LSR Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 23, 2024

W. Cheng
China Mobile
D. Li
Tsinghua University
C. Lin
New H3C Technologies
S. Yue
China Mobile

February 23,2024

Intra-domain SAV Support via IGP
draft-cheng-savnet-intra-domain-sav-igp-01

Status of this Memo

Copyright Notice

Abstract

This document describes a Dynamic calculation SAVNET mechanism by extending IGP protocol in intra-domain scenarios. This mechanism can propagate SAV-related information through IGP messages to help routers automatically generate accurate SAV rules which are for checking the validity of data packets.

Table of Contents

1. Introduction....3
2. Terminology....4
3. Design Goals....5
4. Solution....6
4.1. Overview....6
4.2. SAVA RULE....8
4.2.1. Composition of the SAVNET Rule....8
4.2.2. Origin of the Source Prefix....8
4.2.3. Advertisement of the Source Prefix....9
4.3. Procedure....12
5. Protocol Extension....15
5.1. IS-IS Protocol Extension....15
5.1.1. IS-IS Extended Source Prefix sub-TLV....15
5.2. OSPF Protocol Extension....15
5.2.1. OSPF Extended Source Prefix sub-TLV....15
5.3. OSPFv3 Protocol Extension....16
5.3.1. OSPFv3 Extended Source Prefix sub-TLV....16
6. Example....16
7. Manageability Considerations....18
8. Deployment Considerations....18
9. IANA Considerations....19
10. Security Considerations....19
11. References....19
11.1. Normative References....19
11.2. Informative References....20
Acknowledgments....20
Authors' Addresses....20

1. Introduction

In communication networks, network devices typically forward packets based only on their destination addresses, without verifying the authenticity of the source addresses. As a result, forging the source addresses raises a large number of network security problems. The main problems are as follows, as shown in Figure 1:

* Attackers attack important websites, causing them to be inaccessible and interfering with the normal use of important services by legitimate user.

* Attackers conceal their true identity and location, making it difficult to trace the source of illegal network activities.

* Attackers interfere with the normal operation of services such as accounting, management, and security authentication based on real source addresses, causing a large amount of network resources to be misappropriated.

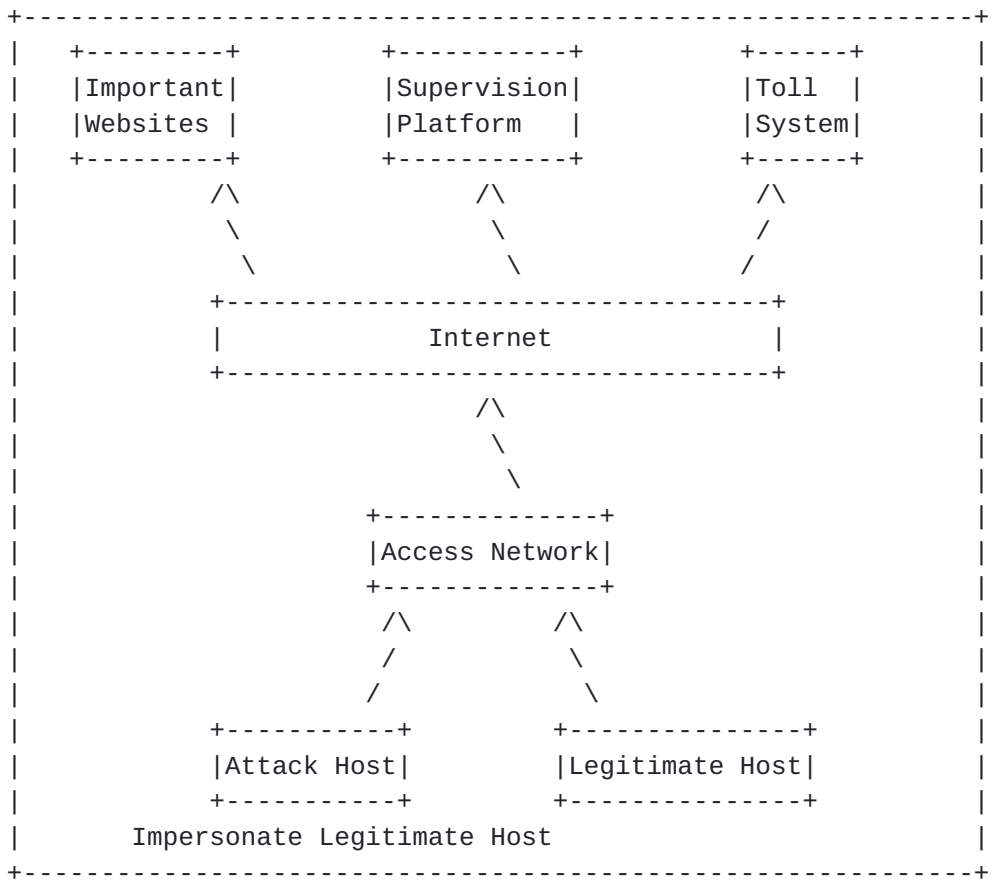


Figure 1: Scenario of source address spoofing.

Before SAVNET was proposed [I-D.ietf-savnet-intra-domain-problem-statement], several Source Address Validation (SAV) technical schemes have been proposed, such as ACL, uRPF, etc., which are dedicated to solving the illegal attacks based on source address spoofing. However, these SAV technologies still have limitations, which restrict the application of SAV technology in existing networks.

ACL SAV: This scheme can be used for both outbound traffic verification and inbound traffic verification. The ACL rules need to be updated manually in time to make them consistent with the latest filter conditions [RFC2827] [RFC3704].

Strict uRPF SAV: This scheme is typically used for outbound traffic verification. The SAV rules can be automatically generated and updated, but there is a serious problem of inappropriate blocking in asymmetric routing scenarios [RFC3704].

Loose uRPF SAV This scheme is typically used for inbound traffic verification. The SAV rules can be automatically generated and updated, but most spoofed data will be inappropriately allowed to forward [RFC3704].

In order to optimize the limitations of the above schemes, the SAVNET mechanisms based on SAV-related information is proposed. The SAVNET mechanisms, working in an incremental or partial deployment manner, can automatically adapt to network dynamics such as routing changes or prefix changes, instead of purely relying on manual update. The SAVNET mechanisms also improve the verification accuracy upon existing intra-domain SAVNET mechanisms, and allow for rapid updating of SAV rules so as to minimize the impact of improper block and permit during the convergence process [I-D.ietf-savnet-intra-domain-problem-statement] [I-D.li-savnet-intra-domain-architecture].

This document introduces a new method for generating SAV rules based on the SAVNET mechanism. This method generates SAV rules layer by layer through the topology of the link state database formed by the IGP protocol.

2. Terminology

The following terminologies are used in this document.

SAV Rule: The rule that indicates the source validity of a specific IP address or an IP prefix.

SAV Table: The table or data structure that implements the SAV rules and is used for source address validation in the data plane.

IGP: Interior Gateway Protocol.

IGP LSDB: IGP Link-State Database.

IGP node: It is anchored by a Router-ID that is used by the underlying IGP, i.e., a 48-bit ISO System-ID for IS-IS and a 32-bit Router-ID for OSPFv2 and OSPFv3.

IGP link Each link is anchored by a pair of Router-IDs that are used by the underlying IGP, i.e., a 48-bit ISO System-ID for IS-IS and a 32-bit Router-ID for OSPFv2 and OSPFv3.

Source prefix: The source prefixes are used to validate source addresses in the data plane.

BFS: Breadth-First Search, a graph search algorithm. It starts at the source node and explores all the neighbor nodes at the present depth prior to moving on to nodes at the next depth level. BSF uses a queue to aid in the search.

3. Design Goals

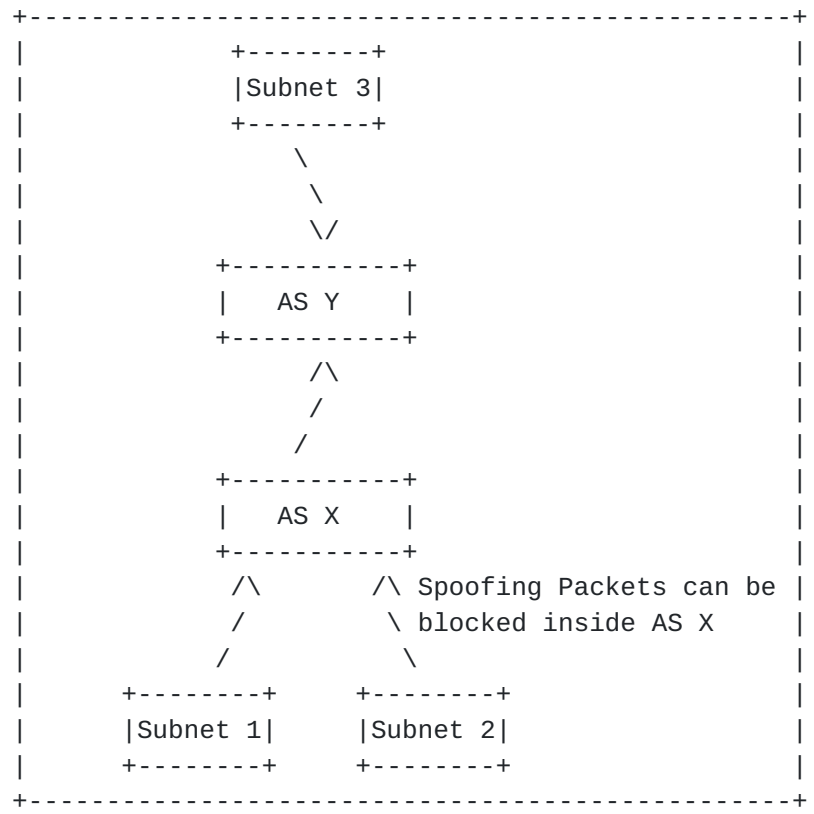


Figure 2: The case of outbound traffic verification

This method is designed to enhance the intra-domain SAVNET and achieve the following goals:

* Outbound traffic verification. As shown in Figure 2, Subnet 2 of AS X sends packets which spoof the source addresses of Subnet 1 or Subnet 3. If AS X deploys the intra-domain SAVNET solution, the spoofing packet from Subnet 2 can be blocked inside AS X.

* Incoming traffic verification. As shown in Figure 3, AS X would receive incoming traffic packets which spoofs source addresses of AS X. If AS X also can deploy intra-domain SAVNET solution, the spoofing packets from AS Y could be blocked by AS X.

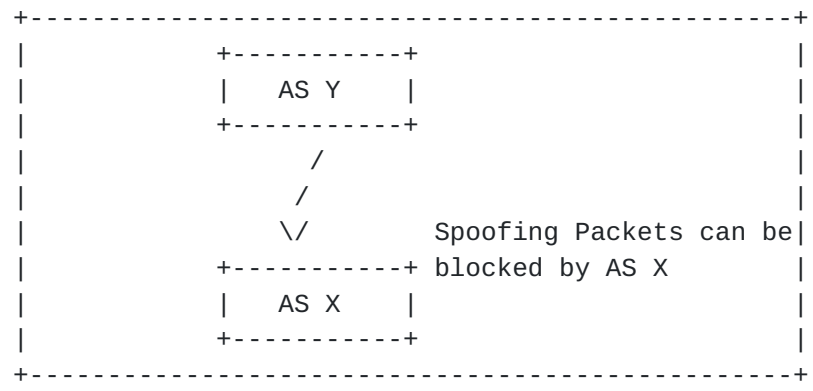


Figure 3: The case of incoming traffic verification

4. Solution

4.1. Overview

This section introduces a new approach for generating SAV rules within intra-domain scenarios using the SAVNET mechanism.

The method relies on two essential pieces of information: source prefix information and reachability information.

The source prefix information indicates the origin of the source address. Nodes that support this method disseminate their source address to the entire domain using a new flag in the IGP protocol extension information, as described in Section 5 Alternatively, for nodes that do not support this method, the source prefix information can be manually configured. In such cases, the calculation and classification of source address prefixes (e.g., intra-area, inter-area, or external routes) can be managed through configuration settings.

Leveraging the acquired source prefix and reachability information, the method dynamically calculates the inbound interface information for the source addresses within the domain and generates the corresponding Source Address Validation (SAV) Rule. The general process framework of the method is illustrated in Figure 4, where the SAVNET Agent acts as the processing unit responsible for generating SAV rules.

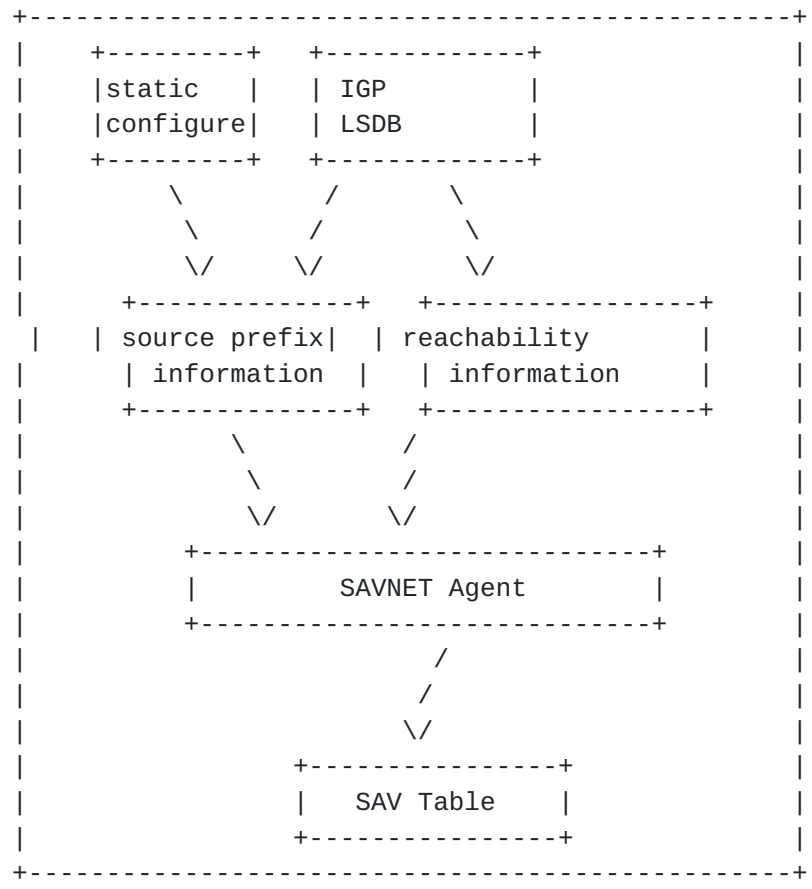


Figure 4: The overall process framework

SAV Agent first selects the checking node, which can be triggered by specific nodes actively requesting it or in response to changes in the topology, thereby re-checking the corresponding affected nodes.

The SAV checking node extracts connection information between nodes from the IGP Link State Database (LSDB). It traverses each link of the SAV checking node and, using topology information, determines all the node information that can be reached via that link. Finally, the source prefix address ranges of the nodes are obtained to generate SAV Rule entries for that link. During the traversal process, topology information should not loop back to the SAV checking node.

As depicted in Figure 5, when considering the topology information of Node A, it includes the link connection L1 between A and B, as well as the link connection L2 between A and C. Upon calculating this information on Node A, the result indicates that LINK L1 can reach Node B, while LINK L2 connects to Node C.

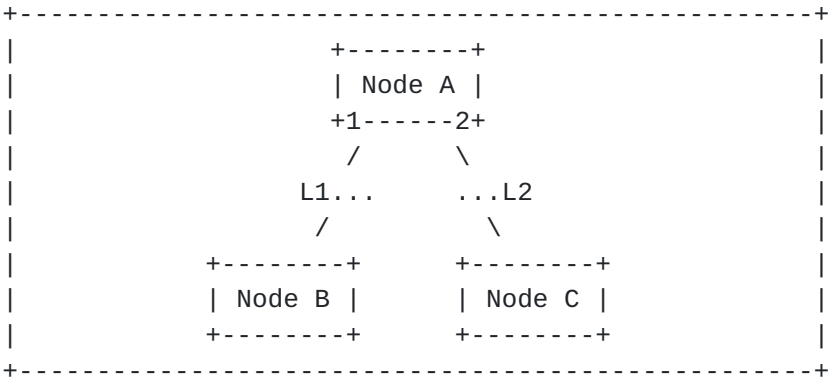


Figure 5: Example 1 of Topology Calculation

This method can solve the problem of intra-domain outbound and inbound traffic mentioned in Section 3, and it can automatically adjust SAV table entries according to topology changes to achieve security protection of intra-domain source addresses.

4.2. SAVA RULE

4.2.1. Composition of the SAVNET Rule

The composition of the SAVNET rule is illustrated in Figure 6, with each SAVNET rule comprising a source prefix and a list of IGP interfaces.

```
SAVA Rule 1              SAVA Rule 2
|                        |
+----Source prefix1      +----Source prefix2
        |                        |
        +----IGP Interface1      +----IGP Interface1
        +----IGP Interface2      +----IGP Interface2
        ...                      ...
```

Figure 6: Composition of the IGP SAVNET Table

4.2.2. Origin of the Source Prefix

If an IGP node supports SAVNET source prefix advertisement, it advertises the source prefix through the IGP LSDB. A detailed explanation of the process through which IGP nodes advertise various types of prefixes is provided in Section 4.2.3.

However, if an IGP node does not support SAVNET source prefix advertisement, the SAVNET Agent can manually configure the source prefix for each IGP node. Alternatively, the source prefix can be extracted from the LSDB advertised by each IGP node. This means that the source prefix information can be generated from the routing information advertised by each IGP node.

4.2.3. Advertisement of the Source Prefix

1) IS-IS Protocol

For the IS-IS protocol, IPv4 source prefixes are advertised using the "IP Extended Reach TLV", while IPv6 source prefixes are advertised using the "IPv6 Reachability TLV", without specific distinction between different types of source prefixes. The "Source Prefix Flag" is utilized to indicate that the advertised information represents a source prefix rather than a route, as explained in section 5.1.1.

The source prefixes are categorized into Level-1 prefixes and Level-2 prefixes. When a Level-1/Level-2 node learns a Level-1 or Level-2 source prefix, it redistributes this prefix into Level-2 or Level-1 through route leaking and copies the "Source Prefix Flag" marking from the source prefix.

When computing source prefixes, only the source prefixes advertised by the current node need to be taken into account. The "Source Prefix Flag" is optional. When this flag is not included, the calculation of the source prefix can still be selected through configuration.

2) OSPF Protocol

The OSPF source prefixes can be further categorized into intra-area source prefixes, inter-area source prefixes, and external source prefixes.

* intra-area source prefix:
When advertising an intra-area route, if the SAVNET source prefix advertisement is supported, the corresponding source prefix for this route is advertised using the "OSPFv2 Extended Prefix Opaque LSA" with the "Source Prefix Flag" set.

When computing the Intra-area source prefixes for the current node, the "Source Prefix Flag" is optional. When this flag is not included, the calculation of the source prefix can still be selected through configuration, the intra-area source prefix can be extracted from the Router LSA and Network LSA of OSPF.

When configuring to calculate only the source prefix with the "Source Prefix Flag" flag included, only the "OSPFv2 Extended Prefix Opaque LSA" advertisements with the "Source Prefix Flag" issued by the current ABR node need to be processed.

* Inter-area Source Prefix:
Inter-area routes are advertised by ABRs. When an ABR advertises an inter-area route, if the ABR supports the SAVNET source prefix advertisement, the corresponding source prefix is advertised using the "OSPFv2 Extended Prefix Opaque LSA" with the "Source Prefix Flag" set.

When computing the Inter-area source prefixes for the current node, the "Source Prefix Flag" is optional. When this flag is not included, the calculation of the source prefix can still be selected through configuration, the inter-area source prefix can be extracted from the Summary LSA of OSPF.

When configuring to calculate only the source prefix with the "Source Prefix Flag" flag included, only the "OSPFv2 Extended Prefix Opaque LSA" advertisements with the "Source Prefix Flag" issued by the current node need to be processed.

* External Source Prefix:
External routes are advertised by ASBRs. When an ASBR advertises an external route, if the ASBR supports the SAVNET source prefix advertisement, the corresponding source prefix is advertised using the "OSPFv2 Extended Prefix Opaque LSA" with the "Source Prefix Flag" set. The "Opaque Type" is set to AS-Wide (11) to indicate that this source prefix is an external prefix [RFC7684].

When computing the external source prefixes for the current node, the "Source Prefix Flag" is optional. When this flag is not included, the calculation of the source prefix can still be selected through configuration, the external source prefix can be extracted from the AS-External LSA of OSPF.

When configuring to calculate only the source prefix with the "Source Prefix Flag" flag included, only the "OSPFv2 Extended Prefix Opaque LSA" advertisements with the "Source Prefix Flag" issued by the current ASBR node need to be processed.

3) OSPFv3 Protocol

Similar to the OSPF protocol, OSPFv3 source prefixes are also categorized into intra-area source prefixes, inter-area source prefixes, and external source prefixes.

* Intra-area Source Prefix:
When advertising an intra-area route, if SAVNET source prefix advertisement is supported, the corresponding source prefix of this route is advertised through "E-Intra-Area-Prefix-LSA" with the "Source Prefix Flag" set.

When calculating the intra-area source prefixes for the current node, the "Source Prefix Flag" is optional. When this flag is not included, the calculation of the source prefix can still be selected through configuration, the intra-area source prefix can be extracted from the Intra-Area-Prefix-LSA.

When configuring to calculate only the source prefix with the "Source Prefix Flag" flag included, only the "E-Intra-Area-Prefix-LSA" advertisements with the "Source Prefix Flag" issued by the current node need to be processed.

* Inter-area Source Prefix:
Inter-area routes are advertised by ABRs. When an ABR advertises an inter-area route, if the ABR supports the SAVNET source prefix advertisement, the corresponding source prefix is advertised through "E-Inter-Area-Prefix-LSA" with the "Source Prefix Flag" set.

When calculating the inter-area source prefixes for the current node, the "Source Prefix Flag" is optional. When this flag is not included, the calculation of the source prefix can still be selected through configuration, the inter-area source prefix can be extracted from the Inter-Area-Prefix-LSA.

When configuring to calculate only the source prefix with the "Source Prefix Flag" flag included, only the "E-Inter-Area-Prefix-LSA" advertisements with the "Source Prefix Flag" issued by the current node need to be processed.

* External Source Prefix:
External routes are advertised by ASBRs. When an ASBR advertises an external route, if the ASBR supports the SAVNET source prefix advertisement, the corresponding source prefix is advertised through "E-AS-External-LSA" with the "Source Prefix Flag" set.

When calculating the external source prefixes for the current node, the "Source Prefix Flag" is optional. When this flag is not included, the calculation of the source prefix can still be selected through configuration, the external source prefix can be extracted from the AS-External-LSA.

When configuring to calculate only the source prefix with the "Source Prefix Flag" flag included, only the "E-AS-External-LSA"

advertisements with the "Source Prefix Flag" issued by the current ASBR node need to be processed.

4.3. Procedure

The SAVNET Agent is responsible for generating SAV rules based on the source prefix and topology information. The source prefix information can be dynamically disseminated by nodes that support SAVNET functionality or manually configured on inspection nodes.

The principle for calculating topology information is as follows:

Starting from the designated start node, the SAVNET rules for each interface are calculated sequentially. For a specific interface, the calculation begins from that interface and traverses to find out all reachable nodes. The SAVNET rules for this interface, (Prefix, IF), are then generated based on the source prefixes advertised by these reachable nodes. Finally, the interface SAVNET rules are merged based on prefixes. The entries with the same prefix are merged into one entry indexed by the prefix with a list of interfaces. This process ensures the comprehensive generation of SAV rules based on source prefixes and reachability information, allowing for effective security enforcement within the domain.

Here is the refined and optimized process of computation based on the Breadth-First Search (BFS) algorithm:

Step 1: Before initiating the SAVNET rule calculation, save the existing SAVNET rule table to facilitate the identification of changes in SAVNET rule table entries.

Step 2: Traverse all interfaces of the starting node and perform SAVNET rule calculation for each interface. Choose an interface as the calculating interface in a sequential manner, following steps 3 to 8; calculate all the reachable nodes through this interface. Based on the source prefixes advertised by each reachable node, compute the SAVNET rule (Prefix, IF) for this interface.

Step 3: Clear the visited flag for all nodes and mark the starting node as visited to initialize the BFS traversal.

Step 4: Add the neighboring nodes of the calculated interface to the queue and mark them as visited. These neighbor nodes must be in a bidirectional connected state.

Step 5: Retrieve the first node from the queue.

Step 6: Process current node, add all adjacent unvisited nodes to the queue, and mark them as visited.

Step 7: Generate SAVNET rules for the calculated interface based on the source prefixes of current node. If the current node supports SAVNET, it will advertise the SAVNET source prefix in the link state information. Otherwise, the source prefix can be manually configured on the computing node. The SAVNET rules are indexed by prefix. Firstly, process the source prefix: If the source prefix does not exist in the SAVNET rules, add a new SAVNET rule. Then, process the interface under the source prefix: If the interface is not in the interface list, add the new interface to the list. Refer to section 4.2 for detailed information on obtaining the source prefixes for different types of prefixes.

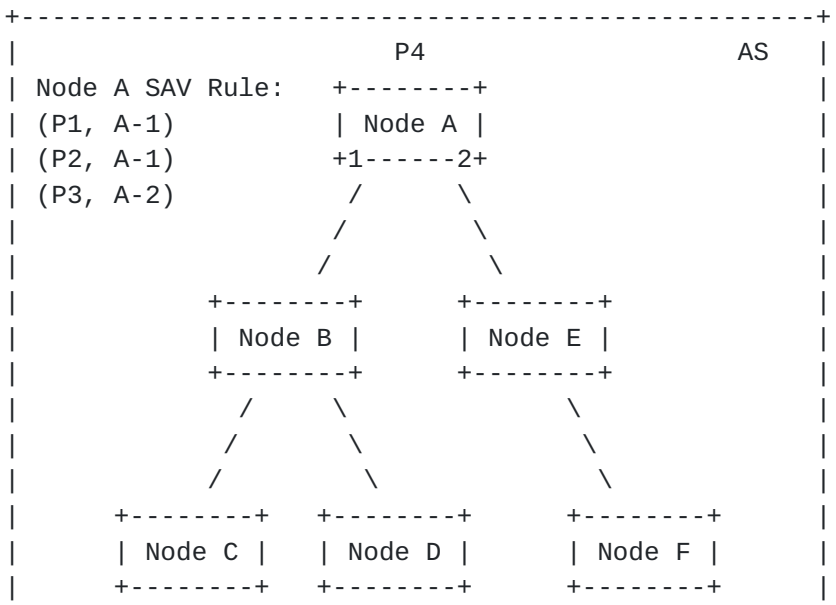
Step 8: Repeat steps 5 to 7 until the queue is empty.

Step 9: Repeat steps 2 to 8 until SAVNET rules for each interface are individually calculated.

Step 10: Merge the SAVNET rule entries obtained by all interfaces, combining entries with the same prefix into a single entry and consolidating the interfaces from each entry into the interface list of the merged entry.

Step 11: Deploy SAVNET rules. By comparing the newly generated SAVNET rules with the saved old SAVNET rules, perform add/modify/delete operations on SAVNET rule entries.

An example of the above process is shown in Figure 7 below.



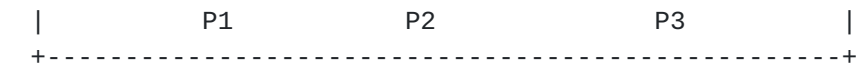


Figure 7: The case of the SAVNET Procedure

The steps provided illustrate the procedure for Node A to obtain SAV rules based on the source prefix and reachability information obtained through the IGP protocol extension. The process involves traversing the network topology to gather source prefix information and generate SAVNET rules for each interface separately.

Based on the information presented, the following SAVNET rules are generated for Node A:

1) Before initiating the SAVNET rule calculation, save the existing SAVNET rule table of Node A to facilitate the identification of changes in SAVNET rule table entries

2) Traverse all the IGP links of Node A and generate SAVNET rules for each interface separately. Select interface 1 first.

3) Clear the visited flag for all notes. Mark Node A as visited.

4) Add node B to the queue and mark it as visited.

5) Retrieve node B from the queue.

6) Add all adjacent nodes of node B that have not been visited to the queue and mark them as visited. Node C and Node D are added to the queue and marked as visited.

7) Process the source prefix information of the current node to generate SAVNET rules. For node B, there is no source prefix advertised.

8) Retrieve node C from the queue.

9) Add all adjacent nodes of node C that have not been visited to the queue and mark them as visited. No adjacent nodes were added to the queue.

10) Process the source prefix information of node C to generate SAVNET rules. Generate SAVNET rule of prefix P1 according to the source prefix advertised by Node C, and add interface A-1 to interface list.

11) Retrieve node D from the queue.

12) Add all adjacent nodes of node D that have not been visited to the queue and mark them as visited. No adjacent nodes were added to the queue.

13) Process the source prefix information of node D to generate SAVNET rules, Generate SAVNET rule of P2 according to the source prefix advertised by Node D, and add interface A-1 to interface list.

Through the above calculation process, generate SAVNET rules (P1, A-1) and (P2, A-1) for interface 1 of node A.

Similarly, for interface 2 of node A, the SAVNET rule (P3, A-2) can be generated.

5. Protocol Extension

5.1. IS-IS Protocol Extension

5.1.1. IS-IS Extended Source Prefix sub-TLV

IPv4 SAVNET source prefixes are advertised using "IP Extended Reach TLV" (type 135), while IPv6 SAVNET source prefixes are advertised using "IPv6 Reachability TLV" (type 236, RFC5308).

A new bit in the IPv4/IPv6 Extended Reachability Attribute Flags [RFC7794] is defined:

S-Flag: Source Prefix Flag (Bit TBD)

When set, it indicates that the prefix is used for source address validation in the data plane.

5.2. OSPF Protocol Extension

5.2.1. OSPF Extended Source Prefix sub-TLV

SAVNET source prefixes are advertised using "OSPFv2 Extended Prefix Opaque LSA"[RFC7684].

A new bit in Flags field of the OSPFv2 Extended Prefix TLV [RFC7684] is defined:

S-Flag: Source Prefix Flag (Bit TBD)

When set, it indicates that the prefix is used for source address validation in the data plane.

5.3. OSPFv3 Protocol Extension

5.3.1. OSPFv3 Extended Source Prefix sub-TLV

SAVNET source prefixes are advertised using "OSPFv3 Extended LSA", including "E-Intra-Area-Prefix-LSA", "E-Inter-Area-Prefix-LSA" and "E-AS-External-LSA".[RFC8362].

A new bit in the prefix Attribute Flags [I-D. draft-ietf-lsr-ospf-prefix-extended-flags-00] are defined:

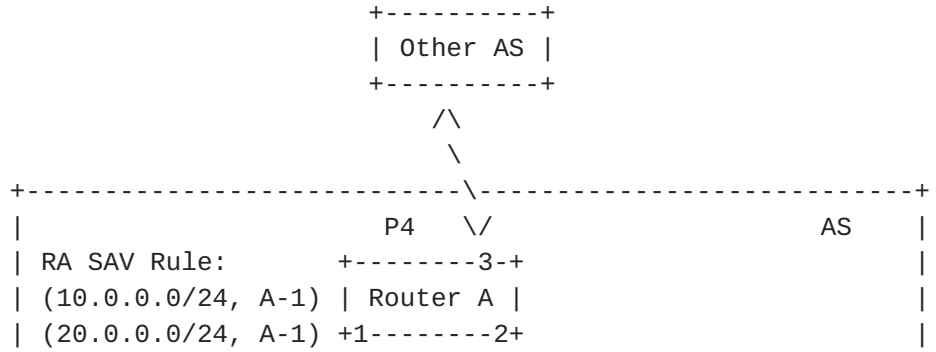
S-Flag: Source Prefix Flag (Bit TBD)

When set, it indicates that the prefix is used for source address validation in the data plane.

6. Example

The intra-domain SAVNET method commonly applies to scenarios involving intra-domain outbound traffic and inter-domain incoming traffic. Devices close to the upper layer can intercept traffic from intra-domain nodes that forge source addresses of other nodes, thereby preventing inbound traffic attacks within the domain. Similarly, attack packets received from inter-domain sources that forge intra-domain source addresses can also be blocked to protect incoming traffic from external domains.

Taking the network topology depicted in Figure 8 as an example, the source address P4 belongs to router A, the source address 10.0.0.0/24 belongs to router C, the source address 20.0.0.0/24 belongs to router D, and the source address 30.0.0.0/24 belongs to router F. All these source addresses are advertised through an IGP protocol extension, and the intra-domain path is calculated via the IGP protocol. The connecting links from routers C, D, and F to A are as follows: C->B->A, D->B->A, and F->E->A, respectively.



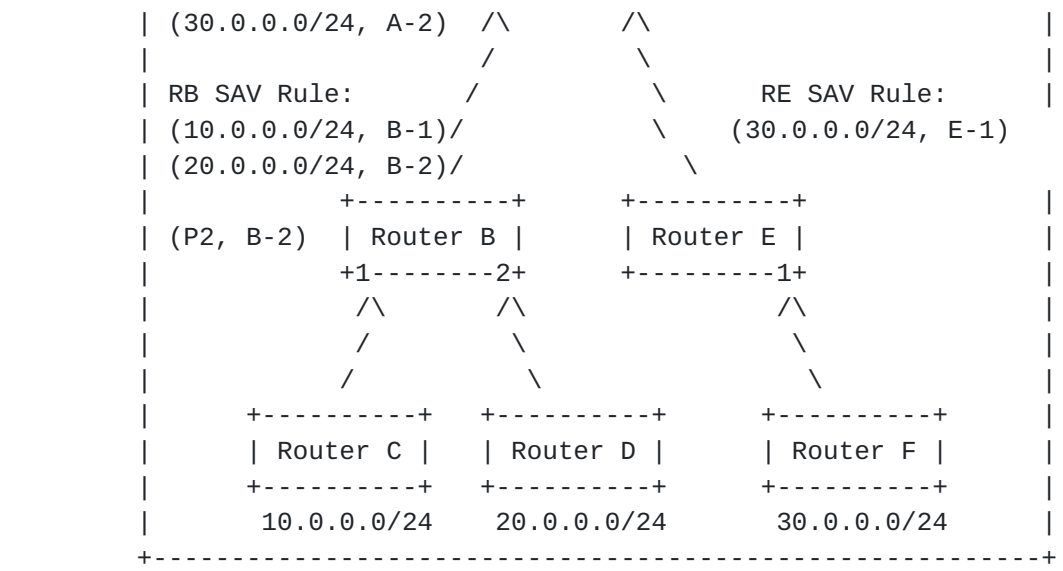


Figure 8: The Intra-domain Outbound Traffic Scenario

Based on the provided link and source address information, the intra-domain SAVNET method processes as follows:

For Router A:

The legal incoming interface for source prefixes of Router C and D is A-1.

The legal incoming interface for the source address of Router F is A-2.

For Router B:

The legal incoming interface for source prefixes of Router C is B-1.

The legal incoming interface for source prefixes of Router D is B-2.

For Router E:

The legal incoming interface for source prefixes of Router F is E-1.

Based on this information, each router in the intra-domain generates corresponding SAVNET rules.

With the SAVNET function enabled, the following scenarios will occur:

If Router C sends attack traffic with the source address of Router D or F, the counterfeit traffic will be intercepted by Router B.

If Router D sends attack traffic with the source address of Router C or F, the traffic with the fake source address will be intercepted by Router B.

If Router F sends attack traffic carrying the source address of Router C or D, the traffic will be blocked by Router E.

Furthermore, when Router A receives traffic from other Autonomous Systems (ASs), if the traffic forges the source addresses of intra-domain routers, Router A can intercept the traffic.

7. Manageability Considerations

This document extends the link state information of existing Interior Gateway Protocol (IGP) protocols, adding support for SAVA (Source Address Validation Architecture) source prefixes, as specified in section 6. IGP nodes advertise their own source prefix information through the extended link state information.

The SAVA detection feature only requires activation on a select few key access nodes, rather than all nodes. For nodes that do not support dynamic SAVA prefix advertising, the source prefix information can be directly configured on the computing nodes through static configuration.

The dynamic calculation of SAVA rules can be uniformly performed by the SAVA Agent, and then distributed to the detection nodes through the north-south interface.

Dynamic SAVA detection can be selectively deployed as needed or discontinued on specific nodes when deemed unnecessary. This approach allows for flexible management of SAVA detection based on the requirements and capabilities of different network nodes.

8. Deployment Considerations

It is desirable that all nodes in the intra-domain network could deploy this SAVNET method to automatically and accurately generate SAV rules, and therefore preventing source address spoofing attacks in the direction of outbound and inbound traffic.

However, in the existing network, only partial nodes in the intra-domain network support this method, due to asynchronous upgrades of devices. This results in that the deployed node cannot perceive the source addresses of non-deployed nodes and generate corresponding SAV rules, in spite of having all topology information. In this case of partial deployment, the deployment node can statically configure the specified source address of the non-deployment node to make up

for the above shortcomings and meet the conditions for generating SAV rules.

9. IANA Considerations

TBD

10. Security Considerations

TBD

11. References

11.1. Normative References

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[I-D.li-savnet-intra-domain-architecture]Li, D., Wu, J., Huang, M., Chen, L., Geng, N., Qin, L., and F. Gao, "Intra-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-li-savnet-intra-domain-architecture-03, 25 July 2023, <https://datatracker.ietf.org/doc/html/draft-li-savnet-intra-domain-architecture-03>.

[RFC7794] Ginsberg, L., Ed., Decraene, B., Previdi, S., Xu, X., and U. Chunduri, "IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability", RFC 7794, DOI 10.17487/RFC7794, March 2016, <https://www.rfc-editor.org/info/rfc7794>.

[RFC7684] Psenak, P., Gredler, H., Shakir, R., Henderickx, W., Tantsura, J., and A. Lindem, "OSPFv2 Prefix/Link Attribute Advertisement", RFC 7684, DOI 10.17487/RFC7684, November 2015, <https://www.rfc-editor.org/info/rfc7684>.

[I-D.draft-ietf-lsr-ospf-prefix-extended-flags-00] Ran Chen , Detao Zhao , Peter Psenak , Ketan Talaulikar,"Prefix Flag Extension for OSPFv2 and OSPFv3", Work in Progress, Internet-Draft, draft-ietf-lsr-ospf-prefix-extended-flags-00, 10 December 2023, <https://datatracker.ietf.org/doc/html/ draft-ietf-lsr-ospf-prefix-extended-flags-00>.

[RFC8362] Lindem, A., Roy, A., Goethals, D., Reddy Vallem, V., and F. Baker, "OSPFv3 Link State Advertisement (LSA) Extensibility", RFC 8362, DOI 10.17487/RFC8362, April 2018, <https://www.rfc-editor.org/info/rfc8362>.

11.2. Informative References

[I-D.ietf-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-ietf-savnet-intra-domain-problem- statement-02, 17 August 2023, https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-02>.

Acknowledgments

TBD

Authors' Addresses

Weiqiang Cheng
China Mobile
China

Email: chengweiqiang@chinamobile.com

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn

Changwang Lin
New H3C Technologies
Beijing
China

Email: linchangwang.04414@h3c.com

Shengnan Yue
China Mobile
China
yueshengnan@chinamobile.com