IPv6 Operations Working Group (v6ops)
Internet-Draft
Intended status: Best Current Practice
Expires: August 31, 2017

F. Gont
SI6 Networks / UTN-FRH
G. Doering
SpaceNet AG
M. Garcia Corbo
SITRANS
G. Gont
SI6 Networks

February 27, 2017

On the Dynamic/Automatic Configuration of IPv6 Hosts
draft-gont-v6ops-host-configuration-00

Abstract

IPv6 has two different mechanisms for dynamic/automatic host configuration: SLAAC and DHCPv6. These two mechanisms allow for the configuration of IPv6 addresses and a number of network parameters. While there is overlap in the parameters that can be configured via these two protocols, different implementations support only subsets of such parameters with either mechanism, or have no support for DHCPv6 at all. This document analyzes a problem that arises from this situation, and mandates that all host implementations support RFC 6105 (DNS options for SLAAC) and the stateless DHCPv6 functionality in RFC 3315.

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 http://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 August 31, 2017.

Table of Contents

1. Introduction

IPv6 has two different mechanisms for dynamic/automatic host configuration: Stateless Address Autoconfiguration (SLAAC) [RFC4862] and Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315]. SLAAC allows for distributed address assignment (where each host automatically configures its own IPv6 addresses) and basic network configuration (such as recursive DNS servers and DNS search lists). On the other hand, DHCPv6 provides for centralized address assignment (the DHCPv6 server leases IPv6 addresses to hosts) and richer network configuration (NTP servers, web proxys, etc.).

Traditionally, SLAAC has been seen as a more lightweight mechanism, suitable for resource-constrained devices, while DHCPv6 has been seen more as heavy-weight and full-fledged mechanism. We note that this

distinction is rather questionable, and is essentially meaningless for typical mobile devices or home appliances.

Among the possible configuration information that can be conveyed with both SLAAC and DHCPv6 is DNS related configuration: recursive DNS servers and DNS search lists. Configuring this information is probably as vital in practice as configuring IPv6 addresses, since for obvious reasons both humans and popular applications operate on names (rather than on IPv6 addresses). The ability to convey this information has always been part of DHCPv6, while for the SLAAC case, support was added in a separate document that standardizes "IPv6 Router Advertisement Options for DNS Configuration" [RFC6106].

Unfortunately, different host and router implementations provide support for only a subset of these options. For example, some host implementations (e.g., Android) support SLAAC DNS options [RFC6106], but do not support stateless DHCPv6. On the other hand, other host implementations (e.g., Microsoft Windows) support stateless DHCPv6, but do not support [RFC6106]. Similarly, some router implementations support [RFC6106], while others do not.

This represents a problem for IPv6 deployment, since:

1. in order to support most popular IPv6 host implementations, IPv6 networks are required to support *both* SLAAC and DHCPv6.

2. some router implementations do not support [RFC6106] and hence support for the SLAAC DNS options may be impossible or require yet an additional network element or network service to support [RFC6106]

We note that, in most cases, this problem is currently masked by the fact that most IPv6 deployments are actually dual-stack, and hence hosts can currently rely DNS-related information being obtained via IPv4-based DHCP. However, at the point such deployments disable IPv4 to become IPv6-only, the aforementioned problems will become evident,

possibly as a surprise to network operators.

2. Terminology

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. Requirements for IPv6 Hosts

IPv6 hosts MUST support the SLAAC DNS options specified in [RFC6106], and the stateless DHCPv6 mechanism specified in [RFC3315].

4. Requirements for IPv6 Routers

IPv6 routers MUST support the SLAAC DNS options specified in [RFC6106].

5. IANA Considerations

This document has no actions for IANA. The RFC-Editor should remove this section prior to publication of this document as an RFC.

6. Security Considerations

Host implementations supporting SLAAC are subject to a number of attacks based on forged ICMPv6 Router Advertisement [RFC4861] messages. Such attacks can be mitigated by means of RA-Guard [RFC6105] [RFC7113]. Hosts supporting DHCPv6 are subject to a number of attacks based on forged DHCPv6-server messages. Such attacks can be mitigated by means of DHCPv6-Shield [RFC7610].

7. Acknowledgements

The authors would like to thank Brian Carpenter for providing valuable comments on earlier versions of this document.

Fernando Gont would like to thank Nelida Garcia and Jorge Oscar Gont for their love and support, and Ivan Arce and Diego Armando Maradona for their inspiration.

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

[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>.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, DOI 10.17487/RFC6106, November 2010, <http://www.rfc-editor.org/info/rfc6106>.

8.2. Informative References

[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, <http://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, <http://www.rfc-editor.org/info/rfc7113>.

[RFC7610] Gont, F., Liu, W., and G. Van de Velde, "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers", BCP 199, RFC 7610, DOI 10.17487/RFC7610, August 2015, <http://www.rfc-editor.org/info/rfc7610>.

Authors' Addresses

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: http://www.si6networks.com

Gert Doering
SpaceNet AG
Joseph-Dollinger-Bogen 14
Muenchen D-80807
Germany

Email: gert@space.net

Madelen Garcia Corbo
Servicios de Informacion del Transporte
Neptuno 358
Havana City 10400
Cuba

Email: madelen.garcia16@gmail.com

Guillermo Gont
SI6 Networks
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: ggont@si6networks.com
URI: https://www.si6networks.com