IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 6106 (if approved)
Intended status: Standards Track
Expires: December 17, 2012

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

June 15, 2012

Current issues with DNS Configuration Options for SLAAC
draft-gont-6man-slaac-dns-config-issues-00

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. This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

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 December 17, 2012.

Copyright Notice

Table of Contents

1. Introduction

RFC 6106 [RFC6106] specifies to 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, host 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.

Section 2 proposes a number of ALTERNATIVE solutions to the problem, such that the 6man wg can discuss both of them. It is expected that once the 6man wg converges on a preferred solution, the other ones will be removed from the document.

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. Possible Solutions

This section describes a number of possible ALTERNATIVE solutions to the problem, such that the 6man wg can discuss both of them. It is expected that once the 6man wg converges on a preferred solution, the other one will be removed from the document.

2.1. Summary of possible solutions

Section 2.2 proposes to change the semantics of the RDNSS/DNSSL 'Lifetime', thus fixing the 'expiration' problem outlined in Section 1 and the potential of 'network configuration oscillation'. Section 2.3 proposes to increase the 'Lifetime' value at the sending routers, fixing the "expiration" problem outlined in Section 1, but without addressing the potential of 'network configuration oscillation'. Section 2.4 proposes to send Router Solicitations when expiration of RDNSS/DNSSL information is imminent, to elicit Router Advertisement messages. Section 2.5 proposes to enforce a lower limit on the received RDNSS/DNSSL 'Lifetime' values at the client side.

2.2. 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.

- If the information received in a RDNSS or DNSSL option is already present in the corresponding 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.

The rationale for the suggested change is as follows:

- It is a backwards-compatible local-policy change that solves the problem described in Section 1 without requiring changes to router software or router configuration in existing deployments (over which the user is likely to have no control at all).

- Since different RDNSS and DNSSL information could be sent by the same router in different Router Advertisement messages, the updated semantics of the 'Lifetime' parameter prevents oscillations in network configuration.

This situation could arise for a number of reasons. For example, if the desire for different 'Lifetime' values warrants the use of different RDNSS or DNSSL options, and because of packet size issues each option must be included in a separate Router Advertisement message, each burst of RAs could cause DNS-related information to be reconfigured.

Another possible scenario that could lead to the same situation is that in which there is more than one local router, and each of the local routers announces different RDNSS (or DNSSL) information. If the number of RDNSS addresses (or DNS search domain names) that the local host considers "sufficient" prevents the aggregate set of RDNSS (or DNSSL) information, the local RDNSS (or DNSSL) information would oscillate between that advertised by each of the local routers.

- The original motivation for enforcing a short expiration timeout value was to allow mobile nodes to prefer local RDNSSes to remote RDNSSes. However, the recommendation in the last bullet above already allows for a timely update of the corresponding DNS-related information. Additionally, since it is already recommended by [RFC6106] to maintain some RDNSS addresses (or DNS search domain names) per source, in the typical scenarios in which a single router (per subnet) advertises configuration information, one of this 'slots' will be free (or have expired information) and readily available to be populated with information learned from

the new subnet to which the host has moved.

2.3. 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.

The default value of AdvRDNSSLifetime and AdvDNSSLLifetime MUST be at least 5*MaxRtrAdvInterval so that the probability of hosts receiving unsolicited Router Advertisements is increased.

This solution leaves out the following situations:

- In those scenarios in which the involved routers cannot be updated this solution will not be applicable. This also limitation also applies to nomadic hosts that can connect to many different networks. This case will be discussed later in this document.

- The affected network has a huge multicast packet loss. This unfortunately happens in some real networks.

- This solution does not address the potential 'network configuration oscillation' issue described in Section 2.2.

2.4. Use 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.

Hosts SHOULD start sending multicast Router Solicitation when most of

the Lifetime of the last RDNSS server is consumed. The precise time should be a randomized value chosen from 70% to 90% of the original Lifetime to avoid bursts of packets from other hosts on the network. Hosts MAY send up to MAX_RTR_SOLICITATIONS Router Solicitation messages, each separated by at least RTR_SOLICITATION_INTERVAL seconds (please see Section 6.3.7 of [RFC4861].

Problems of this approach:

- If no IPv6 router responds, all previously connected hosts will repeatedly send Router Solicitations and only stop doing so when their RDNSS and DNSSL information finally expires. This could disrupt IPv4 networking in larger networks and that must be avoided.

- If IPv6 router responds with unicast Router Advertisement, it may need to respond to many clients.

- There is no other SLAAC information that requires or would benefit from this kind of "active probing".

- This approach does not mitigate the potential 'network configuration oscillation' problem described in Section 2.2.

NOTE: We should either state a very good reason to specialcase DNS timeouts or deprecate Router Solicitations in RFC 6106 entirely. Deprecation is the more favorable option in our opinion.

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

Another possible approach would be to enforce a lower limit on the received RDNSS/DNSSL 'Lifetime' values on the client side. The challenge this technique is the selection of a reasonable value. On the router side, it can be derived from MaxRtrAdvInterval but this value is not known to the client side.

Therefore we would have to assume some maximum value of MaxRtrAdvInterval and use it to derive minimum value of lifetimes instead of the actual MaxRtrAdvInterval.

It should be noted that this approach would not address the potential

'network configuration oscillation' issue described in Section 2.2.

3. Security Considerations

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

4. Acknowledgements

5. References

5.1. 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.

5.2. Informative References

Appendix A. Additional notes regarding RFC 6106

Section 5.2 of [RFC6106] states:

> An RDNSS address or a DNSSL domain name MUST be used only as long as both the RA router Lifetime (advertised by a Router Advertisement message [RFC4861]) and the corresponding option Lifetime have not expired.

This requirement could introduce problems in scenarios in which the router advertising the RDNSS or DNSSL options is not expected to be employed as a "default router", and hence the 'Router Lifetime' value of its Router Advertisement messages is set to 0.

> As noted in Section 4.2 of [RFC4861], the Router Lifetime applies only to the router's usefulness as a default router, and it does not apply to information contained in other message fields or options.

Therefore, it would be sensible to exclude the 'Router Lifetime information when deciding about the validity or "freshness" of the DNS-related configuration information.

Section 5.3.1 of [RFC6106] states:

> When the IPv6 host has gathered a sufficient number (e.g., three) of RDNSS addresses (or DNS search domain names), it SHOULD maintain RDNSS addresses (or DNS search domain names) by the sufficient number such that the latest received RDNSS or DNSSL is more preferred to the old ones; that is, when the number of RDNSS addresses (or DNS search domain names) is already the sufficient number, the new one replaces the old one that will expire first in terms of Lifetime.

As noted earlier in this document, this policy could lead (in some scenarios) to network configuration oscillations. Therefore, it would be sensible to enforce some minimum stability of the configured information, such as that resulting from the update in Section 2.2.

Section 6.3 of [RFC6106] states:

> Step (d): For each DNSSL domain name, if it does not exist in the DNS Search List, register the DNSSL domain name and Lifetime with the DNS Search List and then insert the DNSSL domain name in front of the Resolver Repository. In the case where the data structure for the DNS Search List is full of DNSSL domain name entries (that is, has more DNSSL domain names than the sufficient number discussed in Section 5.3.1), delete from the DNS Server List the

> entry with the shortest Expiration-time (i.e., the entry that will expire first).

This policy could lead to the same network configuration oscillation problems as described above for the RDNSS addresses. Therefore, it would be sensible to enforce some minimum stability of the configured information, such as that resulting from the update in Section 2.2.

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