Internet Engineering Task Force (IETF)
Request for Comments: 8074
Category: Standards Track
ISSN: 2070-1721

J. Bi
Tsinghua University
G. Yao
Tsinghua University/Baidu
J. Halpern
Ericsson
E. Levy-Abegnoli, Ed.
Cisco

February 2017

Source Address Validation Improvement (SAVI) for Mixed Address Assignment Methods Scenario

Abstract

In networks that use multiple techniques for address assignment, the spoofing of addresses assigned by each technique can be prevented using the appropriate Source Address Validation Improvement (SAVI) methods. This document reviews how multiple SAVI methods can coexist in a single SAVI device and how collisions are resolved when the same binding entry is discovered by two or more methods.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8074.

Copyright Notice

Table of Contents

1. Introduction

There are currently several Source Address Validation Improvement (SAVI) documents ([RFC6620], [RFC7513], and [RFC7219]) that describe the different methods by which a switch can discover and record bindings between a node's IP address and a binding anchor and use that binding to perform source address validation. Each of these documents specifies how to learn on-link addresses, based on the technique used for their assignment: StateLess Address Autoconfiguration (SLAAC), the Dynamic Host Control Protocol (DHCP), and Secure Neighbor Discovery (SEND), respectively. Each of these documents describes separately how one particular SAVI method deals with address collisions (same address but different binding anchor).

While multiple IP assignment techniques can be used in the same layer 2 domain, this means that a single SAVI device might have to deal with a combination or mix of SAVI methods. The purpose of this document is to provide recommendations to avoid collisions and to review collision handling when two or more such methods come up with competing bindings.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Problem Scope

Three different IP address assignment techniques have been analyzed for SAVI:

1. StateLess Address Autoconfiguration (SLAAC) -- analyzed in FCFS SAVI (First-Come, First-Served) [RFC6620]

2. Dynamic Host Control Protocol address assignment (DHCP) -- analyzed in SAVI-DHCP [RFC7513]

3. Secure Neighbor Discovery (SEND) address assignment -- analyzed in SEND SAVI [RFC7219]

In addition, there is a fourth technique for managing (i.e., creation, management, and deletion) a binding on the switch, referred to as "manual". It is based on manual binding configuration. How to manage manual bindings is determined by operators, so there is not a new SAVI method for manual addresses.

All combinations of address assignment techniques can coexist within a layer 2 domain. A SAVI device MUST implement the corresponding binding setup methods (referred to as "SAVI methods") for each such technique that is in use if it is to provide source address validation.

SAVI methods are normally viewed as independent from each other, each one handling its own entries. If multiple methods are used in the same device without coordination, each method will attempt to reject packets sourced with any addresses that method did not discover. To prevent addresses discovered by one SAVI method from being filtered out by another method, the SAVI binding table SHOULD be shared by all the SAVI methods in use in the device. This in turn could create some conflict when the same entry is discovered by two different methods. The purpose of this document is twofold: to provide recommendations and methods to avoid conflicts and to resolve conflicts when they happen. Collisions happening within a given method are outside the scope of this document.

4. Architecture

A SAVI device may implement and use multiple SAVI methods. This mechanism, called "SAVI-MIX", is proposed as an arbiter of the binding generation algorithms from these multiple methods, generating the final binding entries as illustrated in Figure 1. Once a SAVI method generates a candidate binding, it will request that SAVI-MIX set up a corresponding entry in the binding table. Then, SAVI-MIX will check if there is any conflict in the binding table. A new binding will be generated if there is no conflict. If there is a conflict, SAVI-MIX will determine whether to replace the existing binding or reject the candidate binding based on the policies specified in Section 6.

As a result of this, the packet filtering in the SAVI device will not be performed by each SAVI method separately. Instead, the table resulting from applying SAVI-MIX will be used to perform filtering. Thus, the filtering is based on the combined results of the different SAVI mechanisms. It is beyond the scope of this document to describe the details of the filtering mechanism and its use of the combined SAVI binding table.

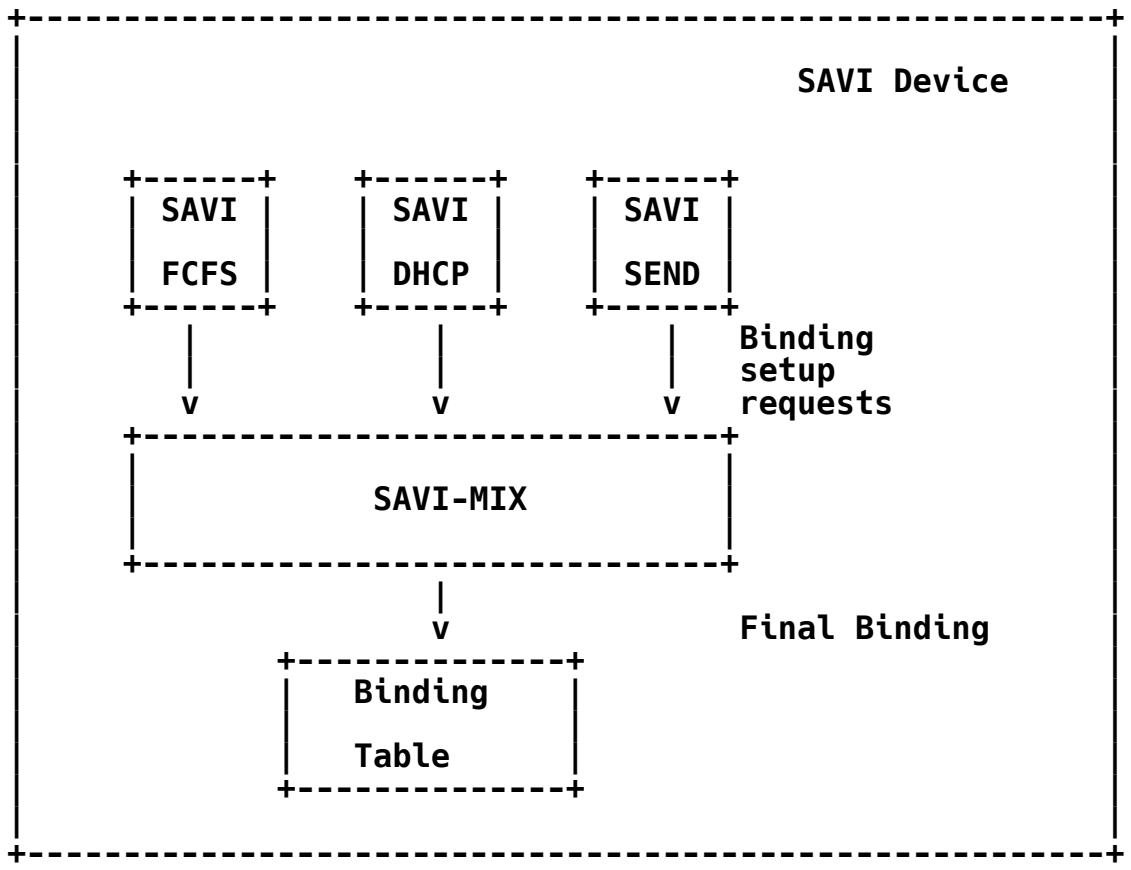

Figure 1: SAVI-MIX Architecture

Each entry in the binding table will contain the following fields:

1. IP source address
2. Binding anchor [RFC7039]
3. Lifetime
4. Creation time
5. Binding methods: the SAVI method used for this entry

5. Recommendations for Assignment Separation

If each address assignment technique uses a separate portion of the IP address space, collisions won't happen. Using non-overlapping address space across address assignment techniques, and thus across SAVI methods, is therefore recommended. To that end, one should:

1. DHCP and SLAAC: use a non-overlapping prefix for DHCP and SLAAC. Set the A bit in the Prefix Information option of the Router Advertisement for the SLAAC prefix, and set the M bit in the Router Advertisement for the DHCP prefix. For detailed explanations of these bits, refer to [RFC4861] and [RFC4862].

2. SEND and non-SEND: avoid mixed environments (where SEND and non-SEND nodes are deployed) or separate the prefixes announced to SEND and non-SEND nodes. One way to separate the prefixes is to have the router(s) announcing different (non-overlapping) prefixes to SEND and to non-SEND nodes, using unicast Router Advertisements [RFC6085], in response to SEND/non-SEND Router Solicit.

6. Resolving Binding Collisions

In situations where collisions cannot be avoided by assignment separation, two cases should be considered:

1. The same address is bound on two different binding anchors by different SAVI methods.

2. The same address is bound on the same binding anchor by different SAVI methods.

6.1. Same Address on Different Binding Anchors

This would typically occur if assignment address spaces could not be separated. For instance, an address is assigned by SLAAC on node X, installed in the binding table using FCFS SAVI, and anchored to "anchor-X". Later, the same address is assigned by DHCP to node Y, and SAVI-DHCP will generate a candidate binding entry, anchored to "anchor-Y".

6.1.1. Basic Preference

If there is any manually configured binding, the SAVI device SHOULD choose the manually configured binding anchor.

For an address not covered by any manual bindings, the SAVI device must decide to which binding anchor the address should be bound (anchor-X or anchor-Y in this example). Current standard documents of address assignment methods have implied the prioritization relationship based on order in time, i.e., First-Come, First-Served.

- SLAAC: Section 5.4.5 of [RFC4862]
- DHCPv4: Section 3.1, Point 5 of [RFC2131]
- DHCPv6: Section 18.1.8 of [RFC3315]
- SEND: Section 8 of [RFC3971]

In the absence of any configuration or protocol hint (see Section 6.1.2), the SAVI device SHOULD choose the first-come binding anchor, whether it was learned from SLAAC, SEND, or DHCP.

6.1.2. Exceptions

There are two identified exceptions to the general prioritization model, one being Cryptographically Generated Addresses (CGA) [RFC3971] and the other controlled by the configuration of the switch.

6.1.2.1. CGA Preference

When CGA addresses are used and a collision is detected, preference should be given to the anchor that carries the CGA credentials once they are verified, in particular, the CGA parameters and the RSA options. Note that if an attacker was trying to replay CGA credentials, he would then compete on the base of the "First-Come, First-Served" (FCFS) principle.

6.1.2.2. Configuration Preference

For configuration-driven exceptions, the SAVI device may allow the configuration of a triplet ("prefix", "anchor", "method") or ("address", "anchor", "method"). The "prefix" or "address" represents the address or address prefix to which this preference entry applies. The "anchor" is the value of a known binding anchor that this device expects to see using this address or addresses from this prefix. The "method" is the SAVI method that this device

expects to use in validating address binding entries from the address or prefix. At least one of "anchor" and "method" MUST be specified. Later, if a Duplicate Address Detection (DAD) message [RFC4861] is received with the following conditions verified:

1. The target in the DAD message does not exist in the binding table,

2. The target is within the configured "prefix" (or equal to "address"),

3. The anchor bound to the target is different from the configured anchor, when specified, and

4. The configured method, if any, is different from FCFS SAVI,

then the switch SHOULD defend the address by responding to the DAD message, with a Neighbor Advertisement (NA) message, on behalf of the target node. It SHOULD NOT install the entry into the binding table. The DAD message SHOULD be discarded and not forwarded. Forwarding it may cause other SAVI devices to send additional defense NAs. SEND nodes in the network MUST disable the option to ignore unsecured advertisements (see Section 8 of [RFC3971]). If the option is enabled, the case is outside the scope of this document. It is suggested to limit the rate of defense NAs to reduce security threats to the switch. Otherwise, a malicious host could consume the resource of the switch heavily with flooding DAD messages.

This will simply prevent the node from assigning the address and will de facto prioritize the configured anchor. It is especially useful to protect well-known bindings (such as a static address of a server) against any other host, even when the server is down. It is also a way to give priority to a binding learned from SAVI-DHCP over a binding for the same address, learned from FCFS SAVI.

6.1.3. Multiple SAVI Device Scenario

A single SAVI device doesn't have the information of all bound addresses on the perimeter. Therefore, it is not enough to look up local bindings to identify a collision. However, assuming DAD is performed throughout the security perimeter for all addresses regardless of the assignment method, then the DAD response will inform all SAVI devices about any collision. In that case, "First-Come, First-Served" will apply the same way as in a single switch scenario. If the admin configured a prefix (or a single static binding) on one of the switches to defend, the DAD response generated by this switch will also prevent the binding from being installed on

other switches on the perimeter. The SAVI-MIX preferences of all the SAVI devices in the same layer 2 domain should be consistent. Inconsistent configurations may cause network breaks.

6.2. Same Address on the Same Binding Anchor

A binding may be set up on the same binding anchor by multiple methods, typically FCFS SAVI and SAVI-DHCP. If the binding lifetimes obtained from the two methods are different, priority should be given to 1) manual configuration, 2) SAVI-DHCP, 3) and FCFS SAVI as the least authoritative. The binding will be removed when the prioritized lifetime expires, even if a less authoritative method had a longer lifetime.

7. Security Considerations

Combining SAVI methods (as in SAVI-MIX) does not improve or eliminate the security considerations associated with each individual SAVI method. Therefore, security considerations for each enabled SAVI method should be addressed as described in that method's associated RFC. Moreover, combining methods (as in SAVI-MIX) has two additional implications for security. First, it may increase susceptibility to DoS attacks, because the SAVI binding setup rate will be the sum of the rates of all enabled SAVI methods. Implementers must take these added resource requirements into account. Second, because SAVI-MIX supports multiple binding mechanisms, it potentially reduces the security level to that of the weakest supported method, unless additional steps (e.g., requiring non-overlapping address spaces for different methods) are taken.

8. Privacy Considerations

When implementing multiple SAVI methods, privacy considerations of all methods apply cumulatively.

9. IANA Considerations

This document does not require any IANA registrations.

10. References

10.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <http://www.rfc-editor.org/info/rfc2131>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <http://www.rfc-editor.org/info/rfc3971>.

[RFC6085] Gundavelli, S., Townsley, M., Troan, O., and W. Dec, "Address Mapping of IPv6 Multicast Packets on Ethernet", RFC 6085, DOI 10.17487/RFC6085, January 2011, <http://www.rfc-editor.org/info/rfc6085>.

[RFC6620] Nordmark, E., Bagnulo, M., and E. Levy-Abegnoli, "FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses", RFC 6620, DOI 10.17487/RFC6620, May 2012, <http://www.rfc-editor.org/info/rfc6620>.

[RFC7219] Bagnulo, M. and A. Garcia-Martinez, "SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI)", RFC 7219, DOI 10.17487/RFC7219, May 2014, <http://www.rfc-editor.org/info/rfc7219>.

[RFC7513] Bi, J., Wu, J., Yao, G., and F. Baker, "Source Address Validation Improvement (SAVI) Solution for DHCP", RFC 7513, DOI 10.17487/RFC7513, May 2015, <http://www.rfc-editor.org/info/rfc7513>.

10.2. Informative References

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <http://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <http://www.rfc-editor.org/info/rfc7039>.

Acknowledgments

Thanks to Christian Vogt, Eric Nordmark, Marcelo Bagnulo Braun, David Lamparter, Scott G. Kelly, and Jari Arkko for their valuable contributions.

Authors' Addresses

Jun Bi
Tsinghua University
Institute for Network Sciences and Cyberspace, Tsinghua University
Beijing 100084
China

Email: junbi@tsinghua.edu.cn

Guang Yao
Tsinghua University/Baidu
Baidu Science and Technology Park, Building 1
Beijing 100193
China

Email: yaoguang.china@gmail.com

Joel M. Halpern
Ericsson

Email: joel.halpern@ericsson.com

Eric Levy-Abegnoli (editor)
Cisco Systems
Village d'Entreprises Green Side - 400, Avenue Roumanille
Biot-Sophia Antipolis 06410
France

Email: elevyabe@cisco.com