Stream: Internet Engineering Task Force (IETF)
RFC: 9032
Category: Standards Track
Published: May 2021
ISSN: 2070-1721
Authors: D. Dujovne, Ed. *Universidad Diego Portales*
M. Richardson *Sandelman Software Works*

RFC 9032
Encapsulation of 6TiSCH Join and Enrollment Information Elements

Abstract

In the Time-Slotted Channel Hopping (TSCH) mode of IEEE Std 802.15.4, opportunities for broadcasts are limited to specific times and specific channels. Routers in a TSCH network transmit Enhanced Beacon (EB) frames to announce the presence of the network. This document provides a mechanism by which additional information critical for new nodes (pledges) and long-sleeping nodes may be carried within the EB in order to conserve use of broadcast opportunities.

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/rfc9032.

Copyright Notice

Table of Contents

1. Introduction

[RFC7554] describes the use of the Time-Slotted Channel Hopping (TSCH) mode of [IEEE.802.15.4].

In TSCH mode of IEEE Std 802.15.4, opportunities for broadcasts are limited to specific times and specific channels. Routers in a TSCH network transmit Enhanced Beacon (EB) frames during broadcast slots in order to announce the time and channel schedule.

This document defines a new IETF Information Element (IE) subtype to place into the EB to provide join and enrollment information to prospective pledges in a more efficient way.

The following subsections explain the problem being solved, which justifies carrying the join and enrollment information in the EB.

1.1. 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.

Other terminology can be found in Section 2.1 of [RFC9030].

1.2. Layer 2 Synchronization

As explained in Section 4.5.2 of [RFC8180], the EB has a number of purposes: it carries synchronization information such as the Absolute Slot Number (ASN) and Join Metric and identifiers for the timeslot template and the channel hopping sequence, and it indicates the TSCH slotframe.

An EB announces the existence of a TSCH network and the nodes already joined to that network. Receiving an EB allows a Joining Node (pledge) to learn about the network and to synchronize with it.

The EB may also be used as a means for a node already part of the network to resynchronize [RFC7554].

There are a limited number of timeslots designated as broadcast slots by each router in the network. Considering 10 ms slots and a slotframe length of 100, these slots are rare and could result in only 1 slot per second for broadcasts, which needs to be used for the beacon. Additional broadcasts for Router Advertisements (RA) or Neighbor Discovery (ND) could be even more scarce.

1.3. Layer 3 Synchronization: IPv6 Router Solicitations and Advertisements

At Layer 3, [RFC4861] defines a mechanism by which nodes learn about routers by receiving multicast RAs. If no RA is received within a set time, then a Router Solicitation (RS) may be transmitted as a multicast, to which an RA will be received, usually unicast.

Although [RFC6775] reduces the amount of multicast necessary for address resolution via Neighbor Solicitation (NS) messages, it still requires multicast of either RAs or RSes. This is an expensive operation for two reasons: there are few multicast timeslots for unsolicited RAs; and if a pledge node does not receive an RA, and decides to transmit an RS, a broadcast Aloha slot (see Appendix A.5 of [RFC7554]) is consumed with unencrypted traffic. [RFC6775] already allows for a unicast reply to such an RS.

This is a particularly acute issue for the join process for the following reasons:

1. Use of a multicast slot by even a non-malicious unauthenticated node for a Router Solicitation (RS) may overwhelm that timeslot.

2. It may require many seconds of on-time before a new pledge receives a Router Advertisement (RA) that it can use.
3. A new pledge may have to receive many EBs before it can pick an appropriate network and/or closest Join Proxy to attach to. If it must remain in the receive state for an RA as well as find the EB, then the process may take dozens of seconds, even minutes for each enrollment attempt that it needs to make.

1.4. Layer 2 Selection

In a complex Low-power and Lossy Network (LLN), multiple LLNs may be connected together by Backbone Routers (technology such as [RFC8929]), resulting in an area that is serviced by multiple, distinct Layer 2 instances. These are called Personal Area Networks (PANs). Each instance will have a separate Layer 2 security profile and will be distinguished by a different PANID. The PANID is part of the Layer 2 header as defined in [IEEE.802.15.4]: it is a 16-bit value that is chosen to be unique, and it contributes context to the Layer 2 security mechanisms. The PANID provides a context similar to the Extended Service Set ID (ESSID) in 802.11 networking and can be considered similar to the 802.3 Ethernet VLAN tag in that it provides context for all Layer 2 addresses.

A device that is already enrolled in a network may find after a long sleep that it needs to resynchronize with the Layer 2 network. The device's enrollment keys will be specific to a PANID, but the device may have more than one set of keys. Such a device may wish to connect to a PAN that is experiencing less congestion or that has a shallower Routing Protocol for LLNs (RPL) tree [RFC6550]. It may even observe PANs for which it does not have keys, but for which it believes it may have credentials that would allow it to join.

In order to identify which PANs are part of the same backbone network, the network ID is introduced in this extension. PANs that are part of the same backbone will be configured to use the same network ID. For RPL networks [RFC6550], configuration of the network ID can be done with a configuration option, which is the subject of future work.

In order to provide some input to the choice of which PAN to use, the PAN priority field has been added. This lists the relative priority for the PAN among different PANs. Every EB from a given PAN will likely have the same PAN priority. Determination of the PAN priority is the subject of future work; but it is expected that it will be calculated by an algorithm in the 6LoWPAN Border Router (6LBR), possibly involving communication between 6LBRs over the backbone network.

The parent selection process [RFC6550] can only operate within a single PAN because it depends upon receiving RPL DIO messages from all available parents. As part of the PAN selection process, the device may wish to know how deep in the LLN mesh it will be if it joins a particular PAN, and the rank priority field provides an estimation of each announcer's rank. Once the device synchronizes with a particular PAN's TSCH schedule, it may receive DIOs that are richer in their diversity than this value. The use of this value in practice is the subject of future research, and the interpretation of this value of the structure is considered experimental.

2. Protocol Definition

[RFC8137] creates a registry for new IETF IE subtypes. This document allocates a new subtype.

The new IE subtype structure is as follows. As explained in [RFC8137], the length of the subtype content can be calculated from the container, so no length information is necessary.

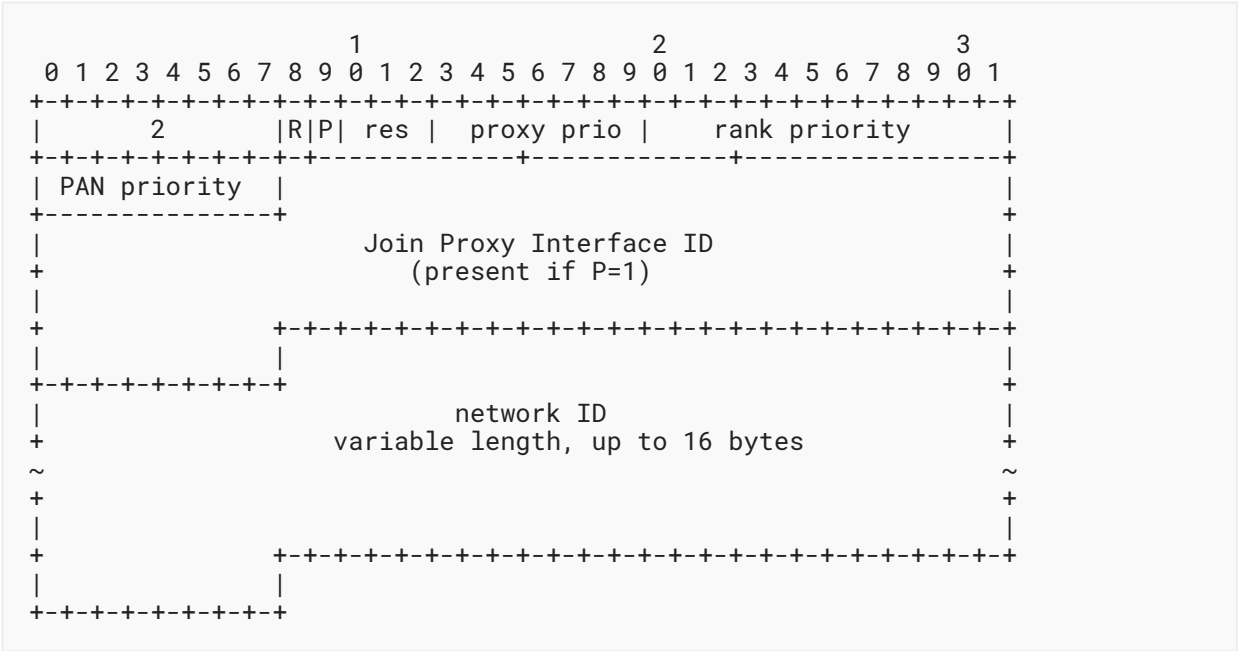

Figure 1: IE Subtype Structure

res: Reserved bits **MUST** be ignored upon receipt and **SHOULD** be set to 0 when sending.

R: The RA R-flag is set if the sending node will act as a router for host-only nodes relying on stateless address auto-configuration (SLAAC) to get their global IPv6 address. Those hosts **MUST** send a unicast RS message in order to receive an RA with the Prefix Information Option.

In most cases, every node sending a beacon will set this flag, and in a typical mesh, this will be every single node. When this bit is not set, it might indicate that this node may be under provisioned or that it may have no additional slots for additional nodes. This could make this node more interesting to an attacker.

P: If the Proxy Address P-flag is set, then the Join Proxy Interface ID bit field is present. Otherwise, it is not provided.

This bit only indicates if another part of the structure is present, and it has little security or privacy impact.

proxy prio (proxy priority): This field indicates the willingness of the sender to act as a Join Proxy. Lower value indicates greater willingness to act as a Join Proxy as described in [RFC9031]. Values range from 0x00 (most willing) to 0x7e (least willing). A priority of 0x7f indicates that the announcer should never be considered as a viable Join Proxy. Only unenrolled pledges look at this value.

Lower values in this field indicate that the transmitter may have more capacity to handle unencrypted traffic. A higher value may indicate that the transmitter is low on neighbor cache entries or other resources. Ongoing work such as [NETWORK-ENROLLMENT] documents one way to set this field.

rank priority: The rank priority is set by the IPv6 LLN Router (6LR) that sent the beacon and is an indication of how willing this 6LR is to serve as a RPL parent [RFC6550] within a particular network ID. Lower values indicate more willingness, and higher values indicate less willingness. This value is calculated by each 6LR according to algorithms specific to the routing metrics used by the RPL [RFC6550]. The exact process is a subject of significant research work. It will typically be calculated from the RPL rank, and it may include some modifications based upon current number of children or the number of neighbor cache entries available. Pledges **MUST** ignore this value. It helps enrolled devices only to compare connection points.

An attacker can use this value to determine which nodes are potentially more interesting. Nodes that are less willing to be parents likely have more traffic, and an attacker could use this information to determine which nodes would be more interesting to attack or disrupt.

PAN priority: The PAN priority is a value set by the Destination-Oriented Directed Acyclic Graph (DODAG) root (see [RFC6550], typically the 6LBR) to indicate the relative priority of this LLN compared to those with different PANIDs that the operator might control. This value may be used as part of the enrollment priority, but typically it is used by devices that have already enrolled and need to determine which PAN to pick when resuming from a long sleep. Unenrolled pledges **MAY** consider this value when selecting a PAN to join. Enrolled devices **MAY** consider this value when looking for an eligible parent device. Lower values indicate more willingness to accept new nodes.

An attacker can use this value, along with the observed PANID in the EB to determine which PANIDs have more network resources, and may have more interesting traffic.

Join Proxy Interface ID: If the P bit is set, then 64 bits (8 bytes) of address are present. This field provides the Interface ID (IID) of the link-local address of the Join Proxy. The associated prefix is well-known as fe80::/64. If this field is not present, then IID is derived from the Layer 2 address of the sender per SLAAC [RFC4862].

This field communicates the IID bits that should be used for this node's Layer 3 address, if it should not be derived from the Layer 2 address. Communication with the Join Proxy occurs in the clear. This field avoids the need for an additional service-discovery process for the case where the Layer 3 address is not derived from the Layer 2 address. An attacker will see both Layer 2 and Layer 3 addresses, so this field provides no new information.

network ID: This is a variable length field, up to 16-bytes in size that uniquely identifies this network, potentially among many networks that are operating in the same frequencies in overlapping physical space. The length of this field can be calculated as being whatever is left in the IE.

In a 6TiSCH network, where RPL [RFC6550] is used as the mesh routing protocol, the network ID can be constructed from a truncated SHA-256 hash of the prefix (/64) of the network. This will be done by the RPL DODAG root and communicated by the RPL Configuration Option payloads, so it is not calculated more than once. This is just a suggestion for a default algorithm: it may be set in any convenient way that results in a non-identifying value. In some LLNs where multiple PANIDs may lead to the same management device (the Join Registrar/Coordinator (JRC)), then a common value that is the same across all the PANs **MUST** be configured. Pledges that see the same network ID will not waste time attempting to enroll multiple times with the same network when the network has multiple attachment points.

If the network ID is derived as suggested, then it will be an opaque, seemingly random value and will not directly reveal any information about the network. An attacker can match this value across many transmissions to map the extent of a network beyond what the PANID might already provide.

3. Security Considerations

All of the contents of this IE are transmitted in the clear. The content of the EB is not encrypted. This is a restriction in the cryptographic architecture of the 802.15.4 mechanism. In order to decrypt or do integrity checking of Layer 2 frames in TSCH, the TSCH ASN is needed. The EB provides the ASN to new (and long-sleeping) nodes.

The sensitivity of each field is described within the description of each field.

The EB is authenticated at the Layer 2 level using 802.15.4 mechanisms using the network-wide keying material. Nodes that are enrolled will have the network-wide keying material and can validate the beacon.

Pledges that have not yet enrolled are unable to authenticate the beacons and will be forced to temporarily take the contents on faith. After enrollment, a newly enrolled node will be able to return to the beacon and validate it.

In addition to the enrollment and join information described in this document, the EB contains a description of the TSCH schedule to be used by the transmitter of this packet. The schedule can provide an attacker with a list of channels and frequencies on which communication will occur. Knowledge of this can help an attacker to more efficiently jam communications, although there is future work being considered to make some of the schedule less visible. Encrypting the schedule does not prevent an attacker from jamming, but rather increases the energy cost of doing that jamming.

4. Privacy Considerations

The use of a network ID may reveal information about the network. The use of a SHA-256 hash of the DODAGID (see [RFC6550]), rather than using the DODAGID itself directly provides some privacy for the addresses used within the network, as the DODAGID is usually the IPv6 address of the root of the RPL mesh.

An interloper with a radio sniffer would be able to use the network ID to map out the extent of the mesh network.

5. IANA Considerations

IANA has assigned the following value in the "IEEE Std 802.15.4 IETF IE Subtype IDs" registry, as defined by [RFC8137].

Value	Subtype ID	Reference
2	6tisch-Join-Info	RFC 9032

Table 1

6. References

6.1. Normative References

[IEEE.802.15.4] IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE Standard 802.15.4-2015, DOI 10.1109/IEEESTD.2016.7460875, April 2016, <https://ieeexplore.ieee.org/document/7460875>.

[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>.

[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>.

[RFC8137] Kivinen, T. and P. Kinney, "IEEE 802.15.4 Information Element for the IETF", RFC 8137, DOI 10.17487/RFC8137, May 2017, <https://www.rfc-editor.org/info/rfc8137>.

[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>.

[RFC9031] Vučinić, 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/info/rfc9031>.

6.2. Informative References

[NETWORK-ENROLLMENT] Richardson, M., Jadhav, R. A., Thubert, P., and H. She, "Controlling Secure Network Enrollment in RPL networks", Work in Progress, Internet-Draft, draft-ietf-roll-enrollment-priority-04, 7 February 2021, <https://tools.ietf.org/html/draft-ietf-roll-enrollment-priority-04>.

[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>.

[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/info/rfc7554>.

[RFC8180] Vilajosana, X., Ed., Pister, K., and T. Watteyne, "Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration", BCP 210, RFC 8180, DOI 10.17487/RFC8180, May 2017, <https://www.rfc-editor.org/info/rfc8180>.

[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>.

[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>.

Acknowledgments

Thomas Watteyne provided extensive editorial comments on the document. Carles Gomez Montenegro generated a detailed review of the document at Working Group Last Call. Tim Evens provided a number of useful editorial suggestions.

Authors' Addresses

Diego Dujovne (EDITOR)
Universidad Diego Portales
Escuela de Informática y Telecomunicaciones
Av. Ejército 441
Santiago
Región Metropolitana
Chile
Phone: +56 (2) 676-8121
Email: diego.dujovne@mail.udp.cl

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