IPv6 Maintenance (6man) Working Group
Internet-Draft
Updates: 4191, 4861, 4862, 8504, 8028, 6724 (if approved)
Intended status: Standards Track
Expires: 4 September 2025

F. Gont
SI6 Networks

3 March 2025

Improving Support for Multi-Router, Multi-Interface, and Multi-Prefix Scenarios
draft-gont-6man-multi-ipv6-spec-01

Abstract

This document specifies a improvements to IPv6 Stateless Address Autoncofiguration (SLAAC) to fully support common multi-router, multi-interface, and multi-prefix scenarios. It formally updates RFC 4191, RFC 4861, RFC 4862, and RFC 8504, RFC 8028, and RFC 6724, such that these scenarios are properly supported by IPv6 host implementations.

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 4 September 2025.

Copyright Notice

Table of Contents

1. Introduction

IPv6 Stateless Address Autoconfiguration (SLAAC) is based on the premise that SLAAC routers advertise network configuration information on a local network, and SLAAC hosts aggregate this information and use it as they see fits. In the case of simple network scenarios such as a local network with a single SLAAC router, or a network with multiple SLAAC routers where all routers advertise the same network configuration information, SLAAC works just fine. However, other more complex (yet very common) scenarios are very badly supported (if at all supported). THese scenarios include, but are not limited to, the following:

* Two Customer Premises Equipment (CPE) routers are attached to a local network, whether to perform basic load-sharing across two upstream connctions, or for improved resiliency (i.e. provide a fall-back upstream Internet connection).

* An IPv6 host attaches to two different local networks via different network interfaces. For example, an IPv6 host employs a wired Ethernet connection and a Wi-Fi wireless connection, or a mobile node employs a 4G mobile connection, and also leverages WiFi connectivity where available.

As discussed in [I-D.gont-v6ops-multi-ipv6], these scenarios are not only common, but support for these scenarios may actually represent a pre-requisite for deploying IPv6 in an Enterprise or home office environemnt. Therefore, they warrant native and proper support by IPv6 hosts.

[RFC8028] discusses the challenge of selecting an appropriate default router in Multi-IPv6 scenarios, and specifies some recommendations for the selection of a next-hop router in multi-ipv6 scenarios. However, as noted in [I-D.gont-v6ops-multi-ipv6], there still exists specification gaps that prevent full support of multi-ipv6 scenarios. This document builds upon [RFC8028] to provide a more comprehensive solution to the problem at hand.

2. Terminology

Multi-prefix scenario:
: A network scenario where a host employs two or more IPv6 prefixes for address configuration with SLAAC. This may be the result of attaching to two or more networks via two or more network interfaces, or simply the result of attaching to a single local network where multiple prefixes are advertised via one or more SLAAC routers.

Multi-router scenario:
: A network scenario where a SLAAC hosts employs two or more SLAAC routers. This may be the result of attaching to two o more networks via two or more network interfaces, or simply the result of attaching to a single local network where multiple prefixes are advertised via one or more SLAAC routers.

Multi-interface scenario:
: A network scenario where a host employs two or more network interfaces (without considering the "loopback" interface). Some bibliography refer to these hosts as being "multihomed". In the vast majority of cases, hosts employing multiple interfaces will result in "multi-prefix" and "multi-router" scenarios. In the specific corner case where a host attaches to the same network via two (or more) network interfaces, this will typically result in a multi-router scenario, where the same router that is available via multiple is interfaces is considered, fo all practical purposes, as a different router -- .e.g., the same router will result in different default routes, one via each of the network interfaces.

Multi-IPv6:
: The term "Multi-IPv6" (case insensitive) is employed throughout this document as a short-hand for network scenarios where multiple IPv6 routers, multiple interfaces, and/or multiple IPv6 prefixes

are employed. We note that "multi-prefix", "multi-interface", and "multi-router" scenarios are not mutually-exclusive: for instance, a host that employs multiple interfaces will usually also employ multiple prefixes and multiple routers.

SLAAC prefix set:
The SLAAC prefix set for an SLAAC router is composed of all prefixes that are being advertised by the router via SLAAC PIOs (irrespective of how e.g. the "A" and "L" flags of the PIO were set).

3. Conceptual model

In order to properly properly support multi-ipv6 scenarios, IPv6 hosts should adhere to the following principles:

* Network configuration information advertised by each SLAAC router is an atomic set of information that must be associated with the router that advertised it. This means that:

  - Hosts should maintain state for SLAAC information on a per-slaac-router basis (as opposed to a "per-host" or "per-interface" basis. If the same piece of information is advertised by multiple SLAAC routers, a SLAAC host must maintain state information for the advertised information on a per-router basis -- i.e., one record (with an associated timer, where applicable) for each advertising router.

  - As a result of this consideration, in scenarios where the same network configuration information is advertised by multiple local SLAAC routers, such information may eventually expire or be considered invalid for one of the SLAAC routers that advertised it, but may still be valid for some of the other routers that have advertised it (since state is maintained on a per-router basis as opposed to a per-host or per-interface basis).

  - IPv6 addresses configured from a given SLAAC prefix should only be employed with the SLAAC routers that have advertised such prefix on the local network. RDNSS should only be queried from SLAAC prefixes advertised by the same router that advertised the RDNSS, via the router that advertised such prefixes.

- Hosts must not employ information advertised by one SLAAC in conjunction with information advertised by other SLAAC routers. For example, in a network scenario where SLAAC router ROUTER_A advertises {RDNSS_A, autoconfiguration prefix PREFIX_A} and SLAAC router ROUTER_B advertises {RDNSS_B, autoconfiguration prefix PREFIX_B}, SLAACs hosts should NOT do any of the following:

  o Send packets from PREFIX_A via ROUTER_B (or packets from PREFIX_B via ROUTER_A)

  o Send DNS queries from PREFIX_A to RDNSS_B (or queries from PREFIX_B to RDNSS_A)

  o Send packets from PREFIX_A to an IPv6 address obtained via RDNSS_B (or packets from PREFIX_B to an IPv6 address obtained via RDNSS_A)

* IPv6 addresses configured from a given SLAAC prefix should only be employed with the SLAAC routers that have advertised such prefix on the local network: it is quite common for IPv6 routers to enforce ingress/egress filtering, and thus in a scenario where SLAAC router ROUTER_A advertises {RDNSS_A, autoconfiguration prefix PREFIX_A} and SLAAC router ROUTER_B advertises {RDNSS_B, autoconfiguration prefix PREFIX_B}, ROUTER_A might drop outgoing packets (from the local network) that are not sourced from PREFIX_A, while ROUTER_B might drop outgoing packets that are not sourced from PREFIX_B.

* It is not uncommon for servers to enforce Access Control Lists (ACLs) based on the IPv6 address of incoming requests. Thus, as noted above, this means that:

  - In a scenario where SLAAC router ROUTER_A advertises {RDNSS_A, autoconfiguration prefix PREFIX_A} and SLAAC router ROUTER_B advertises {RDNSS_B, autoconfiguration prefix PREFIX_B}, RDNSS_A might drop DNS queries that do not originate from PREFIX_A, while RDNSS_B might drop DNS queries that do not originate from PREFIX_B.

  - Communications with addresses obtained via a RDNSS should be carried out using source addresses from the prefix-set of the router that advertised the RDNSS that was employed for DNS resoltion: In a scenario where SLAAC router ROUTER_A advertises {RDNSS_A, autoconfiguration prefix PREFIX_A} and SLAAC router ROUTER_B advertises {RDNSS_B, autoconfiguration prefix PREFIX_B}, RNDSS_A might resolve e.g. "www.example.com" to an IPv6 address that will drop incoming requests unless they

originate from PREFIX_A, while RDNSS_B might resolve the same domain name ("www.example.com") to a different IPv6 address that will drop incoming requests unless they originate from PREFIX_B. In other scenarios, RDNSS_A might resolve a domain name to an IPv6 address that is topologically close to RDNSS_A. Thus, and address from PREFIX_B is employed to communicate with the corresponding address, this might result in suboptimal service (when compared to communicating with that address from PREFIX_A).

4. Protocol Specification

4.1. Processing and Usage of SLAAC information

* SLAAC hosts MUST maintain state information for each piece of SLAAC information advertised by each SLAAC router, on a per-router basis. This means, for example, that for each piece of SLAAC information that employs "lifetimes", the associated current lifetimes should be computed/maintained on a per-router basis. If a per-router lifetime expires, such information should be disassociated with that router -- that is, this should only affect the usage of such information via the router for which the "lifetime" has expired (please see Appendix A.2 for a more detailed discussion).

* SLAAC hosts MUST associate each SLAAC router with an IPv6 prefix set, that is composed of all prefixes that are being advertised as "valid" by such router via SLAAC PIOs (irrespective of how e.g. the "A" and "L" flags of the PIO were set).

* When sending packets via a SLAAC router, SLAAC hosts MUST employ an address from the prefix-set of that router.

* Any routing information (e.g., as that conveyed by RIOs [RFC4191] and Redirect messages [RFC4861]) MUST NOT be employed for packets sent with a Source Address that does not belong to the IPv6 prefix set of the SLAAC router that advertised this information .

* DNS queries sent to a RDNSS MUST employ source addresses from the prefix set of the router that advertised the RDNSS. For example, if ROUTER_A is the only SLAAC router that has advertised RDNSS_A, DNS queries sent to RDNSS_A MUST employ addresses from PREFIX_A.

* Information obtained from a RDNSS server MUST only be employed using an IPv6 source address from the same prefix employed for the source address of the DNS queries used to obtain that IPv6 address.

4.2. Improvement to Default Address Selection for Internet Protocol Version 6 (IPv6)

This document formally updates Section "5. Source Address Selection" of [RFC6724], by adding the following rule:

> Rule 5.7: Prefer addresses that will employ a REACHABLE next-hop. If SA or will employ a next-hop that is known to be REACHABLE, and SB will employ a next-hop that is not known to be REACHABLE, then prefer SA. Similarly, If SB or will employ a next-hop that is known to be REACHABLE, and SA will employ a next-hop that is not known to be REACHABLE, then prefer SB.
>
> > Discussion: This rule prefers next-hops that are known to be reachable (i.e., working next-hops). An IPv6 implementation is not required to remember which next-hops advertised which prefixes. The conceptual models of IPv6 hosts in Section 5 of [RFC4861] and Section 3 of [RFC4191] have no such requirement. Hence, Rule 5.3 is only applicable to implementations that track this information.

5. IANA Considerations

This document has no actions for IANA.

6. Security Considerations

This document does not introduce any new attack vectors. A host that were to implement the behavior described in this document might actually reduce the impact of some Neighbor discovery attacks. For example, an ND attack meaning to disable an IPv6 prefix by forging a Router Advertisement (RA) with a PIO for the target prefix with a zero lifetime would only succeed if:

* the RA impersonates an existing router (i.e., it employs the address of an existing router as the source address of the RA packet).
* No other router on the same network segment is currently advertising the target prefix.

Similarly, in a scenario where a host is employing multiple interfaces, and an attacker tries to disable the usage of a RDNSS by sending forged RAs advertising a RDNSS with a zero lifetime, the attacker would only be able to affect usage of that RDNSS via the network interface attached to network on which the attacker is performing the attack. However, RDNSS servers employed via network interfaces attached to different networks would remain unaffected.

If attacks based on forged RA packets are a concern, technologies such as RA-Guard [RFC6105] [RFC7113] should be deployed.

7. Acknowledgments

The authors would like to thank (in alphabetical order) Brian Carpenter for providing valuable comments on earlier versions of this document.

Fernando would also like to thank Brian Carpenter who, over the years, has answered many questions and provided valuable comments that has benefited his protocol-related work.

8. References

8.1. 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>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc4862>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <https://www.rfc-editor.org/info/rfc6724>.

[RFC8028] Baker, F. and B. Carpenter, "First-Hop Router Selection by Hosts in a Multi-Prefix Network", RFC 8028, DOI 10.17487/RFC8028, November 2016, <https://www.rfc-editor.org/info/rfc8028>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

[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>.

[RFC8504] Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019, <https://www.rfc-editor.org/info/rfc8504>.

8.2. Informative References

[I-D.gont-v6ops-multi-ipv6] Gont, F., "Problem Statement about IPv6 Support for Multiple Routers, Multiple Interfaces, and Multiple Prefixes", Work in Progress, Internet-Draft, draft-gont-v6ops-multi-ipv6-02, 3 March 2025, <https://datatracker.ietf.org/api/v1/doc/document/draft-gont-v6ops-multi-ipv6/>.

[I-D.ietf-6man-rfc6724-update] Buraglio, N., Chown, T., and J. Duncan, "Prioritizing known-local IPv6 ULAs through address selection policy", Work in Progress, Internet-Draft, draft-ietf-6man-rfc6724-update-17, 27 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-rfc6724-update-17>.

[I-D.link-v6ops-gulla] Linkova, J., "Using Subnet-Specific Link-Local Addresses to Improve SLAAC Robustness", Work in Progress, Internet-Draft, draft-link-v6ops-gulla-01, 25 February 2024, <https://datatracker.ietf.org/doc/html/draft-link-v6ops-gulla-01>.

[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>.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/info/rfc6105>.

[RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014, <https://www.rfc-editor.org/info/rfc7113>.

Appendix A. Sample scenarios

A.1. Normal Usage of SLAAC Information by IPv6 Hosts

Consider the following scenario:

* Two SLAAC routers (ROUTER_A and ROUTER_B) from different ISPs (ISP_A and ISP_B, respectively) are attached to NETWORK_C

* Router A advertises:

  - Prefix PREFIX_A for address configuration (by means of a Prefix Information Option (PIO) [RFC4861]).

  - One Recursive DNS server (RDNNSS_A) (by means of Recursive DNS Server option [RFC8106]).

* Router B advertises:

  - Prefix PREFIX_B for address configuration (by means of a Prefix Information Option (PIO) [RFC4861]).

  - One Recursive DNS server (RDNSS_B) (by means of Recursive DNS Server option [RFC8106]).

An IPv6 host that attaches to Network C and receives the aforementioned information should interpret it as follows:

* It may configure IPv6 addresses from PREFIX_A, and send packets from such addresses via ROUTER_A. It may send DNS queries to RDNSS_A from addresses in PREFIX_A, via ROUTER_A, and initiate communication with the resulting IPv6 addresses using source addresses from PREFIX_A (via ROUTER_A, as noted above).

* It may configure IPv6 addresses from PREFIX_B, and send packets from such addresses via ROUTER_B. It may send DNS queries to RDNSS_B from addresses in PREFIX_B, via ROUTER_B, and initiate communication with resulting IPv6 addresses using source addresses from PREFIX_B (via ROUTER_B, as noted above).

Any other combination of the network configuration information that mixes information from ROUTER_A and ROUTER_B is likely to result in interoperability problems and/or suboptimal service, since e.g.:

* ROUTER_A may implement network ingress filtering, and thus drop packets originating from NETWORK_C if they do not employ a source address from PREFIX_A.

* RDNSS_A may implement Access Control Lists (ACLs) such that it only accepts DNS queries from addresses in PREFIX_A.

* DNS Resolution of a domain name (e.g. "www.example.com may") may employ "split-horizon" DNS, and the domain name may map to different IPv6 addreses depending on the RDNSS employed for name resolution and/or the IPv6 addresses employed for the source address of the DNS queries. When "www.example.com" is resolved by means of RDNSS_A, the resulting IPv6 addresses are likely to be topologically close to ISP_A. Thus, a host that resolves "www.example.com" via RDNSS_A but then initiates communication with the resulting IPv6 addresses via ISP_B is likely to receive sub-optimal service (e.g. longer Round-Trip Times (RTTs)). The corresponding systems might as well be prepared to only service ISP_A, and enforce ACLs dropping traffic that does not originate from PREFIX_A.

A.2. Information Advertised by Multiple Routers on the Same Link

Similarly, consider this other network scenario:

* Two SLAAC routers (ROUTER_A1 and ROUTER_A2), both from ISP_A, are attached to NETWORK_C

* Router A1 advertises:

  - Prefix PREFIX_A for address configuration (by means of a Prefix Information Option (PIO) [RFC4861]).

  - One Recursive DNS server (RDNSS_A) (by means of Recursive DNS Server option [RFC8106]).

* Router A2 advertises:

  - Prefix PREFIX_A for address configuration (by means of a Prefix Information Option (PIO) [RFC4861]).

  - One Recursive DNS server (RDNSS_A) (by means of Recursive DNS Server option [RFC8106]).

Let us assume that, at some point in time, ROUTER_A2 starts invalidating the previously-advertised information. Namely,

* Router A2 starts to advertise prefix PREFIX_A for address configuration (by means of a Prefix Information Option (PIO) [RFC4861]) with a "valid lifetime" of 0.

* Router A2 starts to advertise RDNSS_A (by means of Recursive DNS Server option [RFC8106]) with a "lifetime" of 0.

A SLAAC host that receives this (updated) information should interpret it as:

* As far as ROUTER_A2 is concerned, addresses in PREFIX_A are no longer valid, and should not be used when sending IPv6 packets via ROUTER_A2.

* As far as ROUTER_A2 is concerned, RDNSS_A is no longer a valid RDNSS.

* However, this should not affect the validity of this information (ot its usage) with other SLAAC routers. Namely, in our scenario, a SLAAC host attached to NETWORK_C should still consider addresses in PREFIX_A to be valid when e.g. used in conjunction with ROUTER_A1, and should still consider RDNSS_A to be a valid RDNSS to send queries from PREFIX_A via ROUTER_A1.

* Only when a piece of SLAAC information is no longer valid for any of SLAAC router would the corresponding information be completely removed from the SLAAC host.

Author’s Address

Fernando Gont
SI6 Networks
Segurola y Habana 4310, 7mo Piso
Villa Devoto
Ciudad Autonoma de Buenos Aires
Argentina
Email: fgont@si6networks.com
URI: https://www.si6networks.com