V6OPS
Internet-Draft
Intended status: Informational
Expires: April 30, 2015

B. Liu
Huawei Technologies
R. Bonica
Juniper Networks
T. Yang
China Mobile

October 27, 2014

DHCPv6/SLAAC Interaction Operational Guidance
draft-liu-v6ops-dhcpv6-slaac-guidance-03

Abstract

The IPv6 Neighbor Discovery (ND) Protocol [RFC4861] specifies an ICMPv6 Router Advertisement (RA) message. The RA message contains three flags that indicate which address autoconfiguration mechanisms are available to on-link hosts. These are the M, O and A flags. The M, O and A flags are all advisory, not prescriptive.

In [I-D.ietf-v6ops-dhcpv6-slaac-problem], test results show that in several cases the M, O and A flags elicit divergent host behaviors, which might cause some operational problems. This document aims to provide some operational guidance to eliminate the impact caused by divergent host behaviors as much as possible.

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 April 30, 2015.

Table of Contents

1. Introduction

The IPv6 Neighbor Discovery (ND) Protocol [RFC4861] specifies an ICMPv6 Router Advertisement (RA) message. The RA message contains three flags that indicate which address autoconfiguration mechanisms are available to on-link hosts. These are the M, O and A flags. The M, O and A flags are all advisory, not prescriptive.

In [I-D.ietf-v6ops-dhcpv6-slaac-problem], test results show that in several cases the M, O and A flags elicit divergent host behaviors, which might cause some operational problems. This document aims to provide some operational guidance to eliminate the impact caused by divergent host behaviors as much as possible.

This document does not intent to cover the topic of selection between RA and DHCPv6 [RFC3315] for the overlapped functions. There always

are arguments about what should be done through RA options or through DHCPv6 options. For this general issue, draft [I-D.yourtchenko-ra-dhcpv6-comparison] could be referred.

2. Operational Guidance

2.1. Always Turn RAs On

Currently, turning RAs on is actually a basic requirement for running IPv6 networks since only RAs could advertise default route(s) for the end nodes. And if the nodes want to communicate with each other on the same link via DHCPv6-configured addresses, they also need to be advertised with L flag set in RAs. So for current networks, an IPv6 network could NOT run without RAs, unless the network only demands a communication via link-local addresses.

2.2. Guidance for DHCPv6/SLAAC Provisioning Scenarios

2.2.1. DHCPv6-only

In IPv4, there is only one method (DHCPv4) for automatically configuring the hosts. Many network operations/mechanisms, especially in enterprise networks, are built around this central-managed model. So it is reasonable for people who are accustomed to DHCPv4-only deployment still prefer DHCPv6-only in IPv6 networks. Besides, some networks just prefer central management of all IP addressing. These networks may want to assign addresses only via DHCPv6.

This can be accomplished by sending RAs that indicate DHCPv6 is available (M=1), installing DHCPv6 servers or DHCPv6 relays on all links, and setting A=0 in the Prefix Information Options of all prefixes in the RAs. (Instead of forcing the A flag off, simply not including any PIO in RAs could also make the same effect). But before doing this, the administrators need to be sure that every node in their intended management scope supports DHCPv6.

Note that RAs are still necessary in order for hosts to be able to use these addresses. This is for two reasons:

- If there is no RA, some hosts will not attempt to obtain address configuration via DHCPv6 at all.

- DHCPv6 can assign addresses but not routing. Routing can be implemented on hosts by means of accepting and implementing information from RA messages containing default-route, Prefix Information Option with O=1, or Route Information Option, or by configuring manual routing. Without routing, IPv6 addresses won’t

be used for communication outside the host. Thus, for example, if there is no RA and no static routing, then addresses assigned by DHCPv6 cannot be used even for communication between hosts on the same link.

Also note that unlike SLAAC [RFC4862], DHCPv6 is not a strict requirement for IPv6 hosts [RFC6434], and some nodes do not support DHCPv6. Thus, this model can only be used if all the hosts that need IPv6 connectivity support DHCPv6.

2.2.2. SLAAC-only

In contrast with DHCPv6-only, some scenarios might be suitable for SLAAC-only which allows minimal administration burden and node capability requirement.

The administrators MUST turn the A flag on, and MUST turn M flag off. Note that some platforms (e.g. Windows 8) might still initiate DHCPv6 session regardless of M flag off. But since there is no DHCPv6 service available, the only problem is that there would be some unnecessary traffic.

2.2.3. DHCPv6/SLAAC Co-existence

- Scenarios of DHCPv6/SLAAC Co-existence

  * For provisioning redundancy: If the administrators want all nodes at least could configure a global scope address, then they could turn A flag and M flag both on in case some nodes only support one of the mechanisms. For example, some hosts might only support SLAAC; while some hosts might only support DHCPv6 due to manual/mistaken configurations.

  * For different provisioning: the two address configuration mechanisms might provide two addresses for the nodes respectively. For example, SLAAC-configured address is for basic connectivity and another address configured by DHCPv6 is for a specific service.

- Cautions

  * Notice that enabling both DHCPv6 and SLAAC would cause one host to configure more IPv6 addresses. Typically, there would be one more DHCPv6-configured address than SLAAC-only configuration; and two more addresses based on SLAAC and privacy extension than DHCPv6-only configuration. Too many addresses might cause ND cache overflow problem in some

situations (please refer to Section 3.4 of [I-D.liu-v6ops-running-multiple-prefixes] for details).

* For provisioning redundancy scenario, there is a concern that SLAAC/DHCPv6 addresses based on the same prefix might cause some applications confusing. [Open Question] Call for real experiences on this issues.

* Besides address configuration, DNS can also be configured both by SLAAC and DHCPv6. If the DNS information in RAs and DHCPv6 are different, the host might confuse. So in terms of operation, the operators should make sure DNS configuration in RAs and DHCPv6 are the same.

2.3. Guidance for Renumbering

This document only considers the renumbering cases where DHCPv6/SLAAC interaction is involved. These renumbering operations need the A/M flags transition which might cause unpredictable host behaviors. Two renumbering cases are discussed as the following.

2.3.1. Adding a New Address from another Address Configuration Mechanisms

o Adding a DHCPv6 Address for a SLAAC-configured Host

As discussed in Section 2.2.3, some operating systems that having configured SLAAC addersses would NOT care about the newly added DHCPv6 provision unless the current SLAAC address lifetime is expired. In theory, one possible way is to stop advertising RAs and wait the SLAAC addresses expired (this makes the hosts return to the initial stage), then advertise RAs again with the M flag set, so that the host would configure SLAAC and DHCPv6 addresses simultaneously. However, there would be some outage period during this operation, which might be unacceptable for many situations. Thus, It is better for the administrators to carefully plan the network provisioning so that to make SLAAC and DHCPv6 available simultaneously (through RA with M=1) at the initial stage rather than configuring one and then configuring another.

o Adding a SLAAC Address for a DHCPv6-configured Host

As tested in [I-D.ietf-v6ops-dhcpv6-slaac-problem].), current mainstream operating systems all support this renumbering operation. The only thing need to care about is to make sure the M flag is on in the RAs, since some operating systems would immediately release the DHCPv6 addresses if M flag is off.

2.3.2. Switching one Address Configuration Mechanism to another

- DHCPv6 to SLAAC

  This operation is supported by all the tested operating systems in [I-D.ietf-v6ops-dhcpv6-slaac-problem]. However, the behaviors are different. As said above, if A flag is on while M flag is off, a flash switching renumbering would happen on some operating systems. So while turning the A flag on, it is recommended to retain the M flag on and stop the DHCPv6 server to response the renew messages so that the DHCPv6 addresses could be released when the lifetimes expired.

- SLAAC to DHCPv6

  This operation is also supported by all the tested operating systems. And the behaviors are the same since no operating systems would immediatly release the SLAAC addresses when A flag is off. However, for safe operation, while turning the M flag on, it is also recommended to retain the A flag on and stop advertising RAs so that the SLAAC addresses could be released when the lifetimes expired.

3. Security Considerations

No more security considerations than the Neighbor Discovery protocol [RFC4861].

4. IANA Considerations

This draft does not request any IANA action.

5. Acknowledgements

Valuable comments were received from Sheng Jiang and Brian E Carpenter to initiate the draft. Some texts in Section 2.2.1 were based on Lorenzo Colitti and Mikael Abrahamsson’s proposal. There were also comments from Erik Nordmark, Ralph Droms, John Brzozowski, Andrew Yourtchenko and Wesley George to improve the draft. The authors would like to thank all the above contributors.

This document was produced using the xml2rfc tool [RFC2629]. (This document was initiallly prepared using 2-Word-v2.0.template.dot.)

6. References

6.1. Normative References

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

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

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011.

6.2. Informative References

[I-D.ietf-v6ops-dhcpv6-slaac-problem]
Liu, B., Jiang, S., Bonica, R., Gong, X., and W. Wang, "DHCPv6/SLAAC Address Configuration Interaction Problem Statement", draft-ietf-v6ops-dhcpv6-slaac-problem-02 (work in progress), October 2014.

[I-D.liu-v6ops-running-multiple-prefixes]
Liu, B., Jiang, S., and Y. Bo, "Considerations for Running Multiple IPv6 Prefixes", draft-liu-v6ops-running-multiple-prefixes-02 (work in progress), October 2014.

[I-D.yourtchenko-ra-dhcpv6-comparison]
Yourtchenko, A., "A comparison between the DHCPv6 and RA based host configuration", draft-yourtchenko-ra-dhcpv6-comparison-00 (work in progress), November 2013.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

Authors' Addresses

Bing Liu
Huawei Technologies
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: leo.liubing@huawei.com

Ron Bonica
Juniper Networks
Sterling, Virginia
20164
USA

Email: rbonica@juniper.net

Tianle Yang
China Mobile
32, Xuanwumenxi Ave.
Xicheng District, Beijing 100053
P.R. China

Email: yangtianle@chinamobile.com