Network Working Group
Internet-Draft
Expires: September 24, 2005

S. Park, Ed.
SAMSUNG Electronics
S. Madanapalli
Samsung ISO
T. Jinmei
Toshiba
March 26, 2005

Considerations on M and O Flags of IPv6 Router Advertisement
draft-ietf-ipv6-ra-mo-flags-01.txt

Status of this Memo

Copyright Notice

Abstract

This document clarifies the processing and behaviour of a host for the M and O flags of IPv6 Router Advertisement and proposes a solution for invoking the DHCPv6 service based on administrator policy in conjunction with new host variables for the M and O flags.

Table of Contents

1. Introduction

To configure a host with network information such as an IP address, DNS server addresses and other configuration information, several mechanisms are proposed in the IETF. In particular, IPv6 stateless address autoconfiguration [RFC2462] and Dynamic Host Configuration Protocol [RFC3315][RFC3736] will be widely used for configuring the network information.

This document proposes two conceptual variables, called DHCPv6 Policy variables corresponding to the M and O flags of Router Advertisement. The values of these policy variables in conjuction with the values of the flags of Router Advertisement decide the host behaviour to invoke DHCPv6 services. These policy variables are controlled by the administrator under a certain level of requirement.

2. Background

This section explains why this document appears in the IETF.

So far, IPv6 WG has being tried to make both [RFC2461] and [RFC2462] mature for the Draft Standard. While updating, the text regarding the M and O flags were removed from [I-D.ietf-ipv6-rfc2462bis] considering the maturity of implementations and operational experiences.

[I-D.ietf-ipv6-2461bis] says:

o M :

1-bit "Managed address configuration" flag. When set, it indicates that Dynamic Host Configuration Protocol [DHCPv6] is available for address configuration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is further described in [ADDRCONF].

o O :

1-bit "Other configuration" flag. When set, it indicates that [DHCPv6lite] is available for autoconfiguration of other (non-address) information. Examples of such information are DNS-related information or information on other servers within the network.

In particular, both "ManagedFlag" and "OtherConfigFlag" which were implementation-internal variables were also removed during the [I-D.ietf-ipv6-rfc2462bis] work based on the WG consensus with ambiguous operational experiences, and thus new variables (or similar

approaches) are required to treat the M and O flags of IPv6 Router Advertisement on the host.

3. Terminology

- Host Configuration Behaviour :

  A host can use DHCPv6 for address autoconfiguration as well as other configuration information via Solicit/Advertise/Request/ Reply message exchanges or Solicit/Reply message exchanges (if rapid commit is enabled) as described in [RFC3315]. In this document, this term is used for host configuration including address and other configuration information in conjunction with the M flag.

- Information Configuration Behaviour :

  A host can use DHCPv6 to obtain configuration information parameters excluding addresses. For this operation, Information-request and Reply messages are used, also as described in [RFC3315]. In this document, this term is used for other configuration information excluding addresses in conjunction with the O flag.

  [RFC3736] gives guidelines for implementing the parts of [RFC3315] required for the configuration information, for clients, servers and relay agents, although [RFC3736] has no additional impact on relay agents. Also, [RFC3736] does not describe procedures or a distinct protocol. It is intended to describe that part of the protocol that a server or a client must implement if all it intends to support is the configuration information.

4. Requirements

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 [RFC2119].

5. IPv6 Host Variables

This document newly introduces two host variables to indicate whether or not configuration information (including addresses) can be configured using DHCPv6. The implicit concept of these variables defined in this document is the same as that of "ManagedFlag" and "OtherConfigFlag", which were described in [RFC2462] and then removed from [I-D.ietf-ipv6-rfc2462bis]. We deliberately use different variable names in this document to avoid confusion with the removed names.

A host maintains the following variables on a per-interface basis:

o M-Flag :

Copied from the M flag field of the most recently received Router Advertisement message. This variable indicates whether or not address can be configured using Host Configuration Behaviour. It starts out in a FALSE state. On receipt of a valid Router Advertisement, a host copies the value of the advertisement's M flag into M-Flag.

Default: FALSE

o O-Flag :

Copied from the O flag field of the most recently received Router Advertisement message. This variable indicates whether or not configuration information (excluding addresses) can be obtained using Information Configuration Behaviour. It starts out in a FALSE state. On receipt of a valid Router Advertisement, a host copies the value of the advertisement's O flag into O-Flag.

Default: FALSE

6. DHCPv6 Policy Variables

This document introduces two administrator policy variables regarding DHCPv6, M-Policy and O-Policy, corresponding to Host Configuration Behaviour and Information Configuration Behaviour. These policy variables will be used by the administrator for controlling the invocation of DHCPv6.

6.1 Dependency Between the Configuraton Behaviours

Prior to introducing specific policies, we note an important dependency between the two Configuraton Behaviours. If we invoke Host Configuration Behaviour for address autoconfiguration (along with other configuration information), we basically should not invoke Information Configuration Behaviour since the former can provide other configuration information as well.

For simplicity, however, we will describe the policies and the corresponding variables for the M and O flags separately. Host's behaviour, with taking into account of the dependency, will be described in Section 7.

6.2 M-Policy

This policy variable takes three values as described below.

- Policy 1 :

  The host should invoke Host Configuration Behaviour for address autoconfiguration (along with other configuration information) regardless of the content of received Router Advertisement messages or the existence of Router Advertisement messages.

- Policy 2 :

  The host should invoke Host Configuration Behaviour for address autoconfiguration (along with other configuration information) if and only if it sees a Router Advertisement changing the M-Flag from FALSE to TRUE.

- Policy 3 :

  The host should not invoke Host Configuration Behaviour for address autoconfiguration (along with other configuration information) regardless of the content of received Router Advertisement messages or the existence of Router Advertisement messages.

6.3 O-Policy

This policy variable takes three values as described below.

- Policy 1 :

  The host should invoke Information Configuration Behaviour for getting other configuration information regardless of the content of received Router Advertisement messages or the existence of Router Advertisement messages.

- Policy 2 :

  The host should invoke Information Configuration Behaviour for getting other configuration information if and only if it sees a Router Advertisement changing the O-Flag from FALSE to TRUE.

- Policy 3 :

  The host should not invoke Information Configuration Behaviour for getting other configuration information regardless of the content of received Router Advertisement messages or the existence of

Router Advertisement messages.

7. Host Behaviour

The M and O flags indicate whether Host Configuration/Information Configuration Behaviours are available, but typically they themselves should not be used as triggers to invoke DHCPv6 services. However, these flags in conjunction with the policy configured may trigger DHCPv6 services for automatic configuration of the IPv6 address and the other information.

The followings are specific host's behaviour based on the policy variables and the change of the host state variables.

If M-Policy is 1, the host SHOULD invoke Host Configuration Behaviour for address and other configuration information, regardless of the change of the state variables. The host SHOULD NOT invoke Information Configuration Behaviour regardless of O-Policy. Note, however, that if the available DHCPv6 servers only provide the service for the Information Configuration Behaviour, the host will even not be able to configure other configuration parameters than addresses. Thus, it is generally inadvisable to set M-Policy to 1, unless there is a particular reason to do so.

If M-Policy is 2, the host SHOULD first wait for initial Router Advertisements. If those advertisements make M-Flag change from FALSE to TRUE, the host SHOULD invoke Host Configuration Behaviour. In this case, the host SHOULD NOT invoke Information Configuration Behaviour regardless of O-Policy. Otherwise, if O-Policy is 1 or the initial advertisements make O-Flag change from FALSE to TRUE with O-Policy being 2, the host SHOULD invoke Information Configuration Behaviour. Even after initial advertisements, the host SHOULD invoke Host Configuration Behaviour whenever M-Flag changes from FALSE to TRUE, unless it has already started the behaviour. If the host has invoked Information Configuration Behaviour by the time it invokes Host Configuration Behaviour, the host SHOULD NOT stop the running Information Configuration Behaviour.

If M-Policy is 3, the host SHOULD NOT invoke Host Configuration Behaviour, regardless of the change of the state variables. In this case, if O-Policy is 1, the host SHOULD immediately invoke Information Configuration Behaviour. Otherwise, when O-Flag changes from FALSE to TRUE with O-Policy being 2, the host SHOULD invoke Information Configuration Behaviour, unless it has already started the behaviour.

8. Other Issues on State Transition of M-Flag and O-Flag

As long as a host resides in the same single network, the behaviour of the host SHOULD NOT be changed with the change of M-Flag or O-Flag from TRUE to FALSE. The host is not expected to store M-Flag and O-Flag state in non-volatile memory. When a host is rebooting (the state of variables starts with FALSE), the host SHOULD update these variables depending on the information received in Router Advertisement messages. Also, the host SHOULD update these variables depending on the information received in Router Advertisement messages, when it moves to a different network and receives a new Router Advertisement including different prefix information.

9. Router Advertisement Unavailability

It is possible that the host does not see any Router Advertisements. Originally, [RFC2462] requested that the host in this case must invoke the stateful configuration protocol (i.e., [RFC3315] in today's interpretation). In addition, [I-D.ietf-ipv6-node-requirements] says that in the absence of a router, the IPv6 nodes that use DHCP for address assignment MUST initiate DHCP to obtain IPv6 addresses and other configuration information.

Based on these prior documents, this document introduces the following rule: if no Router Advertisement appears, a host SHOULD initiate Host Configuration Behaviour using [RFC3315] to get both address and configuration information as if the node receives a Router Advertisement with the M flag being ON and the O flag being OFF. This rule is almost as the same as what the prior documents specified, except that the host can still choose not to initiate Host Configuration Behaviour if its M-policy is 3.

10. Conclusion

To clarify the meaning of the M and O flags of IPv6 Router Advertisement, this document has proposed DHCPv6 Policy variables on the host in conjunction with host state variables corresponding to the M and O flags of Router Advertisement for invoking the DHCPv6 Services. The Policy variables are controlled by the administrator under a certain level of requirement.

Generally, both Host Configuration/Information Configuration Behaviours and IPv6 stateless address autoconfiguration may be used simultaneously. On the other hand, if we invoke Host Configuration Behaviour for address autoconfiguration, we should basically not invoke Information Configuration Behaviour since the former service can provide other configuration information also.

[RFC3736] is just a subset of the full DHCPv6 service. Thus, a host implementing [RFC3315] can do both or either Host Configuration Behaviour for configuring the IPv6 address and Information Configuration Behaviour for the other information. A host implementing only [RFC3736] can only do Information Configuration Behaviour.

11. An Open Issue: Default Policy Values

Once we agree on the basic concept described in this document, we will then have to decide the appropriate default values of the policy variables.

The followings are some initial considerations on the default values at the moment. If the node implements Host Configuration Behaviour using [RFC3315], the default value of M-Policy should be 2. If the node does not implement Host Configuration Behaviour using [RFC3315], the default (and only) value of M-policy should be 3. Assuming Information Configuration Behaviour only using [RFC3736] will be implemented much wider than the full set of [RFC3315] in terms of other configuration information, the default value of O-Policy should be either 1 or 2. Value 1 is presumably better since this service can be crucial for the node (i.e., there may be no alternative to get the other configuration information.)

12. Security Considerations

The concepts in this document do not significantly alter the security considerations for DHCPv6 and Neighbor Discovery Protocol. However, the use of the proposed policies with variables could expedite denial of service attacks by allowing a mischievous host to trigger invalid DHCP exchanges with the M or O flag being ON in a malicious Router Advertisement and with illegitimate DHCPv6 servers. Authenticated DHCPv6 and/or [I-D.ietf-send-ndopt] (SEcure Neighbor Discovery, SEND) can be used to protect the attack.

Even though the threat is only effective from an on-link attacker, it can be significant without a strong security mechanism like SEND, since the attack takes place in the process of autoconfiguration, and it may be difficult for the user to detect the attack. Thus, it is generally advisable to log the change of M-Flag or O-Flag from FALSE to TRUE. In addition, it might be useful to log an event that information provided through DHCPv6 is different form the information of the same type that the host previously received through DHCPv6.

13. IANA Considerations

This document has no consideration for IANA.

14. Acknowledgements

The approach of this document was from the RFC2461/RFC2462, so the authors would appreciate the authors of these RFCs and the editors of RFC2461bis/RFC2462bis. Also, many thanks go to IPv6 Working Group members for their valuable discussion on this thread in the mailing list. Especially to: Greg Daley, Pekka Savola, Ralph Droms, and Stig Venaas. Thanks to Bernie Volz of Cisco for his lots of valuable work on this document. Special thanks to Radakrishnan and OLN Rao of Samsung India Software Operations for their inputs from implementation perspective. Thanks to Noh-Byung Park and Youngkeun Kim for their supports on this work.

Alain Durand indicated an attack changing the M and O flags with a rogue DHCPv6 server and kindly introduced a log message as an effective method to detect a suspicious operation.

15. Appendix A: Handling of M and O flags from multiple routers

This document does not take a hard stance on what happens when a host has multiple routers and inconsistent information (different M and O flags configuration) is learned from different routers. The basic documents [RFC2461]/[RFC2462] already described "Configuration Consistency" and a host will simply handle inconsistent M and O flags of Router Advertisement in the same manner.

If the host frequently receives inconsistent M and O flags of Router Advertisement (e.g., in a mobile environment for supporting fast movement detection), it may need complex consideration on an erroneous case. However, this case is not closely related to this document; rather, it is a general issue on the inconsistent Router Advertisement parameters from multiple routers. In fact, other configuration parameters such as the MTU size and the hop limit are also possible to be inconsistent in different Router Advertisements.

In the end, it is administrator's responsibility to ensure the consistency among Router Advertisement parameters from multiple routers in the same single link as described in Section 5.6 of [RFC2462]. The authors thus remain "Handling of M and O flags from multiple routers" out of scope of this document.

16. References

16.1 Normative References

[I-D.ietf-ipv6-2461bis]
Narten, T., "Neighbor Discovery for IP version 6 (IPv6)", draft-ietf-ipv6-2461bis-02 (work in progress), February

2005.

[I-D.ietf-ipv6-rfc2462bis]
Thomson, S., "IPv6 Stateless Address Autoconfiguration", draft-ietf-ipv6-rfc2462bis-07 (work in progress), December 2004.

[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.

[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.

16.2 Informative References

[I-D.ietf-ipv6-node-requirements]
Loughney, J., "IPv6 Node Requirements", draft-ietf-ipv6-node-requirements-11 (work in progress), August 2004.

[I-D.ietf-send-ndopt]
Arkko, J., Kempf, J., Sommerfeld, B., Zill, B. and P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ndopt-06 (work in progress), July 2004.

Authors' Addresses

Soohong Daniel Park, Ed.
Mobile Platform Laboratory, SAMSNUG Electronics
416 Maetan-3dong, Yeongtong-Gu
Suwon, Gyeonggi-Do 443-742
KOREA

Phone: +82 31 200 4508
EMail: soohong.park@samsung.com

Syam Madanapalli
Samsung India Software Operation
J.P. Techno Park, 3/1
Millers Road, Bangalore 560-052
INDIA

Phone: +91 80 51197777
EMail: syam@samsung.com

Tatuya Jinmei
Toshiba Corporation
1 Komukai Toshiba-cho, Saiwai-ku
Kawasaki-shi, Kanagawa 212-8582
JAPAN

Phone: +81 44 549 2230
EMail: jinmei@isl.rdc.toshiba.co.jp

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.