Internet Engineering Task Force (IETF)
Request for Comments: 6553
Category: Standards Track
ISSN: 2070-1721
March 2012

J. Hui
JP. Vasseur
Cisco Systems

The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams

Abstract

The Routing Protocol for Low-Power and Lossy Networks (RPL) includes routing information in data-plane datagrams to quickly identify inconsistencies in the routing topology. This document describes the RPL Option for use among RPL routers to include such routing information.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

RPL is a distance vector IPv6 routing protocol designed for Low-Power and Lossy Networks (LLNs) [RFC6550]. Such networks are typically constrained in energy and/or channel capacity. To conserve precious resources, a routing protocol must generate control traffic sparingly. However, this is at odds with the need to quickly propagate any new routing information to resolve routing inconsistencies quickly.

To help minimize resource consumption, RPL uses a slow proactive process to construct and maintain a routing topology but a reactive and dynamic process to resolving routing inconsistencies. In the steady state, RPL maintains the routing topology using a low-rate beaconing process. However, when RPL detects inconsistencies that may prevent proper datagram delivery, RPL temporarily increases the beacon rate to quickly resolve those inconsistencies. This dynamic rate control operation is governed by the use of dynamic timers also referred to as "Trickle" timers and defined in [RFC6206]. In contrast to other routing protocols (e.g., OSPF [RFC2328]), RPL detects routing inconsistencies using data-path verification, by including routing information within the datagram itself. In doing so, repair mechanisms operate only as needed, allowing the control and data planes to operate on similar time scales. The main motivation for data-path verification in LLNs is that control-plane traffic should be carefully bounded with respect to the data traffic. Intuitively, there is no need to solve routing issues (which may be temporary) in the absence of data traffic.

RPL constructs a Directed Acyclic Graph (DAG) that attempts to minimize path costs to the DAG root according to a set of metrics and Objective Functions. There are circumstances where loops may occur, and RPL is designed to use a data-path loop detection method. This is one of the known requirements of RPL, and other data-path usage might be defined in the future.

To that end, this document defines a new IPv6 option, called the RPL Option, to be carried within the IPv6 Hop-by-Hop header. The RPL Option is only for use between RPL routers participating in the same RPL Instance.

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 RFC 2119 [RFC2119].

2. Overview

The RPL Option provides a mechanism to include routing information with each datagram that a router forwards. When receiving datagrams that include routing information, RPL routers process the routing information to help maintain the routing topology.

Every RPL router along a packet’s delivery path processes and updates the RPL Option. If the received packet does not already contain a RPL Option, the RPL router must insert a RPL Option before forwarding it to another RPL router. This document also specifies the use of IPv6-in-IPv6 tunneling [RFC2473] when attaching a RPL option to a packet. Use of tunneling ensures that the original packet remains unmodified and that ICMP errors return to the RPL Option source rather than the source of the original packet.

3. Format of the RPL Option

The RPL Option is carried in an IPv6 Hop-by-Hop Options header, immediately following the IPv6 header. This option has an alignment requirement of 2n. The option has the following format:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                    |  Option Type  |  Opt Data Len |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |O|R|F|0|0|0|0|0| RPLInstanceID |          SenderRank           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         (sub-TLVs)                            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: RPL Option

Option Type: 0x63

Opt Data Len: 8-bit field indicating the length of the option, in octets, excluding the Option Type and Opt Data Len fields.

Down 'O': 1-bit flag as defined in Section 11.2 of [RFC6550]. The processing SHALL follow the rules described in Section 11.2 of [RFC6550].

Rank-Error 'R': 1-bit flag as defined in Section 11.2 of [RFC6550]. The processing SHALL follow the rules described in Section 11.2 of [RFC6550].

Forwarding-Error 'F': 1-bit flag as defined in Section 11.2 of [RFC6550]. The processing SHALL follow the rules described in Section 11.2 of [RFC6550].

RPLInstanceID: 8-bit field as defined in Section 11.2 of [RFC6550]. The processing SHALL follow the rules described in Section 11.2 of [RFC6550].

SenderRank: 16-bit field as defined in Section 11.2 of [RFC6550]. The processing SHALL follow the rules described in Section 11.2 of [RFC6550].

The two high order bits of the Option Type MUST be set to '01' and the third bit is equal to '1'. With these bits, according to [RFC2460], nodes that do not understand this option on a received packet MUST discard the packet. Also, according to [RFC2460], the values within the RPL Option are expected to change en route. The RPL Option Data Length is variable.

The action taken by using the RPL Option and the potential set of sub-TLVs carried within the RPL Option MUST be specified by the RFC of the protocol that uses that option. No sub-TLVs are defined in this document. A RPL device MUST skip over any unrecognized sub-TLVs and attempt to process any additional sub-TLVs that may appear after.

4. RPL Router Behavior

Datagrams sent between RPL routers MUST include a RPL Option or RPL Source Route Header ([RFC6554]) and MAY include both. A datagram including a Source Routing Header (SRH) does not need to include a RPL Option since both the source and intermediate routers ensure that the SRH does not contain loops.

When the router is the source of the original packet and the destination is known to be within the same RPL Instance, the router SHOULD include the RPL Option directly within the original packet. Otherwise, routers MUST use IPv6-in-IPv6 tunneling [RFC2473] and place the RPL Option in the tunnel header. Using IPv6-in-IPv6 tunneling ensures that the delivered datagram remains unmodified and that ICMPv6 errors generated by a RPL Option are sent back to the router that generated the RPL Option.

A RPL router chooses the next RPL router that should process the original packet as the tunnel exit-point. In some cases, the tunnel exit-point will be the final RPL router along a path towards the original packet's destination, and the original packet will only traverse a single tunnel. One example is when the final destination or the destination's attachment router is known to be within the same RPL Instance.

In other cases, the tunnel exit-point will not be the final RPL router along a path and the original packet may traverse multiple tunnels to reach the destination. One example is when a RPL router is simply forwarding a packet to one of its Destination-Oriented DAG (DODAG) parents. In this case, the RPL router sets the tunnel exit-point to a DODAG parent. When forwarding the original packet hop-by-hop, the RPL router only makes a determination on the next hop towards the destination.

A RPL router receiving an IPv6-in-IPv6 packet destined to it processes the tunnel packet as described in Section 3 of [RFC2473]. Before IPv6 decapsulation, the RPL router MUST process the RPL Option, if one exists. After IPv6 decapsulation, if the router determines that it should forward the original packet to another RPL router, it MUST encapsulate the packet again using IPv6-in-IPv6 tunneling to include the RPL Option. Fields within the RPL Option that do not change hop-by-hop MUST remain the same as those received from the prior tunnel.

RPL routers are responsible for ensuring that a RPL Option is only used between RPL routers:

1. For datagrams destined to a RPL router, the router processes the packet in the usual way. For instance, if the RPL Option was included using tunneled mode and the RPL router serves as the tunnel endpoint, the router removes the outer IPv6 header, at the same time removing the RPL Option as well.

2. Datagrams destined elsewhere within the same RPL Instance are forwarded to the correct interface.

3. Datagrams destined to nodes outside the RPL Instance are dropped if the outermost IPv6 header contains a RPL Option not generated by the RPL router forwarding the datagram.

To avoid fragmentation, it is desirable to employ MTU sizes that allow for the header expansion (i.e., at least 1280 + 40 (outer IP header) + RPL_OPTION_MAX_SIZE), where RPL_OPTION_MAX_SIZE is the maximum RPL Option header size for a given RPL network. To take advantage of this, however, the communicating endpoints need to be aware of the MTU along the path (i.e., through Path MTU Discovery). Unfortunately, the larger MTU size may not be available on all links (e.g., 1280 octets on IPv6 Low-Power Wireless Personal Area Network (6LoWPAN) links). However, it is expected that much of the traffic on these types of networks consists of much smaller messages than the MTU, so performance degradation through fragmentation would be limited.

5. Security Considerations

The RPL Option assists RPL routers in detecting routing inconsistencies. The RPL message security mechanisms defined in [RFC6550] do not apply to the RPL Option.

5.1. DAG Inconsistency Attacks

Using the Down 'O' flag and SenderRank field, an attacker can cause RPL routers to believe that a DAG inconsistency exists within the RPL Instance identified by the RPLInstanceID field. This attack would cause a RPL router to reset its DODAG Information Object (DIO) Trickle timer and begin transmitting DIO messages more frequently.

In order to avoid any unacceptable impact on network operations, an implementation MAY limit the rate of Trickle timer resets caused by receiving a RPL Option to no greater than MAX_RPL_OPTION_RANK_ERRORS per hour. A RECOMMENDED value for MAX_RPL_OPTION_RANK_ERRORS is 20.

5.2. Destination Advertisement Object (DAO) Inconsistency Attacks

In Storing mode, RPL routers maintain Downward routing state. Under normal operation, the RPL Option assists RPL routers in cleaning up stale Downward routing state by using the Forwarding-Error 'F' flag to indicate that a datagram could not be delivered by a child and is being sent back to try a different child. Using this flag, an attacker can cause a RPL router to discard Downward routing state.

In order to avoid any unacceptable impact on network operations, an implementation MAY limit the rate of discarding Downward routing state caused by receiving a RPL Option to no greater than MAX_RPL_OPTION_FORWARD_ERRORS per hour. A RECOMMENDED value for MAX_RPL_OPTION_FORWARD_ERRORS is 20.

In Non-Storing mode, only the Low-Power and Lossy Network Border Router (LBR) maintains Downward routing state. Because RPL routers do not maintain Downward routing state, the RPL Option cannot be used to mount such attacks.

6. IANA Considerations

IANA has assigned a new value in the Destination Options and Hop-by-Hop Options registry. The value is as follows:

Hex Value	Binary Value				
	act	chg	rest	Description	Reference
0x63	01	1	00011	RPL Option	[RFC6553]

As specified in [RFC2460], the first two bits indicate that the IPv6 node MUST discard the packet if it doesn't recognize the option type, and the third bit indicates that the Option Data may change en route. The remaining bits serve as the option type.

IANA has created a registry called RPL-option-TLV, for the sub-TLVs carried in the RPL Option header. New codes may be allocated only by IETF Review [RFC5226]. The type field is an 8-bit field whose value be between 0 and 255, inclusive.

7. Acknowledgements

The authors thank Jari Arkko, Ralph Droms, Adrian Farrel, Stephen Farrell, Richard Kelsey, Suresh Krishnan, Vishwas Manral, Erik Nordmark, Pascal Thubert, Sean Turner, and Tim Winter, for their comments and suggestions that helped shape this document.

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.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko, "The Trickle Algorithm", RFC 6206, March 2011.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

8.2. Informative References

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, March 2012.

Authors' Addresses

Jonathan W. Hui
Cisco Systems
170 West Tasman Drive
San Jose, California 95134
USA

Phone: +408 424 1547
EMail: jonhui@cisco.com

JP. Vasseur
Cisco Systems
11, Rue Camille Desmoulins
Issy Les Moulineaux 92782
France

EMail: jpv@cisco.com