

6MAN
Internet-Draft
Intended status: Standards Track
Expires: January 29, 2011

J. Hui
Arch Rock Corporation
P. Thubert
JP. Vasseur
Cisco Systems, Inc
July 28, 2010

Using RPL Headers Without IP-in-IP
draft-hui-6man-rpl-headers-00

Abstract

Routing for Low Power and Lossy Networks (RPL) is a routing protocol designed for Low power and Lossy Networks (LLNs). RPL includes routing information in IPv6 data plane datagrams to help maintain the routing topology. When forwarding a datagram into a RPL domain, a RPL router may need to expand the datagram to include routing information in IPv6 Extension headers. A generic solution has been defined that uses IP-in-IP tunneling to include RPL routing information. This document describes an alternative to inserting and removing RPL information in datagrams without the use of IP-in-IP tunneling.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 29, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

Internet-Draft

RPL Headers

July 2010

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	4
2.	Inserting Headers	5
3.	Removing Headers	6
4.	Security Considerations	7
5.	IANA Considerations	8
6.	References	9
6.1.	Normative References	9
6.2.	Informative References	9
	Authors' Addresses	10

1. Introduction

Routing for Low Power and Lossy Networks (RPL) is a distance vector IPv6 routing protocol designed for Low Power and Lossy networks (LLNs) [[I-D.ietf-roll-rpl](#)]. Such networks are typically constrained in resources (limited communication data rate, processing power, energy capacity, memory). When forwarding datagrams within a RPL domain, RPL requires those datagrams to carry routing information. RPL routing information may be included using a RPL Option within an IPv6 Hop-by-Hop Option header to perform routing loop detection and repair [[I-D.ietf-6man-rpl-option](#)]. RPL may also use a strict source route specified in an IPv6 Routing Header [[I-D.ietf-6man-rpl-routing-header](#)]. RPL uses source routing in LLNs composed of resource-constrained nodes that can maintain no more than a few routing entries.

Because the RPL routing information is only useful within a RPL domain, RPL Border Routers (referred to as LBRs in [[I-D.ietf-roll-terminology](#)]) are responsible for inserting and removing RPL information when forwarding datagrams into or out of a RPL domain. However, to nodes outside the RPL domain, there must not be any visible side effects of inserting RPL information. Unwanted side effects include:

1. Mutations to the IPv6 packet headers being processed hop-by-hop are not undone before exiting the RPL domain. Doing so affects how non-RPL routers process the datagram.
2. Mutations to the datagram are not undone before being sent back either partially or in whole to the source (e.g. in an ICMP error). Doing so affects how the source handles the returned datagram, such as examining the payload of an ICMP error.
3. Changing any values included in computing a security signature, such as the IPv6 Payload Length and Next Header values for the Integrity Check Value of the IP Authentication Header [[RFC4302](#)].

4. Generating ICMP Packet Too Big errors that do not correctly reflect the path MTU in the RPL domain due to inclusion of the RPL information.
5. Not being capable of generating the correct path MTU because its value is less than 1280 octets due to the size of RPL routing information.

The default mechanism for inserting and removing RPL information is by using IP-in-IP tunneling, encapsulating the existing packet with a new IPv6 header and including the RPL Option and/or routing header in

the outer IPv6 header. By tunneling the datagram, the original datagram is left unmodified. Furthermore, any ICMP errors return to the RPL router that inserted RPL information into the datagram. IP-in-IP tunneling avoids path MTU issues because the ICMP Packet Too Big error will return to the RPL router that inserted the headers, allowing it to perform IP fragmentation and requires no additional action by nodes outside the RPL domain.

However, where LLNs are severely constrained in resources, IP-in-IP tunneling may not be the most favorable solution. Use of IP-in-IP requires datagrams to carry two IPv6 headers, increasing header overhead and associated communication and memory requirements. Expanding existing header compression techniques to efficiently support IP-in-IP necessarily adds complexity. LLN nodes must also implement packet processing code that supports IP-in-IP, further increasing code complexity.

This document describes how to insert and remove RPL routing information without IP-in-IP tunneling such that no side effects are visible to nodes outside the RPL domain. This mode of forwarding without IP-in-IP tunneling is defined as transport mode. Note that transport mode is only provided as an option when IP-in-IP tunneling is not possible.

[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](#)].

[2.](#) Inserting Headers

This section specifies how a RPL router inserts RPL routing information into an existing IPv6 datagram. We define `rpl_info_size` as the number of octets required to carry RPL information in a particular datagram and can vary between datagrams (e.g. due to different lengths in source route).

1. If the source node is within the RPL domain, it MUST compute any security integrity checks as if no RPL information was inserted into the datagram. For example, the IPv6 Payload Length used for computing the integrity check should not include the octets required for carrying RPL information.
2. The RPL router SHOULD respect the IPv6 Extension header ordering recommended in [[RFC2460](#)].
3. If the datagram size after inserting RPL information exceeds the MTU of the directly attached link used to reach the next hop, the RPL router MUST send either an ICMP Packet Too Big error to the source. The RPL router MUST subtract `rpl_info_size` from the MTU value of the error-causing link and report that as the MTU value.

If the resulting MTU value is less than 1280 octets, the RPL router MUST suppress the ICMP Packet Too Big error and send an ICMP Destination Unreachable error back to the source instead.

[3.](#) Removing Headers

All RPL routing information MUST be removed in the following cases:

1. When forwarding datagrams outside the RPL domain.
2. Before computing any integrity check values for verification. For example, the IPv6 Payload Length used for computing the integrity check should not include the octets required for carrying RPL information.

The remainder of this section specifies how a RPL router removes RPL routing information in an existing IPv6 datagram.

1. Any RPL-specific IPv6 Extension headers MUST be removed from the

datagram, if any exist. The IPv6 Payload Length and corresponding Next Header fields MUST be updated to reflect their removal.

2. The RPL Option MUST be removed from the IPv6 Hop-by-Hop Options header of the datagram, if one exists.
3. If the RPL router is generating an ICMP error, the RPL router MUST remove any RPL information from the datagram in error before including it in the ICMP error's payload.
4. If the RPL router is generating an ICMP Packet Too Big error, the RPL router MUST subtract `rpl_info_size` from the MTU value of the error-causing link and report that as the MTU value in the message. If the resulting MTU value is less than 1280 octets, the RPL router MUST suppress the ICMP Packet Too Big error and send an ICMP Destination Unreachable error back to the source instead.

4. Security Considerations

The generation of ICMPv6 error messages may be used to attempt denial-of-service attacks by sending a large number of packets that exceed the MTU of the RPL domain. It is RECOMMENDED that an implementation correctly follows [Section 2.4 of \[RFC4443\]](#) to rate limit the generation of ICMPv6 messages.

[5.](#) IANA Considerations

This document does not require any action from IANA.

[6.](#) References

[6.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.
- [RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", [RFC 4443](#), March 2006.

[6.2.](#) Informative References

- [I-D.ietf-6man-rpl-option]
Hui, J. and J. Vasseur, "RPL Option for Carrying RPL Information in Data-Plane Datagrams", [draft-ietf-6man-rpl-option-00](#) (work in progress), July 2010.
- [I-D.ietf-6man-rpl-routing-header]
Hui, J., Vasseur, J., and D. Culler, "An IPv6 Routing Header for Source Routes with RPL", [draft-ietf-6man-rpl-routing-header-00](#) (work in progress), July 2010.
- [I-D.ietf-roll-rpl]
Winter, T., Thubert, P., and R. Team, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks", [draft-ietf-roll-rpl-10](#) (work in progress), June 2010.
- [I-D.ietf-roll-terminology]
Vasseur, J., "Terminology in Low power And Lossy Networks", [draft-ietf-roll-terminology-03](#) (work in progress), March 2010.
- [RFC4302] Kent, S., "IP Authentication Header", [RFC 4302](#), December 2005.

Internet-Draft

RPL Headers

July 2010

Authors' Addresses

Jonathan W. Hui
Arch Rock Corporation
501 2nd St. Ste. 410
San Francisco, California 94107
USA

Phone: +415 692 0828
Email: jhui@archrock.com

Pascal Thubert
Cisco Systems, Inc
Village d'Entreprises Green Side
400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Phone: +33 4 97 23 26 34
Email: pthubert@cisco.com

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

Email: jpv@cisco.com

Hui, et al.

Expires January 29, 2011

[Page 10]