MPL forwarder policy for multicast with admin-local scope
draft-ietf-roll-admin-local-policy-01

Abstract

   The purpose of this document is to specify an automated policy for
   the routing of MPL multicast messages with admin-local scope in a
   border router.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

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

   "Interface-Local, Link-Local, and Realm-Local scope boundaries are
   automatically derived from physical connectivity or other, non-
   multicast related configuration. 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.
   This draft describes an automated policy for the MPL forwarding of
   multicast messages with admin-local scope within a border router.
   This wish is in line with the autonomous networking ideas presented
   in [I-D.irtf-nmrg-an-gap-analysis].

   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 LoWPAN is defined
by an IEEE 802.15.4 layer-2 mesh network, composed of all connected
nodes sharing the same 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 it originated in 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 permits(forbids) the
forwarding of MPL messages.

It is expected that the network of an organization, building, or
home, is connected to the Internet via the edge routers provided by
an ISP. The intention is that within the network of an organization,
building, or home, MPL messages with multicast addresses of admin-
local scope are freely forwarded but are never forwarded to edge
routers which MUST not enable their interfaces for MPL messages.

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
[I-D.ietf-roll-trickle-mcast] and [RFC7346]. In addition, the
following terms are used in this document:

   o MPL4 message: an MPL DATA message with a destination multicast
      address of scope 4.

   o MPL4 router: automatically determines the zone in which MPL
      messages with admin-local scope can be propagated.

   o MPL4 zone: a convex zone of interconnected interfaces over which
      MPL messages with admin-local scope propagate. [RFC4007].

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 "undefined".

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 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 a 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 [I-D.ietf-6lo-lowpanz]. 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 Low Energy

IPv6 over BLUETOOTH Low Energy (BTLE) is specified in
[I-D.ietf-6lo-btle].   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
zone in which MPL messages with an 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 signalled as not being part of the
MPL 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 behaviour of the
MPL4 router as a whole.

o MPL_BLOCKED: Boolean value that indicates whether the associated
   interface belongs to the MPL zone.

o MPL_CHECK_INT: integer that indicates the time interval between
   successive activations of the MPL4 router algorithm in seconds.

o MPL_TO: integer that indicates the interval in which MPL messages
   are expected in seconds.

3.2. Determination of MPL zone

All interfaces of the MPL4 router MUST be associated with following
parameters coming from MPL protocol [I-D.ietf-roll-trickle-mcast]:
PROACTIVE_FORWARDING, DATA_MESSAGE_IMIN, DATA_MESSAGE_IMAX,
DATA_MESSAGE_K, DATA_MESSAGE_TIMER_EXPIRATIONS. At start-up 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:

o 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 and is sent to multicast address
   ALL_MPL_FORWARDERS with scope 4.

   o 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.

   o At reception of an MPL4 message with a multicast address with
      scope 4, 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 A- in the MPL router,
   the TRICKLE algorithm 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 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 can wait for the reception of an MPL4 message to
   announce its intention to be part of the MPL zone.

4. Admin-Local policy

   The section starts with specifying what 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 a MPL interface is specified as 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
   and the destination multicast address. The state of the MPL
   interface is determined by the subscribed multicast addresses, and
   the values of the PROACTIVE_FORWARDING parameter and the MPL_BLOCKED
   parameter of the MPL interface.

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 [I-D.ietf-roll-trickle-mcast].

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

o   The message carries an MPL option (MPL message) and the incoming MPL interface is subscribed to the destination multicast address.

o   The message does not carry an MPL option, the multicast address is unequal to ALL_MPL_FORWARDERS scope 4 or scope 3, and the interface has expressed interest to receive messages with the specified multicast address via MLD [RFC3810] or via IGMP [RFC3376]. The message was sent on according to PIM-DM [RFC3973] or according to 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: (1) MPL messages, and (2) multicast messages which 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:

o   Link-local (scope 2) MPL messages are not forwarded.

o   Realm-local (scope 3) MPL messages are forwarded on all MPL interfaces that are subscribed to the same multicast address and have PROACTIVE-FORWARDING set to true, and the assigned network identifier of the multicast message is identical to the network identifier of the MPL interface, or the assigned network identifier of the multicast message is "any".

o   Admin-local (scope 4) MPL messages are forwarded on all MPL interfaces that are subscribed to the same multicast address, have PROACTIVE-FORWARDING set to true, and have MPL_BLOCKED set to false.

o MPL messages with a multicast scope of 5 or higher MUST
   encapsulate a message with the same multicast address without MPL
   option. The decapsulated message can be forwarded over an
   interface when the interface is subscribed with MLD to the same
   multicast address.

4.2.2. Multicast messages without MPL option

Multicast messages without MPL option are forwarded on MPL interfaces
according to the following rules:

o Link-local (scope 2) messages or realm-local (scope 3) multicast
   messages are not forwarded.

o Admin-local (scope 4) multicast messages are encapsulated with a
   header carrying the MPL option and are forwarded on al MPL
   interfaces that are subscribed to the multicast address, have
   PROACTIVE_FORWARDING set to true, and have MPL_BLOCKED set to
   false.

o Multicast messages with a multicast scope of 5 or higher are
   encapsulated with a header carrying the MPL option and are
   forwarded on al MPL interfaces that are subscribed to the
   multicast address, have PROACTIVE_FORWARDING set to true, and have
   MPL_BLOCKED set to false. In addition these messages follow the
   Multicast forwarding rules as specified by PIM [RFC3973],
   [RFC4601] according to group specifications enabled by MLD
   [RFC3810] or IGMP [RFC3376].

5. MPL domains and zones

An MPL domain is a scope zone in which MPL interfaces subscribe to
the same MPL Domain Address [I-D.ietf-roll-trickle-mcast]. In
accordance with [RFC4007] a zone boundary passes through a node. For
example, a small LLN node usually has one MPL mesh interface which is
enabled 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 enabled to the
multicast address ALL_MPL_FORWARDERS with scope value 3, the zone
includes usually 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 zone.

In an MPL4 router, every MPL interface subscribes to the admin_local
ALL_MPL_FORWARDERS multicast address next 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 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 which
subscribe to the ALL_MPL_FORWARDERS address with scope 4 and for
which MPL_BLOCKED is false belong to the same zone.

6. Default parameter values

Three parameters are created in this draft. Their values are related
to the trickle timer intervals.

MPL_TO = DATA_MESSAGE_IMAX times 2. Which leaves the time to receive
the second response message.

MPL_CHECK_INT = 5 minutes. Which means that a reaction to network
malfunctioning happens within 5 minutes.

MPL_BLOCKED = true. Which means that the interface must have
received MPL-enabled messages to include the interface to the zone.

7. Security Considerations

Refer to the security considerations of
[I-D.ietf-roll-trickle-mcast].

MPL enabled interfaces MUST subscribe to the ALL_MPL_FORWARDERS
address with scope 3 and scope 4. In the latter case the nodes may
become flooded by multicast messages with as destination
ALL_MPL_FORWARDERS address with scope 4 coming from outside the zone
corresponding with the connected mesh networks. Therefore, Multicast
messages with address ALL_MPL_FORWADERS scope 4 and scope 3 cannot be
forwarded from sources out of the zone corresponding with the scope 4
address.

The enabling of the interfaces for a given set of multicast addresses
and the setting of the MPL parameter values must be done in a secure
way, such that they cannot be set or modified by unauthorized nodes.
That means a setting of the parameters with secured means, or
initializing the parameter values in the factory without
possibilities for change afterwards.

8. IANA Considerations

No considerations for IANA are formulated in this document.

9. Acknowledgements

This document reflects discussions and remarks from several
individuals including (in alphabetical order): Esko Dijk, Matthew
Gillmore, Michael Richardson, and Pascal Thubert.

10. Change log

Version 00 - version 01

o Default parameter values declared

o Security section extended

o scope 5 of higher messages specified

o messages with address ALL_MPL_FORWARDERS are not allowed from
   outside zone

Changes from personal version to WG version-00.

o Aligned terminology with MPL terminology
   [I-D.ietf-roll-trickle-mcast]

o Text on MPL4 router included

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery
           Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
           Architecture", RFC 4291, February 2006.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler,
           "Transmission of IPv6 Packets over IEEE 802.15.4
           Networks", RFC 4944, September 2007.

   [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A.
              Thyagarajan, "Internet Group Management Protocol, Version
              3", RFC 3376, October 2002.

   [RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and
              B. Zill, "IPv6 Scoped Address Architecture", RFC 4007,
              March 2005.

   [RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and
              Provisioning of Wireless Access Points (CAPWAP) Protocol
              Binding for IEEE 802.11", RFC 5416, March 2009.

   [RFC7346] Droms, R., "IPv6 Multicast Address Scopes", RFC 7346,
              August 2014.

   [I-D.ietf-roll-trickle-mcast]
              Hui, J. and R. Kelsey, "Multicast Protocol for Low power
              and Lossy Networks (MPL)", draft-ietf-roll-trickle-
              mcast-09 (work in progress), April 2014.

   [IEEE802.15.4]
              "IEEE 802.15.4 - Standard for Local and metropolitan area
              networks -- Part 15.4: Low-Rate Wireless Personal Area
              Networks", <IEEE Standard 802.15.4>.

   [IEEE802.11]
              "IEEE 802.11 - Telecommunications and information exchange
              between systems Local and metropolitan area networks --
              Part 11: Wireless LAN Medium Access Control (MAC) and
              Physical Layer (PHY) Specifications", <IEEE Standard
              802.11>.

   [G.9959]   "ITU-T G.9959 Short range narrow-band digital
              radiocommunication transceivers - PHY and MAC layer
              specifications", <ITU-T G.9959>.

   [btle]   "BLUETOOTH Specification Version 4.0", <BLUETOOTH low
              energy>.

11.2. Informative References

   [RFC3973] Adams, A., Nicholas, J., and W. Siadak, "Protocol
              Independent Multicast - Dense Mode (PIM-DM): Protocol
              Specification (Revised)", RFC 3973, January 2005.

   [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,
              "Protocol Independent Multicast - Sparse Mode (PIM-SM):
              Protocol Specification (Revised)", RFC 4601, August 2006.

   [I-D.irtf-nmrg-an-gap-analysis]
              Jiang, S., Carpenter, B., and M. Behringer, "Gap Analysis
              for Autonomic Networking", draft-irtf-nmrg-an-gap-
              analysis-02 (work in progress), October 2014.

   [I-D.ietf-6lo-lowpanz]
              Brandt, A. and J. Buron, "Transmission of IPv6 packets
              over ITU-T G.9959 Networks", draft-ietf-6lo-lowpanz-07
              (work in progress), September 2014.

   [I-D.ietf-6lo-btle]
              Nieminen, J., Savolainen, T., Isomaki, M., Patil, B.,
              Shelby, Z., and C. Gomez, "Transmission of IPv6 Packets
              over BLUETOOTH(R) Low Energy", draft-ietf-6lo-btle-03
              (work in progress), September 2014.

Authors' Addresses

   Peter van der Stok
   Consultant

   Email: consultancy@vanderstok.org

   Robert Cragie
   Gridmerge

   Email: robert.cragie@gridmerge.com