceability and visualization.

1.1. Terminology

* SAV: Source Address Validation

* AS: Autonomous System

* SAV-Specific Information: Information specialized for SAV rule generation, exchanged between routers or from the network controller.

* SAV-related Information: The information used by a router to make SAV decisions. For intra-domain SAV, SAV-related information includes both local routing information and SAV-specific information.

* SAV-specific Information Communication Mechanism: The mechanism for exchanging SAV-specific information between routers. It can be either a new protocol or an extension to an existing protocol.

* SAV Information Base: A table or data structure in a router that stores specific SAV information and local routing information.

* SAV Rule: The rule in a router that describes the mapping relationship between a source address (prefix) and the valid incoming interface(s). It is used by a router to make SAV decisions and is inferred from the SAV Information Base or from network controller.

* SAVNET Router: An intra-domain router which runs intra-domain SAVNET.

* SAVNET Agent: The agent in a SAVNET router that is responsible for communicating SAV-specific information, processing SAV-related information, and generating SAV rules.

* AS Edge Router: An intra-domain router of an AS which is connected to client subnets.

* AS Border Router: An intra-domain router of an AS which is connected to other ASes.

* Improper Block: The validation results that the packets with legitimate source addresses are blocked improperly due to inaccurate SAV rules.

* Improper Permit: The validation results that the packets with spoofed source addresses are permitted improperly due to inaccurate SAV rules.

* ISP: Internet Service Provider.

2. Scenarios and Requirements for Centralized SAVNET

This section introduces the scenarios and requirements of centralized SAVNET, including incremental/partial deployment scenario, obtain information from external systems, automated configuration, analysis and traceability requirements,etc.

2.1. Challenges and Limitations of Distributed SAVNET in Incremental/ partial deployment

The current distributed solution which exchanges SAV-specific information between SAVNET routers depends on devices upgrade. Devices utilize the source prefix advertisement (SPA) information to notify other routers about their subnet and prefix information. Unique subnet ID for each subnet should be planned by network manager, and additional identification information such as subnet ID and access mode on the corresponding port of the device should be configured manually, so as to generate more accurate SAV rules.

However, devices are upgraded gradually due to various limitations such as device performance、version and vendor. As a result, in an AS, there are some routers support SAVNET and others do not.

Routers with distributed solution could not generate accurate SAV rules in incremental/partial deployment scenario. Refer to [I-D.li-savnet-intra-domain-architecture] and [I-D.li-savnet-inter-domain-architecture].Though the SAVNET router can obtain routing information from the local RIB/FIB and generate SAV rules for certain prefixes, in the absence of SAV-specific information, the SAV generated based on the local RIB/FIB has the risk of the improper block and improper permit in special scenarios such as asymmetric routing scenario.

Figure 1 illustrates the asymmetric routing in a multi-homing subnet scenario which has been raised in [I-D.ietf-savnet-intra-domain-problem-statement]. Subnet 1 has a prefix of 10.0.0.0/15 and is connected to two edge routers, Router 1 and Router 2. Due to the load balancing policy in the inbound direction of subnet 1, R1 can only learn subnet prefix 10.1.0.0/16 from subnet 1, while R2 can only learn subfix 10.0.0.0/16 from subnet 1. After that, R1 learns another subnet prefix through the intra-domain routing protocol, and so does R2. The FIB of R1 and R2 are shown in Figure 1. R1 is a SAVNET router and R2 is a non-SAVNET router, and R1 and R2 communicate with each other through R3, regardless of whether R3 is a SAVNET router or not, the SPA message cannot be delivered and R2 cannot generate its own SAV-specific information or recognize the SAV-specific information transmitted from R1. Therefore, R1 can only collect part of the prefix information of the subnet to generate SAV rules, and R2 uses the FIB for SAV, then improper block will occur in both R1 and R2 due to incomplete information.

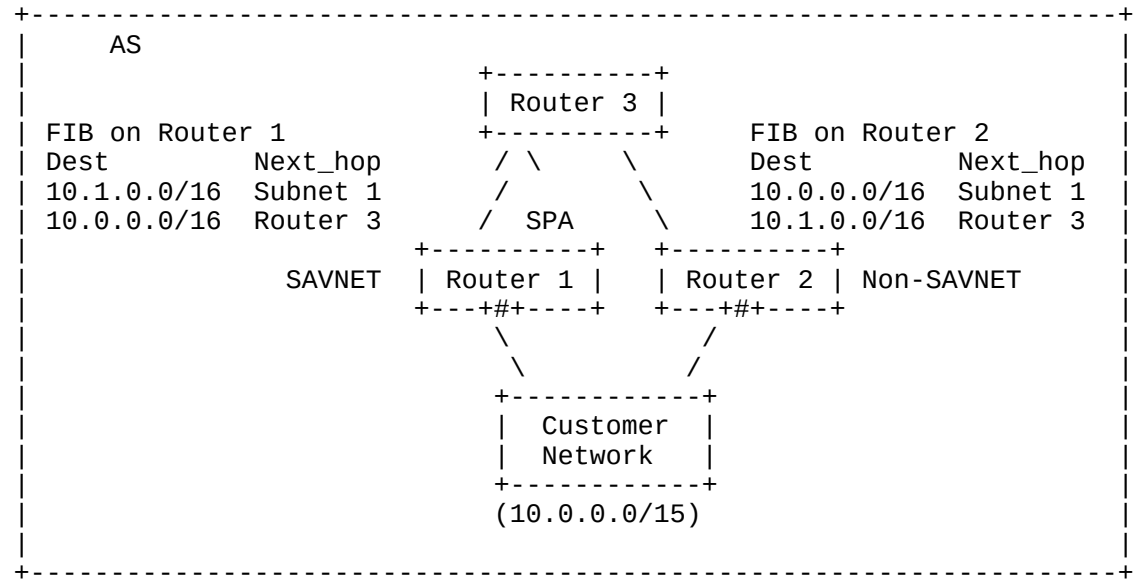

Figure 1: Asymmetric multi-homing scenario in incremental deployment of intra- domain

Incremental/partial deployment for inter-domain include: (1) devices partially support SAVNET in an AS; (2) some ASs support SAVNET, while others do not. Figure 2 shows that ASBR1/2/3 are SAVNET routers while ASBR4 is a non-SAVNET router, ASBR4 cannot generate accurate source address verification rules without obtaining SAV-specific information from other AS and other routers in its AS.

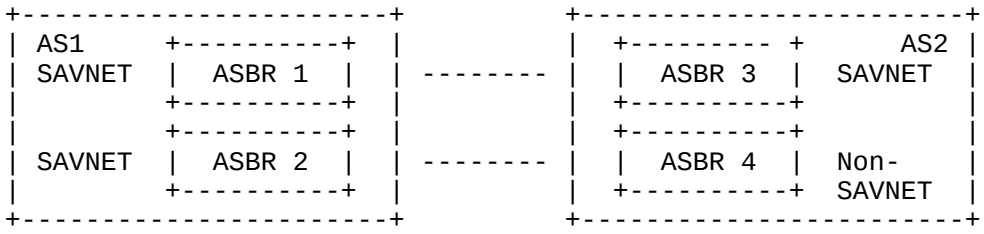

Figure 2: Partial deployment of Savnet for inter-domain

As a result, there is a problem of low accuracy in partial/ incremental deployment scenarios. In addition, how to improve the protection effect and enhance the incentive is also one of the enhanced capabilities.

2.2. Obtain information from external systems

ASBR in each AS collects the SAV-specific information in its AS domain and synchronizes the SAV-specific information with the ASBR of the adjacent AS domain, and also obtains the RPKI ROA and ASPA information, as well as general information such as RIB, FIB, IRR, etc.Based on the above information sources, each AS generates a relatively complete source address verification table. So each AS needs to establish an information exchange channel and mechanism with the RPKI ROA to ensure network security, but routers shouldn't directly interact with the RPKI ROA and other external systems, and a controller is appropriate to obtain information such as RPKI ROA and ASPA.

2.3. Automated configuration

Due to the existence of special addresses in the network, such as anycast addresses, the existing distributed SAVNET solutions need to manually identify special addresses and adopt corresponding policies, which brings high management overhead.

For example, in Figure 3, P1~P4 are common prefixes, P5 is an anycast prefix with multiple legitimate origins including customer network 1, customer network 3 and external Internet. SAVNET with whitelist to be generated on interfaces a, b, and c, and SAVNET blacklist can be generated on interfaces d and e. If subnet 1 could not recognize P5 as an anycast prefix, the blacklist of interfaces d and e includes prefix P5, causing legitimate packets with P5 as the source to be filtered by mistake when they enter from interfaces d and e. Therefore, in order not to include an anycast prefix in a blacklist, it needs to use a special flag to indicate the anycast prefix when subnet 1 advertises the prefix P5 through the SPA. Prefix type can be obtained and configured on the edge router through the controller if centralized management is possible,.

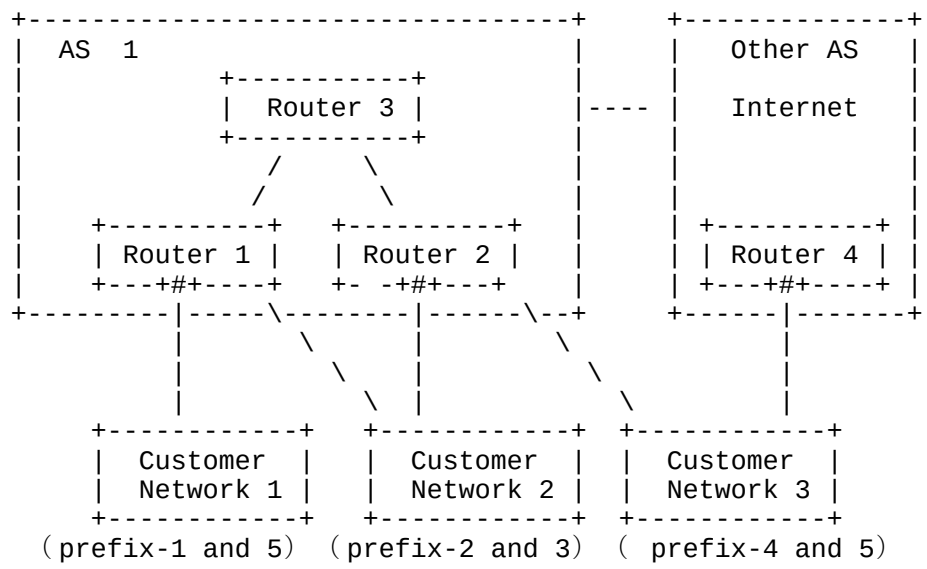

Figure 3: Impact of anycast prefix

In addition, network providers assign access devices, access ports, and public IP addresses to users who connect to their networks, so that the address allocation system in the carrier’s network contains information about the customer’s network. Source address verification technology can be combined with address allocation systems to automate configuration and achieve traceability based on source prefix. Centralized network controller can switch the authentication mode of all SAVNET routers flexibly through the delivery configuration.

2.4. Analysis and traceability requirements

Current scheme provides flexible verification modes such as dropping, rate limiting, or allow for the forged packets in the latest draft sav_table [I-D.huang-savnet-sav-table]. It will play a great role if the controller can collect more source address forgery information from the router, analyze and trace the source in a centralized manner, visualize the source and target of the attack and threat tracing. Besides, with the continuous expansion of the network scale and the increasing allocation of IP addresses, IP address conflicts include IP address conflicts and IP prefix conflicts will appear, which affects the normal network operation. The controller can find whether the prefixes are reused by checking the prefixes and their binding subnet ID.

3. Centralized SAVNET capability enhancement solution

A high-level view of the Centralized SAVNET framework, without expanding the functional entities in network controller and Savnet devices, is illustrated in Figure 4.

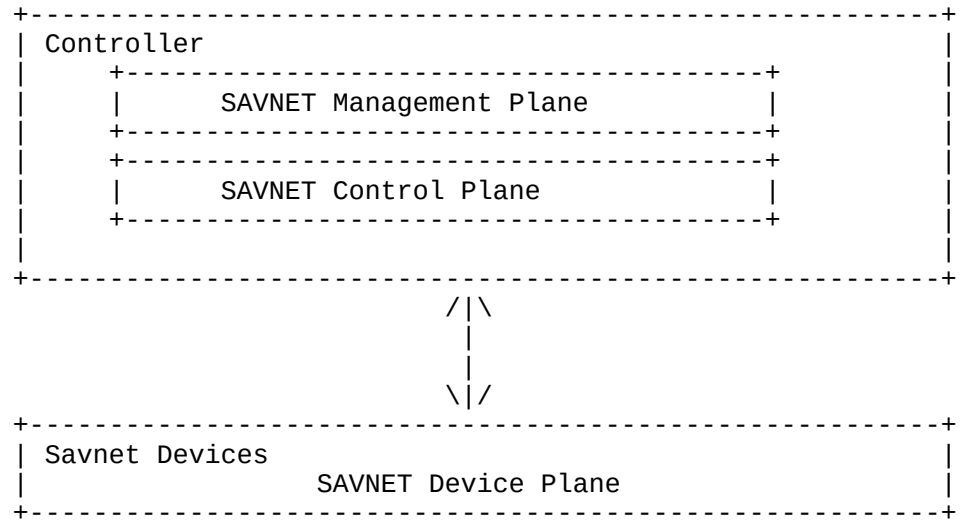

Figure 4: SAVNET capability enhancement architecture based on network controller

The following planes are defined: SAVNET Management Plane：Responsible for monitoring, configuring and maintaining SAVNET devices and Non-SAVNET devices,including delivering configuration to the devices, displaying and managing source address prefixes and SAV rules on devices.

SAVNET Control Plane: Responsible for generating SAV rules. The incoming interfaces of source address prefixes are calculated based on topology informations, the source address prefixes, roles of devices. Finally, SAVNET entries/rules are generated and sent to the corresponding network devices.

SAVNET device data plane: Responsible for maintaining and updating SAVNET entries from different sources, source address verification on the data forwarding plane and forwarding packets. The SAVNET entries can have multiple sources. SAV rules may be derived from intra-domain or inter-domain control plane protocols, see [I-D. draft-ietf-savnet-intra-domain-architecture-01] and [I-D.Raft -wu-savnet-inter-domain-architecture-11] for detail. SAV rules may be from the controller as well.

The following interfaces are defined: Report the network topology: The basic BGP-LS as specified in [RFC9552] applies to this document to advertise the network information to the controller. Report source address prefixes and SAVNET capabilities of network devices: Extend BGP-LS or YANG model to report source address prefixes and SAVNET capabilities of devices. For BGP-LS extensions, see [I-D.draft-cheng-lsr-adv-savnet-capbility-00].

Report SAV rules: Monitor and manage SAV rules through a centralized controller. The protocol extensions of BGP Link-State to collect source address validation (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]. Detailed definition of SAV rules can see [I-D.draft -huang-savnet-sav-table-07]. When some network devices do not support SAVNET, the controller can deliver other protection policies, such as ACL rules, to the corresponding network devices.

3.1. Key technologies in Intra-domain SAVNET enhancement

This section describes the intra-Domain SAV Enhancement based on Controller. Figure 5 illustrates Centralized SAVNET capability enhancement architecture in an intra-domain network. Centralized Controller can support accurate verification, automated configuration, threat analysis, traceability and visualization.

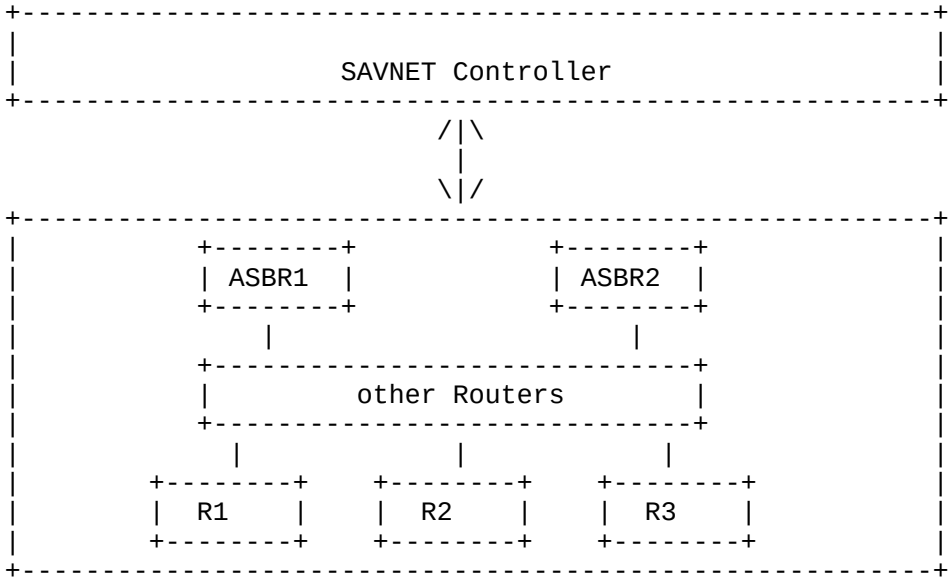

Figure 5: intra-domain SAVNET capability enhancement architecture based on network controller

As shown in the figure above, when SAVNET is deployed in the intra-domain, controller can implement different control policies based on roles of devices. For the boundary devices in the domain, the blacklist policy is adopted. For the multi-homing access devices in the domain, the controller delivers multi-homing SAV rules in a centralized manner.

Deliver SAV rules in intra-domain: (1) AS Boundary Router (ASBR): The controller collects source address prefixes of all subnets in the AS domain, removes special IP addresses or prefixes, such as anycast IP addresses, generates the SAV rules/policies（in blacklist mode）containing all source address prefixes of the AS, and sends the SAV rules/policies to the ASBR. The SAV rules are generated and delivered to the routers that support SAVNET, and other defense policies, such as ACL (filtering specific source addresses on specific incoming interfaces), are generated and delivered to the routers that do not support SAVNET.

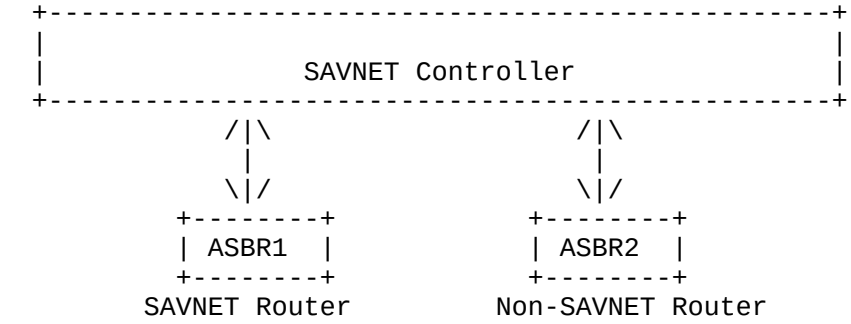

Figure 6: Deliver SAV rules to AS Border Routers

(2) Access Router: If a subnet is connected to two access routers and only one router supports SAVNET and the other does not, the controller can generate the SAV entry of P2 and send it to access router R1. The prefix-interface whitelist of access router R1 includes P1 and P2 to avoid false blocking. The controller can also generate ACL entries with prefixes P1 and P2 and send them to the access interface of access router R2 which does not support SAVNET.

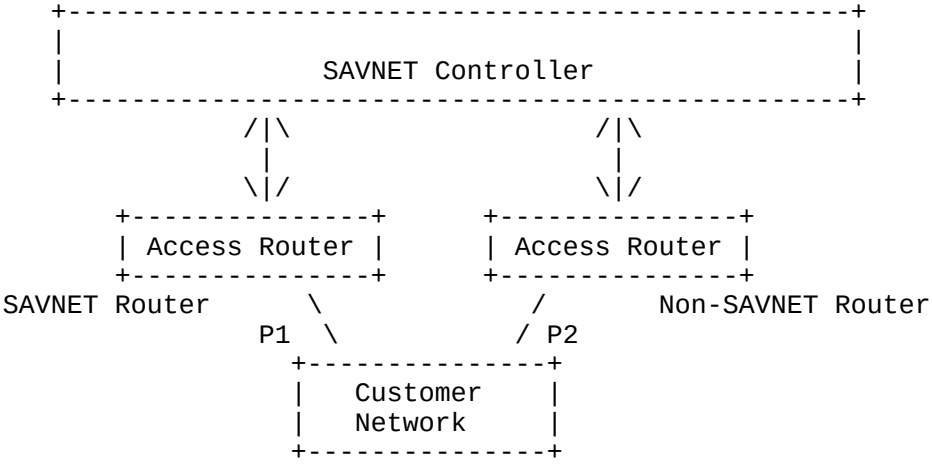

Figure 7: Deliver SAV rules to access routers

3.2. Key technologies in Inter-domain SAVNET enhancement

In inter-domain source address verification, the controller can also play an important role.

* Scenario 1: Centralized controller in single management domain including multiple ASes:

An ISP has multiple ASes in actual network deployment. If a unified controller manages multiple ASes, the controller can deliver SAV rules to the devices of each AS as required.

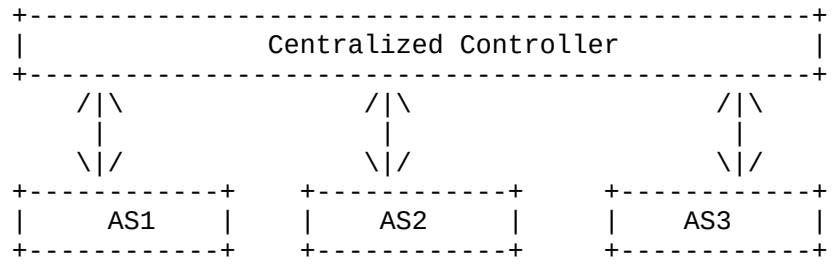

Figure 8: Centralized controller in single management domain with multiple ASes

Based on the source addresses prefixes of the entire network, relationships between ASes, and third-party authentication information such as ROA objects and ASPA objects, the controller can calculate the SAV rules of the entire management domain and deliver SAV rules to the corresponding devices. For a description of the delivery of SAV rules, see 5.1.

* Scenario 2: Different ASes has different controllers

When different ASes have their own controllers, each controller collects the complete source address prefixes of the local AS and sends them to the ASBR. The ASBR generates the inter-domain SAV-Specific information and advertises it to the ASBR of the neighboring AS. As shown in Figure 9, not all routers in AS1 and AS2 support SAVNET, AS1 and AS2 controllers collect the complete source address prefixes and send to their own ASBRs respetively. The controller can also deliver the synchronization key to the ASBR to ensure the reliability and flexibility of inter-domain SAV-Specific information transmission.

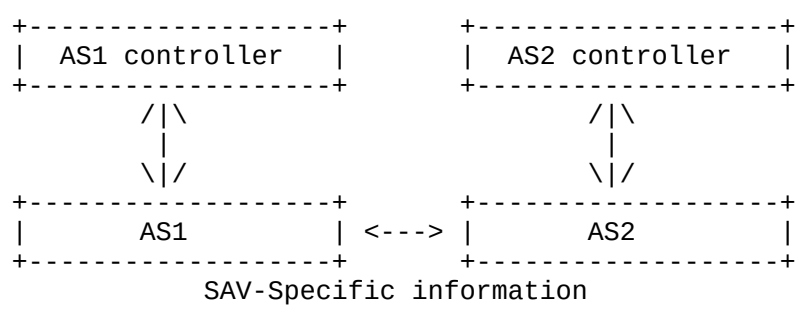

Figure 9: Centralized controller with one controller within multiple ASes

Besides, if ASBR of an AS do not support SAVNET and can not generate the inter-domain SAV-Specific information, SAV-Specific information can be advertised through network cooperator for rapid deployment as shown in Figure 9. Each controller can generate SAV rules based on SAV-Specific information and advertise to ASBRs to achieve source address verification.

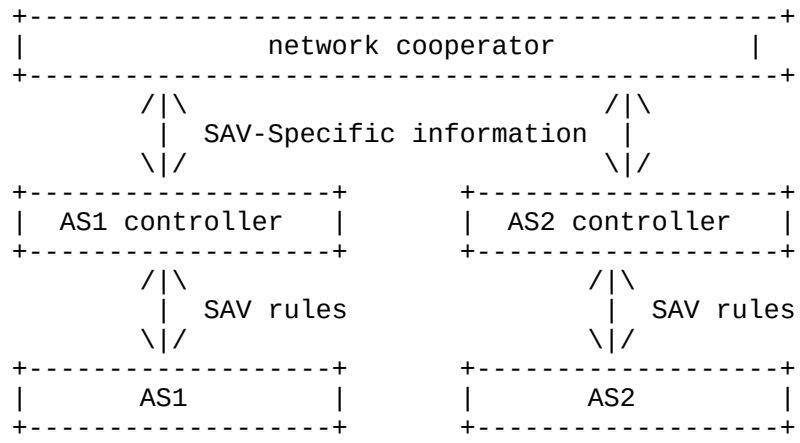

Figure 10: Centralized controller with one controller within multiple ASes

4. Use Case

Several use cases will illustrate that centralized SAVNET can achieve more accurate and comprehensive SAV when SAVNET is partially deployed in network.

4.1. Case 1: More effective intra-domain edge and boundary protection in incremental/partial deployment scenario

Figure 11 illustrates the asymmetric routing in a multi-homing subnet scenario. R1 and R2 serves as the edge router. R3 serves as the border egress. Partial SAVNET deployment: R1 lacks SAVNET support, while R2 and R3 are SAVNET-enabled.

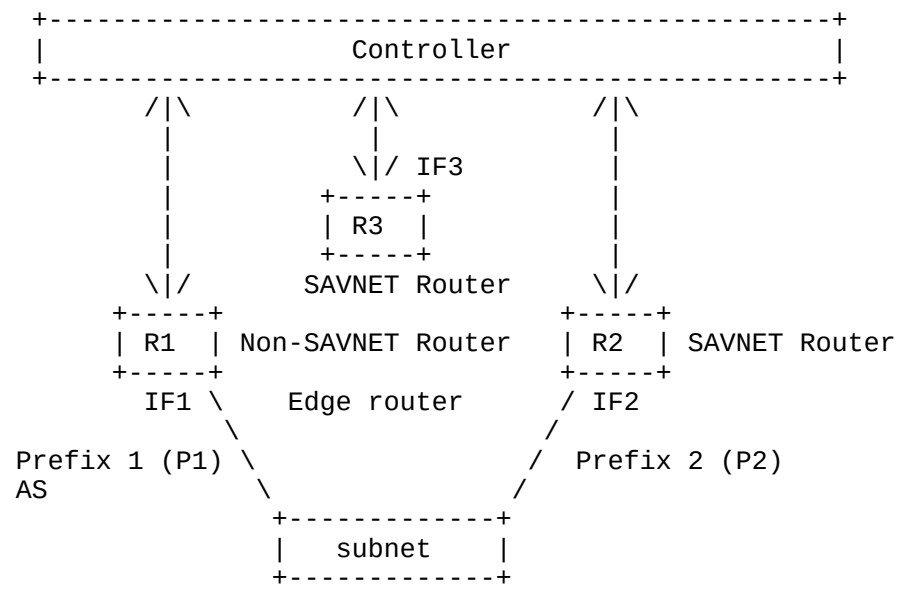

Figure 11: asymmetric routing in a multi-homing subnet scenario

(1)Distributed SAVNET limitations:

R1 (SAVNET-disabled): Fails to advertise P1 via SAVNET protocol. Thus:R2's interface IF2 cannot generate a whitelist covering both P1 and P2.R3's interface IF3 cannot create a blacklist for P1, leaving it unprotected. R2 (SAVNET-enabled): Advertises P2 via SAVNET protocol successfully. R3 (SAVNET-enabled): blocks P2 traffic on IF3 but allows P1 spoofing.

Test Results: Tester A sending P1/P2/P3 traffic to R1 and R2: --R1 (IF1): No blocking (No protection). --R2 (IF2): P1 blocked (improper block).

Tester B spoofing P1/P2/P3 to R3: --R3 (IF3): P2 blocked, P1/P3 allowed (insufficient protection).

(2)SAVNET enhancement with centralized controller:

Controller Actions: --Collects subnet prefix P1 from R1 and P2 from R2. --Delivers ACL whitelist (P1+P2) to R1's IF1 and SAV rules to R2's IF2. --Delivers blacklist (P1+P2) to R3's IF3.

Test Results: Tester A: P1/P2 allowed on R1's IF1 and R2's IF2. P3 blocked. No improper blocking (full protection). Tester B: P1/P2 blocked on IF3, P3 allowed (precise control).

4.2. Case 2: More effective intra-domain boundary protection with Non-SAVNET Border Devices

Edge routers R1/R2 support SAVNET, but border router R3 does not (Figure 12).

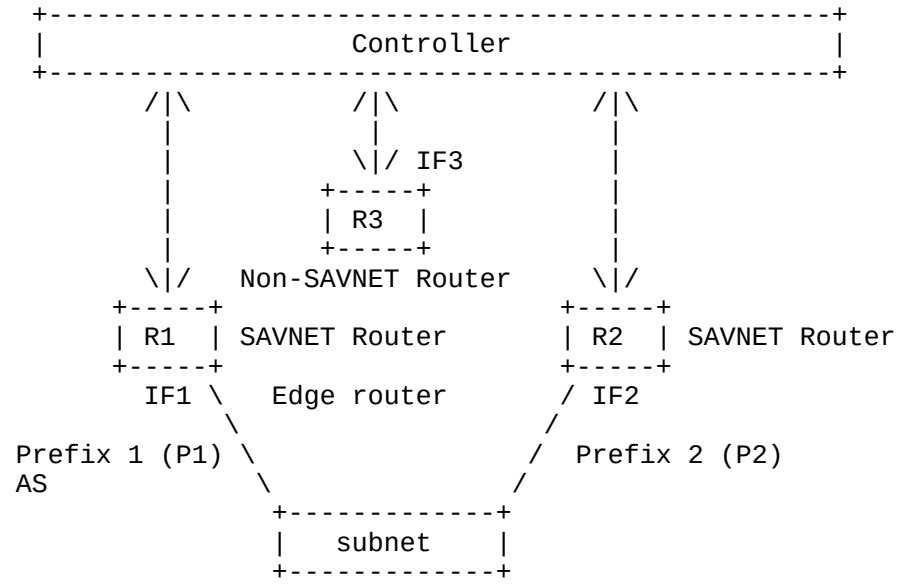

Figure 12: More effective intra-domain boundary protection

(1)Distributed SAVNET limitations: R3 cannot process SAVNET messages from R1/R2, leaving P1/P2 unprotected.

Test Results: Tester B(spoofing P1/P2/P3 to R3): All traffic permitted (zero protection).

(2)SAVNET enhancement with centralized controller:

Controller Actions: - Aggregates P1 (from R1) and P2 (from R2). - Delivers unified blacklist (P1+P2) to R3’s IF3.

Test Results: Tester B: P1/P2 blocked; P3 allowed (boundary secured).

4.3. Case 3: More accurate anycast IP protection

Edge routers R1/R2 and border router R3 all support SAVNET. Subnet advertises sub prefixe P1 (anycast IP) via R1 and P2 via R2.

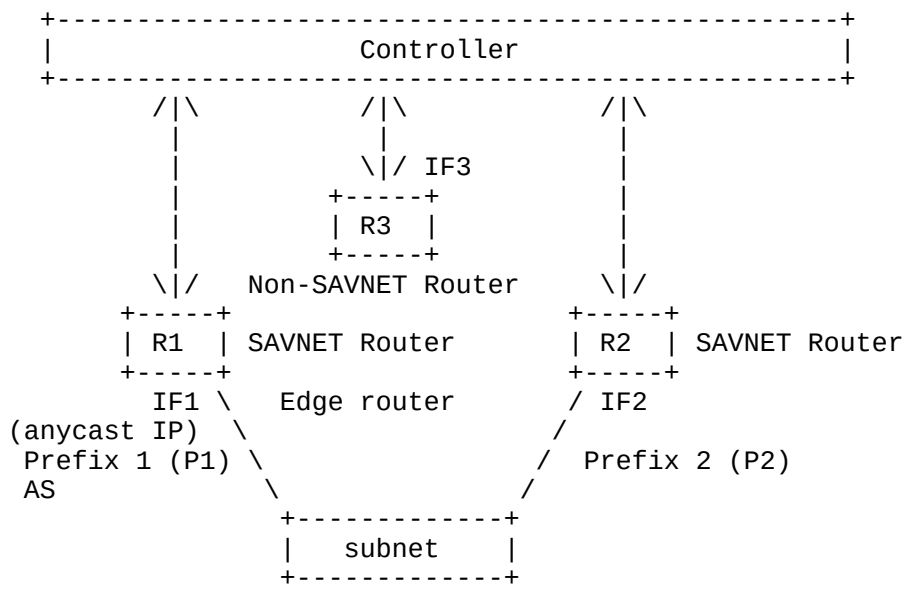

Figure 13: More accurate anycast IP protection

(1)Distributed SAVNET Challenge: Anycast conflict: P1 is also advertised by other AS, leading to ambiguous SAV rules. Risk: Legitimate P1 traffic may be incorrectly blocked by boundary router.

Test Results: Tester B sending P1/P2 traffic to R3: P2 blocked; anycast P1 blocked (improper block).

(2)SAVNET enhancement with centralized controller: Controller Actions: Correlates P1 with AS-specific topology data. Generates context-aware SAV rules to distinguish legitimate anycast traffic.

Test Results: Tester B: P2 blocked; P1 permitted (Prevent improper block).

4.4. Case 4: Enhanced inter-domain SAV via SDN controller

Operators obtain IP blocks and AS numbers from registries, assigning them to network segments or business units. Controller-Driven Optimization: SDN controller aggregates AS-number-to-IP mappings from carrier registries. Delivers complete SAV tables to ASBRs (Autonomous System Border Routers). Impact: Eliminates spoofed inter-domain traffic (e.g., forged source IPs outside assigned ranges).Achieves more accuracy in inter-domain SAVNET.

5. Security Considerations

TBD.

6. IANA Considerations

TBD.

7. Acknowledgments

TBD.

8. References

8.1. Normative References

[RFC9552] Talaulikar, K., Ed., "Distribution of Link-State and Traffic Engineering Information Using BGP", RFC 9552, DOI 10.17487/RFC9552, December 2023, <https://www.rfc-editor.org/rfc/rfc9552>.

8.2. Informative References

[I-D.huang-savnet-sav-table]
Huang, M., Cheng, W., Li, D., Geng, N., Liu, Chen, L., and C. Lin, "General Source Address Validation Capabilities", Work in Progress, Internet-Draft, draft-huang-savnet-sav-table-08, 10 December 2024, <https://datatracker.ietf.org/doc/html/draft-huang-savnet-sav-table-08>.

[I-D.li-savnet-inter-domain-architecture]
"*** BROKEN REFERENCE ***".

[I-D.li-savnet-intra-domain-architecture]
Li, D., Wu, J., Qin, L., Geng, N., Chen, L., Huang, M., and F. Gao, "Intra-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-li-savnet-intra-domain-architecture-07, 16 March 2024, <https://datatracker.ietf.org/doc/html/draft-li-savnet-intra-domain-architecture-07>.

[I-D.li-savnet-intra-domain-problem-statement]
Li, D., Wu, J., Qin, L., Huang, M., and N. Geng, "Source Address Validation in Intra-domain Networks Gap Analysis, Problem Statement, and Requirements", Work in Progress, Internet-Draft, draft-li-savnet-intra-domain-problem-statement-07, 11 March 2023, <https://datatracker.ietf.org/doc/html/draft-li-savnet-intra-domain-problem-statement-07>.

[I-D.li-savnet-source-prefix-advertisement]
Li, D., Geng, N., and L. Qin, "Source Prefix Advertisement for Intra-domain SAVNET", Work in Progress, Internet-Draft, draft-li-savnet-source-prefix-advertisement-01, 20 October 2024, <https://datatracker.ietf.org/doc/html/draft-li-savnet-source-prefix-advertisement-01>.

Authors' Addresses

Tian Tong
China Unicom
Email: tongt5@chinaunicom.cn

Changwang Lin
New H3C Technologies
Email: linchangwang.04414@h3c.com

Nan Wang
China Unicom
Email: wangn161@chinaunicom.cn