Internet Engineering Task Force (IETF)
Request for Comments: 7732
Category: Informational
ISSN: 2070-1721

P. van der Stok
Consultant
R. Cragie
ARM Ltd.

February 2016

Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)

Abstract

The purpose of this document is to specify an automated policy for the routing of Multicast Protocol for Low-Power and Lossy Networks (MPL) multicast messages with Admin-Local scope in a border router.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see 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/rfc7732.

Table of Contents

1. Introduction

Multicast scopes are defined in [RFC4291]. [RFC7346] extends the scope definition with this text:

"Interface-Local, Link-Local, and Realm-Local scope boundaries are automatically derived from physical connectivity or other non-multicast-related configurations. Global scope has no boundary. The boundaries of all other non-reserved scopes of Admin-Local or larger are administratively configured."

The Admin-Local scope must therefore be administratively configured. In this document, "administratively configured" does not imply actions by a human beyond installing the protocol specified herein. "Administratively configured" means an automatic derivation as described in this document.

This document describes an automated policy for the Multicast Protocol for Low-Power and Lossy Networks (MPL) [RFC7731] forwarding of multicast messages with Admin-Local scope within a border router that lies between a network running MPL and some other network. This policy is in line with the autonomous networking ideas presented in [RFC7576].

The Realm-Local multicast address is currently used by MPL to propagate the multicast message to all receivers and forwarders within a mesh network. The multicast propagation is limited to a mesh network with a common Layer 2. For example, a Low-Power Wireless Personal Area Network (LoWPAN) is defined by an IEEE 802.15.4 Layer 2 mesh network, composed of all connected nodes sharing the same Personal Area Network (PAN) ID [RFC4944].

The network concept differs between mesh network technologies. This document maps a general network identifier to the specific network identifier of existing mesh technologies.

In current and projected deployments, there is a requirement to propagate a multicast message beyond the boundaries of the mesh network in which it originated, independent of the mesh technology.

Consider the case where propagation over two mesh networks is required. In one example, each mesh network has a border router and the two border routers are connected with an Ethernet link. In another example, each mesh network is connected to its own network interface connected to the same border router. In both cases, an Admin-Local multicast message originating in one network needs to propagate into the other mesh network. The boundary of the Admin-Local scope is administratively configured.

This document describes an "MPL4 router" that forwards MPL messages with a multicast address with Admin-Local scope to all interfaces connected to links that connect to other MPL-enabled interfaces. The MPL4 router enables all its interfaces for MPL messages and allocates an additional variable, MPL_BLOCKED, that either permits or forbids the forwarding of MPL messages.

The MPL4 router uses the following technique to establish over which links MPL4 messages must be forwarded: The MPL4 router listens on its interfaces for the arrival of MPL4 messages. When MPL4 messages arrive over an interface, the MPL4 router records this interface in the set of interfaces over which incoming MPL4 messages are forwarded. The MPL4 router regularly sends MPL4 messages over its interfaces to provoke the return of MPL4 messages to maintain the set of forwarding interfaces.

It is expected that the private network of an organization, building, or home is connected to the Internet via the edge routers provided by an ISP. The intention is that MPL messages with multicast addresses of Admin-Local scope are freely forwarded within the private network but are never forwarded outside the private network by edge routers.

1.1. 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 [RFC2119].

1.2. Terminology and Acronyms

This document uses terminology defined in [RFC7731] and [RFC7346]. In addition, the following terms are used in this document:

- MPL4: MPL with Admin-Local scope 4.
- MPL4 message: an MPL Data Message with a destination multicast address of scope 4.
- MPL4 zone: a convex zone of interconnected interfaces over which MPL messages with Admin-Local scope propagate. An MPL4 zone is bounded by a zone as defined in [RFC4007].
- MPL4 router: automatically determines the MPL4 zone in which MPL messages with Admin-Local scope can be propagated.

2. Network Identifier

Links may have the concept of a channel. For example, in wireless networks, such a channel is associated with a communication frequency. Additionally, for some link technologies, several networks can coexist using the same channel. For these link technologies, a network identifier exists. The network identifier is determined by the link technology specification. When no network identifier exists for a given link, the network identifier has the value "any".

2.1. IEEE 802.15.4

IPv6 over IEEE 802.15.4 is described in [RFC4944]. A LoWPAN is composed of the nodes connected by an IEEE 802.15.4 mesh sharing the same PAN ID. The PAN ID identifies a network in the IEEE 802.15.4 mesh. Several networks with different PAN IDs can coexist on the same channel [IEEE802.15.4]. The PAN ID of an interface is defined when the interface is enabled. The value of the network identifier of an IEEE 802.15.4 link is the value of the PAN ID.

2.2. IEEE 802.11

IP over IEEE 802.11 is described in [RFC5416]. The Service Set Identifier (SSID) identifies a network in the IEEE 802.11 link. Several networks with different SSIDs can coexist on the same channel [IEEE802.11]. The SSID of an interface is defined when the interface is switched on. The value of the network identifier of an IEEE 802.11 link is the value of the SSID.

2.3. ITU-T G.9959

IPv6 over ITU-T G.9959 is specified in [RFC7428]. The HomeID identifies a network of connected nodes [G.9959]. Several HomeIDs can coexist within communication range, but nodes adhering to a network with a given HomeID cannot communicate with nodes adhering to a network with a different HomeID. The value of the network identifier of a G.9959 link is the value of the HomeID.

2.4. BLUETOOTH(R) Low Energy

IPv6 over Bluetooth low energy (BTLE) is specified in [RFC7668]. The medium is specified in [BTLE]. BTLE does not know the concept of multiple networks in one channel. The value of the network identifier of a BTLE link is "any".

3. MPL4 Router

The concept of an MPL4 router serves to automatically determine the MPL4 zone in which MPL messages with a scope 4 multicast address can propagate. The MPL4 router periodically executes an algorithm that determines the presence of MPL Interfaces on the links connected to its interfaces. When no MPL Interfaces are present on a given link, the corresponding MPL Interface is signaled as not being part of the MPL4 zone.

3.1. MPL Interface Parameters

One parameter is associated with every MPL Interface in the MPL4 router, and two parameters are associated with the behavior of the MPL4 router as a whole.

- MPL_BLOCKED: Boolean value that indicates whether or not the associated interface belongs to the MPL4 zone.
- MPL_CHECK_INT: Integer that indicates the time interval between successive activations of the MPL4 router algorithm, in seconds.
- MPL_TO: Integer that indicates the interval in which MPL messages are expected to be received, in seconds.

3.2. Determination of MPL4 Zone

All interfaces of the MPL4 router MUST be associated with the following MPL protocol parameters, as described in [RFC7731]: PROACTIVE_FORWARDING, DATA_MESSAGE_IMIN, DATA_MESSAGE_IMAX, DATA_MESSAGE_K, and DATA_MESSAGE_TIMER_EXPIRATIONS. Upon startup of the MPL4 router, the parameters associated with all interfaces are assigned the following values: PROACTIVE_FORWARDING = TRUE, MPL_BLOCKED = false. All interfaces MUST subscribe to the multicast addresses ALL_MPL_FORWARDERS scope 3 and scope 4.

The MPL4 router executes the following algorithm for each interface:

- With a frequency determined by the value of MPL_CHECK_INT, the MPL4 router sends an MPL4 message on each interface with a header that includes the MPL Option [RFC7731]; the message is sent to multicast address ALL_MPL_FORWARDERS with scope 4.
- When, within an interval determined by the value of MPL_TO no MPL message is received, the value of MPL_BLOCKED is set to TRUE.
- On reception of an MPL4 message, the value of MPL_BLOCKED of the receiving interface is set to false.

This protocol leads to a state where for each interface MPL_BLOCKED is set to false if and only if MPL-enabled interfaces are connected to the link associated with the interface. When an MPL message is submitted to an MPL-enabled interface called "Interface A" in the MPL router, the Trickle algorithm [RFC6206] is activated to send the MPL message. The MPL4 message with multicast address ALL_MPL_FORWARDERS scope 4 is accepted by every interface connected to the link that has subscribed to ALL_MPL_FORWARDERS with scope 4. On acceptance of the MPL4 message by an interface called "Interface B", the MPL4 message

is returned with Trickle over Interface B. Consequently, the MPL4 message is received by the originating Interface A, after which MPL_BLOCKED is set to false.

When a new node is connected to the link, it can immediately send an MPL4 message, or it can wait for the reception of an MPL4 message to announce its intention to be part of the MPL4 zone.

4. Admin-Local Policy

This section begins by specifying what types of multicast messages arriving at an interface are legal. It continues with a description of forwarding legal Admin-Local multicast messages over other MPL Interfaces.

The policy for forwarding Admin-Local multicast messages automatically to an MPL Interface is specified as a function of the state of the MPL Interface and the multicast message. The state of the multicast message is determined by the presence of the MPL Option [RFC7731] and the destination multicast address. The state of the MPL Interface is determined by the subscribed multicast addresses, the zone index [RFC4007], and the values of the PROACTIVE_FORWARDING parameter and the MPL_BLOCKED parameter of the MPL Interface.

When the zone is undefined or not enabled, all interfaces have the same zone index.

4.1. Legal Multicast Messages

Multicast messages can be created within the node by an application or can arrive at an interface.

A multicast message created at a source (MPL Seed) is legal when it conforms to the properties described in Section 9.1 of [RFC7731].

A multicast message received at a given interface is legal when:

- The message carries an MPL Option (MPL message) and the incoming MPL Interface is subscribed to the destination multicast address.
- The message does not carry an MPL Option and the interface has expressed interest in receiving messages with the specified multicast address via Multicast Listener Discovery (MLD) [RFC3810] or IGMP [RFC3376]. The message was forwarded according to Protocol Independent Multicast - Dense Mode (PIM-DM) [RFC3973] or Protocol Independent Multicast - Sparse Mode (PIM-SM) [RFC4601].

Illegal multicast messages are discarded.

4.2. Forwarding Legal Packets

A legal multicast message received at a given interface is assigned the network identifier of the interface of the incoming link. A message that is created within the node is assigned the network identifier "any".

Two types of legal multicast messages are considered in Section 4.1: (1) MPL messages and (2) multicast messages that do not carry the MPL Option.

4.2.1. MPL Message

MPL messages are forwarded on MPL Interfaces using the Trickle parameter values assigned to the MPL Interface according to the following rules:

- Link-Local (scope 2) MPL messages are not forwarded.
- Realm-Local (scope 3) MPL messages are forwarded on all MPL Interfaces where all of the following are true:
  - The multicast address to which the MPL Interface subscribes is the same as the multicast address of the MPL message.
  - The zone index of the MPL Interface is the same as the zone index of the MPL Interface on which the MPL message was received.
  - The MPL Interface has PROACTIVE_FORWARDING set to TRUE.
  - The assigned network identifier of the MPL message is "any", or the assigned network identifier of the MPL message is equal to the network identifier of the MPL Interface.
- Admin-Local (scope 4) MPL messages are forwarded on all MPL Interfaces that are subscribed to the same multicast address, have the same zone index, have PROACTIVE_FORWARDING set to TRUE, and have MPL_BLOCKED set to false.
- MPL messages that encapsulate a message with a multicast scope of 5 or higher are decapsulated and forwarded over the interface when the interface is subscribed to the multicast address of the decapsulated message.

4.2.2. Multicast Messages without MPL Option

Multicast messages without the MPL Option are forwarded on MPL Interfaces according to the following rules:

- Link-Local (scope 2), Realm-Local (scope 3), and Admin-Local (scope 4) multicast messages are not forwarded.
- Multicast messages with a multicast scope of 5 or higher are encapsulated in an MPL message with destination address ALL_MPL_FORWARDERS with scope 4. The resulting message is then treated as described in Section 4.2.1.

4.3. Encryption Rules

An incoming message protected at Layer 2 MUST be subsequently re-protected at Layer 2 at all outgoing interfaces. Incoming messages are integrity checked and optionally decrypted at the incoming interface at Layer 2 using the keys and protection algorithm appropriate to the incoming interface's network and are re-protected at the outgoing interface using the keys and protection algorithm appropriate to the outgoing interface's network. It may be necessary to assess the relative levels of protection on the respective interfaces and apply policy rules -- for example, to avoid downgrading security where one network has a lower level of security than another.

An incoming MPL4 message that is not protected at Layer 2 MUST NOT be re-protected at Layer 2 at all outgoing interfaces.

5. MPL Domains and Zones

An MPL Domain is a scope zone in which MPL Interfaces subscribe to the same MPL Domain Address [RFC7731]. In accordance with [RFC4007], a zone boundary passes through a node. For example, a small Low-Power and Lossy Network (LLN) node usually has one MPL mesh interface that is subscribed to the ALL_MPL_FORWARDERS multicast address with a scope value of 3 (Realm-Local) [RFC7346]. The node interface belongs to the zone, and the corresponding zone boundary does not pass through this node. In the border router with MPL Interfaces subscribed to the multicast address ALL_MPL_FORWARDERS with scope value 3, the zone usually includes this single interface and excludes all other interfaces. A notable exception is provided by a node where MPL Interfaces of the same technology share the same network identifier. These interfaces belong to the same MPL4 zone when the interfaces share the same zone index.

In an MPL4 router, every MPL Interface subscribes to the Admin-Local ALL_MPL_FORWARDERS multicast address in addition to the Realm-Local ALL_MPL_FORWARDERS address.

Every interface that belongs to an MPL Domain that extends over border routers MUST be subscribed to the Admin-Local ALL_MPL_FORWARDERS address.

The MPL4 zone corresponding with the MPL multicast address ALL_MPL_FORWARDERS with scope 4 (Admin-Local) applies to border routers with multiple interfaces, of which at least one interface is MPL enabled and is subscribed to multicast address ALL_MPL_FORWARDERS with scope 4. In a border router, all MPL-enabled interfaces that subscribe to the ALL_MPL_FORWARDERS address with scope 4 and for which MPL_BLOCKED is false belong to the same MPL4 zone when the interfaces share the same zone index.

MPL4 messages remain bounded within a zone as defined in [RFC4007]. Consequently, MPL4 messages cannot be routed between interfaces belonging to different zones. When the concept of zone is unknown or disabled in a router, all interfaces belong to the same zone. For example, consider a router with five interfaces, where Interfaces A and B belong to zone 1 and Interfaces C, D, and E belong to zone 2. MPL4 messages can be routed freely between Interfaces A and B, and freely between Interfaces C, D, and E. However, an MPL4 message MUST NOT be routed from Interface A to Interface D.

6. Default Parameter Values

Three parameters are created by this document. Their values are related to the Trickle timer intervals.

- MPL_TO = DATA_MESSAGE_IMAX times 2, which leaves enough time to receive the second response message.
- MPL_CHECK_INT = 5 minutes, which means that a reaction to a network malfunction happens within 5 minutes.
- MPL_BLOCKED = TRUE, which means that the interface has not received MPL-enabled messages to include the interface in the MPL4 zone.

7. Security Considerations

The security considerations of [RFC7731] also apply to MPL4 routers.

The sending of MPL4 messages by a malicious node can have unwanted consequences, as explained by the following example. It is not unusual for a wired (e.g., Ethernet) link to be used between two floors or sections of an LLN, as radio propagation through reinforced concrete is generally poor. The MPL4 zone can thus envelop multiple routers, meshes, and links. It is possible that a malicious node could connect to a wired link on which no MPL-enabled nodes are foreseen. In this example configuration, the malicious node can send MPL4 messages to the MPL4 router interfaces. When nothing is done, the MPL4 routers will consequently distribute MPL4 messages from one mesh over the wired link to the next mesh, although the wired link was not expected to transport MPL4 messages.

To understand the consequences of this unwanted behavior, the following cases should be distinguished:

- The source mesh uses Layer 2 encryption.
- The MPL4 router can be managed.

The four possible combinations are discussed below:

Layer 2 unsecured, router unmanaged: In this case, MPL4 messages are freely distributed over meshes and links that are interconnected by MPL4 routers within a zone. The MPL-enabled (malicious) nodes can read all MPL4 messages and distribute MPL4 messages over a network limited by a zone. This situation can be acceptable for an isolated network within a clearly defined space, where the connection of nodes can be tightly controlled. A completely wired LLN, e.g., such as is seen in BACnet (a protocol for building automation and control networks) [BACnet] is an example of an unencrypted LLN that would be considered physically secure.

Layer 2 secured, router unmanaged: In this case, MPL4 messages are freely distributed over meshes and links that are interconnected by MPL4 routers within a zone. Following the rules of Section 4.3, the MPL4-enabled (malicious) nodes cannot read the MPL4 messages, and MPL4 messages sent by the malicious node are not accepted by other nodes. This situation is acceptable for a home network or managed network extending over precisely one zone, occupying a clearly defined physical space, where ease of installation is important. In such a network, the presence of the malicious node is not different from any other malicious node that

tries to send messages over Layer 2 protected links. Because the network occupies exactly one zone, the MPL4 message distribution cannot be extended outside the network.

Layer 2 unsecured, router managed: In this case, the distribution of MPL4 messages over MPL4 router interfaces can be limited to those interfaces for which a manager has enabled MPL, as well as a set of multicast addresses. The malicious node cannot extend the distribution of MPL4 messages over unwanted interfaces. It is important that the handling of the interfaces by the manager is protected. However, MPL4 messages sent over the mesh can be interpreted by malicious nodes, and malicious messages can be injected into the set of meshes and links that are connected by the MPL4 routers for which the manager enabled the interfaces. This situation can be practical for interconnected links and meshes that are connected to a LAN over a limited period -- for example, during installation of the interconnected meshes and links.

Layer 2 secured, router managed: In this case, the distribution of MPL4 messages over MPL4 router interfaces can be limited to those interfaces for which a manager has enabled MPL, as well as a set of multicast addresses. Following the rules of Section 4.3, the malicious node cannot extend the distribution of MPL4 messages over unwanted interfaces, and MPL4 messages sent by the malicious node are not accepted by other nodes. It is important that the handling of the interfaces by the manager is protected. The MPL-enabled (malicious) nodes cannot read the MPL4 messages, and MPL4 messages sent by the malicious node are not accepted by other nodes. Depending on the number of managed interfaces, the network can progressively pass from autoconfigured to fully administratively controlled.

8. References

8.1. 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>.

[RFC3810] Vida, R., Ed., and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <http://www.rfc-editor.org/info/rfc3810>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, DOI 10.17487/RFC3376, October 2002, <http://www.rfc-editor.org/info/rfc3376>.

[RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, DOI 10.17487/RFC4007, March 2005, <http://www.rfc-editor.org/info/rfc4007>.

[RFC5416] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, DOI 10.17487/RFC5416, March 2009, <http://www.rfc-editor.org/info/rfc5416>.

[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>.

[RFC7346] Droms, R., "IPv6 Multicast Address Scopes", RFC 7346, DOI 10.17487/RFC7346, August 2014, <http://www.rfc-editor.org/info/rfc7346>.

[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>.

[IEEE802.15.4] IEEE, "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE 802.15.4, DOI 10.1109/ieeestd.2011.6012487, <http://ieeexplore.ieee.org/servlet/opac?punumber=6012485>.

[IEEE802.11] IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE 802.11-2012, DOI 10.1109/ieeestd.2012.6178212, <http://ieeexplore.ieee.org/servlet/opac?punumber=6178209>.

[G.9959] International Telecommunication Union, "Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications", ITU-T Recommendation G.9959, January 2015, <http://www.itu.int/rec/T-REC-G.9959>.

[BTLE] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 4.1", December 2013, <https://www.bluetooth.org/en-us/specification/adopted-specifications>.

8.2. Informative References

[RFC3973] Adams, A., Nicholas, J., and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, DOI 10.17487/RFC3973, January 2005, <http://www.rfc-editor.org/info/rfc3973>.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, DOI 10.17487/RFC4601, August 2006, <http://www.rfc-editor.org/info/rfc4601>.

[RFC7576] Jiang, S., Carpenter, B., and M. Behringer, "General Gap Analysis for Autonomic Networking", RFC 7576, DOI 10.17487/RFC7576, June 2015, <http://www.rfc-editor.org/info/rfc7576>.

[RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015, <http://www.rfc-editor.org/info/rfc7428>.

[RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <http://www.rfc-editor.org/info/rfc7668>.

[BACnet] "BACnet Webpage", <http://www.bacnet.org>.

Acknowledgements

This document reflects discussions and remarks from several individuals, including (in alphabetical order) Scott Bradner, Esko Dijk, Adrian Farrel, Matthew Gillmore, Joel Halpern, Steve Hanna, Michael Richardson, and Pascal Thubert.

Authors' Addresses

Peter van der Stok
Consultant

Email: consultancy@vanderstok.org

Robert Cragie
ARM Ltd.
110 Fulbourn Road
Cambridge CB1 9NJ
United Kingdom

Email: robert.cragie@arm.com