Stream: Internet Engineering Task Force (IETF)
RFC: 9035
Updates: 8138
Category: Standards Track
Published: April 2021
ISSN: 2070-1721
Authors: P. Thubert, Ed. *Cisco Systems*
L. Zhao *Cisco Systems*

RFC 9035
A Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration Option for the 6LoWPAN Routing Header

Abstract

This document updates RFC 8138 by defining a bit in the Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration option to indicate whether compression is used within the RPL Instance and to specify the behavior of nodes compliant with RFC 8138 when the bit is set and unset.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9035.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
2.1. Related Documents 3
2.2. Glossary 3
2.3. Requirements Language 4
3. Extending RFC 6550 4
4. Updating RFC 8138 5
5. Transition Scenarios 5
5.1. Coexistence 6
5.2. Inconsistent State While Migrating 6
5.3. Rolling Back 6
6. IANA Considerations 7
7. Security Considerations 7
8. References 7
8.1. Normative References 7
8.2. Informative References 8
Acknowledgments 9
Authors' Addresses 9

1. Introduction

The design of Low-Power and Lossy Networks (LLNs) is generally focused on saving energy, which is the most constrained resource of all. The routing optimizations in "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" [RFC6550], such as routing along a Destination-

Oriented Directed Acyclic Graph (DODAG) to a Root Node and the associated routing header compression and forwarding technique specified in [RFC8138], derive from that primary concern.

Enabling [RFC8138] on a running network requires a "flag day", where the network is upgraded and rebooted. Otherwise, if acting as a leaf, a node that does not support compression per [RFC8138] would fail to communicate; if acting as a router, it would drop the compressed packets and black-hole a portion of the network. This specification enables a hot upgrade where a live network is migrated. During the migration, compression remains inactive until all nodes are upgraded.

This document complements [RFC8138] and signals whether it should be used within a RPL DODAG with a new flag in the RPL DODAG Configuration option. The setting of this new flag is controlled by the Root and propagates as is in the whole network as part of the normal RPL signaling.

The flag is cleared to ensure that compression remains inactive during the migration phase. When the migration is complete (e.g., as known by network management and/or inventory), the flag is set and compression is globally activated in the whole DODAG.

2. Terminology

2.1. Related Documents

The terminology used in this document is consistent with, and incorporates the terms provided in, "Terms Used in Routing for Low-Power and Lossy Networks" [RFC7102]. Other terms in use as related to LLNs are found in "Terminology for Constrained-Node Networks" [RFC7228].

"RPL", "RPL Packet Information" (RPI), and "RPL Instance" (indexed by a RPLInstanceID) are defined in "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" [RFC6550]. The RPI is the abstract information that RPL defines to be placed in data packets, e.g., as the RPL Option [RFC6553] within the IPv6 Hop-By-Hop Header. By extension, the term "RPI" is often used to refer to the RPL Option itself. The DODAG Information Solicitation (DIS), Destination Advertisement Object (DAO), and DODAG Information Object (DIO) messages are also specified in [RFC6550].

This document uses the terms "RPL-Unaware Leaf" (RUL) and "RPL-Aware Leaf" (RAL) consistently with "Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane" [RFC9008]. The term "RPL-Aware Node" (RAN) refers to a node that is either a RAL or a RPL router. A RAN manages the reachability of its addresses and prefixes by injecting them in RPL by itself. In contrast, a RUL leverages "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery" [RFC8505] to obtain reachability services from its parent router(s) as specified in "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves" [RFC9010].

2.2. Glossary

This document often uses the following abbreviations:

6LoRH: 6LoWPAN Routing Header
6LoWPAN: IPv6 over Low-Power Wireless Personal Area Network
DIO: DODAG Information Object (a RPL message)
DODAG: Destination-Oriented Directed Acyclic Graph
LLN: Low-Power and Lossy Network
MOP: RPL Mode of Operation
RAL: RPL-Aware Leaf
RAN: RPL-Aware Node
RPI: RPL Packet Information
RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks
RUL: RPL-Unaware Leaf
SRH: Source Routing Header
Sub-DODAG: The sub-DODAG of a node is a DODAG rooted at that node that is a subset of a main DODAG the node belongs to. It is formed by the other nodes in the main DODAG whose paths to the main DODAG root pass through that node.

2.3. Requirements Language

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.

3. Extending RFC 6550

The DODAG Configuration option is defined in Section 6.7.6 of [RFC6550]. Its purpose is extended to distribute configuration information affecting the construction and maintenance of the DODAG, as well as operational parameters for RPL on the DODAG, through the DODAG. The DODAG Configuration option was originally designed with four bit positions reserved for future use as flags.

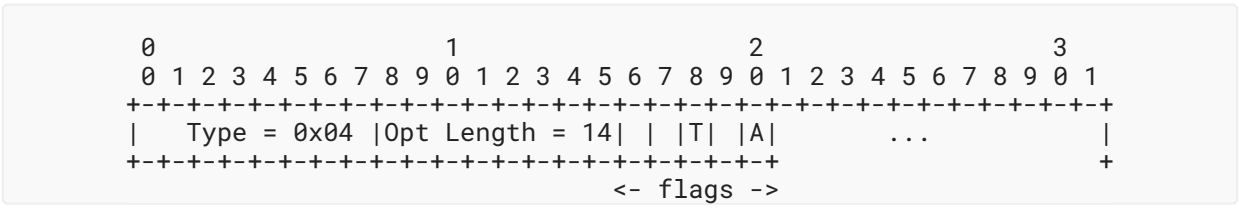

Figure 1: DODAG Configuration Option (Partial View)

This specification defines a new flag, "Enable Compression per RFC 8138 (T)". The 'T' flag is set to turn on the use of [RFC8138] within the DODAG. The 'T' flag is encoded in position 2 of the reserved flags in the DODAG Configuration option (counting from bit 0 as the most significant bit) and set to 0 in legacy implementations as specified in Sections 20.14 and 6.7.6 of [RFC6550], respectively.

Section 4.1.2 of [RFC9008] updates [RFC6550] to indicate that the definition of the flags applies to Mode of Operation (MOP) values zero (0) to six (6) only. For a MOP value of 7, [RFC8138] **MUST** be used on links where 6LoWPAN Header Compression [RFC6282] applies and **MUST NOT** be used otherwise.

The RPL DODAG Configuration option is typically placed in a DIO message. The DIO message propagates down the DODAG to form and then maintain its structure. The DODAG Configuration option is copied unmodified from parents to children. [RFC6550] states that "Nodes other than the DODAG root **MUST NOT** modify this information when propagating the DODAG Configuration option." Therefore, a legacy parent propagates the 'T' flag as set by the Root, and when the 'T' flag is set, it is transparently flooded to all the nodes in the DODAG.

4. Updating RFC 8138

A node **SHOULD** generate packets in compressed form using [RFC8138] if and only if the 'T' flag is set. This behavior can be overridden by configuration or network management. Overriding may be needed, e.g., to turn on compression in a network where all nodes support [RFC8138] but the Root does not support this specification and cannot set the 'T' flag, or to disable it locally in case of a problem.

The decision to use [RFC8138] is made by the originator of the packet, depending on its capabilities and its knowledge of the state of the 'T' flag. A router encapsulating a packet is the originator of the resulting packet and is responsible for compressing the outer headers per [RFC8138], but it **MUST NOT** perform compression on the encapsulated packet.

An external target [RFC9008] is not expected to support [RFC8138]. In most cases, packets to and from an external target are tunneled back and forth between the border router (referred to as a 6LoWPAN Router (6LR)) that serves the external target and the Root, regardless of the MOP used in the RPL DODAG. The inner packet is typically not compressed per [RFC8138], so for outgoing packets, the border router just needs to decapsulate the (compressed) outer header and forward the (uncompressed) inner packet towards the external target.

A border router that forwards a packet to an external target **MUST** uncompress the packet first. In all other cases, a router **MUST** forward a packet in the form that the source used, either compressed or uncompressed.

A RUL [RFC9010] is both a leaf and an external target. A RUL does not participate in RPL and depends on the parent router to obtain connectivity. In the case of a RUL, forwarding towards an external target actually means delivering the packet.

5. Transition Scenarios

A node that supports [RFC8138] but not this specification can only be used in a homogeneous network. Enabling compression per [RFC8138] without a turn-on signaling method requires a flag day, by which time all nodes must be upgraded and at which point the network can be rebooted with 6LoRH compression [RFC8138] turned on.

The intent of this specification is to perform a migration once and for all, without the need for a flag day. In particular, the intent is not to undo the setting of the 'T' flag. Though it is possible to roll back (see Section 5.3), the rollback operation **SHOULD** be complete before the network operator adds nodes that do not support [RFC8138].

5.1. Coexistence

A node that supports this specification can operate in a network with 6LoRH compression [RFC8138] turned on or off with the 'T' flag set accordingly and in a network in transition from off to on or on to off (see Section 5.2).

A node that does not support [RFC8138] can interoperate with nodes that do in a network with 6LoRH compression [RFC8138] turned off. If compression is turned on, all the RANs are expected to be able to handle packets in compressed form. A node that cannot do so may remain connected to the network as a RUL as described in [RFC9010].

5.2. Inconsistent State While Migrating

When the 'T' flag is turned on by the Root, the information slowly percolates through the DODAG as the DIO gets propagated. Some nodes will see the flag and start sourcing packets in compressed form, while other nodes in the same RPL DODAG will still not be aware of it. In Non-Storing mode, the Root will start using [RFC8138] with a Source Routing Header 6LoRH (SRH-6LoRH) that routes all the way to the parent router or to the leaf.

To ensure that a packet is forwarded across the RPL DODAG in the form in which it was generated, it is required that all the RPL nodes support [RFC8138] at the time of the switch.

Setting the 'T' flag is ultimately the responsibility of the network administrator. The expectation is that the network management or upgrading tools in place enable the network administrator to know when all the nodes that may join a DODAG were migrated. In the case of a RPL Instance with multiple Roots, all nodes that participate in the RPL Instance may potentially join any DODAG. The network **MUST** be operated with the 'T' flag unset until all nodes in the RPL Instance are upgraded to support this specification.

5.3. Rolling Back

When turning 6LoRH compression [RFC8138] off in the network, the network administrator **MUST** wait until each node has its 'T' flag unset before allowing nodes that do not support compression in the network. Information regarding whether compression is active in a node **SHOULD** be exposed in the node's management interface.

Nodes that do not support [RFC8138] **SHOULD NOT** be deployed in a network where compression is turned on. If that is done, the node can only operate as a RUL.

6. IANA Considerations

This specification updates the "DODAG Configuration Option Flags for MOP 0..6" registry [RFC9008] (formerly the "DODAG Configuration Option Flags" registry, which was created for [RFC6550]), by allocating one new flag as follows:

Bit Number	Capability Description	Reference
2	Enable Compression per RFC 8138 (T)	RFC 9035

Table 1: New DODAG Configuration Option Flag

IANA has added this document as a reference for MOP 7 in the RPL "Mode of Operation" registry.

7. Security Considerations

It is worth noting that in RPL [RFC6550], every node in the LLN that is RPL aware and has access to the RPL domain can inject any RPL-based attack in the network; see [RFC7416] for details. This document typically applies to an existing deployment and does not change its security requirements and operations. It is assumed that the security mechanisms as defined for RPL are followed.

Setting the 'T' flag before all routers are upgraded may cause a loss of packets. The new bit benefits from the same protection as the rest of the information in the DODAG Configuration option that transports it. Touching the new bit is just one of the many attacks that can happen if an attacker manages to inject a corrupted configuration option in the network.

Setting and unsetting the 'T' flag may create inconsistencies in the network, but as long as all nodes are upgraded to provide support for [RFC8138], they will be able to forward both forms. The source is responsible for selecting whether the packet is compressed or not, and all routers must use the format that the source selected. So, the result of an inconsistency is merely that both forms will be present in the network, at an additional cost of bandwidth for packets in uncompressed form.

An attacker may unset the 'T' flag to force additional energy consumption of child or descendant nodes in its sub-DODAG. Conversely, it may set the 'T' flag so that nodes located downstream would compress packets even when compression is not desired, potentially causing packet loss. In a tree structure, the attacker would be in a position to drop the packets from and to the attacked nodes. So, the attacks mentioned above would be more complex and more visible than simply dropping selected packets. The downstream node may have other parents and see the bit with both settings; such a situation may be detected, and an alert may be triggered.

8. References

8.1. Normative References

[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>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <https://www.rfc-editor.org/info/rfc7102>.

[RFC8138] Thubert, P., Ed., Bormann, C., Toutain, L., and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header", RFC 8138, DOI 10.17487/RFC8138, April 2017, <https://www.rfc-editor.org/info/rfc8138>.

[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/info/rfc8174>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

[RFC9010] Thubert, P., Ed. and M. Richardson, "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves", RFC 9010, DOI 10.17487/RFC9010, April 2021, <https://www.rfc-editor.org/info/rfc9010>.

8.2. Informative References

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

[RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, DOI 10.17487/RFC6553, March 2012, <https://www.rfc-editor.org/info/rfc6553>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[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/info/rfc7416>.

[RFC9008] Robles, M.I., Richardson, M., and P. Thubert, "Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane", RFC 9008, DOI 10.17487/RFC9008, April 2021, <https://www.rfc-editor.org/info/rfc9008>.

Acknowledgments

The authors wish to thank Murray Kucherawy, Meral Shirazipour, Barry Leiba, Tirumaleswar Reddy, Nagendra Kumar Nainar, Stewart Bryant, Carles Gomez, Éric Vyncke, Roman Danyliw, and especially Benjamin Kaduk, Alvaro Retana, Dominique Barthel, and Rahul Jadhav for their in-depth reviews and constructive suggestions.

Also, many thanks to Michael Richardson for always being helpful and responsive when the need arises.

Authors' Addresses

Pascal Thubert (EDITOR)
Cisco Systems, Inc.
Building D
45 Allee des Ormes - BP1200
06254 MOUGINS - Sophia Antipolis
France
Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Li Zhao
Cisco Systems, Inc.
Xinsi Building
No. 926 Yi Shan Rd
Shanghai
200233
China
Email: liz3@cisco.com