SAVNET
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

N. Geng
Huawei
L. Qin
Zhongguancun Laboratory
K. Sriram
USA NIST
D. Li
Tsinghua University

7 July 2025

Source Prefix Advertisement for Inter-domain SAVNET
draft-geng-savnet-inter-domain-spa-00

Abstract

This document proposes to use Source Prefix Advertisement (SPA) messages for advertising hidden source prefixes and discovering the hidden paths of source prefixes. The accuracy of existing inter-domain SAV mechanisms like EFP-uRPF can be improved by SPA.

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 8 January 2026.

Table of Contents

1. Introduction

EFP-uRPF [RFC8704] is a promising inter-domain Source Address Validation (SAV) mechanism and works well in most cases. [I-D.ietf-savnet-inter-domain-problem-statement] does an analysis of existing inter-domain SAV mechanisms including EFP-uRPF. The analysis shows that EFP-uRPF may have improper blocking problems in the scenarios of i) "hidden source prefixes" in the Direct Server Return (DSR) scenario (see section 4.1.2 of [I-D.ietf-savnet-inter-domain-problem-statement]) and ii) "hidden paths of source prefixes" caused by "Limited Propagation of Prefixes" (see section 4.1.1 of [I-D.ietf-savnet-inter-domain-problem-statement]).

The source prefix allowlists at customer-facing or lateral peer-facing interfaces are built by EFP-uRPF primarily based on the local BGP routing information. When source prefixes or paths are "hidden" in normal BGP Update messages, EFP-uRPF will fail to generate accurate prefix allowlists.

This document follows the idea of sharing SAV-specific information between ASes proposed in [I-D.ietf-savnet-inter-domain-architecture]. A new inter-domain message called Source Prefix Advertisement (SPA) is defined. SPA messages can help advertise hidden source prefixes and discover hidden paths, and thus improve the accuracy of existing inter-domain SAV mechanisms like EFP-uRPF.

SPA messages can be possibly delivered by extended BGP messages, but the design of protocol extensions are not the focus of this document.

1.1. Terminology

SPA: Source Prefix Advertisement (SPA) for advertising the origin source prefixes of an AS.

Source AS: The AS which originates SPA messages.

Validating AS: The AS which receives SPA messages, generates SAV rules, and conducts source address validation.

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. Inter-domain Source Prefix Advertisement

A new inter-domain message called SPA message is defined in this section. An SPA message SHOULD include the following items:

* Source Prefixes: The source prefixes that the source addresses of the locally originated data packets of Source AS belong to. These source prefixes are to be updated or withdrawn, which is indicated by the Update/Withdraw Flag. The updated source prefixes are incremental to the previously announced prefixes.

* Source AS Number: The AS number of the Source AS (aka origin AS) that originates data packets with the source addresses belonging to the Source Prefixes.

* AS Path: It has the same meaning as the AS_PATH attribute in BGP [RFC4271].

* Update/Withdraw Flag: It indicates whether the Source Prefixes in the message are to be updated or withdrawn.

A Source AS can advertise its "hidden source prefixes" through SPA messages to its neighboring ASes. The neighboring ASes can further propagate the messages to next-hop ASes, and so do the next-hop ASes. The manner of the propagation is similar to that of BGP Updates. In the DSR scenario, the anycast prefixes, which are not in the BGP routes originated by the Source AS, can be advertised to remote Validating ASes through SPA messages.

3. Inter-domain Source Path Discovery

SPA messages can be used for source path discovery at the same time as advertising source prefixes. In the "Limited Propagation of Prefixes" scenarios (see section 4.1.1 of [I-D.ietf-savnet-inter-domain-problem-statement]), the propagation of BGP Update messages may be limited due to routing propagation policies (e.g., NO_EXPORT), but the SPA messages will be propagated because they are separate from routing Updates and do not have NO_EXPORT attached. Thus, the "hidden paths of source prefixes" can be discovered through SPA messages by the Validating ASes.

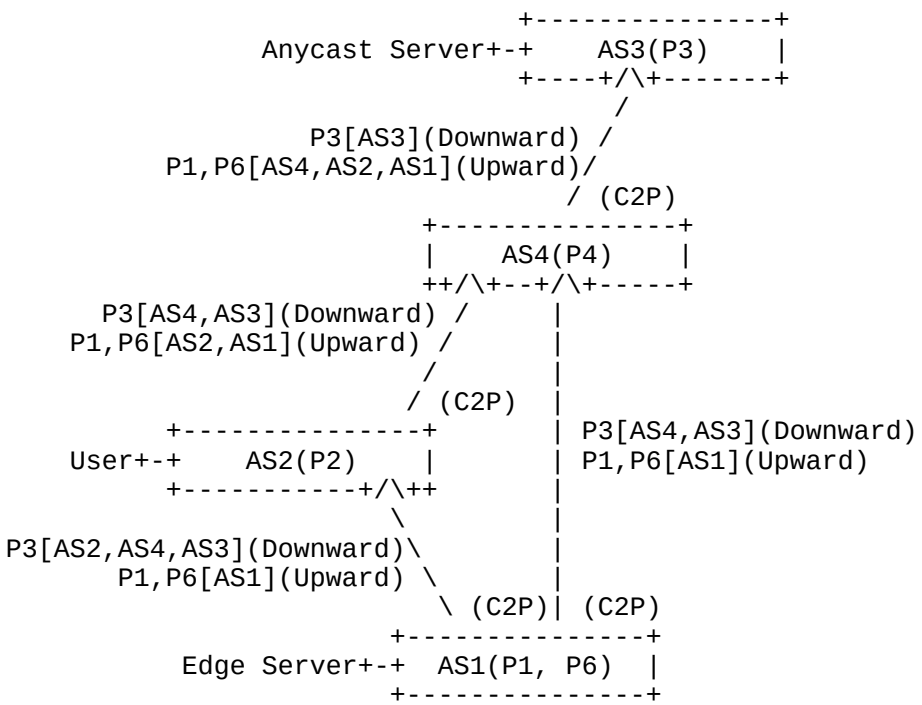
4. EFP-uRPF Enhanced by SPA

This section describes how to use SPA for enhancing EFP-uRPF.

4.1. "Hidden Prefixes" Scenario

Consider the "Hidden Prefixes" scenario (e.g., the DSR scenario) described in section 4.1.2 of [I-D.ietf-savnet-inter-domain-problem-statement]. Figure 1 shows an example of the DSR scenario, which is similar to Figure 3 in [I-D.ietf-savnet-inter-domain-problem-statement]. The propagation of BGP Updates of P1, P3 and P6 are shown in the figure. The anycast server in AS3 receives requests from users and tunnels the requests to the edge server in AS1. Then, the edge server will respond directly to the users by using the anycast IP address (belonging in P3) as the source address in the response packets.

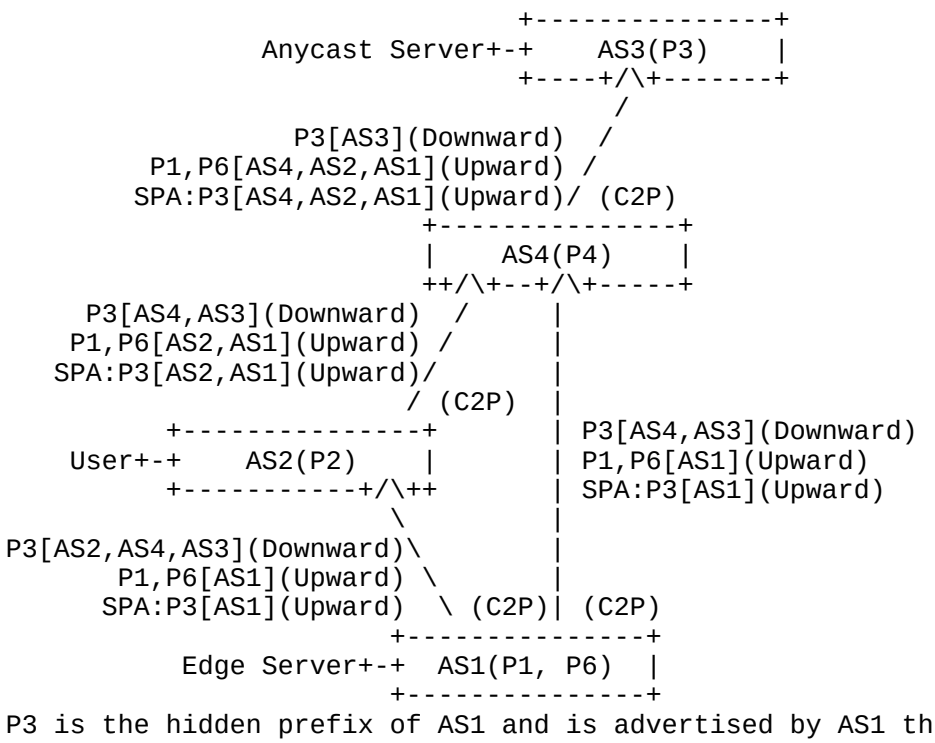
Prefix P3 is the anycast prefix and is only advertised by AS3 through BGP. Suppose AS2 or AS4 enables EFP-uRPF at customer-facing interfaces. The packets with source addresses belonging in P3 sent by AS1 will be blocked improperly when the packets arrive at the customer-facing interfaces of AS2/AS4. In this example, P3 is the hidden source prefix of AS1.



P3 is the anycast prefix and is only advertised by AS3 through BGP.

Figure 1: An example of the DSR scenario.

SPA can be used to solve the improper blocking problems in the "Hidden Prefixes" scenarios. In the above DSR scenario, AS1 can advertise the hidden source prefix P3 to Validating ASes (i.e., AS2 and AS4) through SPA messages. The propagation process of SPA messages is illustrated in Figure 2. After receiving the SPA message, AS2 and AS4 will take a union of the prefixes in the SPA messages and the BGP Update messages for constructing SAV tables (allowlists). As a result, P3 will be included in the source prefix allowlist at the customer-facing interfaces at AS2 and AS4. When AS1 sends packets with source address in P3, they will pass the validation at AS2 and AS4.



P3 is the hidden prefix of AS1 and is advertised by AS1 through SPA.

Figure 2: SPA for the DSR scenario.

4.2. "Limited Propagation of Prefixes" Scenario

Consider the "Limited Propagation of Prefixes" scenario (e.g., the NO_EXPORT scenario) described in section 4.1.1 of [I-D.ietf-savnet-inter-domain-problem-statement]. Figure 3 shows the NO_EXPORT scenario, which is similar to Figure 2 in [I-D.ietf-savnet-inter-domain-problem-statement]. AS1 advertises only prefix P1 to AS2 through a BGP Update message with the NO_EXPORT community. As a result, AS4 learns no route of AS1 directly from AS2.

If AS4 enables EFP-uRPF with algorithm A at the customer-facing interface connected to AS2, the packets with source addresses in P1 or P6 will be blocked improperly.

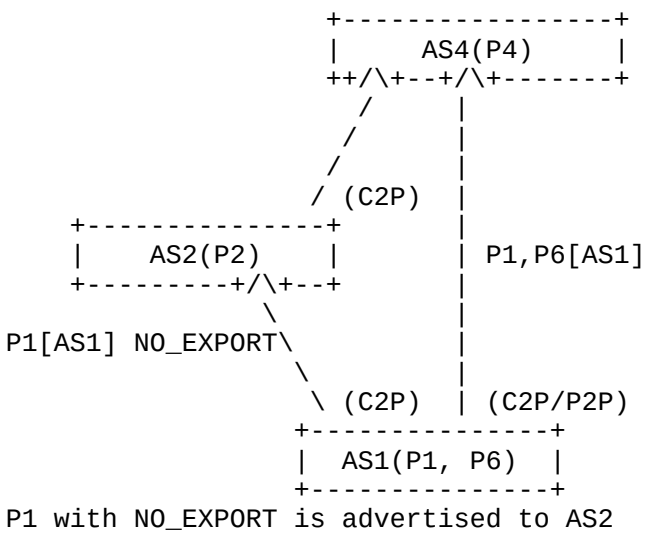
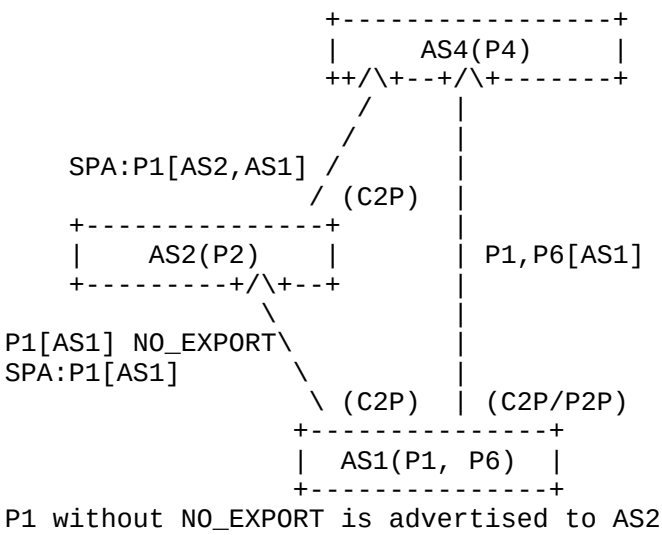


Figure 3: An example of the NO_EXPORT scenario.

SPA can be used to solve the improper blocking problems in the "Limited Propagation of Prefixes" scenarios. In the above NO_EXPORT scenario, AS1 can send an SPA message to AS2, and then AS2 will propagate the message to AS4. Note that NO_EXPORT community does not apply and never attached to SPA messages. The propagation process of SPA messages is illustrated in Figure 4. AS4 deploying EFP-uRPF with either Algorithm A or Algorithm B will learn the existence of AS1 from the interface connected to AS2. AS4 will take the union of prefixes (and also AS paths) learned from BGP and SPA messages. Thus AS4 will include the source prefixes P1 and P6 of AS1 in the source prefix allowlist for the interface with AS2. When data packets with source addresses in P1 or P6 arrive at AS4 via AS2, they will pass the validation at AS4.



P1 without NO_EXPORT is advertised to AS2 through SPA

Figure 4: SPA for the NO_EXPORT scenario.

5. Convergence Considerations

Validating AS needs to update SAV rules when source prefixes of Source AS or the paths of source prefixes change. The following RECOMMENDED actions will result in more effective re-convergence:

* Applying hysteresis in the case of withdrawal of source prefixes or paths of source prefixes: During the re-convergence, the SAV source prefix lists will include some withdrawn prefixes for a little longer, and there may exist improper permitting shortly but no improper blocking.

* Updating source prefixes or paths of source prefixes as soon as possible when SPA message is received: During the convergence, any possibility of improper blocking will be minimized or eliminated if new source prefixes are announced in SPA first and then some delay is allowed before the related services (utilizing the new source prefixes) are activated online.

6. Security Considerations

There are two main threats associated with SPA: prefix hijacking and path hijacking.

* Prefix hijacking. A malicious AS may send an SPA message which hijacks the source prefixes of a Source AS. The Validating AS that receives the message may improperly include the source prefixes in some source prefix lists, which results in improper permitting but no improper blocking.

* Path hijacking. A malicious AS may send an SPA message which carries a manipulated AS_PATH, which can be a forged-origin attack or a forged-path-segment attack. The Validating AS that receives the message may improperly include the source prefixes in some source prefix lists, which results in improper permitting but no improper blocking.

Existing mechanisms for detecting and preventing BGP prefix hijacking and BGP path hijacking can be used to deal with the above two threats.

7. IANA Considerations

There is no IANA requirement.

Acknowledgements

Many thanks to the comments from XXX.

References

Normative References

[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.ietf-savnet-inter-domain-problem-statement] Li, D., Wu, J., Liu, L., Huang, M., and K. Sriram, "Source Address Validation in Inter-domain Networks Gap Analysis, Problem Statement, and Requirements", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-problem-statement-09, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-problem-statement-09>.

[I-D.ietf-savnet-inter-domain-architecture]
Li, D., 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-01, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-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>.

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>.

Authors' Addresses

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

Lancheng Qin
Zhongguancun Laboratory
Beijing
China
Email: qinlc@mail.zgclab.edu.cn

Kotikalapudi Sriram
USA NIST
Gaithersburg, MD 20899,
United States of America
Email: ksriram@nist.gov

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