Workgroup: ROLL
Internet-Draft:
draft-jadhav-roll-storing-rootack-03
Published: 9 November 2021
Intended Status: Standards Track
Expires: 13 May 2022
Authors: R.A. Jadhav, Ed.

RPL Storing Root-ACK

Abstract

This document explains problems with DAO-ACK handling in RPL Storing MOP and provides updates to RFC6550 to solve those problems.

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 https://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 13 May 2022.

Table of Contents

1. Introduction

RPL [RFC6550] specifies a proactive distance-vector routing scheme designed for LLNs (Low Power and Lossy Networks). RPL enables the network to be formed as a DODAG and supports storing mode and non-storing mode of operations. Non-storing mode allows reduced memory resource usage on the nodes by allowing non-BR nodes to operate without managing a routing table and involves use of source routing by the Root to direct the traffic along a specific path. In storing mode of operation the routing happens on hop-by-hop basis and intermediate routers need to maintain routing tables.

DAO messaging helps to install downstream routing paths in the DODAG. DAOs are generated on hop-by-hop basis. DAO may contain multiple RPL Control Options. The Target Option identifies the address prefix for which the route has to be installed and the corresponding Transit Information Option identifies the parameters (such as lifetime, freshness-counter, etc) for the target. The DAO base object contains the 'K' flag indicating that a DAO-ACK is sought by the sender. The DAO, DAO-ACK progresses on hop-by-hop basis all the way till Root. In non-storing MOP, the DAO from the target node is directly addressed to the Root and the Root responds with a DAO-ACK indicating path establishment status. However, in storing MOP, the DAO-ACK is immediately sent by the upstream parent. Thus in case of storing MOP, the target node cannot rely on DAO-ACK as an indication that the end to end (from the target node to Root) path has been established.

This draft highlights various issues with RPL DAO-ACK handling in Storing MOP. Section 4 of [I-D.ietf-roll-rpl-observations] provides

more context to the problem statement. The draft provides requirements to solve the issues and provides an updates to RFC6550 based on these requirements.

1.1. Requirements Language and Terminology

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].

MOP: Mode of Operation

NS-MOP: RPL Non-Storing Mode of Operation

S-MOP: RPL Storing Mode of Operation

Root-ACK: The Root-ACK syntax is same as DAO-ACK except that the Root-ACK is addressed directly to the peer who owns the target prefix. DAO-ACK in contrast is always sent using link-local IPv6 address in storing MOP.

DelayDAO: Section 9.5 of RFC6550 introduces a delay before the DAO transmission is initiated.

TIO: (Transit Information Option) Section 6.7.8 of RFC6550. TIO is an option usually carried in DAO message and augments control information for the advertised Target.

RUL: (RPL Unaware Leaf) [I-D.ietf-roll-unaware-leaves]

This document uses terminology described in [RFC6550].

2. Problems with DAO-ACK in Storing MOP

Consider the following topology for the subsequent description:

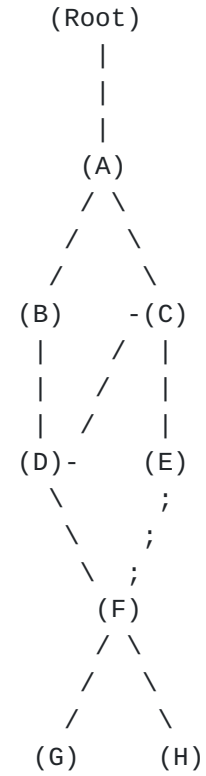

Figure 1: Sample topology

2.1. End to End Path Establishment Indication

Nodes need to know whether the end to end path till the Root has been established before they can initiate application traffic. In case of NS-MOP, the DAO is addressed to the Root from the Target node and the Root sends DAO-ACK directly addressed back to the target node. Thus in case of NS-MOP, the node can make use of this DAO-ACK as an indication whether the necessary routes have been installed. However, in case of Storing MOP, the DAO/DAO-ACK signaling happens at every hop.

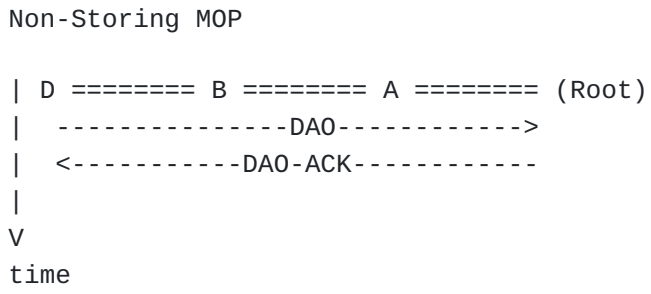

Figure 2: NS-MOP DAO/DAO-ACK handling

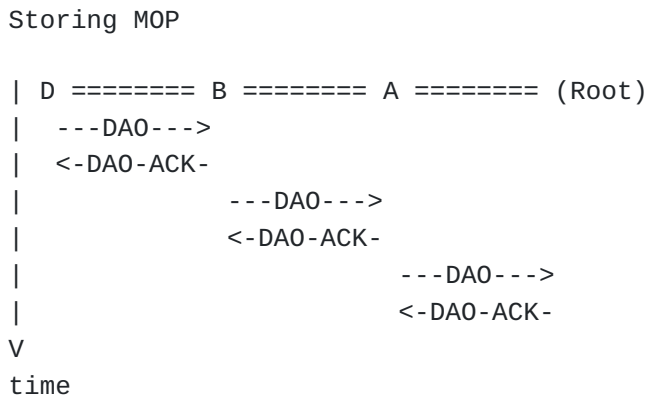

Figure 3: Storing MOP DAO/DAO-ACK handling

Note that in Storing-MOP, the DAO/DAO-ACK signaling happens on hop-by-hop basis and a DelayDAO timer is used before intermediate 6LRs generate the DAO. This would mean that the DAO reaching the Root may take several seconds. The target node should not generate the application traffic unless the end to end path is established.

Consider Figure 1, when node D sends a DAO, the node B receives the DAO and instantly sends back DAO-ACK. Node B then subsequently generates the DAO with Target as Node D and sends it to node A. The DAO with Target as Node D may take time (since the DAO is scheduled with DelayDAO timer by every node) to finally reach the Root at which point the end to end path is established. There is no way for node D to know when the end to end path is established. This information is needed for node D to initiate its application traffic. Initiating application traffic prior to this might almost certainly lead to application packet retries causing congestion in the network.

2.2. Target node is unaware if it needs to retry the DAO

It is possible that the intermediate 6LR goes down while attempting to generate DAO on behalf of the target node. In this case, the target node has no way of knowing to retry the DAO, in which case the route installation may not happen until the target node's DAO lifetime expires.

Consider Figure 1, assume that node A was generating DAO with Target node D and sending it to Root. Node A reboots before attempting to send DAO to Root. Node A has already sent DAO-ACK downstream to node B. In this case, the target node D is not aware that sending DAO has failed somewhere upstream. Note that as per RFC6550 upstream DAO is scheduled based on DelayDAO but DAO-ACK is sent instantaneously on DAO reception from downstream node.

2.3. RPL node acting as router for RULs

An RPL node may act as a router for RPL unware leaves as described in [I-D.ietf-roll-unaware-leaves]. Ideally an RPL node should start accepting RULs solicitation only after making sure that it has established itself in the network first. In Storing-MOP, there is no way to ascertain this.

3. Requirements for Root-ACK handling in Storing MOP

Following are the requirements:

Indicate end to end path establishment The Target node must know when to initiate the application traffic based on end to end path establishment.

Handle multiple targets in DAOs A DAO message may contain multiple Target Options. The Root-ACK mechanism must handle multiple targets in DAO.

Handle DAOs with address prefix RPL DAO Target Option may contain an address prefix i.e., not the full address.

Provide suitable way for target node to retry The Target node must have a way to know and retry the DAO in case the DAO transmission fails enroute.

Backward compatible with current DAO-ACK The current per hop DAO-ACK must function as it is. Legacy nodes should be able to operate without any changes.

4. Root-ACK from Root

The draft defines a way for the RPL Root to send the Root-ACK back directly addressed to the Target node. The Target node can receive the Root-ACK directly thus getting an indication that the end to end path till the Root has been successfully established. The Root-ACK uses the same syntax and message code as DAO-ACK. The only difference is that the Root-ACK is directly addressed to the Target node who owns the advertised prefix in the Target Option.

4.1. Transit Information Option update in DAO message

The Target node indicates that it wishes to receive Root-ACK directly from Root by setting the newly defined 'K' flag in Transit Information Option.

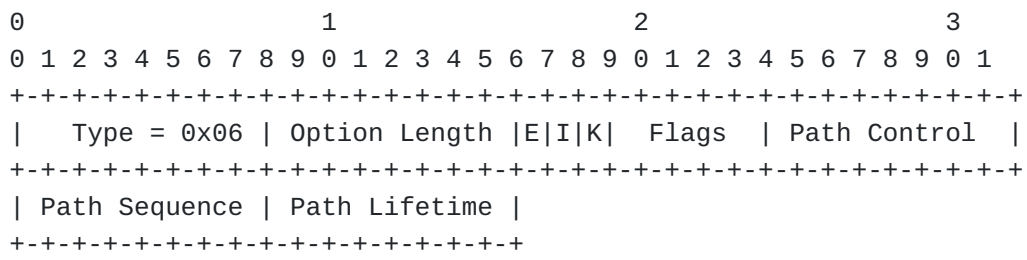

Figure 4: Updated Transit Information Option (New K flag added)

The K flag indicates that the Root of the RPLInstance MUST send a Root-ACK directly to the target node.

4.2. Root sends Root-ACK addressed to Target

On receiving a DAO with Transit Information Option with 'K' flag set, the Root MUST respond with a Root-ACK immediately to the address extracted from the corresponding Target Option.

The Root-ACK MUST contain the Transit Information Option with parameters copied from the DAO's Transit Information Option based on which this Root-ACK was generated. The PathSequence in the Transit Information Option helps the Target node to identify for which DAO it generated it has received the Root-ACK. The DAOSequence in the base Root-ACK(DAO-ACK) base object is ignored by the Target node.

5. IANA Considerations

IANA is requested to allocate bit 2 from the Transit Information Option Flags registry for the 'K' flag (Section 4.1).

6. Security Considerations

This node introduces a new flag in response to which the Root of the DODAG would send a Root-ACK which serves as an indication for the target node that the end to end route/path is established. The Root-ACK indication eventually would be used by the end node for application layer processing such as initiating the application traffic. A malicious node could generate the Root-ACK pre-maturely i.e, before the end-to-end path is established and cause the application to do some processing pre-maturely. However, the application layer would always account for application layer failures and thus shouldn't result in any security issues. This could result in more control overhead which is currently the case where nodes do not support this specification.

A malicious 6LR or 6LN could set the 'K' flag indicating the Root to send a Root-ACK. The Root would generate a Root-ACK for the indicated target. The Root need not keep any additional state for handling the 'K' flag.

This document assumes that the security mechanisms as defined in [RFC6550] are followed, which means that all the nodes are part of the RPL network because they have the required credentials. A non-secure RPL network needs to take into consideration the risks highlighted in this section as well as those highlighted in [RFC6550].

7. References

7.1. Normative References

[I-D.ietf-roll-unaware-leaves] Thubert, P. and M. C. Richardson, "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves", Work in Progress, Internet-Draft, draft-ietf-roll-unaware-leaves-30, 22 January 2021, <https://www.ietf.org/archive/id/draft-ietf-roll-unaware-leaves-30.txt>.

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

[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, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

7.2. Informative References

[I-D.ietf-roll-rpl-observations] Jadhav, R. A., Sahoo, R. N., and Y. Wu, "RPL Observations", Work in Progress, Internet-Draft, draft-ietf-roll-rpl-observations-06, 3 June 2021, <https://www.ietf.org/archive/id/draft-ietf-roll-rpl-observations-06.txt>.

Author's Address

Rahul Arvind Jadhav (editor)
Marathahalli
Bangalore 560037
Karnataka
India

Email: rahul.ietf@gmail.com