

Internet Engineering Task Force  
Internet-Draft  
Intended status: Standards Track  
Expires: December 10, 2008

H. Cha, Ed.  
SAMSUNG Electronics, Inc.  
B. Volz  
Cisco Systems, Inc.  
June 8, 2008

Clarifying Handling of M & O Flags of IPv6 Router Advertisement  
draft-cha-ipv6-ra-mo-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 10, 2008.

Abstract

This document clarifies how clients are supposed to use the RA M & O flags.

Internet-Draft

Handling of M &amp; O Flags of IPv6 RA

June 2008

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Requirements Language . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">4.</a>	An Algorithm for the Management of Internal State Variables . .	<a href="#">4</a>
<a href="#">5.</a>	The Revocation of DHCPv6 clients . . . . .	<a href="#">5</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">8.</a>	References . . . . .	<a href="#">6</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">6</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">7</a>
	Authors' Addresses . . . . .	<a href="#">7</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">8</a>

## 1. Introduction

According to [[RFC4861](#)], the M flag indicates that addresses are available via DHCPv6 and the O flag indicates that other configuration information is available via DHCPv6. However, since [RFC 2462](#) which is deprecated by [RFC4861](#) already specified how IPv6 host should handle flags values in the received RA messages, current IPv6 stack and DHCPv6 client implementations have been developed according to the specification. In [[RFC 2462](#)] 5.5.3, it is required that a host should invoke the DHCPv6 client to request both address and other information when received Router Advertisement message change an internal state variable (ManagedFlag) from FALSE to TRUE and the DHCPv6 client is not running. In addition, if the value of the ManagedFlag changes from TRUE to FALSE, the host should continue running the DHCPv6 client, i.e., the change in the value of the ManagedFlag has no effect. However, the existing documents have the operational problems described below.

Firstly, there is no method to revoke the operation of a DHCPv6 client invoked by IPv6 RA flags. When a network administrator changes the addressing policy for the network, i.e to shutdown DHCPv6 servers or change stateful DHCPv6 servers into stateless, he/she can not revoke operation of DHCPv6 clients by changing the configuration of RA flags. The reason for this problem is that DHCPv6 clients would keep searching for a server from which to obtain stateful address and other configuration information after all existing bindings will expire.

Secondly, per-interface state variables regarding availability of the DHCPv6 service cannot be maintained consistently in case that inconsistent M & O flags are contained in RAs sent by different routers. The reason of this problem is that these state variables are copied from the M & O flag fields of the most recently received Router Advertisement message respectively.

To address these problems, this document describes a handling scheme

of M & O flags in RA messages. which consists of an algorithm for the management of internal state variables and options regarding how these variables can be utilized to revoke DHCPv6 clients.

## [2.](#) Requirements Language

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.](#) Terminology

RA Router Advertisement. More information can be found in [[RFC4861](#)].

M flag 1-bit "Managed address configuration" flag in RA message. More information can be found in [[RFC4861](#)] [section 4.2](#).

O flag 1-bit "Other configuration" flag in RA message. More information can be found in [[RFC4861](#)] [section 4.2](#).

ManagedFlag an internal state variable maintained on a per-interface basis according to algorithms presented in [section 4](#). Possible values are TRUE and FALSE. The transition from FALSE to TRUE have a stateful DHCPv6 client invoked and reverse transition SHOULD have the DHCPv6 client revoked as specified in [section 5](#).

OtherConfigFlag an internal state variable maintained on a per-interface basis according to algorithms presented in [section 4](#). Possible values are TRUE and FALSE. The transition from FALSE to TRUE have a stateless DHCPv6 client invoked and reverse transition SHOULD have the DHCPv6 client revoked as specified in [section 5](#).

DHCPv6 related terminologies DHCPv6, client, server, binding, etc can be found in [[RFC3315](#)] [section 4.2](#)

#### 4. An Algorithm for the Management of Internal State Variables

We introduce an algorithm for the management of the internal state variables as follows. In this algorithm, two timers (M-timer and O-timer) are used, lifetimes of which is chosen to be 3 times of MaxRtrAdvInterval in [[RFC4861](#)]. When an RA is received that has the M flag set, ManagedFlag is set to TRUE and the M-timer is started or restarted. When an RA is received that has the O flag set, the OtherConfigFlag is set to TRUE and O-timer is started or restarted. If the M-timer goes off, the ManagedFlag is set to FALSE. If the O-timer goes off, OtherConfigFlag is set to FALSE. Thus, once ManagedFlag or OtherConfigFlag is set to TRUE, it can only be changed into FALSE after no RA is received with the bit set within lifetime of timers. Thus, state variables can be managed consistently even when a host is connected to multiple routers sending conflicting RA messages, because the RA messages with the bit set will overrule the ones with the bit clear.

As an optional feature in the above algorithm, M & O flags in

received RA with source address may be kept track of. Through this feature, following benefits can be obtained:

##### i. Faster Transition of State Variables

ManagedFlag or OtherConfigFlag can be set to FALSE as soon as number of valid RA with the corresponding flag set is reduced to zero.

##### ii. Router Information

The ability for hosts to identify routers which invoke and continue the operations of DHCPv6 clients may be helpful to fix mis-configuration of routers or detect malicious routers.

#### 5. The Revocation of DHCPv6 clients

In this section, we introduce several suggestions regarding how state variables can be utilized to control the operation of a DHCPv6 client. As [RFC 2462](#) 5.5.3 specifies, a DHCPv6 client is invoked when a state variable is changed from FALSE to TRUE and the DHCPv6 client is not already running. As for the transition (negative transition) of state variables from TRUE to FALSE, there are many possible

implementational choices which can be classified into two types.

- 01 To let a DHCPv6 client determine whether the client should keep its operation or not depending on state variables.

For example, whenever the DHCPv6 client sends a Solicit or Inform-Request, it may check whether to continue doing DHCPv6 based on the ManagedFlag or OtherConfigFlag. In this option, the existing bindings will go through their normal lifecycle regardless of negative transition of the ManagedFlag and the client exit after all of the leases have expired. Thus, a potential benefit from this choice is for existing transport layer sessions to be preserved even while routers send RA messages with flags mistakenly cleared.

- 02 To let a negative transition revoke operation of DHCPv6 clients immediately.

The negative transition of the ManagedFlag makes a DHCPv6 client stop its stateful operation, thereby all bindings are released. A negative transition of the OtherConfigFlag make a DHCPv6 client stop its stateless operation.

## [6.](#) IANA Considerations

This document includes no request to IANA.

## [7.](#) Security Considerations

As [[RA-MO](#)], Handling schemes in M & O flags from RAs in this document could expedite denial of service attacks by allowing a host to trigger invalid DHCP exchanges with the M or O flag set in a malicious Router Advertisement and with illegitimate DHCPv6 servers. Authenticated DHCPv6 and/or [[RFC3971](#)] (SEcure Neighbor Discovery) can be used to protect the attack. This document introduces no additional security risks.

## [8.](#) References

### [8.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.
- [RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [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.
- [RA-MO] Park, S., Madanapalli, S., and T. Jinmei, "Considerations on M and O Flags of IPv6 Router Advertisement", [draft-ietf-ipv6-ra-mo-flags-01.txt](#) (Work in Progress)", March 2005.

### [8.2.](#) 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.

## Authors' Addresses

Hyunwook Joseph Cha (editor)  
SAMSUNG Electronics, Inc.  
416, Maetan-3dong, Yeongtong-Gu  
Suwon, Korea

Phone: +82-31-279-3804  
Email: hyunwook.cha@samsung.com

Bernie Volz  
Cisco Systems, Inc  
1414 Massachusetts Ave.  
Boxborough, MA 01719,  
USA

Phone: +1-978-936-0382  
Email: volz@cisco.com



Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).