SAVNET Group
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

S. Yue
China Mobile
X. Song
ZTE Corporation
C. Lin
New H3C Technologies
N. Geng
Huawei Technologies

3 March 2025

# SAVNET Use Cases
## draft-ys-savnet-use-cases-02

## Abstract

This document introduces the use case for Source Address Validation (SAV) applied in intra-domain and inter-domain telecommunication networks. It describes the typical routing implements and possible improvements for SAV in the use cases.

## 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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 September 2025.

## Copyright Notice

Table of Contents



## 1. Introduction

The Source Address Validation in Intra-domain and Inter-domain Networks (SAVNET) use cases provides the typical applications at telecommunication field. Considering the network topology and technology used in these applications have big difference, the possible improvement schema for Source Address Validation (SAV) may have different considerations.

This document specifically identifies the SAV use case for telecommunication networks and provides possible SAV validation location but does not suggests any specific design for SAV architecture and protocol. The SAVNET architecture introduced at [I-D.ietf-savnet-inter-domain-architecture] and [I-D.ietf-savnet-intra-domain-architecture].

This document serves the purpose of helping those learning SAVNET applications and understand the possible influence brought by SAVNET to telecommunication scenarios and provides necessary considerations for SAV solution design.

## 2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. Mobile Transport Network

### 3.1. Description

A telecom network refers to the network composed of user terminal equipment, transmission equipment, switches and telecom operators room. The communication devices and equipment interconnect to provide high flexible and dedicated services to users. The telecom network in this document is mainly related to 5G transport network, 6G transport network, etc.

### 3.2. Implementation

The following figure shows a typical 5G Transport network architecture.

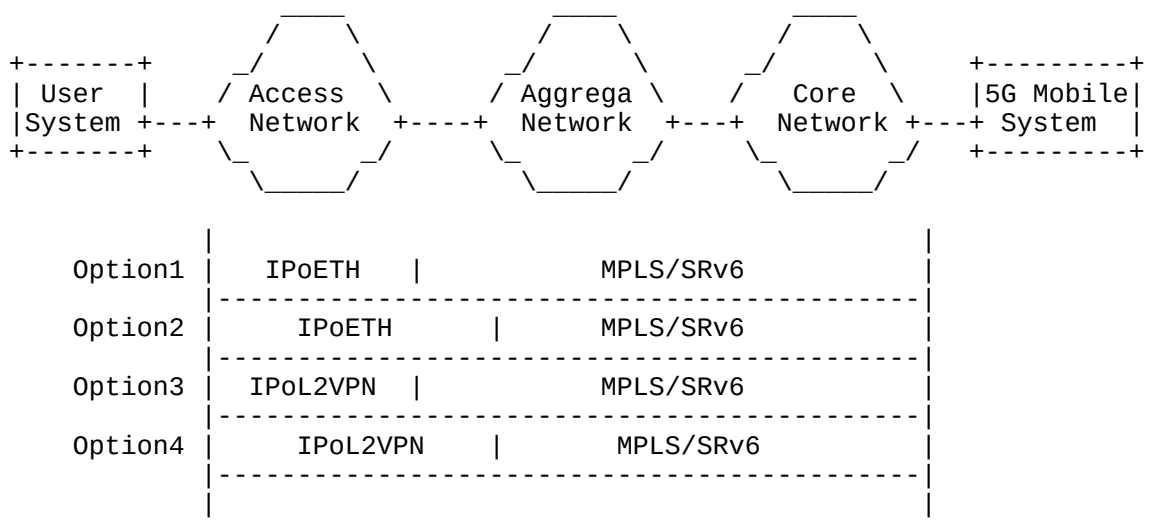


Figure 1: An example for mobile transport network Scenario

From the implementation in NG (R)AN network there are optional connection links between CSG and Edge Node (between Access Network and Aggregation Network) which use IP or Ethernet technology. The

more common deployment is to use MPLS/SRv6 as overlay technology to carry data packets. The LTE or 5G traffic will be transported through either a L3VPN or an L2VPN or EVPN over MPLS or SRv6 with or without segment routing.

Please noted the scope of SAVNET is the validation of IPv4 and IPV6 addresses. The validation of label packets with MPLS deployments in Mobile Transport Network is out of the scope of the SAVNET. When the transport network is an SRv6 network, it may use IGP or BGP protocol extensions to support the necessary SAV information transport.

#### 3.2.1. Possible improvements for SAV

As described and analyzed at the previous section, there is no need for SAVNET in MPLS/VPN network. The only location for SAVNET is in Access Network but SAVI function MAY be required and enough for source address validation.

However, in the case of an AS cross-domain network for the communication between different Service Providers, the raw IPv4/IPv6 traffic is transported through EBGP technology so in order to reduce source address spoofing attack EBGP protocol SHOULD support SAVNET feature to validate the traffic accessed from other external AS domains.

### 3.3. Multi-homing Scenario

The following figure shows an example for multi-homing scenario in mobile transport network. When network access users are dual-homed to aggregation network devices, assume that the network access users have two prefixes, P1 and P2, which are advertised to the aggregation devices. Due to the asymmetric configuration of routing priorities, deploying strict uRPF on the aggregation devices may lead to false blocking, while loose uRPF may result in false passing. The existing technologies cannot solve this problem, and the optimized SAVNET technology needs to be adopted.

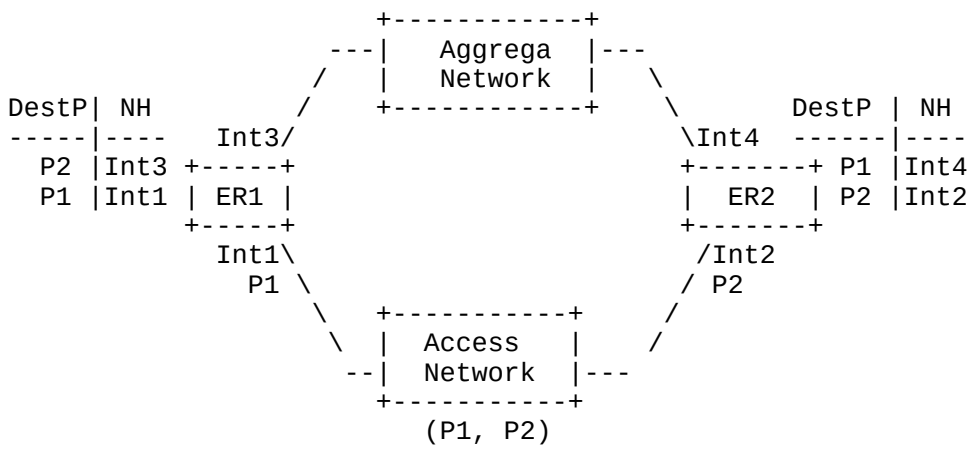


Figure 2: An example for multi-homing network Scenario

Case1: Users from Access Network advertise P1 to ER1 and P2 to ER2. On both ER1 and ER2, the routing priority of the user-side for the same prefix is higher than that of the network-side. The FIB on ER1 and ER2 are showed below:

For ER1: Prefix P1, outgoing interface: Int1; Prefix P2, outgoing interface: Int3.

For ER2: Prefix P2, outgoing interface: Int2; Prefix P1, outgoing interface: Int4.

Case2: Users from Access Network advertise both P1 and P2 to ER1 and ER2. The routing priority settings are as follows:

On ER1, the routing priority of the user-side for P1 is higher than that of the network-side, while the routing priority of the user-side for P2 is lower than that of the network-side.

On ER2, the routing priority of the user-side for P2 is higher than that of the network-side, while the routing priority of the user-side for P1 is lower than that of the network-side. The FIB on ER1 and ER2 are showed below:

For ER1: Prefix P1, the outgoing interface is Int1; Prefix P2, the outgoing interface is Int3.

For ER2: Prefix P2, the outgoing interface is Int2; Prefix P1, the outgoing interface is Int4.

Case3: Users from Access Network advertise the sub-prefix of P1 and the parent prefix of P1+P2 to ER1, and advertise the sub-prefix of P2 and the parent prefix of P1+P2 to ER2. On both ER1 and ER2, the routing priority of the user-side for the same prefix is higher than that of the network-side. The FIB on ER1 and ER2 are showed below:

For ER1: Prefix P1, outgoing interface: Int1; Prefix P2, outgoing interface: Int3; Parent prefix, outgoing interface: Int1.

For ER2: Prefix P2, outgoing interface: Int2; Prefix P1, outgoing interface: Int4; Parent prefix, outgoing interface: Int2.

### 3.3.1. Possible improvements for SAV

In the dual-homing scenario described in Section 3.3.1, there may be traffic with the source address of P1 flowing in through the Int2 interface of the ER2 device. If strict uRPF is deployed, there will be problems of improper filtering. If loose uRPF is deployed, there will be problems of improper passing. Optimized SAVNET rules are required to achieve more accurate source address filtering.

## 4. Fixed Transport Network

### 4.1. Description

A Fixed Transport Network refers to the network consists of optical transport, which physically connects all the fixed network nodes, may involve residential gateway, optical equipment, switch/router and broadband network gateway. The typical fixed transport network may across the wireline and wireless access, metro and backbone IP networks.

### 4.2. Implementation

The following figure shows a typical Fixed Transport Network architecture.

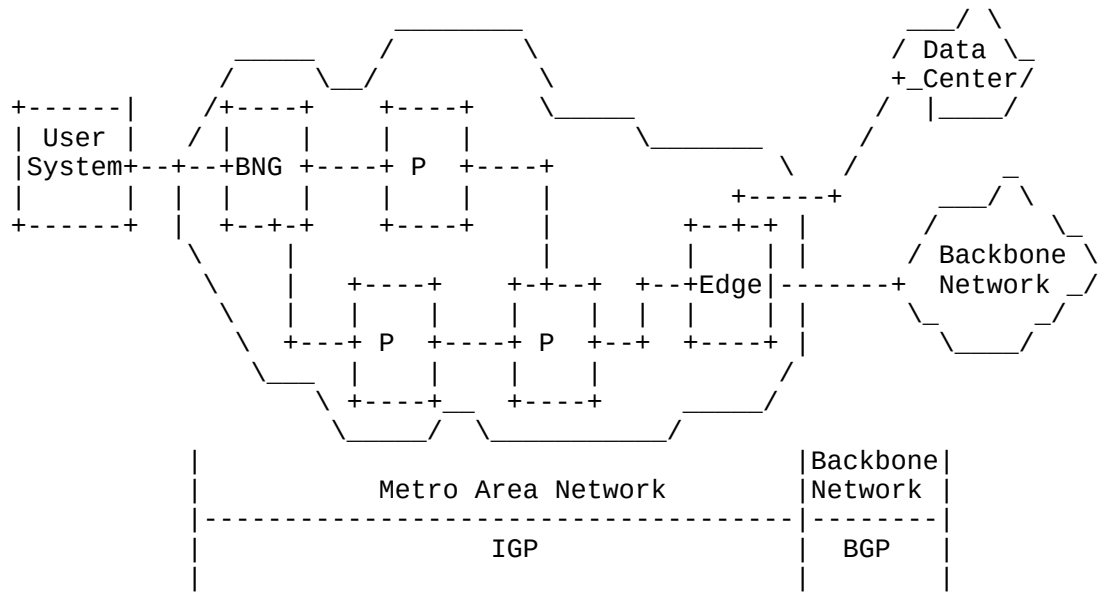


Figure 3: An example for fixed transport network Scenario

From the network levels perspective, it divides into residential Access Network (AN), Metro Area Network (MAN) and Backbone Network (BN).

From the implementation in AN network there are optical connection links between fixed user and broadband network gateway (BNG) nodes which use IP or Ethernet technology. The BNG attached AAA server allocates ipv4/ipv6 address to fixed users the access traffic from user to fixed network will be validated at BNG.

The MAN network usually implements IGP (i.e., ISIS, OSPF) routes to achieve the path connection between network nodes. Meanwhile the service traffic uses MPLS/VPN with/without segment routing technology as traffic overlay.

The BN network usually implements BGP (i.e., eBGP) to achieve inter-domain network path connection.

### 4.3. Possible improvements for SAV

It’s assumed that the most feasible way for packets validation is at the location closest to the traffic for filtering invalid address or mitigating source address spoofing. As described at the previous section, the traffic directed from user to network server the BNG is considered as a suitable validation entity. And for the reverse traffic directed from DC/contents server to user the most feasible way to validate external spoofing traffic is at the location of edge routers of BN network. If there is no SAV function implemented at edge routers of BN network, it’s expected to implement SAV function at MAN network nodes.

With the selection of the SAV validation entity and the use of SAV function to the network nodes at Fixed Transport Network, the incoming traffic from user and the external traffic from DC/content server can be validated effectively. It may use IGP or BGP protocol extension to support necessary SAV information transport.

For the SAV function used at BNG, there is an optional way to achieve source validation function:

For the upstream traffic (from user to server)

1. After receiving a packet from a broadband user, the BNG applies the SAV function to determine whether the source address of the packet belongs to the legitimate user and the inbound port.

2. If yes, packets are forwarded according to the specified rules.

3. If no, packets are discarded or redirected according to the specified rules.

For the downstream traffic (from server to user)

1. BNG advertises the source route prefix of broadband users to the upstream routers and receives the reachable route from the upstream router. The network topology is reachable.

2. After receiving the traffic from the server, the BNG applies the SAV function to check whether the source address of the packet is valid and whether it matches the expected inbound port.

3. If yes, packets are forwarded according to the specified rules.

4. If no, packets are discarded or redirected according to the specified rules.

The SAV policy may be different to upstream and downstream traffic. For example, the upstream traffic is mainly from valid users the SAV function is suggested to use allowlistt filtering policy like ACL; while the downstream traffic from internet or DC servers the SAV policy may apply allowlistt and blocklist filtering policy.

The detailed SAV policy and function is out of the scope of this document. There is an optical way described at [I-D.cheng-savnet-intra-domain-sav-igp].

## 5. Data Center Network

### 5.1. Description

A data center network consists of routers, switches, firewalls, storage systems and servers to provide reliable network connectivity and secured data transport to satisfy applications or business demands. The network components require underlay infrastructure to support the data center hardware and software implementation. Driven by the scale of computing, the traditional network has scaled up and to satisfy large-scale requirements network virtualization is incorporated to data center to optimize network infrastructure. And network topology for data center has evolved from the traditional access-aggregation-core to the Clos-based spine-leaf network architecture.

### 5.2. Implementation

The following figure shows an example for data center network topology.

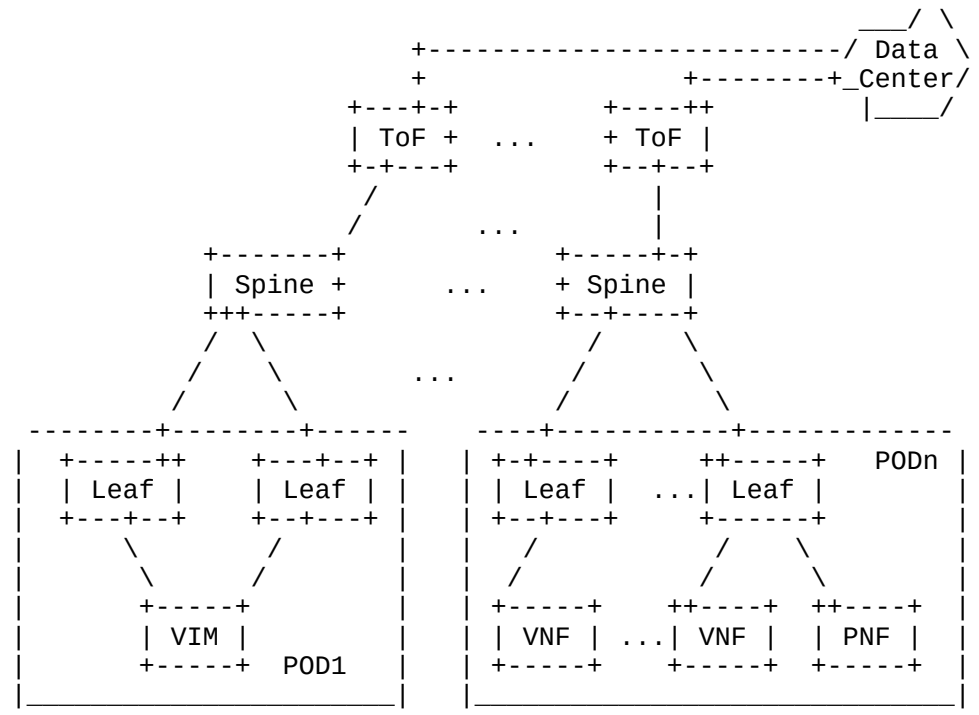


Figure 4: An example for fixed transport network

Data center network deploys as underlay or overlay network model for specific service requirements. Underlay networks typically use Ethernet switching, VLAN, routing (e.g., OSPF, ISIS, BGP) to generate Equal-Cost Multi-Path (ECMP) routs between network nodes at the same level to improve network reliability and reduce network congestion. The packet encapsulation may perform at layer 2 or layer 3. Overlay networks may configure BGP EVPN service over VXLAN or GRE tunnels over IGP or BGP routing connections. RFC7938 introduces a method to support routing in large-scale data centers using BGP. RIFT protocol (see draft-ietf-rift-rift) is designed for spine-leaf Clos networks and naturally support large-scale data center networks.

## 5.3. Possible Improvements for SAV

The data center security is very critical for network storage, management and data processing to protect applications, data and users. Applying security controls to data center to protect it from threats that could compromise integrity, confidentiality, authentication and availability of data or applications. The threats of spoofing traffic with invalid source address for one specific interface is in the scope of the document, other threats are out of

the scope.

If network nodes in the DC communicate with each other at layer 2, then the packet transport using MAC learning and MAC address spoofing is usually done when attacker is on the inside of the network. The MAC address spoofing mitigation is out of the scope. If network nodes communicate with each other at layer 3, the IP address spoofing attacks are usually from outside of the network. The incoming interface of Leaf or Spine nodes requires to deploy SAV methods to filtering spoofing traffic. The ToF nodes MAY require deploy SAV-similar methods to filtering the invalid traffic from other DCs.

To mitigate IP source address spoofing attacks, the physical/virtual switches and routers in data center networks SHOULD have spoofing traffic filtering functions, such as ACL, uRPF-like, and SAVNET mechanisms. The routing protocols such as IGP, BGP and RIFT need extensions to support SAVNET policies for filtering invalid route prefixes and make right decisions for packets processing.

## 6. Security Considerations

TBD.

## 7. IANA Considerations

This document has no requests for IANA.

## 8. Acknowledgements

TBD.

## 9. Informative References

[I-D.cheng-savnet-intra-domain-sav-igp]
Cheng, W., Li, D., Lin, C., and Yue, "Intra-domain SAVNET Support via IGP", Work in Progress, Internet-Draft, draft-cheng-savnet-intra-domain-sav-igp, 27 June 2024, <https://datatracker.ietf.org/doc/html/draft-cheng-savnet-intra-domain-sav-igp>.

[I-D.ietf-savnet-inter-domain-architecture]
Li, D., Wu, J., Huang, M., Chen, L., Geng, N., Liu, L., and L. Qin, "Inter-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-architecture, 6 August 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-architecture>.

[I-D.ietf-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-ietf-savnet-intra-domain-architecture, 16 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-architecture>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

## Authors' Addresses

Shengnan Yue
China Mobile
China
Email: yueshengnan@chinamobile.com

Xueyan Song
ZTE Corporation
China
Email: song.xueyan2@zte.com.cn

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

Nan Geng
Huawei Technologies
China
Email: gengnan@huawei.com