Stream:	Internet Engineering Task Force (IETF)
RFC:	9926
Updates:	4861, 6550, 8505, 8928, 9010
Category:	Standards Track
Published:	January 2026
ISSN:	2070-1721
Author:	P. Thubert, Ed.

RFC 9926
Prefix Registration for IPv6 Neighbor Discovery

Abstract

This document updates IPv6 Neighbor Discovery (RFC 4861) and IPv6 Subnet Neighbor Discovery (RFC 8505, RFC 8928) to enable a node that owns or is directly connected to a prefix to register that prefix to neighbor routers. The registration indicates that the registered prefix can be reached via the advertising node without a loop. The unicast prefix registration allows the node to request one or more neighbor routers to redistribute the prefix in another routing domain regardless of the routing protocol used in that domain. This document updates the Routing Protocol for Low-Power and Lossy Networks (RPL), as specified in RFCs 6550 and 9010, to enable a 6LoWPAN Router (6LR) to inject the registered prefix in RPL.

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/rfc9926.

Copyright Notice

Table of Contents

1. Introduction 3
2. Terminology 5
   2.1. Requirements Language 5
   2.2. Inherited Terms and Concepts 5
   2.3. Acronyms and Initialisms 5
   2.4. New Terms 6
3. Overview 6
4. Updating RFC 4861 7
5. Updating RFC 7400 8
6. Updating RFC 6550 8
7. Updating RFC 8505 9
   7.1. New P-Field Value 9
   7.2. New EARO Prefix Length Field and F flag 10
   7.3. New EDAR Prefix Length Field 11
   7.4. Updating the Registration Operation 13
8. Updating RFC 9010 15
9. Updating RFC 8928 15
10. Updating RFC 8929 16
11. Security Considerations 16
12. Operational Considerations 17
   12.1. Partially Upgraded Networks 17
   12.2. Application to RPL-Based Route-Over LLNs 17
   12.3. Application to a Shared Link 18
   12.4. Application to a Hub Link with Stub Spokes 19
13. IANA Considerations 20
   13.1. Updated P-Field Registry 21

13.2. New 6LoWPAN Capability Bit 21

14. Normative References 21

15. Informative References 22

Acknowledgments 24

Author's Address 24

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. Other design constraints (such as a limited memory capacity, duty cycling of the LLN devices, and low-power lossy transmissions) derive from that primary concern. The radio (both transmitting or simply listening) is a major energy drain, and the LLN protocols must be adapted to allow the nodes to remain sleeping with the radio turned off at most times.

Examples of LLNs include hub-and-spoke access links such as (Low-Power) Wi-Fi [IEEE80211] and Bluetooth (Low Energy) [IEEE802151], Mesh-Under networks where the routing operation is handled at Layer 2 (L2), and route-over networks such as the Wi-SUN [WI-SUN] and 6TiSCH [RFC9030] mesh networks, which leverage 6LoWPAN [RFC4919] [RFC6282] and RPL [RFC6550] over [IEEE802154].

LLNs and constrained devices are the original domain of application for 6LoWPAN protocols. It is thus a foremost concern, when designing those protocols, to minimize energy spendings. In non-LLN environments where lowering carbon emissions is also a priority, it could make sense to apply the 6LoWPAN designs and extend some of the 6LoWPAN protocols. The general design points include:

- Placing the protocol complexity in the less-constrained routers to simplify the host implementation and avoid expanding the control traffic to all nodes.
- Using host-triggered operations to enable transient disconnections with the routers, e.g., to conserve power (sleep), but also to cope with inconsistent connectivity.

These points translate into:

- Stateful proactively built knowledge in the routers that is available at any point of time.
- Unicast host-to-router operations triggered by the host and its applications.
- Minimal use of asynchronous L2 broadcast operations that would keep the host awake and listening with no application-level need to do so.

"RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" [RFC6550] provides IPv6 [RFC8200] routing services within such constraints. To save signaling and routing state in constrained networks, the RPL routing is only performed along a Destination-Oriented Directed Acyclic Graph (DODAG) that is optimized to reach a Root node, as opposed to along the shortest path between two peers, whatever that would mean in each LLN.

The classical Neighbor Discovery Protocol (NDP) [RFC4861] [RFC4862] was defined for serial links and shared transit media such as Ethernet at a time when L2 broadcast was cheap on those media, while memory for neighbor cache was expensive. Thus, it was designed as a reactive protocol that relies on caching and multicast operations for the Duplicate Address Detection (DAD) and Address Resolution (AR), aka address discovery or address lookup, of IPv6 unicast addresses. Those multicast operations typically impact every node on-link when at most one is really targeted, which is a waste of energy, and imply that all nodes are awake to hear the request, which is inconsistent with power-saving (sleeping) modes.

"Architecture and Framework for IPv6 over Non-Broadcast Access" [IPv6-over-NBMA] introduces an evolution of IPv6 ND towards a proactive AR method. Because the IPv6 model for NBMA depends on a routing protocol to reach inside the subnet, the IPv6 ND extension for NBMA is referred to as Subnet Neighbor Discovery (SND). SND is based on work done in the context of Internet of Things (IoT), known as 6LoWPAN ND. As opposed to the classical IPv6 ND protocol, this evolution follows the energy conservation principles discussed above:

- The original 6LoWPAN ND, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC6775], was introduced to avoid the excessive use of multicast messages and enable IPv6 ND for operations over energy-constrained nodes. [RFC6775] changes the classical IPv6 ND model to proactively establish the Neighbor Cache Entry (NCE) associated to the unicast address of a 6LoWPAN Node (6LN) in the one or more 6LoWPAN Routers (6LRs) that serve it. To that effect, [RFC6775] defines a new Address Registration Option (ARO) that is placed in unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages between the 6LN and the 6LRs.
- "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery>" [RFC8505] updates [RFC6775] into a generic Address Registration mechanism and is the foundation for Subnet Neighbor Discovery (SND). SND introduces the Extended Address Registration Option (EARO) to enable the registering node to access services such as routing inside a subnet and ND proxy operations [RFC8929]. This provides a routing-protocol-agnostic method for a host to request that the router inject a unicast IPv6 address in the local routing protocol and provide return reachability for that address.
- "Listener Subscription for IPv6 Neighbor Discovery Multicast and Anycast Addresses" [RFC9685] updates [RFC8505] to enable a listener to subscribe to an IPv6 anycast or multicast address; the document also updates [RFC9010] to enable a 6LR to inject the anycast and multicast addresses in RPL. Similarly, this specification updates [RFC8505] and [RFC9010] to add the capability for a 6LN to register unicast prefixes up to 120 bits long, as opposed to addresses, and to signal in a routing-protocol-independent fashion to a 6LR that it is expected to redistribute the prefixes.

This specification updates the above registration and subscription methods to enable a node to register a unicast prefix to the routing system and get it injected in the routing protocol. As with [RFC8505], the prefix registration is agnostic to the routing protocol in which the router injects the prefix, and the router is agnostic to the method that was used to allocate the prefix to the node. The energy conservation principles in [RFC8505] are retained as well, meaning that the node does not have to send or expect asynchronous multicast messages.

Please note that an energy-conserving node is not necessarily a router, so even when a node is advertising a prefix, it is a design choice not to use Router Advertisement (RA) messages that would make the node appear as a router to peer nodes. From the design principles above, it is clearly a design choice not to leverage (1) broadcasts from or to the node or (2) complex state machines in the node. It is also a design choice to use and extend the EARO as opposed to the Route Information Option (RIO) [RFC4191] because the RIO is not intended to inject routes in routing, and is lacking related control information like the R bit in the EARO. Additionally, an RA with RIO cannot be trusted for a safe injection in the routing protocol for the lack of the equivalent of the Registration Ownership Verifier (ROVR) [RFC8928] in the EARO.

2. Terminology

2.1. 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.

2.2. Inherited Terms and Concepts

This document uses terms and concepts that are discussed in:

- "Neighbor Discovery for IP version 6 (IPv6)" [RFC4861] and
- "IPv6 Stateless Address Autoconfiguration" [RFC4862] for the Neighbor Solicitation operation,
- "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC6775], as well as
- "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery" [RFC8505], and
- "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" [RFC6550] for RPL, which is the routing protocol used in LLNs for SND.

2.3. Acronyms and Initialisms

This document uses the following abbreviations:

6CIO: 6LoWPAN Capability Indication Option [RFC7400]
6LBR: 6LoWPAN Border Router [RFC6775]

6LN: 6LoWPAN Node [RFC6775]
6LR: 6LoWPAN Router [RFC6775]
ARO: Address Registration Option [RFC6775]
DAD: Duplicate Address Detection [RFC4861]
DAO: Destination Advertisement Object [RFC6550]
DODAG: Destination-Oriented Directed Acyclic Graph
EARO: Extended Address Registration Option [RFC8505]
EDAC: Extended Duplicate Address Confirmation [RFC8505]
EDAR: Extended Duplicate Address Request [RFC8505]
ESS: Extended Service Set [IEEE80211]
IPAM: IP Address Management
LLN: Low-Power and Lossy Network
LLA: Link-Layer Address
LoWPAN: Low-Power Wireless Personal Area Network
LR-WPAN: Low-Rate Wireless Personal Area Network [IEEE802154]
MAC: Medium Access Control
NA: Neighbor Advertisement (message) [RFC4861]
NBMA: Non-Broadcast Multi-Access (full mesh)
NCE: Neighbor Cache Entry [RFC4861]
ND: Neighbor Discovery (protocol)
NDP: Neighbor Discovery Protocol
NS: Neighbor Solicitation (message) [RFC4861]
ROVR: Registration Ownership Verifier (pronounced "rover") [RFC8505]
RPL: IPv6 Routing Protocol for LLNs (pronounced "ripple") [RFC6550]
RA: Router Advertisement (message) [RFC4861]
RS: Router Solicitation (message) [RFC4861]
RTO: RPL Target Option [RFC6550]
SLLAO: Source Link-Layer Address Option [RFC4861]
SND: Subnet Neighbor Discovery (protocol)
TID: Transaction ID [RFC8505]
TIO: Transit Information Option [RFC6550]
TLLAO: Target Link-Layer Address Option [RFC4861]

2.4. New Terms

This document introduces the following term:

Origin: The node that issued the prefix advertisement, either in the form of a NS(EARO) or as a DAO(TIO, RTO)

3. Overview

This specification inherits from [RFC6550], [RFC8505], and [RFC9010] to register prefixes as opposed to addresses.

The IPv6 ND operation is agnostic to the routing protocol used in the SND. Route-over LLNs typically leverage RPL. A RPL-based SND deployment consists of:

- one or more 6LBRs that act as RPL Root,
- intermediate routers down the RPL graph that propagate routing information on addresses and prefixes towards the Root,
- 6LRs that are RPL-aware 6LNs and can leverage RPL directly to expose their addresses and prefixes, and
- 6LNs that are the RPL-unaware destinations and need SND to obtain reachability over the RPL LLN for their addresses and, with this specification, their prefixes as well.

The SND operation for prefixes inherits from that for unicast addresses, meaning that it is the same unless specified otherwise herein. In particular, forwarding a packet happens as specified in Section 11 of [RFC6550], including loop avoidance and detection. However, in the case of multicast, multiple copies might be generated.

[RFC8505] is a prerequisite to this specification. A node that implements this **MUST** also implement [RFC8505]. This specification does not introduce a new option; it modifies existing options and updates the associated behaviors to enable the registration for prefixes as an extension to [RFC8505].

This specification updates the P-Field introduced in [RFC9685] for use in EARO, DAR, and RTO, with the new value of 3 to indicate the registration of a prefix, as detailed in Section 7.2. With this extension, the 6LN can now express its willingness to receive the traffic for all addresses in the range of a prefix, using the P-Field value of 3 in the EARO to signal that the registration is for such prefix. Multiple 6LNs acting as border routers to the same external network or as access routers to the same subnet may register the same prefix to the same 6LR or to different 6LRs.

If the R flag is set in the registration of one or more 6LNs for the same prefix, then, according to its redistribution policy, the 6LR **MUST** redistribute the prefix in the routing protocol(s) (e.g., RPL) that it participates in. The duration of the redistribution is based on the longest registration lifetime across the non-expired received registrations for the prefix.`

Examples of use cases where this specification may apply include virtual links, shared links, and hub links as shown in Sections 12.3 and 12.4, respectively. More generally, the 6LN may be a router running a different routing protocol in an external network, e.g., a stub network, and acting as a border router. Using the prefix registration method enables decoupling the routing protocol in the 6LN from the routing protocol that the 6LRs run in the main LLN and provide signaling to stimulate the redistribution.

4. Updating RFC 4861

[RFC4861] expects that the NS/NA exchange is for a unicast address, which is indicated in the Target Address field of the ND message. Section 5.5 of [RFC8505] updates [RFC4861] to signal the Registered Address in the Target Address field.

This specification updates [RFC4861] by allowing a 6LN to advertise a prefix in the Target Address field when the NS or NA message is used for a registration, per Section 5.5 of [RFC8505]. In that case, the prefix length **MUST** be indicated in the EARO of the NS message, overloading the field that is used in the NA response for the Status.

If the 6LN owns at least one IPv6 address that is derived from the registered prefix with a non-zero interface ID, then it **MUST** indicate one of these addresses in full in the Target Address field of the NS(EARO) message. Else, it **MUST** indicate the prefix padded with zeros in the Target Address field.

5. Updating RFC 7400

This specification updates "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC7400] by defining a new capability bit for use in the 6CIO. [RFC7400] was already updated by [RFC8505] for use in IPv6 ND messages.

The new "Registration for prefixes supported" (F) flag indicates to the 6LN that the 6LR (1) accepts IPv6 prefix registrations as specified in this document, (2) will ensure that packets for the addresses that match this prefix will be routed to the 6LNs that registered the prefix, and (3) will ensure that the route to the prefix will be redistributed if the R flag is set to 1.

Figure 1 illustrates the F flag in its position (16, counting 0 to 47 in network order in the 48-bit array).

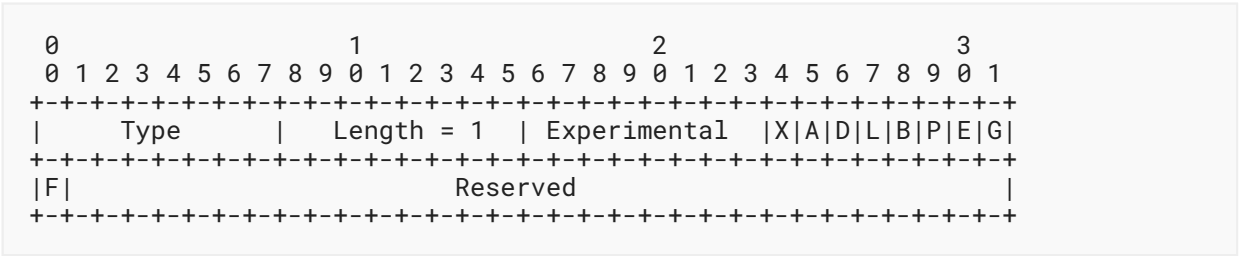

Figure 1: New Capability Bit in the 6CIO

New Option Field:

F: 1-bit flag, set to 1 to indicate "Registration for prefixes supported"

6. Updating RFC 6550

[RFC6550] uses the Path Sequence in the Transit Information Option (TIO) to retain only the freshest unicast route and remove stale ones, e.g., in the case of mobility. [RFC9010] copies the TID from the EARO into the Path Sequence, and the ROVR field into the associated RPL Target

Option (RTO). This way, it is possible to identify both the registering node and the order of registration in RPL for each individual advertisement, so the most recent path and lifetime values are used.

[RFC9685] requires the use of the ROVR field as the indication of the origin of a Target advertisement in the RPL DAO messages, as specified in Section 6.1 of [RFC9010]. For anycast and multicast advertisements (in NS or DAO messages), multiple origins may subscribe to the same address, in which case the multiple advertisements from the different or unknown origins are merged by the common parent. In that case, the common parent becomes the origin of the merged advertisements and uses its own ROVR value. On the other hand, a parent that propagates an advertisement from a single origin uses the original ROVR in the propagated RTO, as it does for unicast address advertisements, so the origin is recognized across multiple hops.

This specification updates [RFC6550] to require that, for prefix routes, the Path Sequence is used between and only between advertisements for the same Target and from the same origin (i.e., with the same ROVR value); in that case, only the freshest advertisement is retained. However, the freshness comparison cannot apply if the origin is not determined (i.e., the origin did not support this specification).

[RFC6550] uses the Path Lifetime in the TIO to indicate the remaining time for which the advertisement is valid for unicast route determination, and a Path Lifetime value of 0 invalidates that route. [RFC9010] maps the Address Registration lifetime in the EARO and the Path Lifetime in the TIO so they are comparable when both forms of advertisements are received.

The RPL router that merges multiple advertisements for the same prefix uses and advertises the longest remaining lifetime across all the origins of the advertisements for that prefix. When the lifetime expires, the router sends a no-path DAO message (i.e., the lifetime is 0) using the same value for the ROVR value as for the previous advertisements. This value refers to either the single descendant that advertised the Target if there is only one or the router itself if there is more than one.

Note that the Registration Lifetime, TID, and ROVR fields are also placed in the EDAR message, so the state created by EDAR is also comparable with that created upon an NS(EARO) or a DAO message. For simplicity, the text below mentions only NS(EARO) but it also applies to EDAR.

7. Updating RFC 8505

This specification updates the EARO and EDAR messages to enable the registration of prefixes and updates the registration operation in the case of a prefix, in particular from the standpoint of the 6LR, e.g., to enable the registration of overlapping prefixes.

7.1. New P-Field Value

[RFC9685] defines a 2-bit P-Field with values 0 through 2 and reserves the value 3 for future use. This specification defines the semantics of P-Field value 3.

When the P-Field is set to 3, it indicates that the Registered Address represents a prefix rather than a single address. Upon receiving an NS(EARO) message with the P-Field set to 3, the receiver **MUST** install a route to the indicated prefix via the source address of the NS(EARO) message.

This specification assigns the value 3 to the P-Field, resulting in the following complete set of defined values:

Value	Meaning
0	Registration for a Unicast Address
1	Registration for a Multicast Address
2	Registration for an Anycast Address
3	Registration for a Unicast Prefix

Table 1: P-Field Values

7.2. New EARO Prefix Length Field and F flag

Section 4.1 of [RFC8505] defines the EARO as an extension to the ARO option defined in [RFC6775].

The Status field is used only when the EARO is placed in an NA message. This specification repurposes that field to carry the prefix length when the EARO is placed in an NS message as illustrated in Figure 2. The prefix length is expressed as 7 bits, and the most significant bit of the field is reserved. A 7-bit value of 0 is understood as a truncated 128, meaning that this registration is for an address as opposed to a prefix. This approach is backward compatible with [RFC8505] and spans both addresses and prefixes.

This specification adds a new F flag to signal that the Registered Prefix is topologically correct through the Registering Node. This means that the Registering Node relays packets that are sourced in the Registered Prefix to the outside, in accordance with "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" [BCP38]. The receiver forwards packets to the Registering Node address when the source address of the packets derives from the Registered Prefix. Note that to avoid loops, the receiver must be in the inside so packets sent by the sender towards the outside may never reach the receiver. The notion of "inside" and "outside" are administratively defined, e.g., "inside" is a particular L2 network such as an Ethernet fabric.

When the F flag is not set, the Registering Node owns the prefix and will deliver packets to the destination if the destination address derives from the prefix. Conversely, if the F flag is set, the Registering Node will forward traffic whose source address derives from the Registered Prefix into a network location (e.g., to an ISP Provider Edge) where this source address is topologically correct (e.g., derives from a prefix assigned by that ISP). The F flag is encoded in the most significant bit of the EARO Status field when the Status field is used to transport a Prefix Length as shown in Figure 2.

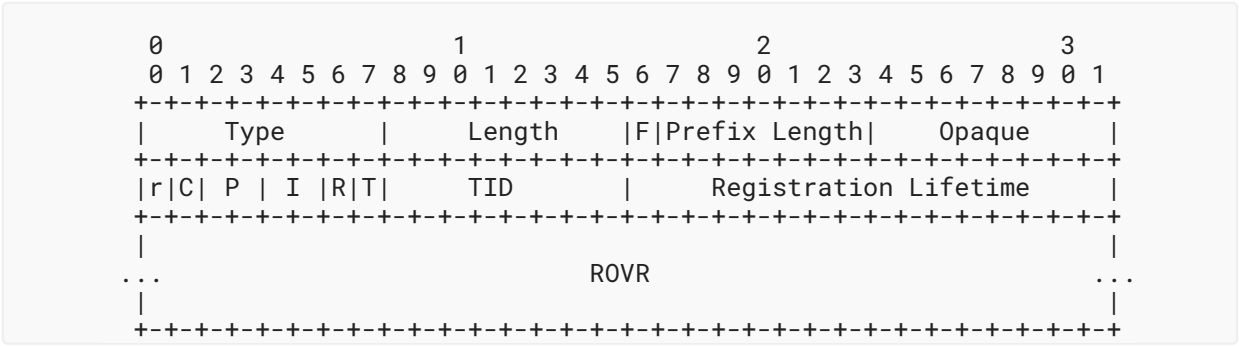

Figure 2: EARO Format for Use in NS Messages

New and updated Option Fields:

F: (Forwarding Flag) A 1-bit flag. When set to 1, it indicates that the sender expects other routers to forward packets to the sender when those packets are sourced from within the registered prefix.

Prefix Length: A 7-bit unsigned integer. When the P-Field is set to 3 and the EARO is included in an NS message, this field **MUST** contain a prefix length expressed in bits, with a value in the inclusive range of 16 to 120. When the EARO is included in an NA message, this field **MUST** carry a status value, regardless of the setting of the P-Field. In all other cases, this field is reserved; it **MUST** be set to zero by the sender and **MUST** be ignored by the receiver.

r (reserved): A 1-bit reserved field. It **MUST** be set to zero by the sender and **MUST** be ignored by the receiver.

7.3. New EDAR Prefix Length Field

This specification adds the new value of 3 to the P-Field to signal that the Registered Address is a prefix. When that is the case, the prefix is assumed to be at most 120 bits long, padded with zeros up to 120 bits, and the remaining byte is dedicated to one reserved bit and the Prefix Length.

Figure 3 illustrates the EDAR message when the value of the P-Field is 3. Figure 4 shows the response EDAC message, with the Status field and the echoed Prefix.

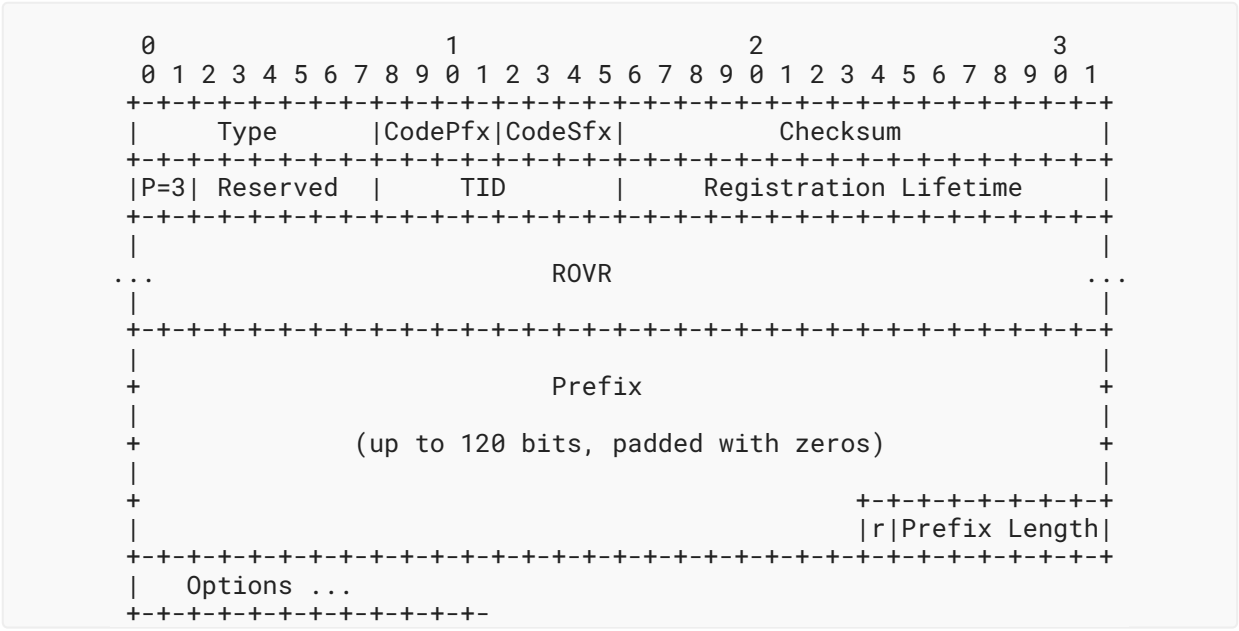

Figure 3: EDAR Message Format with P == 3

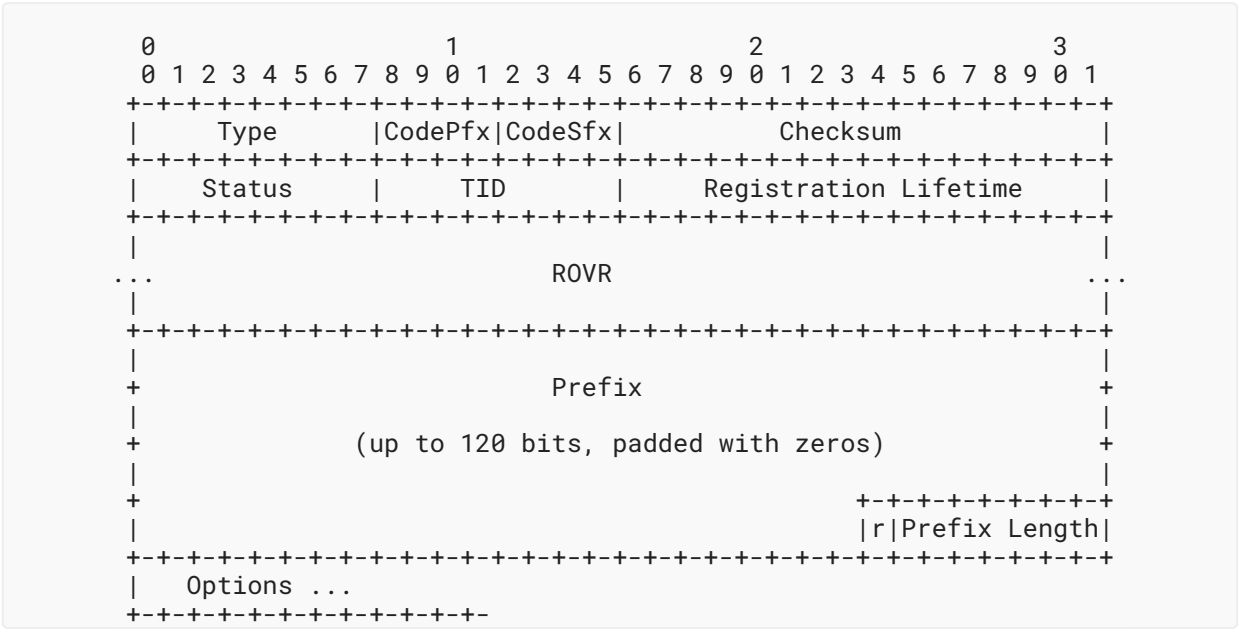

Figure 4: EDAC Message Format

New and updated EDAR/EDAC Message Fields:

Prefix: A 15-byte field that carries up to 120 bits of the prefix. If the prefix is shorter than 120 bits, the remaining bits **MUST** be padded with zeros. The receiver **MUST** treat the padding as zeroed and **MUST** overwrite any unused bits with zeros before using the prefix.

r (reserved): A 1-bit reserved field. It **MUST** be set to zero by the sender and **MUST** be ignored by the receiver.

Prefix Length: A 7-bit unsigned integer indicating the length of the prefix in bits. The value **MUST** be in the inclusive range of 16 to 120.

The capability to place the P-Field and the contiguous "Reserved" field in the EDAR message is specified in Section 7.2 of [RFC9685].

The capability to append ND options to the EDAR and EDAC messages is introduced in Section 3.1 of [RFC8929].

All other fields follow the same definition as specified in [RFC8505]. The values for these fields and RFC references are maintained by IANA under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" [IANA.ICMP] registry group.

7.4. Updating the Registration Operation

With [RFC8505]:

- A router that expects to reboot may send a final RA message, upon which nodes should register elsewhere or redo the registration to the same router upon reboot. In all other cases, a node reboot is silent. When the node comes back to life, existing registration state might be lost if it was not safely stored, e.g., in persistent memory.
- Only unicast addresses can be registered.
- The 6LN must register all its Unique Local Addresses (ULAs) and Global Unicast Addresses (GUAs) with a NS(EARO).
- The 6LN may set the R flag in the EARO to obtain return reachability services from the 6LR, e.g., through ND proxy operations or by injecting the route in a route-over subnet.
- The 6LR maintains a registration state per Registered Address, including an NCE with the Link Layer Address (LLA) of the Registered Node (the 6LN here).

The operation for registering prefixes is similar to that for addresses from the perspective of the 6LN, but shows important differences on the router side, which maintains a separate state for each origin and merges them in its own advertisements. This specification adds the following behavior, similar to that introduced by [RFC9685] for multicast addresses:

- The EARO status indicating a "Registration Refresh Request" applies to prefixes as well.

  This status is used in asynchronous NA(EARO) messages to indicate to peer 6LNs that they are requested to reregister all addresses and prefixes that were previously registered to the originating node. The NA message **MAY** be sent to a unicast or a multicast link-scope address and **SHOULD** be contained within the L2 range where nodes may effectively have registered/subscribed to this router, e.g., a radio broadcast domain to preserve energy and spectrum.

  A device that wishes to refresh its state, e.g., upon reboot if it may have lost some registration state, **SHOULD** send an asynchronous NA(EARO) with this new status value. That asynchronous NA(EARO) **SHOULD** be sent to the all-nodes link-scope multicast address

(ff02::1), and Target **MUST** be set to the link-local address that was exposed previously by this node to accept registrations, and the TID **MUST** be set to 0; the ROVR field **MUST** be set to all zeros and ignored by the receiver.

In an environment with unreliable transmissions, the multicast NA(EARO) message may be resent in a fast sequence, in which case the TID is incremented each time. A 6LN that has recently processed the NA(EARO) indicating a "Registration Refresh Request" ignores the additional NA(EARO) also indicating a "Registration Refresh Request" within the duration of the fast sequence. That duration depends on the environment and has to be configured. By default, it is 10 seconds.

- Registration for prefixes is now supported. The value of 3 in the P-Field of the EARO and the EDAR message signals when the registration is for a prefix as opposed to an address. DAD for prefixes and addresses becomes a prefix overlap match. Whether overlapping addresses and prefixes may be registered is a network policy decision and out of scope. The same prefix may be injected twice (multiple routes) as long as they use the same value of the ROVR.

  Overlaps may be desirable. For instance, it may happen that a router or a proxy (see Section 10) registers a prefix or an aggregation while a host using an address from that prefix or a prefix from that aggregation also registers its piece.

  In case of an overlapping registration, the longest prefix match wins, meaning that if the network policy allows for overlapping registrations, then the routes for the registered prefixes are installed towards the node that registered with the longest prefix match, all the way to /128.

- If the 6LR acts as a border router to external prefixes or owns the prefixes entirely, it **SHOULD** register all those prefixes on all interfaces from which it might be needed to relay traffic to that prefix. It **MUST** set the P-Field in the EARO to 3 for those prefixes and set the R flag to receive the traffic associated to the prefixes. It **MAY** refrain from registering a prefix on one interface if that prefix is already successfully registered on another interface, or the router handled the EDAR/EDAC flow by itself, to ensure that the prefix ownership is known and validated by the 6LBR. Additionally, if the router expects to receive traffic for that prefix on that interface, it needs to ensure that the prefix is advertised some other way, e.g., over a routing protocol such as RPL.
- The 6LN **MAY** set the R flag in the EARO to request the 6LR to redistribute the prefix on other links using a routing protocol. The 6LR **MUST NOT** reregister that prefix to yet another router unless loops are avoided some way, e.g., following a tree structure.
- The 6LR and the 6LBR are extended to accept more than one registration for the same prefix, since multiple 6LNs may register it. The ROVR in the EARO identifies uniquely a registration within the namespace of the Registered Prefix.
- The 6LR **MUST** maintain a registration state per tuple (IPv6 prefix, prefix length, ROVR) for all registered prefixes. It **SHOULD** notify the 6LBR with an EDAR message, unless it determined that the 6LBR is legacy and does not support this specification (see Section 5). In turn, the 6LBR **MUST** maintain a registration state per tuple (IPv6 prefix, ROVR) for all prefixes.

8. Updating RFC 9010

With [RFC9010]:

- The 6LR injects only unicast routes in RPL.
- Upon a registration with the R flag set to 1 in the EARO, the 6LR injects the address in the RPL unicast support.
- Upon receiving a packet directed to a unicast address for which it has an active registration, the 6LR delivers the packet as a unicast L2 frame to the LLA of the node that registered the unicast address.

This specification adds the following behavior:

- Upon a registration with the R flag set to 1 and the P-Field set to 3 in the EARO, the 6LR injects the prefix in RPL using a prefix RTO. The P-Field in the RTP **MUST** be set to 3.
- Upon receiving a packet directed to an address that derives from a prefix for which it has at least one registration, the 6LR delivers a copy of the packet as a unicast L2 frame to the LLA of exactly one of the nodes that registered to that prefix, using the longest prefix match derivation to find the best 6LN.

9. Updating RFC 8928

"Address-Protected Neighbor Discovery for Low-Power and Lossy Networks" [RFC8928] was defined to protect the ownership of unicast IPv6 addresses that are registered with [RFC8505].

With Address-Protected Neighbor Discovery (AP-ND) [RFC8928], it is possible for a node to autoconfigure a pair of public and private keys and use them to sign the registration of addresses that are either autoconfigured or obtained through other methods.

The first-hop router (the 6LR) can then validate a registration and perform source address validation on packets coming from the sender node (the 6LN).

As multiple nodes may register the same prefix, the method specified in [RFC8928] cannot be used with node-local autoconfigured keypairs, which protect a single ownership only.

For a prefix, as for an anycast or a multicast address, it is still possible to leverage AP-ND [RFC8928] to enforce the right to register. If AP-ND [RFC8928] is used, a keypair **MUST** be created and associated with the prefix before the prefix is deployed, and a ROVR **MUST** be generated from that keypair as specified in [RFC8928]. The prefix and the ROVR **MUST** then be installed in the 6LBR at the first registration, or by an external mechanism such as IP Address Management (IPAM) or DHCPv6 snooping prior to the first registration. This way, the 6LBR can recognize the prefix on the future registrations and validate the right to register based on the ROVR.

The keypair **MUST** then be provisioned in each node that needs to register the prefix or a prefix within, so the node can follow the steps in [RFC8928] to register the prefix.

Upon receiving an NA message with the status set to 5 "Validation Requested", the node that registered the address or prefix performs the proof of ownership based on that longest prefix match.

10. Updating RFC 8929

"IPv6 Backbone Router" [RFC8929] defines a proxy operation whereby a 6LoWPAN Border Router (6LBR) may impersonate a 6LN when performing an address registration. In that case, [RFC8505] messages are used as is, with one change that the SLLAO in the proxied NS(EARO) messages indicates the Registering Node (the 6LBR) as opposed to the Registered Node (the 6LN). See Figure 5 of [RFC8929] for an example of proxy operation by the 6LBR, which generates an NS(EARO) upon receiving an EDAR message.

This specification updates that proxy operation with the updates in [RFC9685] and this on the formats and content of the EARO, the EDAR, and the EDAC messages, to support the P-Field and the signaling of prefixes. The proxy **MUST** use the P-Field as received in the EDAR or NS(EARO) message to generate the proxied NS(EARO), and it **MUST** use the exact same prefix and prefix length as received in the case of a prefix registration.

11. Security Considerations

This specification updates [RFC8505], and the security considerations of that document also apply to this document. In particular, the link layer **SHOULD** be sufficiently protected to prevent rogue access, else a rogue node with physical access to the network may inject packets and perform an attack from within.

Section 9 leverages AP-ND [RFC8928] to prevent a rogue node from registering a unicast address that it does not own. The mechanism could be extended to anycast and multicast addresses if the values of the ROVR they use are known in advance, but how this is done is not in scope for this specification. One way would be to authorize in advance the ROVR of the valid users. A less preferred way could be to synchronize the ROVR and TID values across the valid registering nodes as a preshared key material.

In the latter case, it could be possible to update the keys associated to a prefix in all the 6LNs, but the flow is not clearly documented and may not complete in due time for all nodes in LLN use cases. It may be simpler to install an all-new address with new keys over a period of time and switch the traffic to that address when the migration is complete.

12. Operational Considerations

12.1. Partially Upgraded Networks

A mix of devices that support only [RFC8505], both [RFC8505] and [RFC9685], and all of the above plus this specification, may coexist. Different cases may occur:

- A legacy 6LN will not register prefixes, and the service will be the same when the network is upgraded.
- A legacy 6LR will not set the F flag in the 6CIO and an upgraded 6LN will not register prefixes with that router, though it may with other 6LRs that do support this specification.
- Upon an EDAR message, a legacy 6LBR may not realize that the address being registered comes with a whole prefix, and return that it is duplicate in the EDAC status. The 6LR **MUST** ignore a duplicate status in the EDAR for prefixes.

12.2. Application to RPL-Based Route-Over LLNs

This specification also updates [RFC6550] and [RFC9010] in the case of a route-over multilink subnet based on the RPL routing protocol, to add multicast ingress replication in Non-Storing Mode and anycast support in both Storing and Non-Storing modes. A 6LR that implements the RPL extensions specified therein **MUST** also implement [RFC9010].

Figure 5 illustrates the classical situation of an LLN as a single IPv6 subnet, with a 6LoWPAN Border Router (6LBR) that acts as Root for RPL operations and as Address Registrar for 6LowPAN ND.

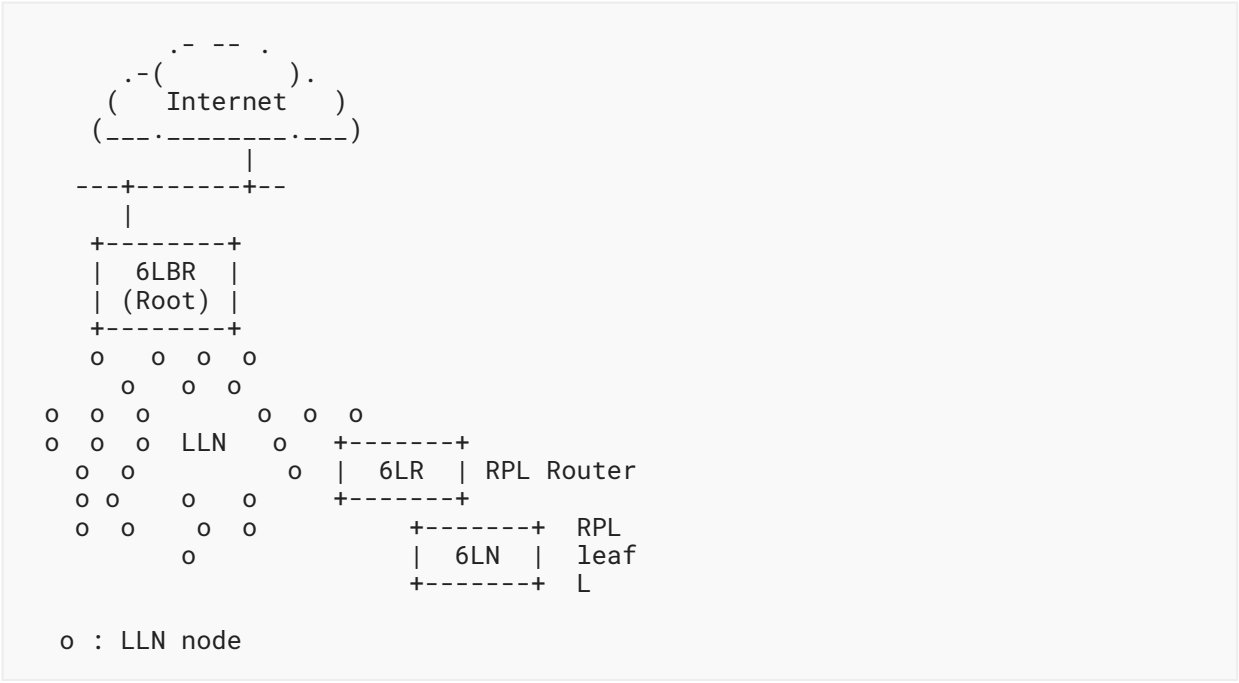

Figure 5: RPL-Based Route-Over LLN

A RPL leaf L acting as a 6LN registers its addresses and prefixes to a RPL router acting as a 6LR, using a L2 unicast NS message with an EARO as specified in [RFC8505] and [RFC9685]. Note that a RPL leaf acting as 6LN may still be a border router for another routing protocol, an access router for an IP link, or a virtual Router serving virtual machines or applications within the same physical node. Note also that a RPL-aware Leaf would preferably leverage RPL directly to inject routes, to fully leverage the routing protocol. The registration state is periodically renewed by the Registering Node (the 6LN), before the lifetime indicated in the EARO expires (at the 6LR). As for unicast IPv6 addresses, the 6LR uses an Extended Duplicate Address Request/ Confirmation (EDAR/EDAC) exchange with the 6LBR to notify the 6LBR of the presence of the listeners. With this specification, a router that owns a prefix or provides reachability to an external prefix but is not a RPL router can also register those prefixes with the R flag set, to enable reachability to the Prefix within the RPL domain.

12.3. Application to a Shared Link

A shared link is a situation where more than one prefix is deployed over an L2 link (say, a switched Ethernet fabric or a Wi-Fi Extended Service Set (ESS) federating multiple Access Points (APs)), and not necessarily all nodes are aware of all prefixes. Figure 6 depicts such a situation, with two routers 6LR1 and 6LR2 that own respective prefixes P1:: and P2:: and expose those in their RA messages over the same link. Note that the shared link maybe operated with any combination of NDP and SND as discussed in Section 7 of [IPv6-over-NBMA].

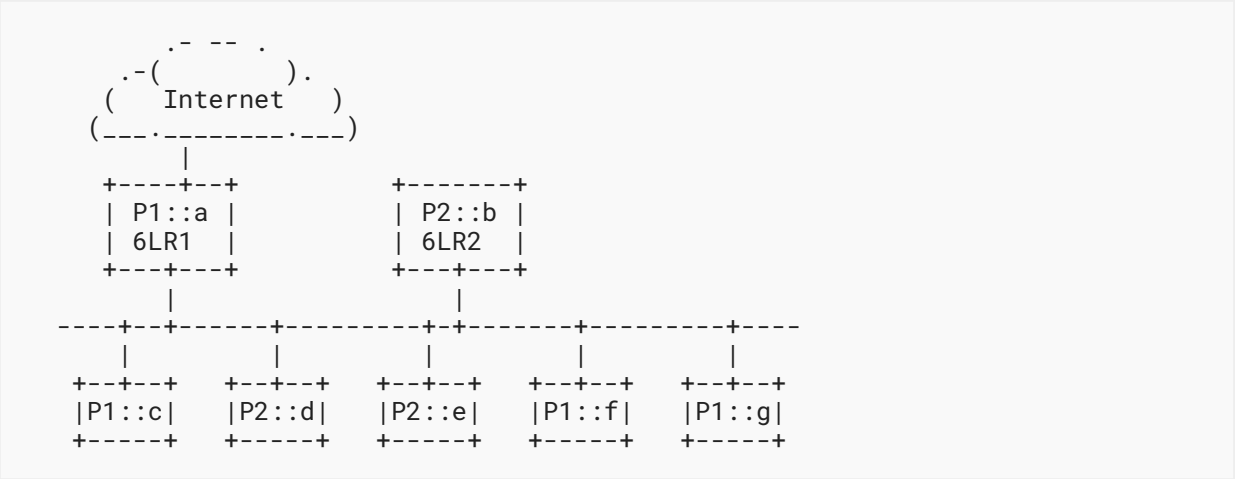

Figure 6: Shared Link

Say that 6LR1 is the router providing access to the outside, and 6LR2 is aware of 6LR1 as its default gateway. With this specification, 6LR2 registers P2:: to 6LR1, and 6LR1 installs a route to P2:: via 6LR2. This way, addresses that derive from P2:: can still be reached via 6LR1 and then 6LR2. 6LR2 may then leverage ICMP Redirect messages [RFC4861] to shorten the path between 6LR1 and the nodes that own those addresses.

If P2 were delegated by 6LR1, e.g., using DHCPv6 [RFC8415], then the expectation is that 6LR1 aggregates P1:: and P2:: in its advertisements to the outside, and there is no need to set the R flag. However, unless 6LR2 knows about such a situation, e.g., through configuration, 6LR2 **SHOULD** set the R flag requesting 6LR1 to advertise P2:: so as to obtain reachability.

12.4. Application to a Hub Link with Stub Spokes

A hub link is a situation where stub links are deployed around a backbone and interconnected by routers. Figure 7 depicts such a situation, with one router 6LR1 serving the hub link and at least one router like 6LR2 and 6LR3 providing connectivity from the stub links to the hub link. In this example, say that there is one prefix on each link -- P1:: on the hub link, and P2:: and P3:: on the stub links.

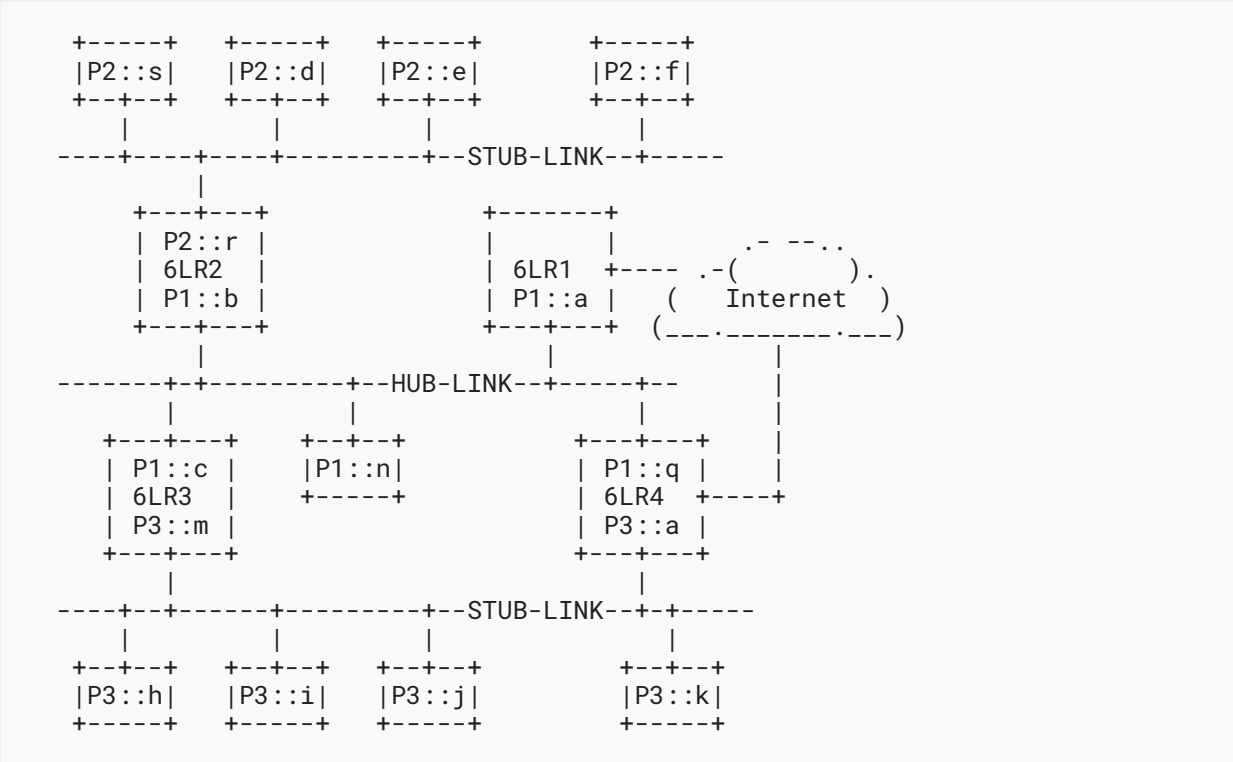

Figure 7: Hub and Stubs

As before, say that 6LR1 is the router providing access to the outside, and 6LR2 is aware of 6LR1 as its default gateway. With this specification, 6LR2 registers P2:: to 6LR1, and 6LR1 installs a route to P2:: via 6LR2. This way, nodes on the stub link behind 6LR2 that derive their addresses from P2:: can still be reached via 6LR1 and then 6LR2. The same goes for 6LR3 and any other routers serving stub links.

If P2 were delegated by 6LR1, then the expectation is that 6LR1 aggregates P1:: and P2:: in its advertisements to the outside, and there is no need to set the R flag. However, unless 6LR2 knows about such a situation, e.g., through configuration, 6LR2 **SHOULD** set the R flag requesting 6LR1 to advertise P2:: so as to obtain reachability.

In this example, routers 6LR3 and 6LR4 both connect to the same stub link where subnet P3 is installed. They may both register P3 to 6LR1, and 6LR1 will apply its own load-balancing logic to use either of the routers.

13. IANA Considerations

IANA has made changes under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" [IANA.ICMP] and the "Routing Protocol for Low Power and Lossy Networks (RPL)" [IANA.RPL] registry groups, as follows.

13.1. Updated P-Field Registry

This specification updates the P-Field introduced in [RFC9685] to assign the value of 3, which is the only remaining unassigned value for the 2-bit field. To that effect, IANA has updated the "P-Field Values" registry in the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry group as indicated in Table 2:

Value	Meaning	Reference
3	Registration for a Unicast Prefix	RFC 9926

Table 2: New P-Field Value

13.2. New 6LoWPAN Capability Bit

IANA has made an addition to the "6LoWPAN Capability Bits" [IANA.ICMP.6CIO] registry in the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry group as indicated in Table 3:

IANA has fixed the description of bit 9 (the "A" flag defined in [RFC8928]). It is not called "1" but "A".

Bit	Description	Reference
9	AP-ND Enabled (A bit)	[RFC8928]
16	Registration for prefixes supported (F bit)	RFC 9926

Table 3: New 6LoWPAN Capability Bit

14. Normative References

[IANA.ICMP] IANA, "Internet Control Message Protocol version 6 (ICMPv6) Parameters", <https://www.iana.org/assignments/icmpv6-parameters>.

[IANA.ICMP.6CIO] IANA, "6LoWPAN Capability Bits", <https://www.iana.org/assignments/icmpv6-parameters>.

[IANA.RPL] IANA, "Routing Protocol for Low Power and Lossy Networks (RPL)", <https://www.iana.org/assignments/rpl>.

[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>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[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>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/info/rfc7400>.

[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>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[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>.

[RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November 2020, <https://www.rfc-editor.org/info/rfc8928>.

[RFC8929] Thubert, P., Ed., Perkins, C.E., and E. Levy-Abegnoli, "IPv6 Backbone Router", RFC 8929, DOI 10.17487/RFC8929, November 2020, <https://www.rfc-editor.org/info/rfc8929>.

[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>.

[RFC9685] Thubert, P., Ed., "Listener Subscription for IPv6 Neighbor Discovery Multicast and Anycast Addresses", RFC 9685, DOI 10.17487/RFC9685, November 2024, <https://www.rfc-editor.org/info/rfc9685>.

15. Informative References

[BCP38] Best Current Practice 38, <https://www.rfc-editor.org/info/bcp38>.
At the time of writing, this BCP comprises the following:

Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[IEEE80211] IEEE, "IEEE Standard for Information Technology -- Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks -- Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2022, DOI 10.1109/IEEESTD.2021.9363693, <https://ieeexplore.ieee.org/document/9363693>.

[IEEE802151] IEEE, "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)", IEEE Std 802.15.1-2002, DOI 10.1109/IEEESTD.2002.93621, <https://ieeexplore.ieee.org/document/1016473>.

[IEEE802154] IEEE, "IEEE Standard for Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)", IEEE Std 802.15.4-2006, DOI 10.1109/IEEESTD.2006.232110, <https://ieeexplore.ieee.org/document/1700009>.

[IPv6-over-NBMA] Thubert, P. and M. Richardson, "Architecture and Framework for IPv6 over Non-Broadcast Access", Work in Progress, Internet-Draft, draft-ietf-6man-ipv6-over-wireless-09, 9 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-ipv6-over-wireless-09>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <https://www.rfc-editor.org/info/rfc4919>.

[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>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC9030] Thubert, P., Ed., "An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)", RFC 9030, DOI 10.17487/RFC9030, May 2021, <https://www.rfc-editor.org/info/rfc9030>.

[WI-SUN] "Wi-SUN Alliance", <https://wi-sun.org/>.

Acknowledgments

Many thanks to Dave Thaler and Dan Romascanu for their early reviews, Adnan Rashid for all his contributions, and Éric Vyncke for his in-depth AD review. Many thanks as well to the reviewers of the IETF Last Call and IESG rounds: Dan Romascanu, Shuping Peng, Mohamed Boucadair, Paul Wouters, Ketan Talaulikar, Gunter Van de Velde, Mike Bishop, and Roman Danyliw.

Author's Address

Pascal Thubert (EDITOR)
06330 Roquefort-les-Pins
France
Email: pascal.thubert@gmail.com