# Source Address Validation enhanced by Network Controller

**draft-tong-savnet-sav-enhanced-by-controller-00**

Tian Tong (China Unicom)

Changwang Lin (New H3C Technologies)

Nan Wang (China Unicom)

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.**

**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.

# 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.

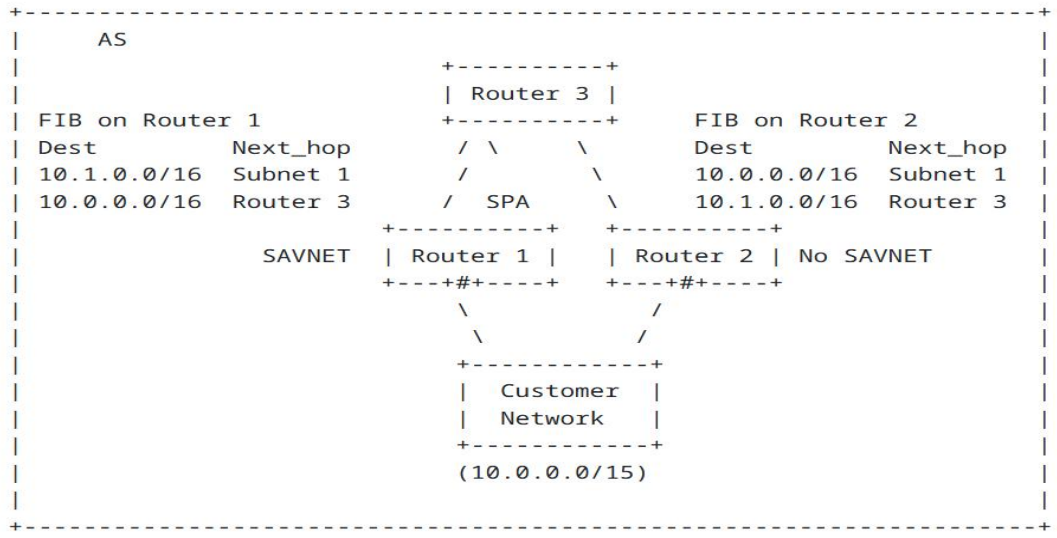


Figure 1: Asymmetric multi-homing scenario in incremental deployment of intra- domain

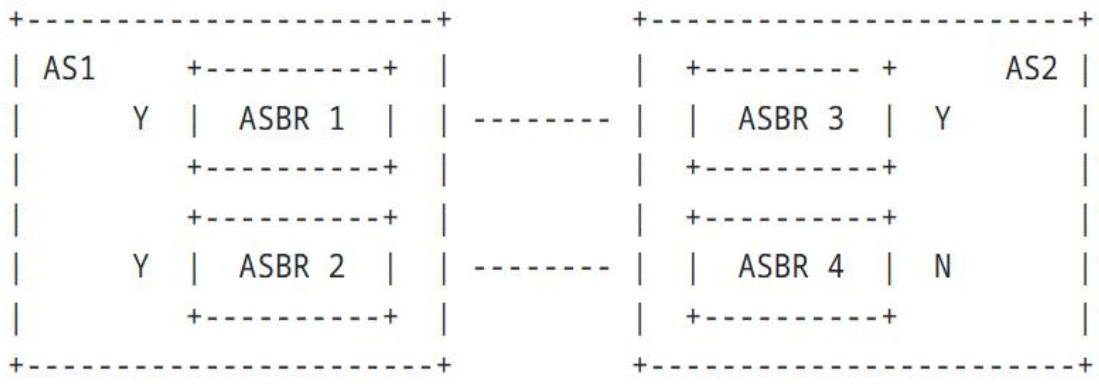


Figure 2: Partial deployment of Savnet for inter-domain

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.

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.

# 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.**

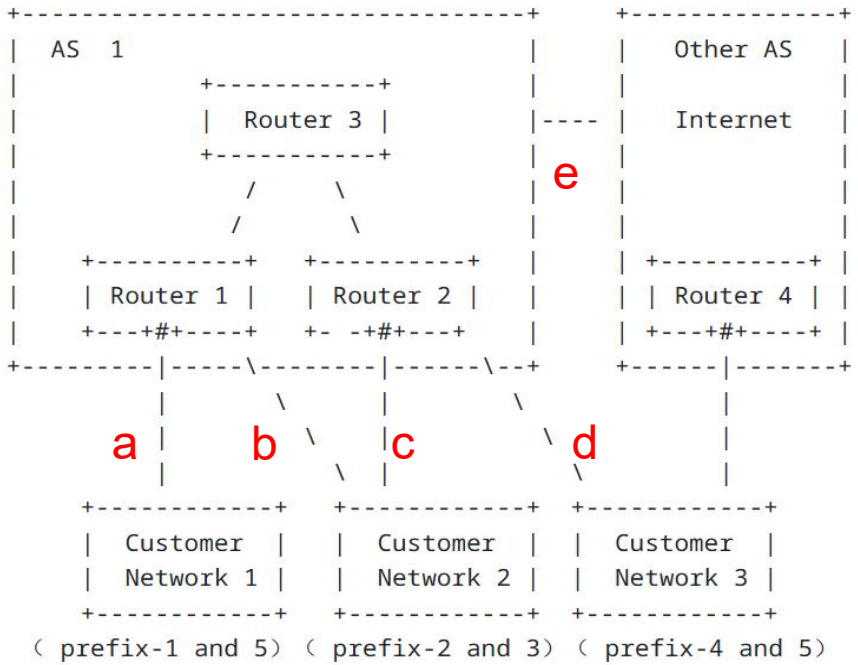


Figure 3: Impact of anycast prefix

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

# Other Requirements for Centralized SAVNET

## ■ SAVNET routers need to be configured

- Disposal strategies shoule 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.

# Centralized SAVNET solution

## Intra-domain SAVNET enhancement

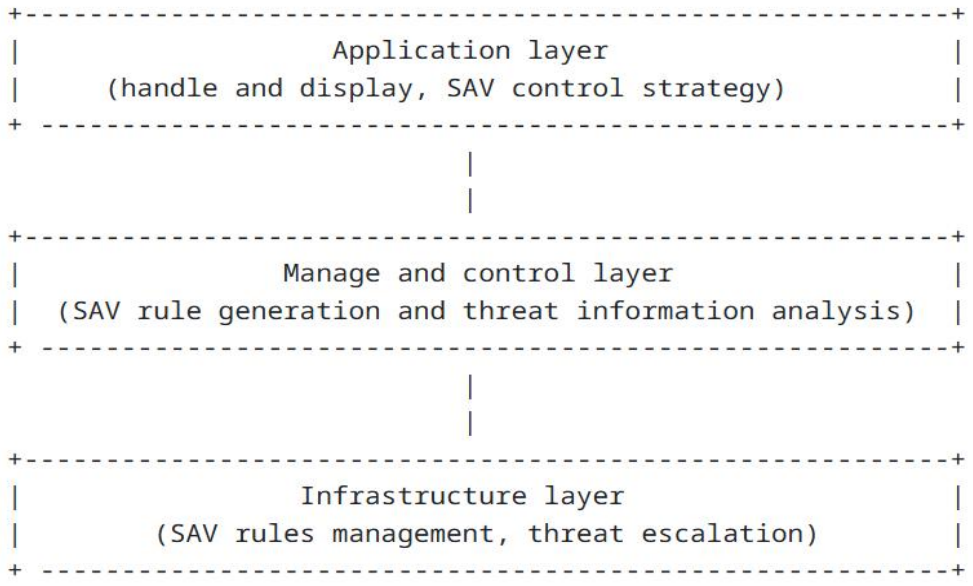


Figure 5: In-domain SAVNET capability enhancement architecture based on network controller

SAV capability enhancement system consists of infrastructure layer, management and control layer, application layer.

- Infrastructure layer is divided into data plane and control plane.
- Management and control layer refers to a centralized network controller.
- Application layer at the upper layer can obtain external SAV control policies and display SAV threat information.

## Inter-domain SAVNET enhancement

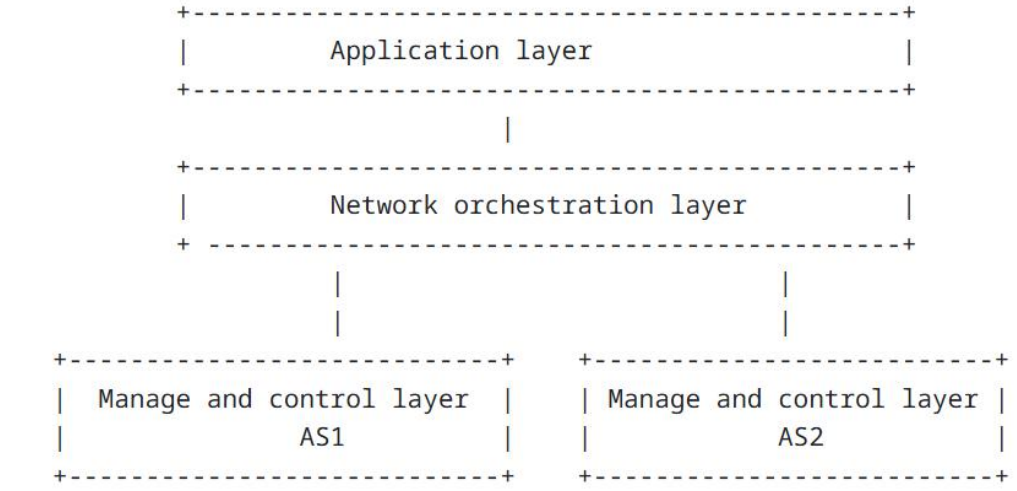


Figure 6: Inter-domain SAVNET capability enhancement architecture based on network controllers

- Controller collect all SAV-related information within an AS, generate SAV rules and deliver them to edge/border routers.
- Controller generates SAV rules based on the SAV-specific information obtained by the SAVNET ASBR and sends them to ASBR that do not support SAVNET.
- Interface with external systems to generate more accurate rules.
- Supports automated configuration, threat analysis, traceability and visualization.

# Next Steps : Scheme design

This section describes the key technologies, centralized SAV rule generation and use cases.

## 4.1. Key technologies

Key function module of devices and controller, and the interfaces between devices and controller. TBD.

## 4.2. Centralized SAV rule generation

Centralized SAV rules generation method and steps. TBD.

## 4.3. Use Case

Several use cases will illustrate that centralized SAVNET can achieve more accurate and comprehensive SAV.

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.

- Possible implementation and verification
- Any comments or any suggestions?

# Thank You