V6OPS
Internet-Draft
Intended status: Informational
Expires: April 17, 2015

B. Liu
S. Jiang
Huawei Technologies
R. Bonica
Juniper Networks
X. Gong
W. Wang
BUPT University
October 14, 2014

DHCPv6/SLAAC Address Configuration Interaction Problem Statement
draft-ietf-v6ops-dhcpv6-slaac-problem-02

Abstract

The IPv6 Neighbor Discovery (ND) Protocol includes an ICMPv6 Router Advertisement (RA) message. The RA message contains three flags, indicating which autoconfiguration mechanisms are available to on-link hosts. These are the M, O and A flags. The M, O and A flags are advisory, not prescriptive.

This document describes divergent host behaviors observed in popular operating systems. It also describes operational problems that divergent behaviors cause.

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 17, 2015.

Table of Contents

1. Introduction

IPv6 [RFC2460] hosts invoke Neighbor Discovery (ND) [RFC4861] procedures in order to discover which autoconfiguration mechanisms are available to them. The following is a list of autoconfiguration mechanisms:

- DHCPv6 [RFC3315]

- Stateless Address Autoconfiguration (SLAAC) [RFC4862]

ND specifies an ICMPv6 [RFC4443] Router Advertisement (RA) message. Routers periodically broadcast the RA message to all on-link nodes.

They also unicast RA messages in response to solicitations. The RA message contains:

- an M (Managed) flag
- an O (OtherConfig) flag
- zero or more Prefix Information (PI) Options

The M flag indicates that addresses are available from DHCPv6. The O flag indicates that other configuration information (e.g., DNS-related information) is available from DHCPv6. The PI Option includes a prefix, an A (Autonomous) flag and other fields. The A flag indicates that the prefix can be used for SLAAC. The M, O and A flags are advisory, not prescriptive. For example, the M flag indicates that addresses are available from DHCPv6. It does not indicate that hosts are required to acquire addresses from DHCPv6. Similar statements can be made about the O and A flags.

In most cases, the M, O and A flags elicit identical behaviors from most popular operating systems. However, in several cases, the M, O and A flags elicit divergent behaviors. For example, when a router changes the settings of the M, O, and A flag from one RA message to the next, it is likely to elicit one behavior from hosts running one operating system and another behavior from hosts running a different operating system.

This document describes divergent host behaviors observed in popular operating systems. It also describes operational problems that divergent behaviors cause.

2. The M, O and A Flags

This section briefly reviews how the M, O and A flags are defined in [RFC4861].

2.1. M (Managed) Flag

The M flag indicates that addresses are available from IPv6. If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.

M and A flag semantics are independent of one another. The M flag indicates that addresses are available from DHCPv6, regardless of the A flag setting. The following setting are all allowed:

- M=0 A=0

- M=0 A=1
- M=1 A=0
- M=1 A=1

2.2. O (Otherconfig) Flag

The O flag indicates that other configuration information (e.g., DNS-related information) is available from IPv6. If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.

O and A flag semantics are independent of one another. The O flag indicates that other configuration is available from DHCPv6, regardless of the A flag setting. The following setting are all allowed:

- O=0 A=0
- O=0 A=1
- O=1 A=0
- O=1 A=1

2.3. A (Autonomous) Flag

The A flag indicates that the prefix that is also carried by the PI option can be used for SLAAC. A flag semantics are independent of M and O flag semantics. The A flag indicates that the prefix can be used by SLAAC, regardless of the M and O flag settings.

3. Problem Statement

3.1. Divergent Host Behaviors

The authors tested several popular operating systems in order to determine what behaviors the M, O and A flag elicit. In some cases, the M, A and O flags elicit identical behaviors from most popular operating systems. However, in several cases, the M, O and A flags elicit divergent behaviors. The table below characterizes those cases:

Host State	Input	Behavior
Host has not acquired any addresses	No RA	Some popular operating systems acquire addresses from DHCPv6. Others do not.
Host has not acquired any addresses	RA with M=0, O=1	Some popular operating systems acquire other information from DHCPv6, regardless of the A flag setting. Others do so, but only if A=1
Host has acquired addresses from DHCPv6 only (M = 1)	RA with M =0	Some operating systems release DHCPv6 addresses immediately. Some release DHCPv6 addresses when they expire.
Host has acquired addresses from SLAAC only (A=1)	RA with M = 1	Some operating systems acquire DHCPv6 addresses immediately. Others do so only if their SLAAC addresses expire and cannot be refreshed.

3.2. Operational Problems

This section describes operational issues caused by the divergent behaviors, described above.

3.2.1. Inappropriate Sources

Some operating systems base their decision to acquire configuration information upon inappropriate sources. For example, some operating systems acquire other configuration information if M = 0, O = 1, and A = 1, but not if M = 0, 0 = 1 and A = 0. In other words, on some operating systems, it is impossible to acquire other information from DHCPv6 unless addresses are acquired from either DHCPv6 or SLAAC.

3.2.2. Renumbering

According to [RFC6879] a renumbering exercise can include the following steps:

- Causing hosts that have acquired addresses from one autoconfiguration mechanism to release those addresses and acquire new addresses from another autoconfiguration mechanism

- Causing hosts that have acquired addresses from one autoconfiguration mechanism to release those addresses and acquire new addresses from the same autoconfiguration mechanism

- Causing hosts that have acquired addresses from one autoconfiguration mechanism to retain those addresses and acquire new addresses from another autoconfiguration mechanism

Ideally, these steps could be initiated by broadcasting RA message onto the subnetwork that is being renumbered. Sadly, this is not possible, because the RA message may elicit a different behavior from each host. According to Section 3.1, renumbering operations would have the following limitations:

- During a flash switch from DHCPv6 to SLAAC, some operating systems release DHCPv6 acquired addresses immediately, while other will retain then until they expire. Therefore, results are unpredictable.

- On some operating systems, if a host has acquired addresses from SLAAC, it is impossible to acquire additional addresses from DHCPv6. This may be required as part of a renumbering operation.

4. Security Considerations

As this memo does not introduce any new protocols or procedures, it does not introduce any new security vulnerabilities.

5. IANA Considerations

This draft does not request any IANA action.

6. Acknowledgements

The authors wish to acknowledge BNRC-BUPT (Broad Network Research Centre in Beijing University of Posts and Telecommunications) for their testing efforts. Special thanks to Xudong Shi, Longyun Yuan and Xiaojian Xue for their extraordinary effort.

The authors also wish to acknowledge Brian E Carpenter, Ran Atkinson, Mikael Abrahamsson, Tatuya Jinmei, Mark Andrews and Mark Smith for their helpful comments.

7. References

7.1. Normative References

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

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[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.

7.2. Informative References

[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.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC6879] Jiang, S., Liu, B., and B. Carpenter, "IPv6 Enterprise Network Renumbering Scenarios, Considerations, and Methods", RFC 6879, February 2013.

Appendix A. Test Results

A.1. Test Environment

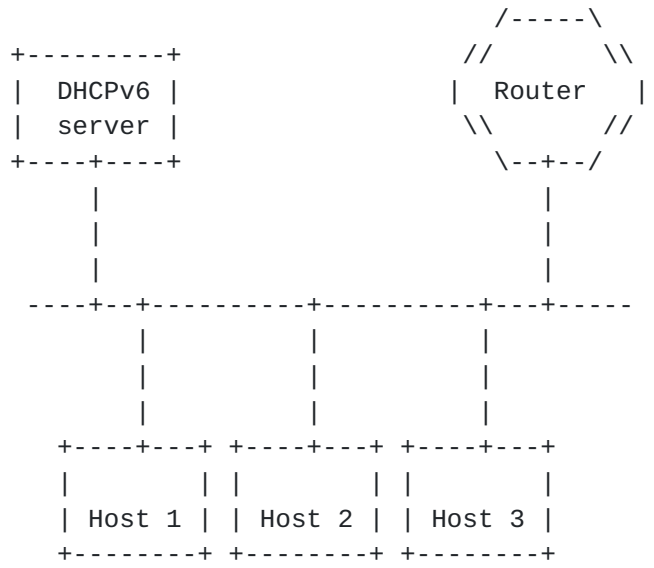

Figure 1: Test Environment

The test environment depicted Figure 1 in was replicated on a single server using VMware. For simplicity of operation, only one host was run at a time. Network elements were as follows:

- Router: Quagga 0.99-19 soft router installed on Ubuntu 11.04 virtual host
- DHCPv6 Server: Dibbler-server installed on Ubuntu 11.04 virtual host
- Host 1: Window 7 / Window 8.1 Virtual Host
- Host 2: Ubuntu 14.04 (Linux Kernel 3.12.0) Virtual Host
- Host 3: Mac OS X v10.9 Virtual Host
- Host 4: IOS 8.0 (model: Apple iPhone 5S, connected via wifi)

A.2. Host Behavior in the Initial State

The bullet list below describes host behavior in the initial state, when the host has not yet acquired any autoconfiguration information. Each bullet item represents an input and the behavior elicited by that input.

- A=0, M=0, O=0
  - Windows 8.1 acquired addresses and other information from DHCPv6.
  - All other hosts acquired no configuration information.
- A=0, M=0, O=1
  - Windows 8.1 acquired addresses and other information from DHCPv6.
  - Windows 7, OSX 10.9 and IOS 8.0 acquired other information from DHCPv6.
  - Ubuntu 14.04 acquired no configuration information.
- A=0, M=1, O=0
  - All hosts acquired addresses and other information from DHCPv6.
- A=0, M=1, O=1

    * All hosts acquired addresses and other information from DHCPv6.

- A=1, M=0, O=0

    * Windows 8.1 acquired addresses from SLAAC and DHCPv6. It also acquired non-address information from DHCPv6.

    * All the other host acquired addresses from SLAAC

- A=1, M=0, O=1

    * Windows 8.1 acquired addresses from SLAAC and DHCPv6. It also acquired other information from DHCPv6.

    * All the other hosts acquired addresses from SLAAC and other information from DHCPv6.

- A=1, M=1, O=0

    * All hosts acquired addresses from SLAAC and DHCPv6. They also acquired other information from DHCPv6.

- A=1, M=1, O=1

    * All hosts acquired addresses from SLAAC and DHCPv6. They also acquired other information from DHCPv6.

As showed above, four inputs result in divergent behaviors.

A.3. Host Behavior in State Transitions

The bullet list below describes behavior elicited during state transitions. The value x can represents both 0 and 1.

- Old state (M = x, O = x, A = 1) , New state (M = x, O = x, A = 0) (This means a SLAAC-configured host, which is regardless of DHCPv6 configured or not, reveiving A transitiong from 1 to 0.)

    * All the hosts retain SLAAC addresses until they expire

- Old state (M = 0, O = x, A = 1), New state (M = 1, O = x, A = 1) (This means a SLAAC-only host receiving M transisioning from 0 to 1.)

    * Windows 7 acquires addresses from DHCPv6, immediately.

    * Ubuntu 14.04/OSX 10.9/IOS 8.0 acquires addresses from DHCPv6 only if the SLAAC addresses are allowed to expire

    * Windows 8.1 was not tested because it always acquire addresses from DHCPv6 regardless of the M flag setting.

- Old state (M = 1, O = x, A = x), New state (M = 0, O = x, A = x) (This means a DHCPv6-configured host receiving M transitioning from 1 to 0.)

    * Windows 7 immediately released the DHCPv6 address

    * Windows 8.1/Ubuntu 14.04/OSX 10.9/IOS 8.0 keep the DHCPv6 addresses until they expire

- Old state (M = 1, O = x, A = 0), New state (M = 1, O = x, A = 1) (This means a DHCPv6-only host receiving A transisioning from 0 to 1.)

    * All host acquire addresses from SLAAC

- Old state (M = 0, O = 1, A = x), New state (M = 1, O = 1, A = x) (This means a Stateless DHCPv6-configured host [RFC3736], which is regardless of SLAAC configured or not, receiving M transisioning from 0 to 1 with keeping O=1)

    * Windows 7 acquires addresses and refreshes other information from DHCPv6

    * Ubuntu 14.04/OSX 10.9/IOS 8.0 does nothing

    * Windows 8.1 was not tested because it always acquire addresses from DHCPv6 regardless of the M flag setting.

- Old state (M = 1, O = 1, A = x), New state (M = 0, O = 1, A = x) (This means a Stateful DHCPv6-configured host, which is regardless of SLAAC configured or not, receiving M transisioning from 0 to 1 with keeping O=1)

    * Windows 7 released all DHCPv6 addresses and refreshes all DHCPv6 other information.

    * Windows 8.1/Ubuntu 14.04/OSX 10.9/IOS 8.0 does nothing

Appendix B. Analysis of the Ambiguities

Following is a comprehensive analysis of the ambiguities as defined in the standards. In theory, all the ambiguities might cause divergent host behavior. Some of the divergence has been identified by the tests while some haven't. It is worth to document all the ambiguities.

1. Dependency between DHCPv6 and RA

   In standards, behavior of DHCPv6 and Neighbor Discovery protocols is specified respectively. But it is not clear that whether there should be any dependency between them. More specifically, is RA (with M=1) required to trigger DHCPv6? If there are no RAs at all, should hosts initiate DHCPv6 by themselves?

2. Behaviors of Flag Transition

   When flags are in transition, e.g. the host is already SLAAC-configured, then M flag changes from FALSE to TRUE, it is not clear whether the host should start DHCPv6 or not; or vise versa, the host is already both SLAAC/DHCPv6 configured, then M flag change from TRUE to FALSE, it is also not clear whether the host should turn DHCPv6 off or not.

3. Distinction between "Address Configuring Method" and "Address Lifetime"

   When one address configuration method is off, that is, the A flag or M flag changes from TRUE to FALSE, it is not clear whether the host should immediately release the corresponding address(es) or just retain it(them) until expired.

4. Dependencies between the flags

   The semantics of the flags seems not totally independent, but the standards didn't clearly clarify it. For example, when both M and O flags are TRUE, it is not clear whether the host should initiate one stateful DHCPv6 session to get both address and info-configuration or initiate two independent sessions of which one is dedicated for address provisioning and the other is for information provision. When A and M flags are FALSE and O flag is TRUE, it is not clear whether the host should initiate a stand-alone stateless DHCPv6 session.

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

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

Email: jiangsheng@huawei.com

Ron Bonica
Juniper Networks
Sterling, Virginia
20164
USA

Email: rbonica@juniper.net

Xiangyang Gong
BUPT University
No.3 Teaching Building
Beijing University of Posts and Telecommunications (BUPT)
No.10 Xi-Tu-Cheng Rd.
Hai-Dian District, Beijing
P.R. China

Email: xygong@bupt.edu.cn

Wendong Wang
BUPT University
No.3 Teaching Building
Beijing University of Posts and Telecommunications (BUPT)
No.10 Xi-Tu-Cheng Rd.
Hai-Dian District, Beijing
P.R. China

Email: wdwang@bupt.edu.cn