Workgroup: IDR
Internet-Draft: draft-geng-idr-bgp-savnet-00
Published: 13 March 2023
Intended Status: Standards Track
Expires: 14 September 2023
Authors: N. Geng
Huawei Technologies
Z. Tan
Huawei Technologies
M. Liu
Huawei Technologies

BGP Extensions for Source Address Validation Networks (BGP SAVNET)

Abstract

Many source address validation (SAV) mechanisms have been proposed for preventing source address spoofing. However, existing SAV mechanisms are faced with the problems of inaccurate validation or high operational overhead in some cases. This paper proposes BGP SAVNET by extending BGP protocol for SAV. This protocol can propagate SAV-related information through BGP messages. The propagated information will help routers automatically generate accurate SAV rules which are for checking the validity of data packets.

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 14 September 2023.

Copyright Notice

Table of Contents

1. Introduction
  1.1. Terminology
  1.2. Requirements Language
2. BGP Protocol Relationship
3. BGP SAVNET Solution
  3.1. Application Scenarios
  3.2. SAV Solution within an AS
    3.2.1. Solution for Edge Routers
    3.2.2. Solution for Aggregation Routers
  3.3. SAV Solution between ASes
    3.3.1. Solution for Border Routers
4. BGP SAVNET Peering Models
  4.1. Full-mesh IBGP Peering
  4.2. Singe-hop IBGP Peering between Directly Connected Routers
  4.3. EBGP Peering between ASes
5. BGP SAVNET Protocol Extension
  5.1. BGP SAVNET SAFI
  5.2. BGP SAVNET NLRI
    5.2.1. SPA TLVs within an AS
    5.2.2. SPA TLVs between ASes
  5.3. BGP SAVNET Refresh
    5.3.1. The SPD TLVs within an AS
    5.3.2. The SPD TLVs between ASes
    5.3.3. The SPD Optional Data Sub-TLVs
6. Decision Process with BGP SAVNET
  6.1. BGP SAVNET NLRI Selection
    6.1.1. Self-Originated NLRI
7. Error Handling
  7.1. Process of BGP SAVNET NLRIs
  7.2. Process of BGP SAVNET SPA TLVs
  7.3. Process of BGP SAVNET Refresh
  7.4. Process of BGP SAVNET SPD TLVs
8. Management Considerations
9. IANA Considerations
10. Security Considerations
11. References
  11.1. Normative References
  11.2. Informative References
Acknowledgements
Authors' Addresses

1. Introduction

Source address validation (SAV) is essential for preventing source address spoofing attacks (e.g., DDoS based on source address spoofing [RFC6959]) and tracing back network attackers. For a network, SAV mechanisms can be deployed on edge routers or aggregation routers for validating the packets from the connected subnets or neighboring ASes [manrs-antispoofing].

ACL-based ingress filtering can be used for SAV, which, however, has high operational overhead problems in dynamic networks [I-D.li-savnet-intra-domain-problem-statement] [I-D.wu-savnet-inter-domain-problem-statement] and also has limited capacity of rules. Many SAV mechanisms, such as strict uRPF, loose uRPF, and EFP-uRPF [RFC3704][RFC8704], leverage routing information to automatically generate SAV rules. The rules indicate the wanted incoming directions of source addresses. The packets with specified source addresses but from unwanted directions will be considered invalid [I-D.huang-savnet-sav-table]. However, there may be inaccurate validation problems under asymmetric routing [I-D.li-savnet-intra-domain-problem-statement] [I-D.wu-savnet-inter-domain-problem-statement]. This is because these uRPF mechanisms are "single-point" designs. They leverage the local FIB or local RIB table to determine the incoming interfaces for source addresses, which may not match the real incoming directions. That is, purely relying on the original IGP or BGP protocols to obtain routing information for SAV rule generation cannot well meet the requirement of accurate validation.

This document proposes an extension of BGP protocol for SAV, i.e., BGP SAVNET. Unlike existing "single-point" mechanisms, BGP SAVNET allows coordination between the routers within the network or the ASes outside the network by propagating SAV-related information through extended BGP messages. The propagated information can provide more accurate source address information and incoming direction information than the local FIB and RIB tables. The routers with BGP SAVNET can automatically generate accurate SAV rules without introducing much overhead.

The BGP SAVNET protocol is suitable to generating SAV rules for both IPv4 and IPv6 addresses. The SAV rules can be used for validating any native IP packets or IP-encapsulated packets.

1.1. Terminology

SAV: Source address validation, an approach to preventing source address spoofing.

SAV Rule: The rule that indicates the valid incoming interfaces for a specific source prefix.

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

SPA: Source prefix advertisement, i.e., the process for advertising the origin source addresses/prefixes of a router or an AS.

SPD: Source path discovery, i.e., the process for discovering the real incoming directions of particular source addresses/prefixes.

1.2. Requirements Language

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.

2. BGP Protocol Relationship

The BGP extensions for BGP SAVNET follow a backward compatible manner without impacting existing BGP functions. New BGP SAVNET subsequent address families will be introduced under the IPv4 address family and the IPv6 address family, respectively. The BGP UPDATE message (specifically the MP_REACH_NLRI and the MP_UNREACH_NLRI attributes) and the BGP Refresh message will be extended. AFI and SAFI can be used for distinguishing the BGP SAVNET messages from other messages.

A few existing path attributes such as Originator_ID and Clister_list or new defined path attributes **MAY** be used for BGP SAVNET. Actually, most existing path attributes are not necessarily required for BGP SAVNET. However, if the unnecessary path attributes are carried in BGP updates, they will be accepted, validated, and propagated consistent with the BGP protocol.

3. BGP SAVNET Solution

3.1. Application Scenarios

BGP SAVNET aims to generate accurate SAV rules for most use cases including asymmetric routing. An SAV rule indicates the valid incoming interfaces for a specific source address/prefix. A router with BGP SVANET will locally maintain a SAV table storing the SAV rules. The SAV table can be used for validating data packets.

Figure 1 shows the application scenarios where BGP SAVNET will enabling SAV in data plane:

*SAV within an AS

-Edge routers connecting subnets: BGP SAVNET can be deployed at '*' for checking the validity of the packets from subnets.

-Aggregation routers: Aggregation routers can do validation at 'x' for any arrival packets.

*SAV between ASes

-Border routers connecting other ASes: BGP SAVNET can be deployed at '#' for checking the validity of the packets from other ASes.

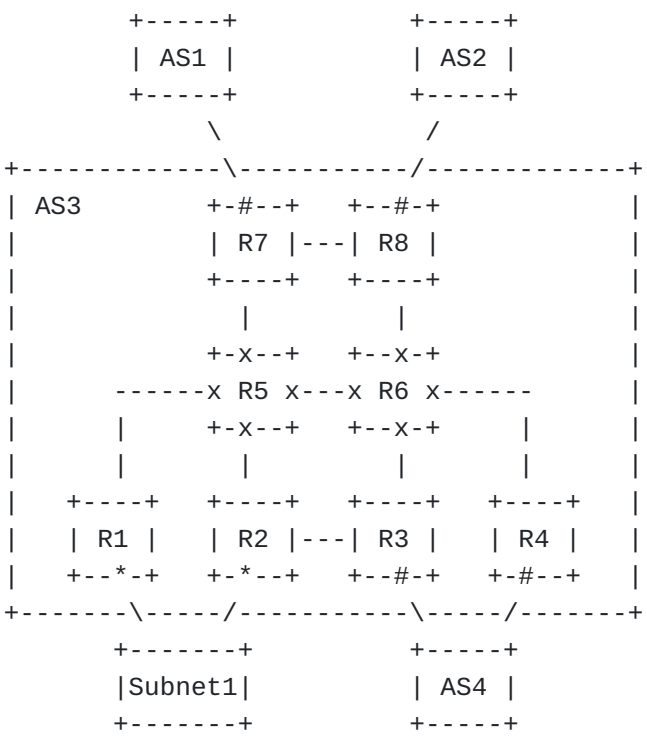

Figure 1: BGP SAVNET application scenarios

3.2. SAV Solution within an AS

The solution consists of two main processes: Source Address Advertisement (SPA) and Source Path Discovery (SPD). Edge routers can generate SAV rules through SPA on the interfaces connecting subnets. SPA and SPD can help aggregation routers generate SAV rules on the interfaces connecting other routers.

3.2.1. Solution for Edge Routers

Edge routers aims to generate SAV rules, i.e., the source prefix allowlist at each interface connecting to a subnet. If the subnet is single-homed, the allowlist can be generated through local RIB. When the subnet is multi-homed to edge routers, asymmetric routing may exist. SPA will help the routers get accurate allowlist. Specifically, edge routers can propagate its source prefixes learned from an interface connecting to a subnet. The source prefixes with a tag will be carried in the SPA message. Other routers will receive the message. The interfaces configured with the same tag value on other routers will include the tagged source prefixes in the corresponding allowlist. More details can be found in the version-00 of [I-D.li-savnet-intra-domain-architecture].

3.2.2. Solution for Aggregation Routers

Aggregation routers are to generate SAV rules for checking the validity of recorded source prefixes and ignore the validation of unrecorded source prefixes. Each edge router can first send SPA messages for propagating its router-id and its source prefixes that need to be validated. Aggregation routers will record the mapping from router-id to source prefixes. Then, each edge router will send an SPD messages to each neighbor router. The message carries the source router-id of the edge router and the destination router-ids whose mapped source prefixes take the neighbor router as the next forwarding hop. The neighbor router (e.g., aggregation router) receiving the message will record the incoming interface of the message, and SAV rules will be generated locally by binding the source router-id's source prefixes to the recorded incoming interface. Then neighbor router will remove its own router-id from the destination router-id list and relay the message to its neighbors according to local forwarding rules. The routers receiving the message will repeat the above process until the destination router-id list is empty. More details can be found in the version-00 of [I-D.li-savnet-intra-domain-architecture].

3.3. SAV Solution between ASes

3.3.1. Solution for Border Routers

The solution consists of two main processes: SPA and SPD. Border routers can generate SAV rules at interfaces connecting to other ASes through SPA and SPD.

Let AS X be the local AS which acts as a validation AS and generates SAV rules for other ASes. Let AS Y be one of the ASes deploying BGP SAVNET, which is named as source AS. Validation AS X will generate SAV rules for protecting the source prefixes of source AS Y.

AS Y first advertise its own AS number and its own source prefixes to AS X through SPA messages. SPA is necessary because AS Y cannot learn the complete set of source prefixes of AS Y purely through BGP updates. Some hidden source prefixes that do not appear can be advertised to AS X through SPA messages.

After SPA, AS Y can send SPD messages for notifying its preferred AS paths from AS Y to AS X. AS X will learn the incoming direction of AS Y's packets. Then, SAV rules can be generated. SPD can help AS X for discovering the real forwarding paths that do not match the control plane paths learned by AS X. More details can be found in the version-00 of [I-D.wu-savnet-inter-domain-architecture].

Note that, the SAV solutions either within an AS or between ASes are under working on. The BGP SAVNET will be updated if the solutions are revised.

4. BGP SAVNET Peering Models

Several BGP SAVNET solutions are introduced that can be applied in different scenarios. Depending on the solution's feature, different peering models need to be taken.

4.1. Full-mesh IBGP Peering

This peering model is required by the SAV solution within an AS so that the edge routers can generate SAV rules. In this model, routers enabling BGP SAVNET **MUST** establish full-mesh iBGP sessions either through direct iBGP sessions or route-reflector. The BGP SAVNET sessions can be established only when the BGP SAVNET address family has been successfully negotiated. SPA messages within an AS can be advertised through the full-mesh BGP SAVNET sessions. The extensions of BGP messages for carrying SPA messages will be introduced in Section 5.

4.2. Singe-hop IBGP Peering between Directly Connected Routers

This peering model meets the requirement of the SAV solution within an AS so that the aggregation routers can generate SAV rules. In this model, routers enabling BGP SAVNET **MUST** establish single-hop iBGP sessions through direct point-to-point links. For each link, a single-hop iBGP session needs to be established, and the messages transmitted over the session **MUST** be carried by the corresponding link. SPD messages within an AS can be advertised through these sessions. The extensions of BGP messages for carrying SPD messages will be introduced in Section 5.

4.3. EBGP Peering between ASes

The SAV solution between ASes requires eBGP sessions which can be single-hop or multi-hop. In this model, for the AS enabling BGP SAVNET, at least one border router in the AS **MUST** establish the BGP SAVNET sessions with other border routers in the neighboring or remote ASes. SPA and SPD messages between ASes will be advertised through these sessions. The extensions of BGP messages for carrying SPA and SPD messages will be introduced in Section 5.

5. BGP SAVNET Protocol Extension

5.1. BGP SAVNET SAFI

In order to transmitting and exchanging data needed to generate an independent SAV table, the document introduces the BGP SAVNET SAFI. The value is TBD and requires IANA registration as specified in Section 9. In order for two BGP SAVNET speakers to exchange BGP SAVNET NLRI (SPA message), they **MUST** establish a BGP SAVNET peer and **MUST** exchange the Multiprotocol Extensions Capability [RFC5492] to ensure that they are both capable of processing such NLRI properly. Two BGP SAVNET speakers **MUST** exchange Route Refresh Capability [RFC2918] to ensure that they are both capable of processing the SPD message carried in the BGP Refresh message.

5.2. BGP SAVNET NLRI

The BGP SAVNET NLRI is used to transmit Source Prefix (either IPv4 or IPv6) information to form a uniform Source Prefix list within a deployment domain.

The BGP SAVNET NLRI TLVs are carried in BGP UPDATE messages as (1) route advertisement carried within Multiprotocol Reachable NLRI (MP_REACH_NLRI) [RFC4760], and (2) route withdraw carried within Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI).

While encoding an MP_REACH_NLRI attribute containing BGP SAVNET NLRI TLVs, the "Length of Next Hop Network Address" field **SHOULD** be set to 0 upon the sender. The "Network Address of Next Hop" field should not be encoded upon the sender, because it has a 0 length and **MUST** be ignored upon the receiver.

5.2.1. SPA TLVs within an AS

The BGP SAVNET NLRI TLV each carries a Source Prefix and related information, therefore it is called an SPA TLV. This type of TLVs are used in SPA process within an AS. The format is shown below:

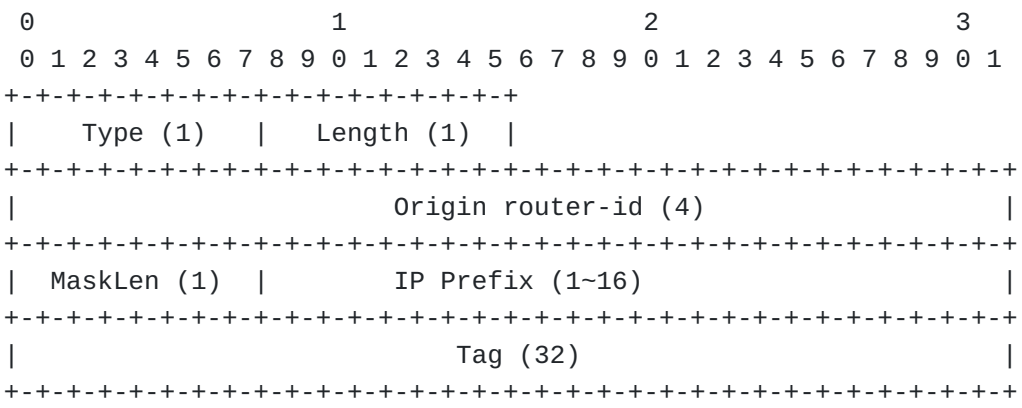

Figure 2: SPA TLV format

The meaning of these fields are as follows:

- *Type: Type of the BGP SAVNET NLRI TLV, the value is 1 for SPA TLV within an AS.
- *Length: The length of the BGP SAVNET NLRI value, the Type and Length fields are excluded.
- *Origin router-id: The router ID of the originating node of the source prefix in the deployment domain.
- *MaskLen: The mask length in bits, which also indicates the valid bits of the IP Prefix field.
- *IP Prefix: IP address. The length ranges from 1 to 16 bytes. Format is consistent with BGP IPv4/IPv6 unicast address.
- *Tag: Interface Tag.

5.2.2. SPA TLVs between ASes

This type of TLVs are used in SPA process between ASes. Type value is 2 for SPA TLV between ASes. The details are TBD.

5.3. BGP SAVNET Refresh

The SPD TLV is carried in a BGP Refresh message after the BGP Refresh message body, as follows:

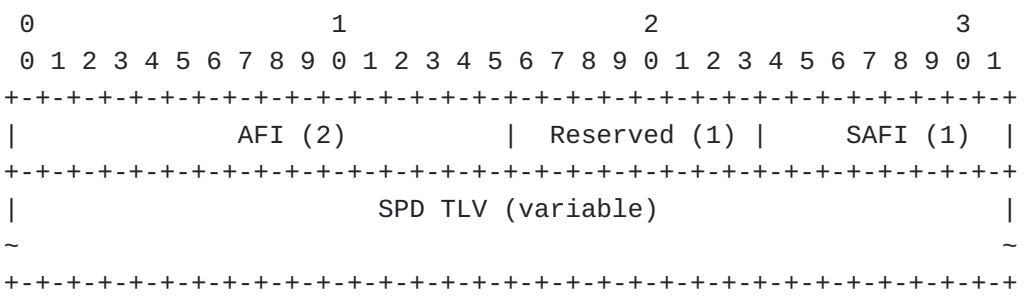

Figure 3: BGP-REFRESH with SPD TLV format

By carrying an SPD TLV, a BGP SAVNET Refresh message **MUST NOT** be processed as a Route-Refresh (as a re-advertisement request) and **SHOULD** only be used in the SPD process. A BGP SAVNET Refresh message without an SPD TLV **SHOULD** be processed as a Route-Refresh as defined in Route Refresh Capability [RFC2918].

5.3.1. The SPD TLVs within an AS

The SPD TLV carries the information that the Source Path Discovery process needed. This type of TLVs are used in SPD process within an AS. The format is shown below:

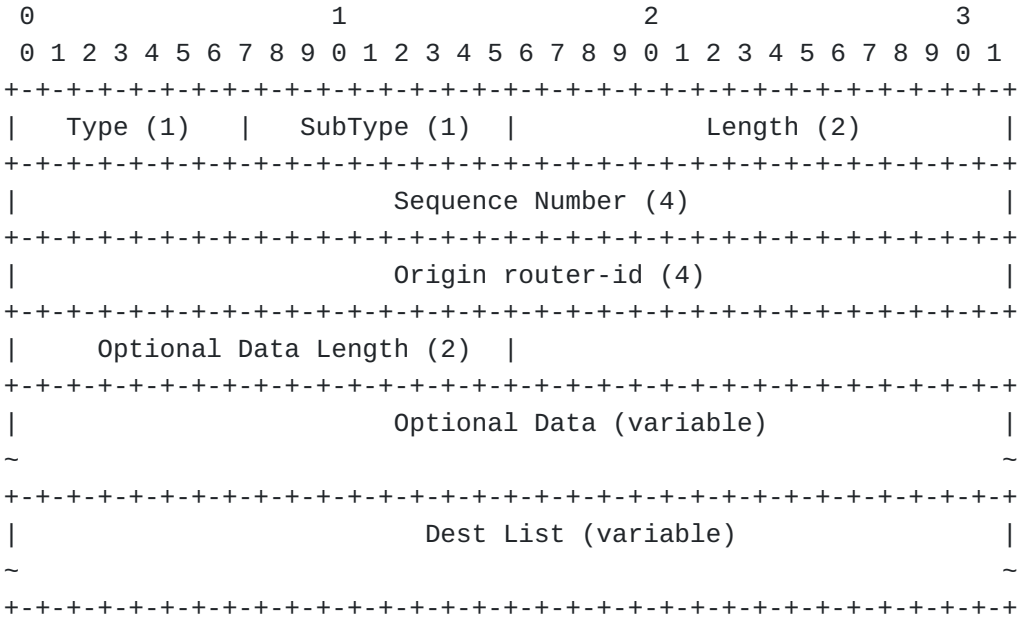

Figure 4: SPD TLV format

The meaning of these fields are as follows:

*Type: TLV Type, the value is 2 for SPD TLV.

*SubType: TLV Sub-Type, value is 1 for SPD TLV within an AS.

*Length: The length of the SPD TLV value, the Type, SubType and Length fields are excluded.

*Sequence Number: Indicates the sequence of Source Path Discovery process. The initial value is 0 and the value increases monotonically.

*Origin router-id: The router ID of the originating node of the Source Path Discovery process.

*Optional Data Length: The length of the optional data field in bytes. The value can be 0 when there is no optional data.

*Optional Data: In Sub-TLV format, see Section 5.3.2 for details.

*Dest List: List of destination router-ids, using 4-bytes route-id, indicates the destinations of this Source Path Discovery process.

5.3.2. The SPD TLVs between ASes

This type of TLVs are used in SPD process between ASes. SubType value is 2 for SPD TLV between ASes. The details are TBD.

5.3.3. The SPD Optional Data Sub-TLVs

Information in the Optional Data field of the SPD TLV is encoded in Sub-TLV format. The format is shown below and applies to all types of Sub-TLVs. Each type of Sub-TLV **SHOULD** appear no more than once in an SPD TLV.

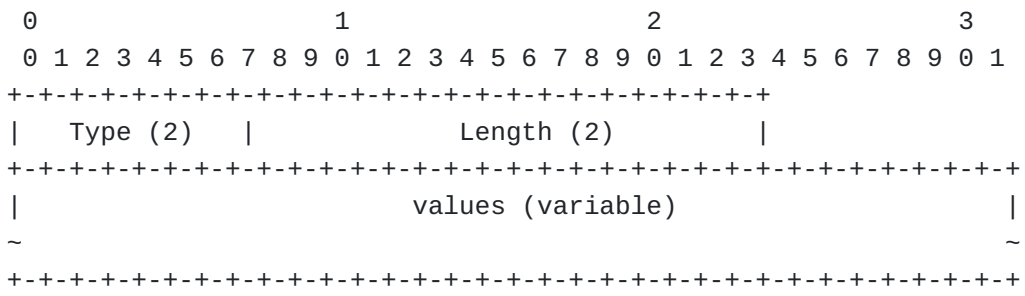

Figure 5: SPD Optional Data Sub-TLV format

The meaning of these fields are as follows:

*Type: Sub-TLV Type. The value 1 and 2 have been taken. The sequence of values is TBD and requires IANA registration as specified in Section 9.

*Length: The length of the Sub-TLV value, the Type and Length fields are excluded.

5.3.3.1. Sub-TLV Type 1: Origin Router-id List

List of agent original router-ids, using 4-bytes route-id. This information is used in the SPD convergence process and can carry a maximum of 254 router-ids.

5.3.3.2. Sub-TLV Type 2: Path Router-id List

List of path router-ids, using 4-bytes route-id, record all the router-id of the routers that the SPD process has passed through. This information is used to prevent loops and can carry a maximum of 254 router-ids.

6. Decision Process with BGP SAVNET

The Decision Process described in [RFC4271] works to determines a degree of preference among routes with the same prefix. The Decision Process involves many BGP Path attributes, which are not necessary for BGP SAVNET SPA and SPD process, such as next-hop attributes and IGP-metric attributes. Therefore, this document introduces a simplified Decision Process for SAVNET SAFI.

The purpose of SPA is to maintain a uniform Source Prefix list, which is the mapping from original router-id to IP addresses, across all routers in the deploy domain. To ensure this, it is **RECOMMENDED** that all routers deploy no ingress or egress route-policies.

6.1. BGP SAVNET NLRI Selection

The Decision Process described in [RFC4271] no longer apply, and the Decision Process for BGP SAVNET NLRI are as follows:

1. The locally imported route is preferred over the route received from a peer.

2. The route received from a peer with the numerically larger originator is preferred.

3. The route received from a peer with the numerically larger Peer IP Address is preferred.

6.1.1. Self-Originated NLRI

BGP SAVNET NLRI with origin router-id matching the local router-id is considered self-originated. All locally imported routes should be considered self-originated by default.

Since the origin router-id is part of the NLRI key, it is very unlikely that a self-originated NLRI would be received from a peer. Unless a router-id conflict occurs due to incorrect configuration. In this case, the self-originated NLRI **MUST** be discarded upon the receiver, and appropriate error logging is **RECOMMENDED**.

On the other hand, besides the route learn from peers, a BGP SAVNET speaker **MUST NOT** advertise NLRI which is not self-originated.

7. Error Handling

7.1. Process of BGP SAVNET NLRIs

When a BGP SAVNET speaker receives a BGP Update containing a malformed MP_REACH_NLRI or MP_UNREACH_NLRI, it **MUST** ignore the received TLV and **MUST NOT** pass it to other BGP peers. When discarding a malformed TLV, a BGP SAVNET speaker **MAY** log a specific error.

If duplicate NLRIs exist in a MP_REACH_NLRI or MP_UNREACH_NLRI attribute, only the last one **SHOULD** be used.

7.2. Process of BGP SAVNET SPA TLVs

When a BGP SAVNET speaker receives an SPA TLV with an undefined type, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives an SPA TLV with a 0 origin router-id, or the origin router-id is the same as the local router-id, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives an SPA TLV with an invalid MaskLen field, which is out of the range 1~32 for IPv4 and 1~128 for IPv6, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives an SPA TLV with an address field, whose length in bytes do not match with the remaining data, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives a malformed SPA TLV, it **MUST** ignore the received TLV and **MUST NOT** pass it to other BGP peers. When discarding a malformed TLV, a BGP SAVNET speaker **MAY** log a specific error.

7.3. Process of BGP SAVNET Refresh

Each BGP Refresh message **MUST** contain at most one SPD TLV. When a BGP SAVNET speaker receives a BGP Refresh packet with multiple SPD TLVs, only the first one **SHOULD** be processed.

7.4. Process of BGP SAVNET SPD TLVs

When a BGP SAVNET speaker receives an SPD TLV with an undefined type or subtype, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives an SPD TLV with a 0 origin router-id, or the origin router-id is the same as the local router-id, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives an SPD TLV with an optional data sub-TLV that is an undefined type, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives an SPD TLV with a DestList field that is not a multiple of 4 in length, it **MUST** be considered malformed.

When a BGP SAVNET speaker receives a Refresh message with a malformed SPD TLV, it **MUST** ignore the received message. When discarding a malformed message, a BGP SAVNET speaker **MAY** log a specific error.

When a BGP SAVNET speaker receives an SPD TLV with a sequence number that does not match the local recorded sequence number:

- If the newly received sequence number is numerically larger, the local recorded sequence number **SHOULD** be updated to the newly received sequence number.

- If the newly received sequence number is numerically smaller, the local recorded sequence number **SHOULD NOT** be updated, and the BGP SAVNET speaker **SHOULD** log a specific error.

8. Management Considerations

TBD

9. IANA Considerations

The BGP SAVNET SAFIs under the IPv4 address family and the IPv6 address family need to be allocated by IANA.

10. Security Considerations

This document does not introduce any new security considerations.

11. References

11.1. Normative References

[RFC2918]

Chen, E., "Route Refresh Capability for BGP-4", RFC 2918, DOI 10.17487/RFC2918, September 2000, <https://www.rfc-editor.org/info/rfc2918>.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <https://www.rfc-editor.org/info/rfc4760>.

[RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, DOI 10.17487/RFC5492, February 2009, <https://www.rfc-editor.org/info/rfc5492>.

[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-01, 12 March 2023, <https://datatracker.ietf.org/doc/html/draft-li-savnet-intra-domain-architecture-01>.

[I-D.wu-savnet-inter-domain-architecture]
Wu, J., Li, D., Huang, M., Chen, L., Geng, N., Liu, L., and L. Qin, "Inter-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-wu-savnet-inter-domain-architecture-01, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-wu-savnet-inter-domain-architecture-01>.

[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>.

11.2. Informative References

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <https://www.rfc-editor.org/info/rfc6959>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <https://www.rfc-editor.org/info/rfc8704>.

[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.wu-savnet-inter-domain-problem-statement] Wu, J., Li, D., Liu, L., Huang, M., and N. Geng, "Source Address Validation in Inter-domain Networks Gap Analysis, Problem Statement, and Requirements", Work in Progress, Internet-Draft, draft-wu-savnet-inter-domain-problem-statement-06, 4 March 2023, <https://datatracker.ietf.org/doc/html/draft-wu-savnet-inter-domain-problem-statement-06>.

[I-D.huang-savnet-sav-table] Huang, M., Cheng, W., Li, D., Geng, N., Liu, and L. Chen, "Source Address Validation Table Abstraction and Application", Work in Progress, Internet-Draft, draft-huang-savnet-sav-table-01, 6 March 2023, <https://datatracker.ietf.org/doc/html/draft-huang-savnet-sav-table-01>.

[manrs-antispoofing] "MANRS Implementation Guide", January 2023, <https://www.manrs.org/netops/guide/antispoofing>.

Acknowledgements

TBD

Authors' Addresses

Nan Geng
Huawei Technologies
Beijing
China

Email: gengnan@huawei.com

Zhen Tan
Huawei Technologies
Beijing
China

Email: tanzhen6@huawei.com

Mingxing Liu
Huawei Technologies
Beijing
China

Email: liumingxing7@huawei.com