Internet Engineering Task Force (IETF)
Request for Comments: 7774
Category: Standards Track
ISSN: 2070-1721

Y. Doi
Toshiba Corporation
M. Gillmore
Itron, Inc.

March 2016

Multicast Protocol for Low-Power and Lossy Networks (MPL) Parameter Configuration Option for DHCPv6

Abstract

This document defines a way to configure a parameter set for MPL (Multicast Protocol for Low-Power and Lossy Networks) via a DHCPv6 option. MPL has a set of parameters to control its behavior, and the parameter set is often configured as a network-wide parameter because the parameter set should be identical for each MPL Forwarder in an MPL Domain. Using the MPL Parameter Configuration Option defined in this document, a network can easily be configured with a single set of MPL parameters.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7774.

Table of Contents

1. Introduction

The Multicast Protocol for Low-Power and Lossy Networks (MPL) [RFC7731] defines a protocol to make a multicast network among low-power and lossy networks, e.g., wireless mesh networks. MPL has a set of parameters to control an MPL Domain. The parameters control the trade-off between end-to-end delay and network utilization. In most environments, the default parameters are acceptable. However, in some environments, the parameter set must be configured carefully in order to meet the requirements of each environment. According to Section 5.4 of [RFC7731], each parameter in the set should be the same for all nodes within an MPL Domain, but [RFC7731] does not define a method to configure the MPL parameter set.

Some managed wireless mesh networks may have a DHCP server to configure network parameters. MPL parameter sets shall be considered as a part of network parameters (nodes in an MPL Domain should use an identical parameter set). A parameter set is required to configure an MPL Domain.

This document defines a way to distribute parameter sets for MPL Forwarders via a new DHCPv6 [RFC3315] option. This document is intended to follow the guidelines provided in [RFC7227].

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].

2. MPL Parameter Configuration Option

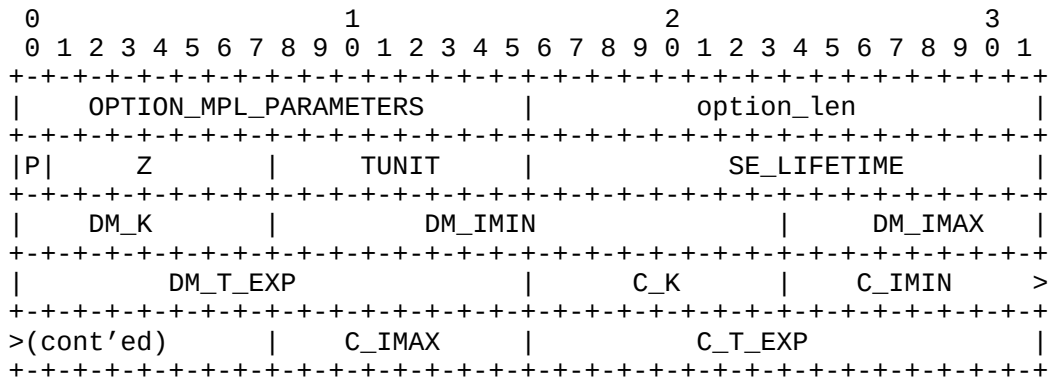
As defined in Section 5.4 of [RFC7731], there are 10 parameters per MPL Domain, as listed below. An MPL Domain is defined by an MPL Domain Address, as described in Section 2 of [RFC7731].

- PROACTIVE_FORWARDING
- SEED_SET_ENTRY_LIFETIME
- DATA_MESSAGE_IMIN
- DATA_MESSAGE_IMAX
- DATA_MESSAGE_K
- DATA_MESSAGE_TIMER_EXPIRATIONS
- CONTROL_MESSAGE_IMIN
- CONTROL_MESSAGE_IMAX
- CONTROL_MESSAGE_K
- CONTROL_MESSAGE_TIMER_EXPIRATIONS

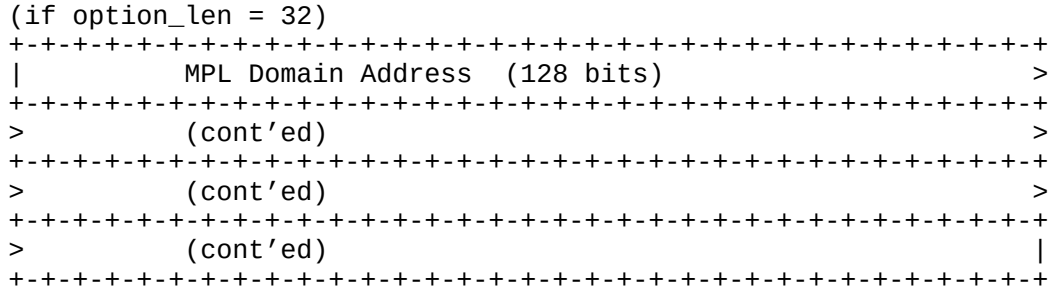
One network may have multiple MPL Domains with different configurations. To configure more than one MPL Domain via DHCP, there may be more than one MPL Parameter Configuration Option given to DHCP clients by a DHCP server.

2.1. MPL Parameter Configuration Option Format

This document defines the OPTION_MPL_PARAMETERS DHCPv6 option. This new option provides a means to distribute a configuration of an MPL Domain or a default value for all MPL Domains (a wildcard) within the network managed by the DHCP server. This option has the following format:



(if option_len = 32)



OPTION_MPL_PARAMETERS: DHCPv6 option identifier (104).

option_len: Length of the option in octets. The value MUST be set to 16 if no MPL Domain Address is present, or 32 if an MPL Domain Address is present.

P (1 bit): A flag to indicate PROACTIVE_FORWARDING. This flag is set if PROACTIVE_FORWARDING = TRUE.

Z (7 bits): Reserved for future use. Servers MUST set them to zero. Clients SHOULD ignore any bits that have been set.

TUNIT (unsigned 8-bit integer): Unit time of timer parameters (SE_LIFETIME and *_IMIN) in this option. 0 and 0xff are reserved and MUST NOT be used.

SE_LIFETIME (unsigned 16-bit integer):
SEED_SET_ENTRY_LIFETIME/TUNIT, in milliseconds. 0 and 0xffff are reserved and MUST NOT be used.

DM_K (unsigned 8-bit integer): DATA_MESSAGE_K.

DM_IMIN (unsigned 16-bit integer): DATA_MESSAGE_IMIN/TUNIT, in milliseconds. 0 and 0xffff are reserved and MUST NOT be used.

DM_IMAX (unsigned 8-bit integer): DATA_MESSAGE_IMAX. The actual maximum timeout is described as a number of doublings of DATA_MESSAGE_IMIN, as described in [RFC6206], Section 4.1. 0 and 0xff are reserved and MUST NOT be used.

DM_T_EXP (unsigned 16-bit integer): DATA_MESSAGE_TIMER_EXPIRATIONS. 0 and 0xffff are reserved and MUST NOT be used.

C_K (unsigned 8-bit integer): CONTROL_MESSAGE_K.

C_IMIN (unsigned 16-bit integer): CONTROL_MESSAGE_IMIN/TUNIT, in milliseconds. 0 and 0xffff are reserved and MUST NOT be used.

C_IMAX (unsigned 8-bit integer): CONTROL_MESSAGE_IMAX. The actual maximum timeout is described as a number of doublings of CONTROL_MESSAGE_IMIN. 0 and 0xff are reserved and MUST NOT be used.

C_T_EXP (unsigned 16-bit integer):
CONTROL_MESSAGE_TIMER_EXPIRATIONS. 0 and 0xffff are reserved and MUST NOT be used.

Note that the time values (SEED_SET_ENTRY_LIFETIME, DATA_MESSAGE_IMIN, and CONTROL_MESSAGE_IMIN) in MPL are defined to a precision of TUNIT milliseconds in MPL Parameter Configuration Options. For example, if TUNIT is 20 and the minimum Data Message interval (DATA_MESSAGE_IMIN) is 1000 ms, then DM_IMIN shall be set to 50.

For the maximum interval size (*_IMAX), [RFC6206] defines them as follows:

> The maximum interval size, Imax, is described as a number of doublings of the minimum interval size (the base-2 log(max/min)). For example, a protocol might define Imax as 16. If the minimum interval is 100 ms, then the amount of time specified by Imax is 100 ms * 65,536, i.e., 6,553.6 seconds or approximately 109 minutes.

Because the minimum interval size in MPL Parameter Configuration Options is described in TUNIT-millisecond precision, the corresponding maximum interval size is also in TUNIT-millisecond precision. For example, if TUNIT is 10 and C_IMIN is 50, the minimum interval size of the Trickle timer for Control Messages is 500 ms. In this case, the maximum interval size of the Trickle timer is 32 seconds (500 ms * 2^6) if C_IMAX is 6.

2.2. DHCPv6 Client Behavior

Clients MAY request the MPL Parameter Configuration Option as described in Sections 17.1.1, 18.1.1, 18.1.3, 18.1.4, 18.1.5, and 22.7 of [RFC3315]. As a convenience to the reader, we mention here that the client includes requested option codes in the Option Request Option.

Clients MUST support multiple MPL Parameter Configuration Options, which are listed in Section 2.

If a DHCPv6 client with an MPL Forwarder configured by the MPL Parameter Configuration Option is unable to receive a valid response from a server within T2 [RFC3315] of the last valid DHCPv6 message sent from the server (if stateful) or twice the information refresh time [RFC4242] (if stateless), it MUST suspend the MPL Forwarders of the MPL Domains configured by the option. MPL Forwarders configured by other methods (e.g., via a static configuration file) MUST NOT be suspended.

Clients MUST ignore all MPL Parameter Configuration Options if the options in a DHCPv6 message contain any invalid values (e.g., reserved all-0 or all-1 values are used in parameters). In this case, in the context of MPL the message is considered not received, and the condition described in the previous paragraph applies.

2.3. MPL Forwarder Behavior

If a DHCPv6 client requests and receives the MPL Parameter Configuration Option, the node SHOULD join the MPL Domain given by the option and act as an MPL Forwarder. Note that there may be cases in which a node may fail to join a domain (or domains) due to local resource constraints. Each joining node SHOULD configure its MPL Forwarder with the given parameter set for the MPL Domain. Each MPL Domain is defined by an MPL Domain Address given by an MPL Parameter Configuration Option. As defined in Section 2 of [RFC7731], an MPL Domain Address is an IPv6 multicast address associated to a set of MPL network interfaces in an MPL Domain.

The priority of MPL parameter configurations applied to an MPL Domain is as follows (high to low):

- Specific MPL parameter configuration for the MPL Domain (option_len = 32 bits).
- Wildcard MPL parameter configuration (option_len = 16 bits).
- Default configuration as described in [RFC7731].

Priorities of other configurations, such as manual configuration of a node, are not defined in this document.

There MUST be no more than one MPL Parameter Configuration Option for an MPL Domain or the wildcard. Thus, the order of DHCPv6 options in the packet has no effect on precedence.

A node MUST leave an MPL Domain if it receives updated and all-valid MPL Parameter Configuration Options without a configuration for the MPL Domain, unless it has an overriding manual configuration for the MPL Domain. In other words, if a node is configured to work as an MPL Forwarder for an MPL Domain regardless of DHCPv6 options, the node MAY stay in the MPL Domain even if it receives an MPL Parameter Configuration Option without a configuration for the MPL Domain.

MPL parameters may be updated occasionally. With stateful DHCPv6, updates can be done when the renewal timer expires. The information refresh time option [RFC4242] shall be used to keep each forwarder updated.

To reduce periodic update traffic, a node may try to use a very long interval between updates. In this case, Reconfigure messages may be used to keep forwarder parameter sets synchronized.

2.4. DHCPv6 Server Behavior

Sections 17.2.2 and 18.2 of [RFC3315] govern server operation in regard to option assignment. As a convenience to the reader, we mention here that the server will send the MPL Parameter Configuration Option only if it was configured with specific values for the MPL Parameter Configuration Option and the client requested it.

Servers MUST ignore an incoming MPL Parameter Configuration Option. Servers MUST support multiple MPL Parameter Configuration Options, which are listed in Section 2.

2.5. DHCPv6 Relay Behavior

It is never appropriate for a relay agent to add options to a message heading toward the client, and relay agents do not actually construct Relay-Reply messages anyway. There are no additional requirements for relays.

2.6. Operational Considerations

This document introduces the dynamic updating of MPL parameters. Because the update process is not synchronized, nodes may have inconsistent parameter sets.

[RFC6206], Section 6 describes various problems that occur if the Trickle timers do not match between communicating nodes. To keep the timers synchronized, it is RECOMMENDED to not update the parameters of an MPL Domain too often. A reasonable update rate would be once per expected information refresh time interval, such as T1 [RFC3315] or information refresh time as defined in [RFC4242].

Inconsistent parameter sets may reduce performance. On the other hand, this situation will work as long as both new and old parameter sets are reasonable parameter sets for a given communication load. Because motivations for parameter updates include updates of the environment, node density, or communication load, operators of MPL networks need to be aware of nodes that are not updated and make sure that old and new parameter sets are reasonable for the expected refresh intervals.

3. IANA Considerations

IANA has assigned an option code to OPTION_MPL_PARAMETERS (104) from the "Option Codes" table of the "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" registry (http://www.iana.org/assignments/dhcpv6-parameters).

4. Security Considerations

Section 23 of [RFC3315], Section 23 of [RFC7227], and Section 12 of [RFC7731] provide detailed discussions regarding security threats for DHCPv6.

Note also that a forged MPL parameter configuration may cause excessive Layer 2 broadcasting. Implementations should set reasonable bounds for each parameter -- for example, not setting DM/C_K too high, not setting DM/C_IMIN too low. These bounds may be implementation dependent or may be derived from MAC/PHY

specifications. DHCPv6 server and client implementations need to take care in setting reasonable bounds for each parameter in order to avoid overloading the network.

The DHCP server or the network itself should be trusted by some means, such as DHCPv6 authentication as described in Section 21 of [RFC3315]. However, Routing Over Low-Power and Lossy (ROLL) network environments often have fewer computing resources, and DHCPv6 authentication may not be available in these environments. In such cases, other methods to protect integrity between DHCPv6 servers and clients should be applied to a ROLL network. Some specifications related to ROLL implementations, such as ZigBee IP [ZigBeeIP] and [RFC5191], assume that joining nodes will be authenticated so that all nodes in the network can be trusted. To protect against attacks from outside of the network, DHCPv6 packets SHOULD be filtered on the border router between the ROLL network and the Internet, except for packets between the ROLL network and a remote DHCPv6 server or DHCPv6 relays configured to manage the network.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC4242] Venaas, S., Chown, T., and B. Volz, "Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 4242, DOI 10.17487/RFC4242, November 2005, <http://www.rfc-editor.org/info/rfc4242>.

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko, "The Trickle Algorithm", RFC 6206, DOI 10.17487/RFC6206, March 2011, <http://www.rfc-editor.org/info/rfc6206>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <http://www.rfc-editor.org/info/rfc7227>.

[RFC7731] Hui, J. and R. Kelsey, "Multicast Protocol for Low-Power and Lossy Networks (MPL)", RFC 7731, DOI 10.17487/RFC7731, February 2016, <http://www.rfc-editor.org/info/rfc7731>.

5.2. Informative References

[RFC5191] Forsberg, D., Ohba, Y., Ed., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, DOI 10.17487/RFC5191, May 2008, <http://www.rfc-editor.org/info/rfc5191>.

[ZigBeeIP] ZigBee Alliance, "ZigBee IP Specification", 2015, <http://www.zigbee.org/>.

Authors' Addresses

Yusuke Doi
Toshiba Corporation
Komukai Toshiba Cho 1
Saiwai-Ku
Kawasaki, Kanagawa 2128582
Japan

Phone: +81-45-342-7230
Email: yusuke.doi@toshiba.co.jp

Matthew Gillmore
Itron, Inc.
2111 N. Molter Rd.
Liberty Lake, WA 99019
United States

Email: matthew.gillmore@itron.com