SAVNET
Internet-Draft
Intended status: Informational
Expires: 26 February 2026

N. Geng
Huawei
L. Qin
Zhongguancun Laboratory

25 August 2025

Currently Used Terminology Related to Source Address Validation
draft-gq-savnet-sav-terms-00

Abstract

This document provides an overview of terms and abbreviations related to Source Address Validation (SAV). Its purpose is to establish a common and consistent set of terminology for use across SAV-related discussions and documents. This document explicitly does not serve as an authoritative source of correct terminology.

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 26 February 2026.

Table of Contents

1. Introduction 2
1.1. Requirements Language 2
2. General Terms 2
2.1. Network and Topology Terms 2
2.2. Router and Interface Terms 3
2.3. Routing Terms 4
2.4. Routing Security Terms 4
2.5. Others 5
3. SAV Terms 5
3.1. General SAV Terms 5
3.2. SAV Enforcement Terms 6
3.3. SAV Mechanism Terms 8
4. Security Considerations 9
5. IANA Considerations 9
6. References 9
6.1. Normative References 9
6.2. Informative References 10
Authors' Addresses 13

1. Introduction

This document provides an overview of terms and abbreviations related to Source Address Validation (SAV). Its purpose is to establish a common and consistent set of terminology for use across SAV-related discussions and documents. This document explicitly does not serve as an authoritative source of correct terminology.

1.1. 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. General Terms

2.1. Network and Topology Terms

* *Autonomous System (AS):* A set of routers under a single technical administration [RFC4271].

* *AS Number (ASN):* A 16-bit [RFC4271] or 32-bit [RFC6793] number uniquely identifying an Autonomous System.

* *Sub Network:* A sub network may operate its own internal routing protocols, but it is considered part of the AS in the global routing system. It is connected to one or more routers of the AS for Internet connectivity. It originates traffic but does not transit traffic for other networks [I-D.ietf-savnet-intra-domain-problem-statement].

* *Provider (aka Provider AS):* The provider in a customer-to-provider relationship (if looked at from the opposite direction, provider-to-customer [caida-asrank]). A Provider may propagate any available route to a Customer [RFC9234].

* *Customer (aka Customer AS):* The customer in a customer-to-provider relationship. A Customer may propagate any route learned from a Customer, or that is locally originated, to a Provider. All other routes must not be propagated [RFC9234].

* *Peer (aka Peer AS or Lateral Peer or Lateral Peer AS):* The peers in a lateral peering relationship. A Peer may propagate any route learned from a Customer, or that is locally originated, to a Peer. All other routes must not be propagated [RFC9234].

* *Customer Cone:* The set of ASes that an AS can reach by using only provider-to-customer links [caida-asrank].

* *Provider Cone:* The set of ASes that an AS can reach by using only customer-to-provider links [I-D.li-sidrops-bicone-sav].

2.2. Router and Interface Terms

* *Edge Router:* The router that is directly connected to a Sub Network or a host [I-D.geng-idr-bgp-savnet].

* *AS Border Router (ASBR):* The router that connects an AS to other ASes.

* *Internal Router:* The router that is neither an edge router nor a border router in an AS.

* *Customer Interface (aka Customer-facing Interface):* The interface of an ASBR facing a Customer [RFC8704].

* *Lateral Peer Interface (aka Lateral Peer-facing Interface):* The interface of an ASBR facing a Lateral Peer [RFC8704].

* *Provider Interface (aka Provider-facing Interface):* The interface of an ASBR facing a Provider [RFC8704].

2.3. Routing Terms

* *Interior Gateway Protocol (IGP):* A type of routing protocol used within a single AS to exchange routing information between routers.

* *Intermediate System to Intermediate System (IS-IS):* A link-state routing protocol belonging to IGP and designed to dynamically exchange routing information within a single AS [RFC1195].

* *Open Shortest Path First (OSPF):* Another link-state routing protocol belonging to IGP and designed to dynamically exchange routing information within a single AS [RFC2328][RFC5340].

* *Border Gateway Protocol (BGP):* A path-vector routing protocol used in the global Internet to exchange routing information between different ASes [RFC4271].

* *Routing Information Base (RIB):* A database within a router or network host that stores routing information. RIB is also known as routing table.

* *Forwarding Information Base (FIB):* The table containing the information necessary to forward IP Datagrams [RFC3222]. FIB is also known as forwarding table. FIB stores the best active routes, which are a subset of those found in the RIB.

* *Virtual Routing and Forwarding (VRF):* The routing (or forwarding) tables separate from the global routing (or forwarding) table in a router [RFC4364][RFC8704].

* *Asymmetric Routing:* Asymmetric routing means a packet traverses from a source to a destination in one path and takes a different path when it returns to the source. Asymmetric routing can occur within an AS due to routing policy, traffic engineering, etc [I-D.ietf-savnet-intra-domain-problem-statement].

2.4. Routing Security Terms

* *Resource Public Key infrastructure (RPKI):* A specialized public key infrastructure (PKI) framework to support improved security for the Internet’s BGP routing infrastructure [RFC6480].

* *Route Origin Authorization (ROA):* A digitally signed object in the RPKI that provides a means of verifying that an IP address block holder has authorized an AS to originate routes to one or more prefixes within the address block [RFC9582].

* *Autonomous System Provider Authorization (ASPA):* A digitally signed object in the RPKI, that authorizes one or more other ASes as its upstream providers [I-D.ietf-sidrops-aspa-profile].

* *Internet Routing Registry (IRR):* A public database which allows Internet service providers to publish and look up Internet number bindings and policy objectives.

* *Resource holder:* A legitimate holder of either IP address or AS number resources [RFC6480].

2.5. Others

* *Direct Server Return (DSR):* A Content Delivery Network (CDN) technique. The anycast server receives requests from users and creates tunnels to the edge server, and the edge server directly sends the requested content to users. The source address of the response packets is the anycast IP address of the anycast server, but the network hosting the edge server does not announce the anycast address in BGP [I-D.ietf-savnet-inter-domain-problem-statement].

3. SAV Terms

3.1. General SAV Terms

* *Source Address Spoofing (aka Source Address Forgery):* The act of using spoofed source IP addresses assigned to other machines. Malicious actors use IP spoofing to invoke a variety of attacks, including Distributed Denial of Service (DDoS) attacks, policy evasion, and a range of application-level attacks [manrs-blog]. A spoofed source address can be either IPv4 or IPv6.

* *Source Address Validation (SAV):* A kind of techniques for the detection and mitigation of Source Address Spoofing [RFC8704]. Routers conduct SAV on data packet in the data plane. SAV focuses on the scenarios of native IP forwarding or IP-encapsulated tunnel (IPsec, GRE, SRv6, etc.). Note that, the SAV mechanisms that the SAVNET working group is interested in should not modify data plane packets [savnet-charter].

* *SAV Rule:* The rule that describes the binding relationship between a source address (prefix) and a valid/invalid incoming interface(s) [I-D.ietf-savnet-intra-domain-problem-statement]. SAV Rules can be used for validating whether a data packet with a source address arrive at the router (enforing SAV based on SAV Rules) from an expected interface, and thus determining whether the source address is spoofed (i.e., valid) or not (i.e., invalid).

* *SAV Table:* The table or data structure that implements the SAV rules and is used for performing source address validation in the data plane [I-D.ietf-savnet-inter-domain-architecture].

* *Access Network SAV:* It prevents a host in a network from spoofing the address of another host in the same network segment. Access Network SAV enables source address-granularity of protection [RFC5210].

* *Intra-domain SAV (aka Intra-AS SAV):* It prevents a Sub Network from using a source address out of the Sub Network or prevents a host from using a source address out of the network segment. Intra-domain SAV mostly enables source prefix-granularity of protection.

* *Inter-domain SAV (aka Inter-AS SAV):* It prevents Source Address Spoofing packets across ASes. Inter-domain SAV mostly enables source prefix-granularity of protection.

* *Source Address Validation Architecture (SAVA):* A multiple-fence architecture that takes Access Network SAV, Intra-AS SAV, and inter-AS SAV [RFC5210]. The assumption here is that when access-network SAV is not universally deployed, Intra-AS SAV and Inter-AS SAV can increase the defense in depth by blocking spoofing packets that have entered the network.

* *Source Address Validation in Intra-domain and Inter-domain Networks (SAVNET):* It refers to both Intra-domain SAV and Inter-domain SAV. The SAVNET working group was created for the evolvement of SAVNET mechanisms [savnet-charter].

3.2. SAV Enforcement Terms

* *Validation Mode:* The mode indicates how SAV Rules are logically organized and used to conduct validation [I-D.ietf-savnet-general-sav-capabilities].

* *Interface-based Source Prefix Allowlist (aka Source Prefix Allowlist):* A Validation Mode that takes effect on a specific interface. The interface enabling this mode maintains a source prefix list. Only the source addresses encompassed by the source prefixes recorded in the list will be considered valid, otherwise invalid [I-D.ietf-savnet-general-sav-capabilities].

* *Interface-based Source Prefix Blocklist (aka Source Prefix Blocklist):* A Validation Mode that takes effect on a specific interface. The interface enabling this mode maintains a source prefix list. Any source addresses encompassed by the source prefixes recorded in the list will be considered invalid, otherwise valid [I-D.ietf-savnet-general-sav-capabilities].

* *Source Prefix-based Interface Allowlist:* A Validation Mode that takes effect at the router scale. The router enabling this mode will record the source prefixes attached with an interface allowlist. For the packet whose source address is encompassed by a recorded source prefix, the packet is considered valid only when its incoming interface is included in the corresponding interface allowlist. Otherwise, the packet is considered invalid. For the packet whose source address is encompassed by no recorded source prefix, the validity of the packet is unknown [I-D.ietf-savnet-general-sav-capabilities].

* *Source Prefix-based Interface Blocklist:* A Validation Mode that takes effect at the router scale. The router enabling this mode will record the source prefixes attached with an interface blocklist. For the packet whose source address is encompassed by a recorded source prefix, the packet is considered valid only when its incoming interface is not included in the corresponding interface allowlist. Otherwise, the packet is considered invalid. For the packet whose source address is encompassed by no recorded source prefix, the validity of the packet is unknown [I-D.ietf-savnet-general-sav-capabilities].

* *Improper Block (aka False Positive):* The problem that the packets with legitimate source addresses are improperly considered invalid due to inaccurate SAV Rules [I-D.ietf-savnet-intra-domain-problem-statement][I-D.ietf-savnet-inter-domain-problem-statement].

* *Improper Permit (aka False Negative):* The problem that the packets with spoofed source addresses are improperly considered valid due to inaccurate SAV Rules [I-D.ietf-savnet-intra-domain-problem-statement][I-D.ietf-savnet-inter-domain-problem-statement].

* *Traffic Handling Policy:* The data plane action taken on the incoming packet after the SAV process on the packet. Besides "Discard", many other actions such as "Permit", "Rate Limit", and "Traffic Redirect" can be chosen and taken for the packet with the invalid state [I-D.ietf-savnet-general-sav-capabilities].

3.3. SAV Mechanism Terms

* *Access Control List (ACL) for SAV:* A filter that checks the source address of a data packet against a list of acceptable or unacceptable prefixes [RFC2827].

* *Strict unicast Reverse Path Forwarding (uRPF):* A mechanism that uses FIB for SAV. An ingress packet is accepted only if the FIB contains a prefix that encompasses the source address and forwarding information for that prefix points back to the interface over which the packet was received [RFC3704].

* *Feasible-Path uRPF (FP-uRPF):* An extension of Strict uRPF. Instead of just inserting one best route there, the alternative paths (if any) have been added as well, and are valid for consideration [RFC3704].

* *Loose uRPF:* A mechanism checks only for the existence of a route (even a default route, if applicable), not where the route points to (At least some implementations of Loose uRPF check where the default route points to) [RFC3704].

* *Loose uRPF Ignoring Default Route:* Loose uRPF checks only for the existence of a explicit route (default routes are excluded) [RFC3704].

* *VRF uRPF:* A mechanism that takes SAV based on VRF table instead of FIB. The specific routes received from external BGP peers will be stored in a dedicated VRF table. VRF uRPF can be implemented to support the strict mode like Strict uRPF or the loose mode like Loose uRPF [RFC8704].

* *Enhanced Feasible-Path uRPF (EFP-uRPF):* A mechanism that is more flexible about directionality than the FP-uRPF and is for enhancing FP-uRPF in some cases. It is based on the principle that if BGP updates for multiple prefixes with the same origin AS were received on different interfaces (at border routers), then incoming data packets with source addresses in any of those prefixes should be accepted on any of those interfaces [RFC8704].

* *BAR-SAV:* A mechanism that generates source prefix allowlists by using BGP UPDATE messages, ASPA, and ROA [I-D.ietf-sidrops-bar-sav].

* *General SAV Information:* The information that is not specialized for SAV but can be utilized to generate SAV rules, and is initially utilized for other purposes. Currently, the General SAV Information consists of the information from RPKI ROA objects and ASPA objects, local routing information, and the information from IRR data [I-D.ietf-savnet-inter-domain-architecture].

* *SAV-specific Information:* The information that is specialized for SAV rule generation, includes the source prefixes and their legitimate incoming directions to enter a router or an AS, and is exchanged among routers or ASes.

* *SAV-related Information:* The information that can be used to generate SAV rules and includes SAV-specific Information and General SAV Information.

* *Source Entity (aka Source Router or Source AS):* The Entity (Router/AS) that propagates its SAV-specific information to Validation Entity (Router/AS) [I-D.ietf-savnet-intra-domain-architecture][I-D.ietf-savnet-inter-domain-architecture]. Source Entity is the producer of SAV-specific information.

* *Validation Entity (aka Validation Router or Validation AS):* The Entity (Router/AS) that receives SAV-specific information from Source Entity (Router/AS) [I-D.ietf-savnet-intra-domain-architecture][I-D.ietf-savnet-inter-domain-architecture]. Validation Entity is the consumer of SAV-specific information.

4. Security Considerations

This document provides an overview of terms and abbreviations related to SAV and does not have security considerations.

5. IANA Considerations

There is no IANA requirement.

6. References

6.1. Normative References

[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>.

6.2. Informative References

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, DOI 10.17487/RFC1195, December 1990, <https://www.rfc-editor.org/info/rfc1195>.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <https://www.rfc-editor.org/info/rfc2328>.

[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>.

[RFC3222] Trotter, G., "Terminology for Forwarding Information Base (FIB) based Router Performance", RFC 3222, DOI 10.17487/RFC3222, December 2001, <https://www.rfc-editor.org/info/rfc3222>.

[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>.

[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>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/rfc4364>.

[RFC5210] Wu, J., Bi, J., Li, X., Ren, G., Xu, K., and M. Williams, "A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience", RFC 5210, DOI 10.17487/RFC5210, June 2008, <https://www.rfc-editor.org/info/rfc5210>.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008, <https://www.rfc-editor.org/info/rfc5340>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, DOI 10.17487/RFC6793, December 2012, <https://www.rfc-editor.org/info/rfc6793>.

[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>.

[RFC9234] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages", RFC 9234, DOI 10.17487/RFC9234, May 2022, <https://www.rfc-editor.org/info/rfc9234>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

[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-17, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-17>.

[I-D.ietf-savnet-inter-domain-problem-statement] Li, D., Qin, L., 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-10, 28 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-problem-statement-10>.

[I-D.ietf-savnet-intra-domain-architecture]
Li, D., Wu, J., Qin, L., Geng, N., and L. Chen, "Intra-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-ietf-savnet-intra-domain-architecture-02, 13 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-architecture-02>.

[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>.

[I-D.ietf-savnet-general-sav-capabilities]
Huang, M., Cheng, W., Li, D., Geng, N., and L. Chen, "General Source Address Validation Capabilities", Work in Progress, Internet-Draft, draft-ietf-savnet-general-sav-capabilities-01, 24 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-general-sav-capabilities-01>.

[I-D.ietf-sidrops-aspa-profile]
Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-20, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-20>.

[I-D.geng-idr-bgp-savnet]
Geng, N., Li, Z., Tan, Z., Liu, Li, D., and F. Gao, "BGP Extensions for Source Address Validation Networks (BGP SAVNET)", Work in Progress, Internet-Draft, draft-geng-idr-bgp-savnet-04, 11 October 2024, <https://datatracker.ietf.org/doc/html/draft-geng-idr-bgp-savnet-04>.

[I-D.li-sidrops-bicone-sav]
Qin, L., Li, D., Chen, L., and L. Liu, "Bicone Source Address Validation", Work in Progress, Internet-Draft, draft-li-sidrops-bicone-sav-07, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-li-sidrops-bicone-sav-07>.

[I-D.ietf-sidrops-bar-sav]
Sriram, K., Lubashev, I., and D. Montgomery, "Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)", Work in Progress, Internet-Draft, draft-ietf-sidrops-bar-sav-07, 20 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-bar-sav-07>.

[caida-asrank]
"CAIDA AS Rank", August 2025, <https://asrank.caida.org/about>.

[manrs-blog]
"Why is Source Address Validation Still a Problem?", April 2023, <https://manrs.org/2023/04/why-is-source-address-validation-still-a-problem>.

[savnet-charter]
"Charter for SAVNET Working Group", March 2023, <https://datatracker.ietf.org/wg/savnet/about>.

Authors' Addresses

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

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