

ROLL
Internet-Draft
Intended status: Standards Track
Expires: 13 May 2022

R.A. Jadhav, Ed.
Huawei
P. Thubert
Cisco
M. Richardson
Sandelman Software Works
R.N. Sahoo
Juniper
9 November 2021

RPL Capabilities
draft-ietf-roll-capabilities-09

Abstract

This draft enables the discovery, advertisement and query of capabilities for RPL nodes.

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.

Copyright Notice

Copyright (c) 2021 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 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 and Terminology	3
1.2.	What are Capabilities?	4
2.	Requirements for this document	4
2.1.	How are Capabilities different from existing RPL primitives?	4
3.	Capabilities	5
3.1.	Capability Control Message Option	5
3.2.	Capabilities Handshake	6
4.	Querying Capabilities	6
4.1.	Capability Query (CAPQ)	6
4.1.1.	Capability Type List Control Option	7
4.1.2.	Secure CAPQ	7
4.1.3.	Base rules for CAPQ handling	7
4.2.	Capability Set Response (CAPS)	7
4.2.1.	Secure CAPS	8
5.	Guidelines for defining new capabilities	8
5.1.	Handling Capability flags	8
5.1.1.	Rules to handle capabilities flag	9
6.	Node Capabilities	9
6.1.	Capability Indicators	9
6.1.1.	Format of Capability Indicators	9
6.2.	Routing Resource Capability	10
6.2.1.	Format of Routing Resource Capability	10
7.	Acknowledgements	11
8.	IANA Considerations	11
8.1.	New option: Capabilities	11
8.2.	Capability Sub-Type	12
8.3.	New Registry for CAPQ Flags	12
8.4.	New Registry for Capabilities Flags	12
8.5.	New Registry for Capabilities Indicators	13
9.	Security Considerations	13

10.	References	13
10.1.	Normative References	13
10.2.	Informative References	14
Appendix A.	Capability Handshake Example	14
A.1.	Query supported Cap Types	14

A.2.	Query specific Cap Set	15
A.3.	CAPS with partial Cap Set	15
	Authors' Addresses	16

[1.](#) Introduction

RPL [[RFC6550](#)] specifies a proactive distance-vector based routing scheme. The protocol creates a DAG-like structure which operates with a given "Mode of Operation" (MOP) determining the minimal and mandatory set of primitives to be supported by all the participating nodes.

This document adds a notion of capabilities using which nodes in the network could inform its peers about its additional capabilities. This document highlights the differences of capabilities from that of Mode of operation and explains the necessity of it.

[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. Identifies the MOP of the RPL Instance as administratively provisioned at and distributed by the DODAG root.

MOPex: Extended MOP: As defined in [[I-D.ietf-roll-mopex](#)].

Capabilities: Additional features or capabilities that are supported by the node.

Cap: Abbreviated term used for Capability.

Caps: Abbreviated term used for Capabilities.

DAO: DODAG Advertisement Object. An RPL message used to advertise

the target information in order to establish routing adjacencies.

DIO: DODAG Information Object. An RPL message initiated by the root and is used to advertise the network configuration information.

Current parent: Parent 6LR node before switching to the new path.

NPDAO: No-Path DAO. A DAO message which has target with lifetime 0.

Upstream path/direction: Path or direction from the node to the Root in a DAG.

Downstream path/direction: Path or direction to the node from the Root in a DAG.

This document uses terminology described in [\[RFC6550\]](#). For the sake of readability all the known relevant terms are repeated in this section.

[1.2](#). What are Capabilities?

Currently RPL specification does not have a mechanism whereby a node can signal the set of features that are available on its end. Such a mechanism could help the root to advertise its capabilities and in response also determine some advanced information about the capabilities of the joining nodes. This document defines Capabilities which could be supported by the nodes and handshaked as part of RPL signaling. Capabilities are embedded as an RPL Control Message Option as defined in [Section 6.7 of \[RFC6550\]](#).

[2](#). Requirements for this document

Following are the requirements considered for this documents:

- REQ1: Backwards compatibility. The new options and new fields in the DIO message should be backward compatible i.e. if there are nodes which support old MOPs they could still operate in their own instances.
- REQ2: Optional capabilities handshake. Capabilities are features, possibly optional, which could be handshaked between the nodes

In storing MOP, the DAO message from the 6LR could contain multiple target options because of the DAO-Aggregation. The targets of the capabilities option are indicated by one or more Target options that precede the Capabilities Option. This handling is similar to the Transit Information Option as supported in [Section 6.7.8. of \[RFC6550\]](#).

4. Querying Capabilities

Nodes may be interested in knowing the capabilities of another node before taking an action. For e.g., Consider [\[I-D.ietf-roll-dao-projection\]](#), the Root may want to know the capabilities of the nodes along a network segment before it initiates a projected DAO to install the routes along that segment.

Caps can be carried in existing RPL Control messages as Control Options, however Caps can also be queried explicitly. This section provides a way for a node to query capability set of another node. The capability query and subsequent response messages are directly addressed between the two peers.

4.1. Capability Query (CAPQ)

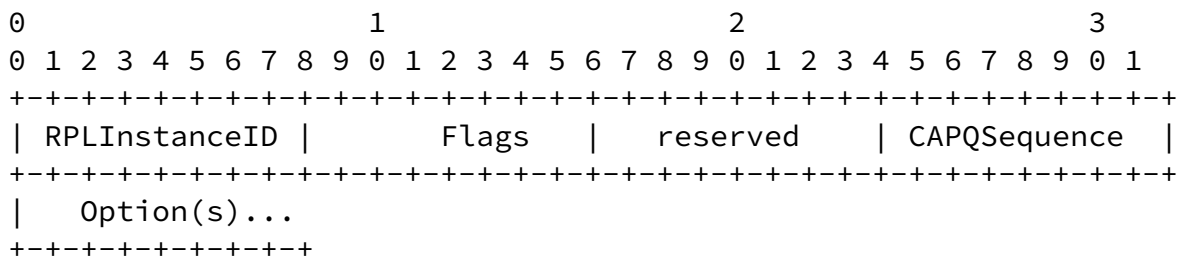


Figure 3: CAPQ base object

CAPQSequence: One byte, Sequence number sent by the CAPQ sender which is reflected back by the responder in the CAPS message.

Flags: One byte, set to zero by sender, ignored by receiver.

reserved: One byte, set to zero by sender, ignored by receiver.

CAPQ base object may be followed by one or more options. The

Capability Type List Control Option Figure 4 is used to carry a set of capability types to query about.

If the sender does not send Figure 4 option, this would indicate that the node intends to query the capability type list Figure 4 supported by the target node.

4.1.1. Capability Type List Control Option

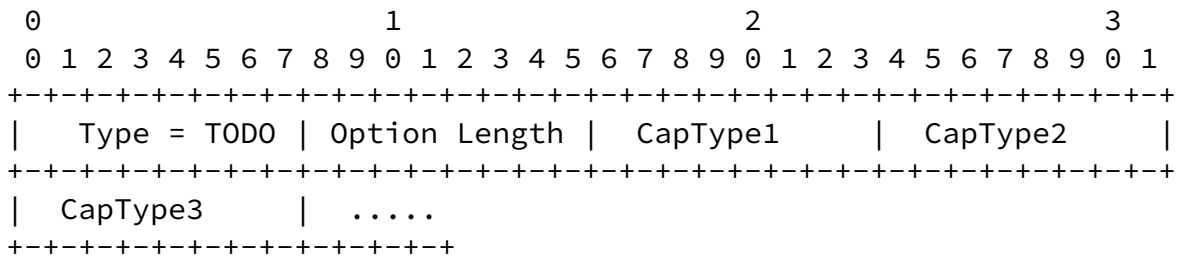


Figure 4: Capability Type List Control Option

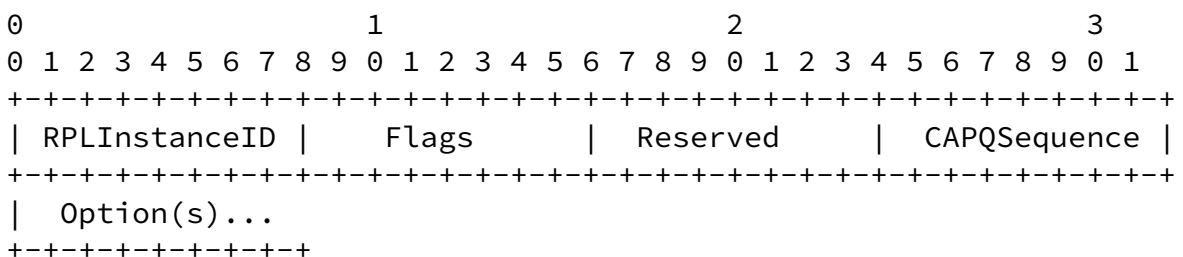
4.1.2. Secure CAPQ

A Secure CAPQ message follows the format in [RFC6550] Figure 7, where the base message format is the CAPQ message shown in Figure 3.

4.1.3. Base rules for CAPQ handling

A CAPQ message may get dropped or lost in the transit. The sender of CAPQ MAY retry the CAPQ message after some delay. The delay SHOULD NOT be less than 1 second.

4.2. Capability Set Response (CAPS)



Flags: One byte, set to zero by sender, ignored by receiver.

reserved: One byte, set to zero by sender, ignored by receiver.

CAPQSequence: One byte, Sequence number copied from CAPQSequence received in the CAPQ message.

CAPS message SHOULD contain the capability set Figure 1 queried by the CAPQ sender. If the target node does not support subset of the queried capabilities then the Figure 4 option with the unsupported cap-types SHOULD be sent back indicating the queried capabilities not-supported by the target node. For an example, check [Appendix A.3](#)

If the CAPQ message does not contain any Figure 4 option then the receiver MUST respond with the cap types it supports using Figure 4.

If the capability set cannot be transmitted in a single message (for e.g., because of MTU limitations) then multiple CAPS messages could be used. All the CAPS message MUST use the same CAPQSequence number copied from the corresponding CAPQ message.

[4.2.1](#). Secure CAPS

A Secure CAPS message follows the format in [[RFC6550](#)] Figure 7, where the base message format is the CAPS message shown in Figure 5.

[5](#). Guidelines for defining new capabilities

This section provides guidelines/recommendations towards defining new capabilities. Note that the capabilities might be carried as part of the multicast messaging such as DIO and hence the set should be used in restrictive manner as far as possible.

[5.1](#). Handling Capability flags

A node MUST drop or discard the message with an unknown capability with 'D' flag set. The message MUST be discarded silently.

The 'J' (join) flag can be set in context to a capability either by a 6LR or the root. The 'J' flag indicates that if the capability is not supported by a node then it can join the instance only as a 6LN (or do not join as 6LR).

The 'C' (copy) flag is set by the node indicating that the capabilities MUST be copied downstream by the node even if the node does not understand the capability.

5.1.1. Rules to handle capabilities flag

On receiving a capability it does not support, the node MUST check the 'J' flag of the capability before joining the Instance. If the 'J' flag is set then it can only join as a 6LN.

If the node is operating as 6LR and subsequently it receives a capability from its preferred parent which it does not understand with 'J' flag set, then the node has to switch itself to 6LN mode. During switching the node needs to inform its downstream peers of its changed status by sending a DIO with infinite rank as mentioned in [RFC6550](#). Alternatively, a node may decide to switch to another parent with compatible and known capabilities.

Capabilities are used to indicate a feature that is supported by the node. Capabilities are not meant for configuration management for e.g., setting a threshold.

6. Node Capabilities

6.1. Capability Indicators

Capability Indicators indicates the capabilities supported by the node in the form of simple flags. Capabilities who do not have additional information to be specified could make use of these flags to indicate their support.

6.1.1. Format of Capability Indicators

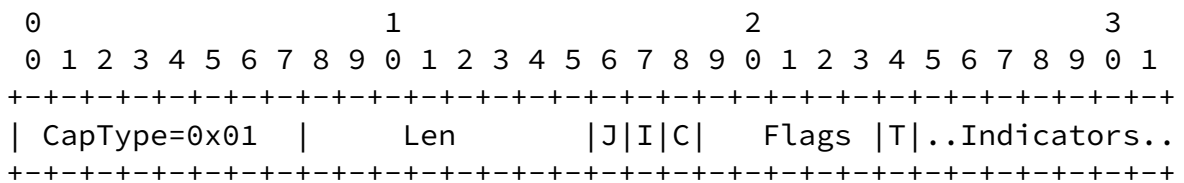


Figure 6: Capability Indicators TLV

Flags: LRs MUST set it to 0. I bit will always be set to 0.

T flag (Bit 1): Indicates whether the node supports 6LoRH [[RFC8138](#)].

[6.2.](#) Routing Resource Capability

Storing mode of operation requires each intermediate router in the LLN to maintain routing states' information in the routing table. LLN routers typically operate with constraints on processing power, memory, and energy (battery power). Memory limits the number of routing states an LR and BR can maintain. When the routing table of an LR or BR is full, it will either reject the new DAO messages received or will use some replacement policy to remove a routing entry and add the new one. Rejection of DAO messages will lead to an increase in DAO message transmission that impacts the energy and network convergence time. Routing state replacement leads to downward path downtime.

One possible way to solve problems due to routing table size constraint is to use this information to add neighbors to the DAO parent set. Routing resource capability can be used by LR and BR to advertise their current routing table usage details in the network. LR or LNs in LLN can use this information in the selection of the DAO parent set. PCE can use this information to select intermediate routers for the projected routes. Routing Resource is an optional capability.

Routing resource capability sent in DIO message has link local scope and it MUST not be forwarded. The 'C' bit of this capability MUST be set to 0.

[6.2.1.](#) Format of Routing Resource Capability

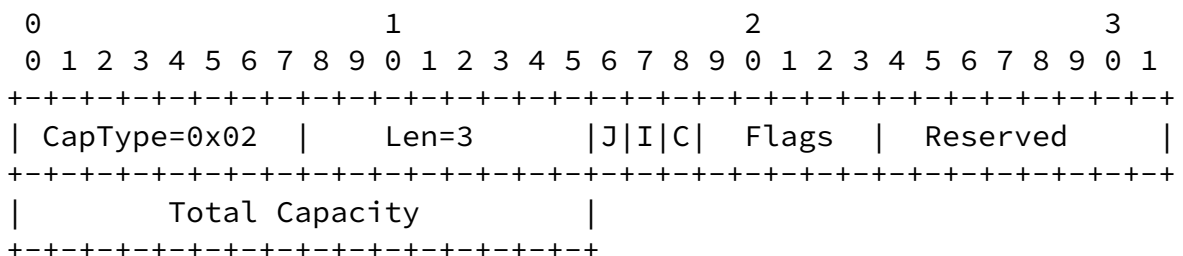


Figure 7: Routing Resource Capability TLV

Type: 0x02.

Flags: I bit MUST be set to 0. C bit MUST be set to 0.

Len: 8-bit unsigned integer, representing the length in octets of the option, not including the Option Type and Length/flags fields.

Resvd: 8-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Total Capacity: 16 bit unsigned integer representing the routing table size.

[7.](#) Acknowledgements

Thanks to Georgios Papadopoulos, Li Zhao for early review and feedback.

[8.](#) IANA Considerations

IANA is requested to allocate new codes for the CAPQ and CAPS messages from the RPL Control Codes registry.

Code	Description	Reference
TBD1	Capability Query	This document
TBD2	Capability Response	This document
TBD3	Secure Capability Query	This document
TBD4	Secure Capability Response	This document

Table 1: New RPL Control Messages

The MSB of the codes allocated to "Secure" messages above should be set.

[8.1.](#) New option: Capabilities

New entry is required for supporting new Capabilities option and new Capability Type List Option in the "RPL Control Message Options" space [[RFC6550](#)].

Value	Meaning	Reference
TODO	Capability Option	This document
TODO	Capability Type List Option	This document

Table 2: New options

8.2. Capability Sub-Type

IANA is requested to create a registry for the Capabilities Type as described in Figure 2 of this document. This registry should be located in TODO. New Capabilities types may be allocated only by an IETF review.

Value	Meaning	Reference
0x01	Capability Indicators	This document
0x02	Routing Resource Capability	This document

Table 3: Type

8.3. New Registry for CAPQ Flags

IANA is requested to create a registry for the Capabilities flags as described in [Section 4.1](#) of this document. This registry should be located in TODO. New Capabilities flags may be allocated only by an IETF review. Currently no flags are defined by this document. Each value is tracked with the following qualities:

- * Flag
- * Description
- * Defining RFC

[8.4.](#) New Registry for Capabilities Flags

IANA is requested to create a registry for the Capabilities flags as described in [Section 2.1](#) of this document. This registry should be located in TODO. New Capabilities flags may be allocated only by an IETF review. Currently no flags are defined by this document. Each value is tracked with the following qualities:

- * Flag
- * Description
- * Defining RFC

[8.5.](#) New Registry for Capabilities Indicators

IANA is requested to create a registry for the Capabilities Indicators as described in [Section 6.1](#) of this document. This registry should be located in TODO. New Capabilities indicators may be allocated only by an IETF review. Each value is tracked with the following qualities:

- * Flag
- * Description
- * Defining RFC

[9.](#) Security Considerations

The options defined in this document are carried in the base message objects as defined in [[RFC6550](#)]. The RPL control message options are

protected by the same security mechanisms that protect the base messages.

Capabilities flag can reveal that the node has been upgraded or is running a old feature set. This document assumes that the base messages that carry these options are protected by RPL security mechanisms and thus are not visible to a malicious node.

[TODO] implications of malicious attack involving setting the capability flags.

10. References

10.1. Normative References

[I-D.ietf-roll-mopex]

Jadhav, R. A., Thubert, P., and M. Richardson, "Mode of Operation extension", Work in Progress, Internet-Draft, [draft-ietf-roll-mopex-03](https://www.ietf.org/archive/id/draft-ietf-roll-mopex-03), 31 March 2021, <<https://www.ietf.org/archive/id/draft-ietf-roll-mopex-03.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

Jadhav, et al.

Expires 13 May 2022

[Page 13]

Internet-Draft

RPL Capabilities

November 2021

Low-Power and Lossy Networks", [RFC 6550](#), DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.

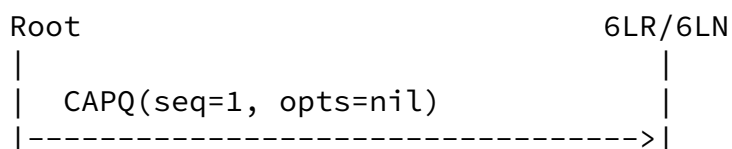
[RFC8138] Thubert, P., Ed., Bormann, C., Toutain, L., and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header", [RFC 8138](#), DOI 10.17487/RFC8138, April 2017, <<https://www.rfc-editor.org/info/rfc8138>>.

10.2. Informative References

- [I-D.ietf-lwig-nbr-mgmt-policy]
 Jadhav, R. A., Sahoo, R. N., Duquennoy, S., and J. Eriksson, "Neighbor Management Policy for 6LoWPAN", Work in Progress, Internet-Draft, [draft-ietf-lwig-nbr-mgmt-policy-03](https://www.ietf.org/archive/id/draft-ietf-lwig-nbr-mgmt-policy-03), 21 February 2019, <<https://www.ietf.org/archive/id/draft-ietf-lwig-nbr-mgmt-policy-03.txt>>.
- [I-D.ietf-roll-dao-projection]
 Thubert, P., Jadhav, R. A., and M. Gillmore, "Root initiated routing state in RPL", Work in Progress, Internet-Draft, [draft-ietf-roll-dao-projection-21](https://www.ietf.org/archive/id/draft-ietf-roll-dao-projection-21), 27 September 2021, <<https://www.ietf.org/archive/id/draft-ietf-roll-dao-projection-21.txt>>.
- [I-D.thubert-roll-turnon-rfc8138]
 Thubert, P. and L. Zhao, "Configuration option for [RFC 8138](https://www.ietf.org/rfc8138)", Work in Progress, Internet-Draft, [draft-thubert-roll-turnon-rfc8138-03](http://www.ietf.org/internet-drafts/draft-thubert-roll-turnon-rfc8138-03), 8 July 2019, <<http://www.ietf.org/internet-drafts/draft-thubert-roll-turnon-rfc8138-03.txt>>.
- [RFC6551] Vasseur, JP., Ed., Kim, M., Ed., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", [RFC 6551](https://www.rfc-editor.org/rfc/6551), DOI 10.17487/RFC6551, March 2012, <<https://www.rfc-editor.org/info/rfc6551>>.

[Appendix A](#). Capability Handshake Example

[A.1](#). Query supported Cap Types



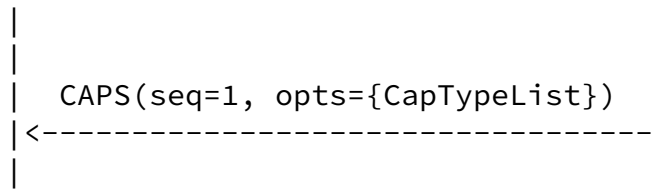


Figure 8: Query supported Cap Types

CAPQ message with no CapTypeList Option results in the peer responding with a CAPS message with CapTypeList Option indicating all the capability set it supports.

[A.2.](#) Query specific Cap Set

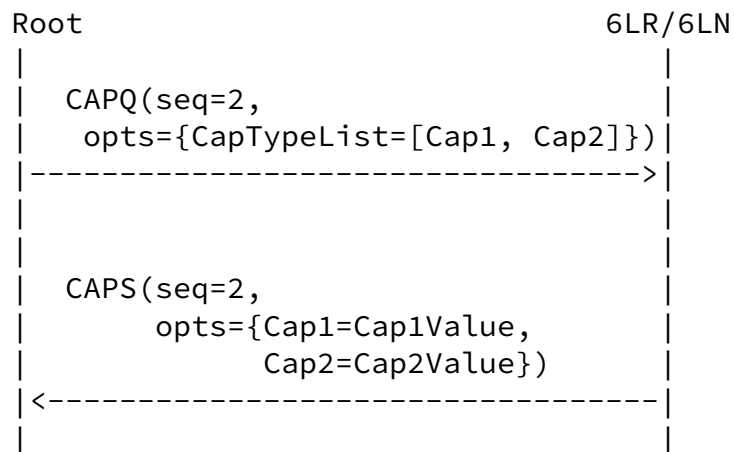


Figure 9: Query specific Cap Set

This flow indicates the case where the Root probes for specific Capabilities of the peer node and the peer node responds with the value of indicated Capability set.

[A.3.](#) CAPS with partial Cap Set

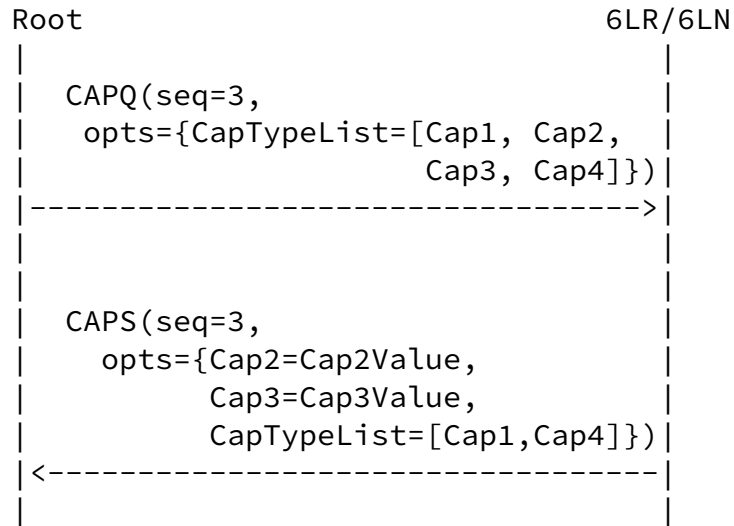


Figure 10: Partial Capability Set handshake

Assume that Root queries for capabilities {Cap1, Cap2, Cap3, Cap4} from the peer node. However the peer node does not support or does not understand capability {cap1, cap4}. In this case the peer node will respond back with value of Cap2 and Cap3 (which it understands) and set the CapTypeList option with {Cap1, Cap4} type.

Authors' Addresses

Rahul Arvind Jadhav (editor)
 Huawei
 Kundalahalli Village, Whitefield,
 Bangalore 560037
 Karnataka
 India

Phone: +91-080-49160700
 Email: rahul.ietf@gmail.com

Pascal Thubert
 Cisco Systems, Inc
 Building D
 45 Allée des Ormes - BP1200
 06254 MOUGINS - Sophia Antipolis
 France

Phone: +33 497 23 26 34
 Email: pthubert@cisco.com

Internet-Draft

RPL Capabilities

November 2021

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Rabi Narayan Sahoo
Juniper

Email: rabinarayans0828@gmail.com

