ROLL Working Group
Internet-Draft
Intended status: Standards Track
Expires: 4 January 2026

M. Richardson
Sandelman Software Works
R. A. Jadhav
Huawei Tech
P. Thubert
H. She
Cisco Systems
K. Iwanicki
University of Warsaw

3 July 2025

Controlling Secure Network Enrollment in RPL networks
draft-ietf-roll-enrollment-priority-13

Abstract

[RFC9032] defines a method by which a potential [RFC9031] enrollment proxy can announce itself as available for new Pledges to enroll on a network. The announcement includes a priority for enrollment. This document provides a mechanism by which a Routing Protocol for Low-Power and Lossy Networks (RPL) Root can globally disable enrollment announcements or adjust the base priority for enrollment operations.

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 4 January 2026.

Copyright Notice

Copyright (c) 2025 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

[RFC7554] describes the use of the Time-Slotted Channel Hopping (TSCH) mode of [ieee802154]. [RFC9031] and [RFC9032] describe mechanisms by which a new node (the "Pledge") can use a nearby router as a Join Proxy. [RFC9032] describes an extension to the 802.15.4 Enhanced Beacon that is used by a Join Proxy to announce its existence such that Pledges can find them.

1.1. Motivation and Overview

It has become clear that not every routing member of the mesh ought to announce itself as a _Join Proxy_. There are a variety of local reasons for which a 6LowPAN Router (6LR) might not want to provide the _Join Proxy_ function. They include low available battery power, already high committed network bandwidth, and available free memory for Neighbor Cache Entry (NCE) slots. (An NCE entry is needed in order to maintain communication with the Pledge nodes trying to enroll)

There are other situations where the operator of the network would like to selectively enable or disable the enrollment process in a specific Destination Oriented Directed Acyclic Graph (DODAG). In particular, as the enrollment process involves permitting unencrypted traffic into the best effort part of a network, it would be better to have the enrollment process off when no new nodes are expected.

This document describes a Routing Protocol for Low-Power and Lossy Networks (RPL) Destination Information Object (DIO) option that can be used to set a minimum enrollment priority. The minimum priority expresses the inability of the RPL DODAG globally to accept new joins. It may derive from multiple constraining factors, for instance, the size of the DODAG, the occupancy of the bandwidth at the DODAG Root, the memory capacity at the Root, or an administrative decision. Each potential _Join Proxy_ utilizes this value as a base on which to add values relating to local conditions, such as its Rank and number of pending joins. As explained in [RFC9032], higher values decrease the likelihood of an unenrolled node sending enrollment traffic via this _Join Proxy_. In particular, by setting the minimum enrollment priority to the maximum value allowed, a network operator can globally disable all new enrollment traffic.

Moreover, when a RPL domain is composed of multiple DODAGs, a node at the edge of more than one such DODAG may not only join any of the DODAGs but also move between them in order to keep their relative sizes balanced. For this, the approximate knowledge of the size of the DODAGs is also an essential metric. Depending on the network policy, the size of the DODAG may or may not affect the minimum enrollment priority. Therefore, since making one proportional to the other would be limiting their value, the current size of the DODAG is advertised separately in the new option.

Updates to the option propagate through the network according to the trickle algorithm. The contents of the option are generated at the DODAG Root and do not change at any hop. If the contents represent an update that is considered important (e.g., quickly disabling any enrollments), the option can trigger trickle timer resets at the nodes to speed up its propagation.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The term 6LR means 6LowPAN Router, and is defined in [RFC6606]. It refers to a router that forwards packets in a 6LowPAN network.

The terms DAO, DODAG, DODAG root, DIO, trickle timer are from [RFC6550]. The lollipop counter function comes from [RFC6550], Section 7.2.

The term (1)"Join" has been used in documents such as [RFC9031] to denote the activity of a new node authenticating itself to the network to obtain authorization to become a member of the network.

In the context of the [RFC6550] RPL protocol, the term (2)"Join" has an alternative meaning: that of a node (already authenticated to the network, and already authorized to be a member of the network), deciding which part of the RPL DODAG to attach to. This term "Join" has to do with preferred parent selection processes.

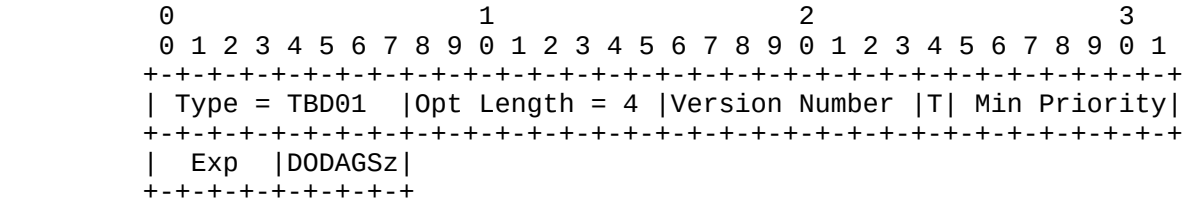
In order to avoid the ambiguity of this term, this document refers to the process (1)"Join" as enrollment, leaving the term "Join" to mean (2)"Join". The term "onboarding" (or "IoT Onboarding") is increasingly used to describe what is now called (1)Join in other documents, and is called enrollment in this document. However, the term _Join Proxy_ is retained with its (1)"Join" meaning from [RFC9031].

3. Protocol Definition

This document uses the extensions mechanism designed into [RFC6550]. No mechanism is needed to enable it.

3.1. Option Format

The following option is defined for transmission in DIOs issued by the DODAG Root to be propagated within the DODAG.



Type To be assigned by IANA.

Version Number An 8-bit unsigned integer set by the DODAG root and

denoting the version number of the contents of the option. The version number is interpreted as a lollipop counter (see Section 7.2 of [RFC6550]).

T A bit indicating whether the particular version of the option is important in that adopting its contents should trigger a trickle timer reset at the node.

Min Priority A 7-bit field providing a base value for the Enhanced Beacon Join priority. A value of 0x7f (127) disables the _Join Proxy_ function entirely.

Exp A 4-bit unsigned integer indicating the power of 2 that defines the unit of the DODAG Size, such that (unit = 2^Exp).

DODAGSz A 4-bit unsigned integer expressing the size of the DODAG in units that depend on the Exp field.

The DODAG Size is calculated as (DODAGSz * 2^Exp).

The DODAG Size can be measured by the Root based on the DAO activity. In such a case, it represents the number of routes not the number of nodes, and can thus be used to infer the load only in a network where each node advertises roughly the same number of addresses and generates roughly the same amount of traffic.

As the DODAG Size is always a multiple of a power of 2, when the actual size falls between two such values, the DODAG Root is to always round up.

Future work such as [I-D.ietf-roll-capabilities] will enable collection of capabilities such as this one in reports to the DODAG Root.

In any case, the DODAG Size may slightly change between a DIO and the next, so the value transmitted is considered as an approximation.

3.2. Option Processing

The contents of the option MUST be generated by the DODAG Root. A 6LR MUST NOT change them when propagating the option.

Whenever the DODAG root changes the values of Min Priority or DODAG Size in the option, it MUST also increment the value of Version Number. Moreover, if the change is considered important (i.e., it is expected to propagate in the DODAG quickly), the DODAG Root SHOULD also set the T bit to 1; otherwise, it MUST set the bit to 0.

Upon receiving the option, a 6LR first checks the value of the Version Number field in the option, _vr_, versus the value of the Version Number it has last adopted locally, _vl_.

* If _vl_ is greater than _vr_ (in the lollipop counter order), then the 6LR MUST ignore the received option.

* Otherwise, the 6LR MUST adopt the contents of the option (i.e., the values of Version Number, Min Priority, DODAG Size, and the T bit) as its local ones. Moreover, if _vl_ was smaller than _vr_ (in the lollipop counter order) and the T bit in the received option was set, then the 6LR MUST reset its DIO trickle timer.

A 6LR, which would otherwise be willing to act as a _Join Proxy_, will examine the locally adopted value of Min Priority and to that number add any additional local consideration (such as upstream congestion, number of NCE slots available, etc.).

The maximum resulting value any 6LR can obtain this way is 0x7f.

The resulting priority, if less than 0x7f, should enable the _Join Proxy_ function.

3.3. Upwards Compatibility

A 6LR that did not support this option would not act on it or propagate it in its DIO messages. In effect, the 6LR’s children and grandchildren nodes could not receive any telemetry. Therefore, 6LRs that support this option but do not receive it via any path SHOULD assume a default value of 0x40 as their base value for the Enhanced Beacon Join Priority.

A 6LR downstream of a 6LR where there was such an interruption in the telemetry could err in two directions:

* If the value implied by the base value of 0x40 was too low, then the 6LR might continue to attract enrollment traffic when none should have been collected. This is a stressor for the network, but this would also be what would occur without this option at all.

* If the value implied by the base value of 0x40 was too high, then the 6LR might deflect enrollment traffic to other parts of the DODAG, possibly refusing any enrollment traffic at all. In order for this to happen, some significant congestion must be seen in the sub-DODAG where the implied 0x40 was introduced. The 0x40 is only the half-way point, so if such an amount of congestion was present, then this sub-DODAG of the DODAG simply winds up being more cautious than it needed to be.

It is possible that the temporal alternation of the above two situations might introduce cycles of accepting and then rejecting enrollment traffic. This is something an operator should consider if they incrementally deploy this option to an existing Low-power/Lossy-Network (LLN). In addition, an operator would be unable to turn off enrollment traffic by sending a maximum value enrollment priority to the sub-DODAG. This situation is unfortunate, but without this option, the situation would occur all over the DODAG, rather than just in the sub-DODAG that the option did not reach.

4. Security Considerations

As per [RFC7416], RPL control frames either run over a secured layer 2 or use the [RFC6550] Secure DIO methods at layer 3. This option can be placed into either a "clear" (layer-2 secured) DIO or a layer-3 Secure DIO.

In most deployments involving wireless technology, layer 2 is always encrypted using a layer-2 specific technology, and so privacy of this option is available.

However, a malicious node that was part of the RPL control plane (i.e., had been enrolled into the layer-2 security) would be able to see the values of this option and, based upon the observed minimal enrollment priority, could signal a confederate that it was a good time to send malicious join traffic.

What is more, such a malicious node, being already part of the RPL control plane, could also send DIOs with a different minimal enrollment priority, which would cause downstream mesh routers to change their _Join Proxy_ behavior: lower minimal priorities would cause downstream nodes to accept more Pledges than the network was expecting; higher minimal priorities could cause the enrollment process to stall.

The use of layer-2 or layer-3 security for RPL control messages prevents the two aforementioned attacks by non-participating nodes by preventing malicious nodes from becoming part of the control plane.

Nevertheless, a node that is attacked and has malware placed on it creates vulnerabilities in the same way such an attack on any node involved in Internet routing protocol does. The rekeying provisions of [RFC9031] exist to permit an operator to remove such nodes from the network.

5. Privacy Considerations

There are no new privacy issues caused by this extension.

6. IANA Considerations

Allocate a new number TBD01 from Registry RPL Control Message Options. This entry should be called Minimum Enrollment Priority.

7. Acknowledgements

This has been reviewed by Thomas Watteyne, Rifaat Shehk-Yusek, Dave Thaler,

8. References

8.1. Normative References

[ieee802154] IEEE standard for Information Technology, "IEEE Std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks", n.d., <http://standards.ieee.org/findstds/standard/802.15.4-2015.html>.

[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/rfc/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/rfc/rfc6550>.

[RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015, <https://www.rfc-editor.org/rfc/rfc7416>.

[RFC7554] Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC 7554, DOI 10.17487/RFC7554, May 2015, <https://www.rfc-editor.org/rfc/rfc7554>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9031] Vuini, M., Ed., Simon, J., Pister, K., and M. Richardson, "Constrained Join Protocol (CoJP) for 6TiSCH", RFC 9031, DOI 10.17487/RFC9031, May 2021, <https://www.rfc-editor.org/rfc/rfc9031>.

[RFC9032] Dujovne, D., Ed. and M. Richardson, "Encapsulation of 6TiSCH Join and Enrollment Information Elements", RFC 9032, DOI 10.17487/RFC9032, May 2021, <https://www.rfc-editor.org/rfc/rfc9032>.

8.2. Informative References

[I-D.ietf-roll-capabilities] Jadhav, R., Thubert, P., Richardson, M., and R. N. Sahoo, "RPL Capabilities", Work in Progress, Internet-Draft, draft-ietf-roll-capabilities-09, 9 November 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-roll-capabilities-09>.

[RFC6606] Kim, E., Kaspar, D., Gomez, C., and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing", RFC 6606, DOI 10.17487/RFC6606, May 2012, <https://www.rfc-editor.org/rfc/rfc6606>.

Authors' Addresses

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca

Rahul Arvind Jadhav
Huawei Tech
Email: rahul.ietf@gmail.com

Pascal Thubert
Cisco Systems
Email: pthubert@cisco.com

Huimin She
Cisco Systems
Email: hushe@cisco.com

Konrad Iwanicki
University of Warsaw
Email: iwanicki@mimuw.edu.pl