Internet Engineering Task Force (IETF)
Request for Comments: 8273
Category: Informational
ISSN: 2070-1721
J. Brzozowski
Comcast Cable
G. Van de Velde
Nokia
December 2017

Unique IPv6 Prefix per Host

Abstract

This document outlines an approach utilizing existing IPv6 protocols to allow hosts to be assigned a unique IPv6 prefix (instead of a unique IPv6 address from a shared IPv6 prefix). Benefits of using a unique IPv6 prefix over a unique service-provider IPv6 address include improved host isolation and enhanced subscriber management on shared network segments.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see 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 https://www.rfc-editor.org/info/rfc8273.

Copyright Notice

Table of Contents

1. Introduction

The concepts in this document were originally developed as part of a large-scale production deployment of IPv6 support for a provider-managed shared-access network service.

A shared-access network service is a service offering in which a particular Layer 2 (L2) access network (e.g., Wi-Fi) is shared and used by multiple visiting devices (i.e., subscribers). Many service providers offering shared-access network services have legal requirements, or find it good practice, to provide isolation between the connected visitor devices to control potential abuse of the shared-access network.

A network implementing a unique IPv6 prefix per host can simply ensure that devices cannot send packets to each other except through the first-hop router. This will automatically provide robust protection against attacks between devices that rely on link-local ICMPv6 packets, such as Duplicate Address Detection (DAD) reply spoofing, Neighbor Discovery (ND) cache exhaustion, malicious redirects, and rogue Router Advertisements (RAs). This form of protection is much more scalable and robust than alternative mechanisms such as DAD proxying, forced forwarding, or ND snooping.

In this document IPv6 support does not preclude support for IPv4; however, the primary objective for this work was to make it so that user equipment (UE) were capable of an IPv6-only experience from a network operator's perspective. In the context of this document, UE can be 'regular' end-user equipment as well as a server in a data center, assuming a shared network (wired or wireless) exists.

Details of IPv4 support are out of scope for this document. This document will also, in general, outline the requirements that must be satisfied by UE to allow for an IPv6-only experience.

In most current deployments, assignment of UE IPv6 addresses is commonly done using IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862] and/or DHCP IA_NA (Identity Association - Non-temporary Address) [RFC3315]. During the time when this approach was developed and subsequently deployed, it was observed that some operating systems did not support the use of DHCPv6 for the acquisition of IA_NA per [RFC7934]. To not exclude any known IPv6 implementations, IPv6-SLAAC-based subscriber and address management is the recommended technology to reach the highest percentage of connected IPv6 devices on a provider-managed shared-access network service. In addition, an IA_NA-only network is not recommended per Section 8 of [RFC7934]. This document will detail the mechanics involved for IPv6-SLAAC-based address and subscriber management coupled with stateless DHCPv6, where beneficial.

This document focuses upon the process for UE to obtain a unique IPv6 prefix.

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. Motivation and Scope of Applicability

The motivation for this work falls into the following categories:

- Give deployment advice for IPv6 that will allow a stable and secure IPv6-only experience, even if IPv4 support is present

- Ensure support for IPv6 is efficient and does not impact the performance of the underlying network and, in turn, the customer experience

- Allow for the greatest flexibility across host implementations to allow for the widest range of addressing and configuration mechanisms to be employed. Ensure that the widest population of UE implementations can leverage the availability of IPv6

- Lay the technological foundation for future work related to the use of IPv6 over shared media, requiring optimized subscriber management

- Ensure that two devices (subscriber/hosts), both attached to the same provider-managed shared-access network, should only be able to communicate through the provider-managed first-hop router. Often, service providers have legal requirements, or find it good practice, to provide isolation between the connected visitor devices in order to control potential abuse of the shared-access network.

- Provide guidelines regarding best common practices around IPv6 ND [RFC4861] and IPv6-address-management settings between the first-hop router and directly connected hosts/subscribers.

3. Design Principles

The first-hop router discussed in this document is the L3 Edge router responsible for the communication with the devices (hosts and subscribers) directly connected to a provider-managed shared-access network; it is also responsible for transporting traffic between the directly connected devices and between directly connected devices and remote devices.

The work detailed in this document is focused on providing details regarding best common practices of the IPv6 ND and related IPv6-address-management settings between the first-hop router and directly connected hosts/subscribers. The documented best current practice helps a service provider to better manage the provider-managed shared-access network on behalf of the connected devices.

This document recommends providing a unique IPv6 prefix to devices connected to the provider-managed shared-access network. Each unique IPv6 prefix can function as a control-plane anchor point to make sure that each device receives expected subscriber policy and service levels (throughput, QoS, security, parental control, subscriber-mobility management, etc.).

4. Assignment of IPv6 Unique Prefixes

When a UE connects to the provider-managed shared-access network, it will initiate the IP configuration phase. During this phase, the UE will, from an IPv6 perspective, attempt to learn the default IPv6 gateway, the IPv6 prefix information, the DNS information [RFC8106], and the remaining information required to establish globally routable IPv6 connectivity. For that purpose, the subscriber sends an RS (Router Solicitation) message.

The first-hop router receives this subscriber RS message and starts the process of composing the response to the subscriber-originated RS message. The first-hop router will answer using a solicited RA to the subscriber.

When the first-hop router sends a solicited RA response, or periodically sends unsolicited RAs, the RA MUST be sent only to the subscriber that has been assigned the unique IPv6 prefix contained in the RA. This is achieved by sending a solicited RA response or unsolicited RAs to the all-nodes group, as detailed in Sections 6.2.4 and 6.2.6 of [RFC4861]; but, instead of using the link-layer multicast address associated with the all-nodes group, the link-layer unicast address of the subscriber that has been assigned the unique IPv6 prefix contained in the RA MUST be used as the link-layer destination [RFC6085]. Or, optionally in some cases, a solicited RA response could be sent (unicast) to the link-local address of the subscriber as detailed in Section 6.2.6 of [RFC4861]; nevertheless, unsolicited RAs are always sent to the all-nodes group.

This solicited RA contains two important parameters for the subscriber to consume: a unique IPv6 prefix (currently a /64 prefix) and some flags. The unique IPv6 prefix can be derived from a locally managed pool or aggregate IPv6 block assigned to the first-hop router or from a centrally allocated pool. The flags indicate that the subscriber should use SLAAC and/or DHCPv6 for address assignment; it may indicate whether the autoconfigured address is on/off-link and if 'Other' information (e.g., DNS server address) needs to be requested.

The IPv6 RA flags used for best common practice in IPv6-SLAAC-based provider-managed shared-access networks are:

- o M-flag = 0 (The subscriber address is not managed through DHCPv6); this flag may be set to 1 in the future if/when DHCPv6-prefix-delegation support is desired.)

- o O-flag = 1 (DHCPv6 is used to request configuration information, i.e., DNS, NTP information, not for IPv6 addressing.)

- o A-flag = 1 (The subscriber can configure itself using SLAAC.)

- o L-flag = 0 (The prefix is not an on-link prefix, which means that the subscriber will never assume destination addresses that match the prefix are on-link and will always send packets to those addresses to the appropriate gateway according to route selection rules.)

The use of a unique IPv6 prefix per subscriber adds an additional level of protection and efficiency. The protection exists because all external communication of a connected device is directed to the first-hop router as required by [RFC4861]. Best efficiency is achieved because the recommended RA flags allow the broadest support on connected devices to receive a valid IPv6 address (i.e., privacy addresses [RFC4941] or SLAAC [RFC4862]).

The architected result of designing the RA as documented above is that each subscriber gets its own unique IPv6 prefix. Each host can consequently use SLAAC or any other method of choice to select its /128 unique address. Either stateless DHCPv6 [RFC3736] or IPv6 Router Advertisement Options for DNS Configuration [RFC8106] can be used to get the IPv6 address of the DNS server. If the subscriber desires to send anything external, including towards other subscriber devices (assuming device-to-device communications is enabled and supported), then, due to the L-bit being unset, [RFC4861] requires that this traffic be sent to the first-hop router.

After the subscriber received the RA and the associated flags, it will assign itself a 128-bit IPv6 address using SLAAC. Since the address is composed by the subscriber device itself, it will need to verify that the address is unique on the shared network. The subscriber will, for that purpose, perform the DAD algorithm. This will occur for each address the UE attempts to utilize on the provider-managed shared-access network.

5. Best Practices for IPv6 Neighbor Discovery

An operational consideration when using IPv6-address assignment with IPv6 SLAAC is that after the onboarding procedure, the subscriber will have a prefix with certain preferred and valid lifetimes. The first-hop router extends these lifetimes by sending an unsolicited RA, the applicable MaxRtrAdvInterval on the first-hop router MUST, therefore, be lower than the preferred lifetime. One consequence of this process is that the first-hop router never knows when a subscriber stops using addresses from a prefix, and additional procedures are required to help the first-hop router to gain this information. When using stateful DHCPv6 IA_NA for IPv6-subscriber-address assignment, this uncertainty on the first-hop router does not have an impact due to the stateful nature of the assignment of DHCPv6 IA_NA addresses.

The following is a reference table of the key IPv6 router and neighbor discovery timers for provider-managed shared-access networks:

- Maximum IPv6 Router Advertisement Interval (MaxRtrAdvInterval) = 300 s (or when battery consumption is a concern 686 s, see note below)
- IPv6 Router Lifetime = 3600 s (see note below)
- Reachable time = 30 s
- IPv6 Valid Lifetime = 3600 s
- IPv6 Preferred Lifetime = 1800 s
- Retransmit timer = 0 s

Note: When servicing large numbers of battery powered devices, [RFC7772] suggests a maximum of seven RAs per hour and a 45-90 minute IPv6 Router Lifetime. To achieve a maximum of seven RAs per hour, the Minimum IPv6 Router Advertisement Interval (MinRtrAdvInterval) is the important parameter, and it MUST be greater than or equal to 514 seconds (1/7 of an hour). Further, as discussed in Section 6.2.1. of [RFC4861], MinRtrAdvInterval <=0.75 * MaxRtrAdvInterval; therefore, MaxRtrAdvInterval MUST additionally be greater than or equal to 686 seconds. As for the recommended IPv6 Router Lifetime, since this technique requires that RAs be sent using the link-layer unicast address of the subscriber, the concerns over multicast delivery discussed in [RFC7772] are already mitigated; therefore, the above suggestion of 3600 seconds (an hour) seems sufficient for this use case.

IPv6 SLAAC requires the router to maintain neighbor state, which implies costs in terms of memory, power, message exchanges, and message processing. Stale entries can prove an unnecessary burden, especially on Wi-Fi interfaces. It is RECOMMENDED that stale neighbor state be removed quickly.

When employing stateless IPv6 address assignment, a number of widely deployed operating systems will attempt to utilize [RFC4941] temporary 'private' addresses.

Similarly, when using this technology in a data center, the UE server may need to use several addresses from the same unique IPv6 prefix, for example, because is using multiple virtual hosts, containers, etc., in the bridged-virtual switch. This can lead to the consequence that a UE has multiple /128 addresses from the same IPv6 prefix. The first-hop router MUST be able to handle the presence and use of multiple globally routable IPv6 addresses.

6. IANA Considerations

This document does not require any IANA actions.

7. Security Considerations

The mechanics of IPv6 privacy extensions [RFC4941] are compatible with assignment of a unique IPv6 prefix per host. However, when combining both IPv6 privacy extensions and a unique IPv6 prefix per host, a reduced privacy experience for the subscriber is introduced. This is because a prefix may be associated with a subscriber, even when the subscriber has implemented IPv6 privacy extensions [RFC4941]. If the operator assigns the same unique prefix to the same link-layer address every time a host connects, any remote party who is aware of this fact can easily track a host simply by tracking its assigned prefix. This nullifies the benefit provided by privacy addresses [RFC4941]. If a host wishes to maintain privacy on such networks, it SHOULD ensure that its link-layer address is periodically changed or randomized.

No other additional security considerations are made in this document.

8. 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>.

[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, <https://www.rfc-editor.org/info/rfc3315>.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, DOI 10.17487/RFC3736, April 2004, <https://www.rfc-editor.org/info/rfc3736>.

[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>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <https://www.rfc-editor.org/info/rfc4941>.

[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, <https://www.rfc-editor.org/info/rfc6085>.

[RFC7772] Yourtchenko, A. and L. Colitti, "Reducing Energy Consumption of Router Advertisements", BCP 202, RFC 7772, DOI 10.17487/RFC7772, February 2016, <https://www.rfc-editor.org/info/rfc7772>.

[RFC7934] Colitti, L., Cerf, V., Cheshire, S., and D. Schinazi, "Host Address Availability Recommendations", BCP 204, RFC 7934, DOI 10.17487/RFC7934, July 2016, <https://www.rfc-editor.org/info/rfc7934>.

[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>.

Acknowledgements

The authors would like to explicitly thank David Farmer and Lorenzo Colitti for their extended contributions and suggested text.

In addition, the authors would like to thank the following, in alphabetical order, for their contributions:

Fred Baker, Ben Campbell, Brian Carpenter, Tim Chown, Killian Desmedt, Wim Henderickx, Brad Hilgenfeld, Erik Kline, Suresh Krishnan, Warren Kumari, Thomas Lynn, Jordi Palet, Phil Sanderson, Colleen Szymanik, Jinmei Tatuya, Eric Vyncke, and Sanjay Wadhwa

Authors' Addresses

John Jason Brzozowski
Comcast Cable
1701 John F. Kennedy Blvd.
Philadelphia, PA
United States of America

Email: john_brzozowski@cable.comcast.com

Gunter Van de Velde
Nokia
Antwerp
Belgium

Email: gunter.van_de_velde@nokia.com