IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 6106 (if approved)
Intended status: Standards Track
Expires: August 30, 2015

F. Gont
SI6 Networks / UTN-FRH
P. Simerda

W. Liu
Huawei Technologies

February 26, 2015

Current issues with DNS Configuration Options for SLAAC
draft-gont-6man-slaac-dns-config-issues-01

Abstract

RFC 6106 specifies two Neighbor Discovery options that can be included in Router Advertisement messages to convey information about DNS recursive servers and DNS Search Lists. Small lifetime values for the aforementioned options have been found to cause interoperability problems in those network scenarios in which these options are used to convey DNS-related information. This document analyzes the aforementioned problem, and formally updates RFC 6106 such that these issues are mitigated.

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 30, 2015.

Table of Contents

1. Introduction

RFC 6106 [RFC6106] specifies two Neighbor Discovery (ND) [RFC4861] options that can be included in Router Advertisement messages to convey information about DNS recursive servers and DNS Search Lists. Namely, the Recursive DNS Server (RDNSS) Option specifies the IPv6 addresses of recursive DNS servers, while the DNS Search List (DNSSL) Option specifies a "search list" to be used when trying to resolve a name by means of the DNS.

Each of this options include a "Lifetime" field which specifies the maximum time, in seconds, during which the information included in the option can be used by the receiving system. The aforementioned "Lifetime" value is set as a function of the Neighbor Discovery parameter 'MaxRtrAdvInterval', which specifies the maximum time allowed between sending unsolicited multicast Router Advertisements from an interface. The recommended bounds (MaxRtrAdvInterval <= Lifetime <= 2*MaxRtrAdvInterval) have been found to be too short for scenarios in which some Router Advertisement messages may be lost. In such scenarios, hosts may fail to receive unsolicited Router Advertisements and therefore fail to refresh the expiration time of the DNS-related information previously learned through the RDNSS and DNSSL options), thus eventually discarding the aforementioned DNS-related information prematurely.

Some implementations consider the lack of DNS-related information as a hard failure, thus causing configuration restart. This situation

is exacerbated in those implementations in which IPv6 connectivity and IPv4 connectivity are bound together, and hence failure in the configuration of one of them causes the whole link to be restarted.

This document formally updates RFC 6106 such that this issue is mitigated.

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].

2. Changing the Semantics of the 'Lifetime' field of RDNSS and DNSSL options

The semantics of the 'Lifetime' field of the RDNSS and DNSSL options is updated as follows:

- The 'Lifetime' field indicates the amount of time during which the aforementioned DNS-related information is expected to be stable. A node is NOT required to discard the DNS-related information once the Lifetime expires.

- If the information received in a RDNSS or DNSSL option is already present in the corresponding local data structures, the corresponding 'Expiration' time should be updated according to the value in the 'Lifetime' field of the received option. A 'Lifetime' of '0' causes the corresponding information to be discarded, as already specified in [RFC6106].

- If a host has already gathered a sufficient number of RDNSS addresses (or DNS search domain names), and additional data is received while the existing entries have not yet expired, the received RDNSS addresses (or DNS search domain names) SHOULD be ignored.

- If a host receives new RDNSS addresses (or DNS search domain names), and some of the existing entries have expired, the newly-learned information SHOULD be used to replace the expired entries.

- A host SHOULD flush configured DNS-related information when it has any reason to believe that its network connectivity has changed in some relevant way (e.g., there has been a "link change event"). When that happens, the host MAY send a Router Solicitation message to re-learn the corresponding DNS-related information.

- The most-recently-updated information SHOULD have higher priority over the other DNS-related information already present on the local host.

We note that the original motivation for enforcing a short expiration timeout value was to allow mobile nodes to prefer local RDNSSes to remote RDNSSes. However, the above rules already allow for a timely update of the corresponding DNS-related information.

3. Changing the Default Values of the 'Lifetime' field of RDNSS and DNSSL options

The default RDNSS/DNSSL "Lifetime" value in current the current router solutions vary between MaxRtrAdvInterval and 2*MaxRtrAdvInterval. This means that common packet loss rates can lead to the problem described in this document.

One possible approach to mitigate this issue would be to avoid 'Lifetime' values that are on the same order as MaxRtrAdvInterval. This solution would require, of course, changes in router software.

When specifying a better default value, the following aspects should be considered:

- IPv6 will be used on many links (including IEEE 802.11) that experience packet loss. Therefore losing a few packets in a short period of time should not invalidate DNS configuration information.

- Unsolicited Router Advertisements sent on Ethernet networks result in packets that employ multicast Ethernet Destination Addresses. A number of network elements (including those that perform bridging between wireless networks and wired networks) have problems with multicasted Ethernet frames, thus typically leading to packet loss of some of those frames. Therefore, SLAAC implementations should be able to cope with devices that can lose several multicast packets in a row.

[RFC6106] is hereby updated as follows:

> The default value of AdvRDNSSLifetime and AdvDNSSLLifetime MUST be at least 10*MaxRtrAdvInterval so that the probability of hosts receiving unsolicited Router Advertisements is increased.

4. Use of Router Solicitations for active Probing

According to RFC 6106, hosts MAY send Router Solicitations to avoid expiry of RDNSS and DNSSL lifetimes. This technique could be employed as a "last resort" when expiration of the RDNSS and DNSSL information is imminent.

5. Sanitize the received RDNSS/DNSSL 'Lifetime' Values

A host that receives a RDNSS or DNSSL option that has a non-zero Lifetime smaller than 10*MaxRtrAdvInterval should employ 10*MaxRtrAdvInterval as the Lifetime value of the corresponding RDNSS or DNSSL option.

6. Security Considerations

This document does not introduce any additional security considerations to those documented in the "Security Considerations" section of [RFC6106].

7. Acknowledgements

The authors would like to thank Erik Nordmark and Mark Smith for their valuable input on the topic covered by this document.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.

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

Pavel Simerda

Phone: +420 775 996 256
Email: pavlix@pavlix.net

Will Liu
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com