IPv6 Maintenance
Internet-Draft
Updates: 4861, 8028 (if approved)
Intended status: Standards Track
Expires: 4 September 2025

J. Linkova
Google

3 March 2025

Using Prefix-Specific Link-Local Addresses to Improve SLAAC Robustness
draft-link-6man-gulla-01

Abstract

When an IPv6 prefix assigned to a link changes, hosts may not be explicitly notified about the change. Similarly, in some scenario a link attachement for the host may change without the host detecting it. In both cases the host does not receive any signals to trigger the network stack configuration refresh, so it may continue to use "old" addresses which are not valid for the link. This leads to packet loss and service disruption. This document proposes a mechanism to mitigate this issue. Routers are advised to send Router Advertisements containing distinct Prefix Information Options (PIOs) from different link-local addresses. This, in conjunction with RFC6724 (Default Source Address Selection) Rule 5.5 and RFC8028 (first-hop selection requirements), enables hosts to detect prefix changes more rapidly and select the correct source address, thereby improving the robustness of SLAAC.

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 2
2. Requirements Language 3
3. Terminology 4
4. Benefits of Subnet-Specific Link-Local Addresses in Renumbering Scenarios 4
4.1. Subnet Change Scenarios 4
4.2. Renumbering with Subnet-Specific Link-Local Addresses . . 6
4.2.1. RFC8028 and Default Router Selection 7
4.3. Outage Duration During Renumbering Event 8
5. Generating Subnet-Specific Link-Local Addresses for Router Interfaces 9
5.1. Subnet-Specific and Stable Link-Local Addresses 10
6. Solution Applicability 10
7. Updates to RFC4861 11
8. Security Considerations 12
9. Privacy Considerations 12
10. IANA Considerations 12
11. References 12
11.1. Normative References 12
11.2. Informative References 13
Acknowledgements 14
Author's Address 14

1. Introduction

IPv6 Stateless Address AutoConfugration (SLAAC, [RFC4862] provides IPv6 hosts with a mechanism to configure their IPv6 stack based on the information (such as an IPv6 prefix and the default router address) received from the on-link routers. If that information changes (e.g. a prefix assigned to the link is changed), the routers need to explicitly invalidate the outdated information (e.g. by sending a Router Advertisement packet which deprecates the old prefix). In the absence of an explicit signal the host would be using the outdated information until its lifetime expires. If the host selects a source IPv6 address from a prefix which is not assigned to the link anymore, packets might be dropped either due to anti-spoofing policies on the routers, or just because the return

traffic can not reach the host. This leads to degraded user experience.

Multiple documents discuss the SLAAC so-called flash renumbering problem and proposed various improvements to the host and router behaviour (see [RFC9096] and [I-D.ietf-6man-slaac-renum]).

The problem of selecting "a correct" source address is not unique for flash renumbering scenarions. In multihomed (more specifically, multi-prefix multi-router) network, where different prefixes are signalled to hosts by different routers, a host need to choose both a first-hop router and a source address for a given packet. Rule 5.5 of the default source address selection algorithm [RFC6724] instructs hosts to prefer a source address from a prefix, advertized by the chosen first-hop router. Additionally, [RFC8028] requires hosts to select default routers for each prefix it is assigned an address in.

As a result, when there are two routers on a link, and each router advertizes its own PIO, hosts supporting Rule 5.5 and [RFC8028] would be capable of selecting the correct {source address, next-hop} pair, and send packets from a source belonging to a given prefix to the router which adverized that prefix in RAs.

If, when the link is renumebered, the old and new prefixes are seen as advertized by two different routers, the renumbering scenario becomes a specific corner case of a multihoming: the host has addresses in multiple prefixes, advertized by different routers, and needs to select a correct address (one from a prefix which is currently assigned to the link). Therefore, the mechanisms (Rule 5.5 of the source address selection and ones proposed by [RFC8028]) can be used for both multihoming and flash renumering scenarios.

To ensure that during the renumbering each prefix is seen as advertized by a different first-hop router, this document suggests that routers sent Router Advertisements with different Prefix Information Options (PIOs) from different link-local addresses. That allows the hosts to select the source address from the prefix advertized by the reachable next-hop and recover from a renumbering or network segment change events much faster.

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.

3. Terminology

DHCPv6-PD: DHCPv6 Prefix Delegation [RFC8415]; a mechanism to delegate IPv6 prefixes to clients.

Flash renumbering: a network renumbering event, when an old prefix, used to address hosts, becomes invalid and is replaced by a new prefix (or just removed, without any replacement). Before the flash renumbering only the old prefix provides connectivity, and after the flash renumbering only the new one can be used. In other words, there is no period of time when addresses from both prefixes provide connectivity. Examples of flash renumbering include, but are not limited to a change of prefix delegated via DHCPv6-PD, or removal of one prefix from the router configuration and replacing it with another. See [RFC8978] for more detailed discussion of various flash-renumbering scenarios.

LLA: Link-Local Address, Section 2.5.6 of [RFC4291].

PIO: Prefix Information Option, [RFC4861].

RA: Router Advertisement, [RFC4861].

SLAAC: IPv6 Stateless Address AutoConfugration, [RFC4862].

SLAAC host: a host which uses SLAAC to configure addresses.

SLAAC Router: a router which advertizes at least one prefix in a PIO with the A flag set to 1, so that prefix can be used for SLAAC.

VRRPv3: Virtual Router Redundancy Protocol verion 3, [RFC9568].

4. Benefits of Subnet-Specific Link-Local Addresses in Renumbering Scenarios

4.1. Subnet Change Scenarios

In various scenarios, an IPv6 subnet assigned to a host’s connected link can change without explicit notification to the host. This can result in outdated IPv6 address configurations, leading to connectivity disruptions and a degraded user experience.

One common scenario is flash renumbering, where a host's connected link undergoes a change in its assigned prefix. For example, a Customer Premises Equipment (CPE) router might receive a new prefix via DHCPv6-PD without deprecating the old prefix. Consequently, hosts may use addresses from both the old and new prefixes until the old prefix's lifetime expires. Flash renumbering scenarios are discussed in detail in [RFC8978].

Another situation arises when a host changes its link attachment. Even without changes in prefixes assigned to links, a host may move from one link to another without detecting the disconnection. For instance, a host connected to a wired port may experience a VLAN (and its corresponding IPv6 subnet) change without detecting it. This often occurs when a switch port is reconfigured to modify the assigned VLAN (e.g., manually by an administrator or by an automated provisioning system), and the host does not reset its interface configuration. Similarly, if the VLAN is configured via 802.1X or MAC-based authentication (e.g., provided by RADIUS), an 802.1X reauthentication event can lead to VLAN assignment changes. Some 802.1X supplicants do not consistently reset the IPv6 stack when the wired interface's 802.1X state changes (e.g., between 'unauthenticated' and 'authenticated'), potentially causing the host to retain IPv6 configurations from the previous VLAN.

A further example involves a host roaming between wireless access points advertising the same SSID but different IPv6 subnets.

The Detecting Network Attachment (DNA) algorithm [RFC6059] allows hosts to determine the validity of their network stack configuration after a link attachment change. However, DNA relies on the assumption that the combination of the link-layer address and the link-local IPv6 address of a router is unique across links. This assumption often fails to hold. For example, network administrators may configure the same, easily remembered link-local address (e.g., 'fe80::1') on router interfaces on different links. Furthermore, some router implementations use the virtual router MAC address to generate Modified Extended Unique Identifier (EUI)-64 identifiers for VRRPv3 virtual link-local addresses, which violates Section 7.4 of [RFC9568]. As a result, all links with the same VRRP ID (and thus the same virtual router MAC address) would also share the same virtual link-local address.

In all those scenarios a host might move between IPv6 subnets without complete disconnection and without detecting the network change. As a result the following sequence of events may occur, leading to broken connectivity:

* The host is connected to a network A, receives an RA from the router with a PIO containing pref_a, forms IPv6 addresses from that prefix using SLAAC.

* The host attachment changes from network A to network B or an IPv6 prefix configured on the network changes from pref_a to pref_b. The host doesn’t detect the network change and doesn’t clear the IPv6 stack.

* The host receives an RA from the router with a new PIO for pref_b and forms new addresses from that prefix.

* Now the host has two sets of IPv6 addresses - one from pref_a and one from pref_b. Addresses from pref_a are unusable: even if the outgoing packets are not dropped by anti-spoofing filters,the return traffic wouldn’t be able to reach the host. So if the host selects an address from pref_a as a source address for outgoing communication (as per RFC6724 or by using any other custom algorithms), the traffic would be dropped, causing user-visible outages.

4.2. Renumbering with Subnet-Specific Link-Local Addresses

Rule 5.5 of the Default Source Address Selection ([RFC6724]) requires the host to prefer addresses in a prefix advertised by the next-hop. It allows the multihomed host to select the source address correctly: when two routers advertize different prefixes, the host will be sending packets with source address from a given prefix to the router the prefix was received from.

In case of renumbering if both old and new prefixes are advertized by the same router (received from a router with the same link-local address), then Rule 5.5 doesn’t help selecting the correct (working) source address. However, if the prefix change also leads to the default router address change, then a host implementing Rule 5.5 could recover from the renumbering quickly, i.e.:

* The host receives a Router Advertisement (RA, [RFC4861]) from the router (link-local address LLA_A) with a PIO containing pref_a, forms IPv6 addresses from that prefix using SLAAC.

* An IPv6 prefix configured on the link changes from pref_a to pref_b. The host does not receive any explicit signal about the prefix change and does not clear stale IPv6 configuration from its interface.

* The host receives an RA from the router (link-local address LLA_B) with a new PIO for pref_b and forms new addresses from that prefix. The host adds the LLA_B to the Default Router List.

* The host changes the network attachement or the router interface on the link doesn't have the original pref_a confgured (so LLA_A is not used by the router anymore). Neighbor Unreachability Detection ([RFC4861]) detects that the next-hop is no longer reachable. As per Section 6.3.6 of [RFC4861], the default router LLA_B is now preferred over the unreachable default router LLA_A.

* The host is using LLA_B as a next-hop for outgoing traffic, so, as per Rule 5.5 of [RFC6724] addresses from the pref_b are selected, while addresses from pref_a are not used anymore.

It should be noted that [RFC6724] does not require all implementations to support Rule 5.5, limiting the support to systems which track which router advertized which prefix. However [I-D.ietf-6man-rfc6724-update] elevates Rule 5.5 support to MUST for all systems.

The proposed solution can still benefit hosts without Rule 5.5 support, as they can use DNA to validate their IPv6 address configuration after a change in link attachment.

4.2.1. RFC8028 and Default Router Selection

[RFC8028] requires that "a host SHOULD select default routers for each prefix it is assigned an address in" and that "Routers that have advertised the prefix in their Router Advertisement message SHOULD be preferred over routers that do not advertise the prefix, regardless of Default Router Preference. ". However it should be noted that as per Section 6.3.6 of [RFC4861], the host can still select default routers even if the router is not reachable (its Neighbor Cache entry is INCOMPLETE). Selecting such router would be undersirable, as it would prevent eliminating unreachable nexthop and defeating the whole purpose of per-prefix link-local addresses. Therefore this document updates [RFC8028]

OLD TEXT:

=====

Routers that have advertised the prefix in their Router Advertisement message SHOULD be preferred over routers that do not advertise the prefix, regardless of Default Router Preference.

=====

NEW TEXT

=====

Routers that that are reachable or probably reachable (i.e., in any state other than INCOMPLETE) and have advertised the prefix in their Router Advertisement message SHOULD be preferred over routers that do not advertise the prefix, regardless of Default Router Preference.

=====

If the host complies with [RFC8028], including the proposed modifications described above, then the proposed mechanism would work even better, and would provide fast recovery from a renumbering event:

* The host selects a default router with link-local address LLA_A for pref_a.

* The prefix on the link changes from pref_a to pref_b.

* When the host receives an RA from LLA_B, containing a PIO for pref_b, the host selects another default gateway, LLA_B.

* Neighbor Unreachability Detection detects that LLA_A is not reachable, and removes it from the neighbor cache table, so the host can not use it as a default gateway anymore. The host switches to using LLA_B as a default gateway and, in accordance with Rule 5.5, starts using addresses from pref_b.

4.3. Outage Duration During Renumbering Event

When the IPv6 subnet changes (either because the given link has been renumbered, or because the client has moved to another link), there are two factors contributing to the duration of the outage:

* Time required for the host to receive new configuration information (RAs containing new PIOs).

* Time required for the host to deprecate the old configuration information.

Without changes proposed in this document, a host might be using the outdated prefix for the duration of the PIO preferred lifetime. As per [RFC4861], the default value for preferred lifetime is 604800 secs (7 days). While [I-D.ietf-6man-slaac-renum] proposes to reduce that value to 14400 seconds (4 hours), it still much longer than can be considered acceptable.

The solution proposed in this document allows hosts which implement Rule 5.5 of the source address selection ([RFC6724]) to stop using the outdated prefix much faster. The time required for the host to detect that the old prefix shouldn't be used for initiating new session is the time required for Neighbor Unreachability Detection (NUD, [RFC4861]) to remove an unreachable entry for the old link-local address of the default router. The default value would be (without taking randomisation factors into account): ReachableTime milliseconds (to move from REACHABLE to STALE) + DELAY_FIRST_PROBE_TIME + MAX_UNICAST_SOLICIT*RetransTimer = 30 seconds + 5 second + 3*1 = 38 seconds.

5. Generating Subnet-Specific Link-Local Addresses for Router Interfaces

Prefix-specific link-local addresses, as described above, allow hosts to quickly identify renumbering or changes to the prefixes advertised in PIOs, improving SLAAC robustness to renumbering. Routers supporting prefix-specific link-local addresses functionality SHOULD:

* Support multiple link-local addresses per interface.

* Generate (using [RFC7217] algorithm but with Prefix set to the prefix in question) or allowing the administrator to configure a dedicated link-local address for each prefix in AdvPrefixList ([RFC4861]);

* Send a PIO for each prefix in a separate RA, using that dedicated link-local address as a source. When populating fields in each RA as per Section 6.2.3 of [RFC4861], AdvPrefixList is treated as containing one specific prefix only. When the AdvPrefixList contains multiple prefixes, so multiple RAs need to be sent, the router SHOULD minimize the time interval between them. Doing so reduces the energy consumption of battery-powered devices that must awaken to receive those RAs. Ideally, all RAs shall be sent together, as a bundle, so MaxRtrAdvInterval and MinRtrAdvInterval are applied to the whole bundle.

* Remove the prefix-specific link-local address from the interface when the corresponding prefix is no longer advertized in a PIO sent from that interface. The router SHOULD also follow recommendations from Section 6.2.8 of [RFC4861] to inform hosts of this change.

When interface subnets are configured statically, network administrators can also configure link-local addresses statically. In some cases, it may be feasible to derive the interface ID directly from the global subnet prefix. For example, if a router has two

interfaces configured with the subnets 2001:db8:1:1::/64 and 2001:db8:2:2::/64, respectively, the link-local addresses fe80::2001:db8:1:1 and fe80::2001:db8:2:2 could be configured for those interfaces. It is important to note that this approach assumes a single router per link; otherwise, duplicate link-local addresses will result. In deployments employing first-hop redundancy with VRRPv3, static link-local interface addresses are not required. Instead, the virtual link-local address SHOULD be configured.

As discussed in Section 6.2.8 of [RFC4861], using multiple link-local address for the same router on the same link may prevent hosts from processing ICMPv6 redirects sent by the router. Therefore, if a router has prefix-specific link-local addresses enabled on its interface, the router needs to select the correct source link-local address when sending ICMPv6 redirects on that interface. In particular, if the source address of the invoking packet belongs to a prefix advertized in a PIO on that interface, the router MUST use the link-local address specific to this prefix as a source address for the ICMPv6 redirects.

5.1. Subnet-Specific and Stable Link-Local Addresses

In many cases it might be beneficial for a router to have a stable link-local address (e.g. if that address is advertized as a DNS server, or for management purposes. Router MAY generate prefix-specific link-local addresses in addition to a stable link-local address.

It should be noted that the proposed mechanism assumes that the router does not use the modified EUI-64 format for generating interface ID. As per Section 3 of [RFC8064], nodes SHOULD NOT use the modified EUI-64 format, and SHOULD use the algorithm defined in [RFC7217] instead.

6. Solution Applicability

While the proposed solution enables hosts to detect IPv6 subnet changes more rapidly, it also has some drawbacks, particularly if the router interface has multiple prefixes configured and advertised in PIOs:

* The router sends an RA for each prefix, increasing the total number of RAs sent within MaxRtrAdvInterval by a factor of the number of prefixes. In some topologies, this can significantly impact host battery life.

* The solution requires the router to support multiple link-local addresses per interface. While [RFC4861] does not explicitly prohibit this (and any router with VRRPv3 enabled needs to support multiple link-local addresses), some implementations are known to assume that only one link-local address is permitted per interface.

Some deployments (e.g. residential networks where CPEs obtain prefixes via DHCPv6-PD, or enterprise networks where hosts can move between VLANs) benefit from the proposed solution more than others. Therefore the mechanism described in this document is considered optional and is not required to be supported by all routers. If the router supports prefix-specific link-local addresses, that functionality SHOULD be configurable and MAY be enabled by default only on interfaces susceptible to flash renumbering, e.g., if AdvPrefixList contains prefixes obtained dynamically from DHCPv6-PD. In all other cases, prefix-specific link-local addresses MUST be disabled by default and MAY be enabled by the administrator.

7. Updates to RFC4861

This document also modifies Section 6.2.8 of [RFC4861]:

===

OLD TEXT:

===

Using the link-local address to uniquely identify routers on the link has the benefit that the address a router is known by should not change when a site renumbers.

===

NEW TEXT:

===

Using the link-local address to uniquely identify routers on the link has the benefit that the address a router is known by should not change when a site renumbers and the renumbering event is explicitly signalled and properly propagated to all hosts. However, in case of flash renumbering without explicit signalling the router SHOULD be able change the link-local address of an interface following renumbering events, to help hosts detect prefix changes and update their configuration accordingly.

===

8. Security Considerations

To be added.

9. Privacy Considerations

This document does not introduce any privacy considerations.

10. IANA Considerations

This memo does not introduce any requests to IANA.

11. References

11.1. 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>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[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>.

[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>.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, <https://www.rfc-editor.org/info/rfc6877>.

[RFC7050] Savolainen, T., Korhonen, J., and D. Wing, "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis", RFC 7050, DOI 10.17487/RFC7050, November 2013, <https://www.rfc-editor.org/info/rfc7050>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[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>.

[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>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC8781] Colitti, L. and J. Linkova, "Discovering PREF64 in Router Advertisements", RFC 8781, DOI 10.17487/RFC8781, April 2020, <https://www.rfc-editor.org/info/rfc8781>.

[RFC8925] Colitti, L., Linkova, J., Richardson, M., and T. Mrugalski, "IPv6-Only Preferred Option for DHCPv4", RFC 8925, DOI 10.17487/RFC8925, October 2020, <https://www.rfc-editor.org/info/rfc8925>.

[I-D.ietf-6man-slaac-renum] Gont, F., Zorz, J., Patterson, R., and J. Linkova, "Improving the Robustness of Stateless Address Autoconfiguration (SLAAC) to Flash Renumbering Events", Work in Progress, Internet-Draft, draft-ietf-6man-slaac-renum-09, 3 March 2025, <https://datatracker.ietf.org/api/v1/doc/document/draft-ietf-6man-slaac-renum/>.

[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>.

11.2. Informative References

[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>.

[RFC6059] Krishnan, S. and G. Daley, "Simple Procedures for Detecting Network Attachment in IPv6", RFC 6059, DOI 10.17487/RFC6059, November 2010, <https://www.rfc-editor.org/info/rfc6059>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <https://www.rfc-editor.org/info/rfc7084>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8978] Gont, F., or, J., and R. Patterson, "Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events", RFC 8978, DOI 10.17487/RFC8978, March 2021, <https://www.rfc-editor.org/info/rfc8978>.

[RFC9096] Gont, F., or, J., Patterson, R., and B. Volz, "Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events", BCP 234, RFC 9096, DOI 10.17487/RFC9096, August 2021, <https://www.rfc-editor.org/info/rfc9096>.

[RFC9568] Lindem, A. and A. Dogra, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 9568, DOI 10.17487/RFC9568, April 2024, <https://www.rfc-editor.org/info/rfc9568>.

Acknowledgements

Thanks to Dale W. Carder, Brian Carpenter, Lorenzo Colitti, Fernando Gont, Alexandre Petrescu, Mark Smith, Ole Troan, Eduard Vasilenko, Eric Vyncke, Tim Winters for the discussions, the input and all contribution.

Author’s Address

Jen Linkova
Google
1 Darling Island Rd
Pyrmont NSW 2009
Australia
Email: furry13@gmail.com, furry@google.com