

6lo Working Group
Internet-Draft
Intended status: Informational
Expires: September 12, 2017

D. Dujovne
Universidad Diego Portales
M. Richardson
Sandelman Software Works
March 11, 2017

**IEEE802.15.4 Informational Element encapsulation of 6tisch Join
Information
draft-richardson-6tisch-join-enhanced-beacon-01**

Abstract

In TSCH mode of IEEE802.15.4, as described by [[I-D.ietf-6tisch-minimal](#)], opportunities for broadcasts are limited to specific times and specific channels. Nodes in a TSCH network typically frequently send Enhanced Beacon (EB) frames to announce the presence of the network. This document provides a mechanism by which small details critical for new nodes (pledges) and long sleeping nodes may be carried within the Enhanced Beacon.

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 <http://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 September 12, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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 [2](#)
- [1.1.](#) Terminology [2](#)
- [1.2.](#) Layer-2 Synchronization [3](#)
- 1.3. Layer-3 synchronization IPv6 Router solicitations and advertisements [3](#)
- [2.](#) Protocol Definition [4](#)
- [2.1.](#) Protocol Example [4](#)
- [3.](#) Security Considerations [5](#)
- [4.](#) Privacy Considerations [5](#)
- [5.](#) IANA Considerations [5](#)
- [6.](#) Acknowledgements [5](#)
- [7.](#) References [5](#)
- [7.1.](#) Normative References [5](#)
- [7.2.](#) Informative References [6](#)
- [Appendix A.](#) Change history [6](#)
- Authors' Addresses [7](#)

1. Introduction

[RFC7554] describes the use of the time-slotted channel hopping (TSCH) mode of [[ieee802154](#)]. As further details in [[I-D.ietf-6tisch-minimal](#)], an Enhanced Beacon is transmitted during a slot designated a broadcast slot.

EDNOTE: Explain why broadcasts are rare, and why we need them. What the Enhanced Beacon is, and what Information Elements are, and how the IETF has a subtype for that area. Explain what kind of things could be placed in Information Elements, how big they could be, and how they could be compressed.

1.1. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [BCP 14](#), [RFC 2119](#) [[RFC2119](#)] and indicate requirement levels for compliant STuPiD implementations.

1.2. Layer-2 Synchronization

As explained in section 6 of [[I-D.ietf-6tisch-minimal](#)], the Enhanced Beacon has a number of purposes: synchronization of ASN and Join Metric, timeslot template identifier, the channel hopping sequence identifier, TSCH SlotFrame and Link IE.

The Enhanced Beacon (EB) is used by nodes already part of a TSCH network to announce its existence. Receiving an EB allows a Joining Node (pledge) to learn about the network and synchronize to it. The EB may also be used as a means for a node already part of the network to re-synchronize [[RFC7554](#)].

There are a limited number of timeslots designated as a broadcast slot by each router. These slots are rare, and with 10ms slots, with a slot-frame length of 100, there may be only 1 slot/s for the beacon.

1.3. Layer-3 synchronization IPv6 Router solicitations and advertisements

At layer 3, [[RFC2461](#)] defines a mechanism by which nodes learn about routers by listening for multicasted Router Advertisements (RA). If no RA is heard within a set time, then a Router Solicitation (RS) may be multicast, to which an RA will be received, usually unicast.

Although [[RFC6775](#)] reduces the amount of multicast necessary to do address resolution via Neighbor Solicitation messages, it still requires multicast of either RAs or RS. This is an expensive operation for two reasons: there are few multicast timeslots for unsolicited RAs; if a pledge node does not hear an RA, and decides to send a RS (consuming a broadcast aloha slot with unencrypted traffic), many unicast RS may be sent in response.

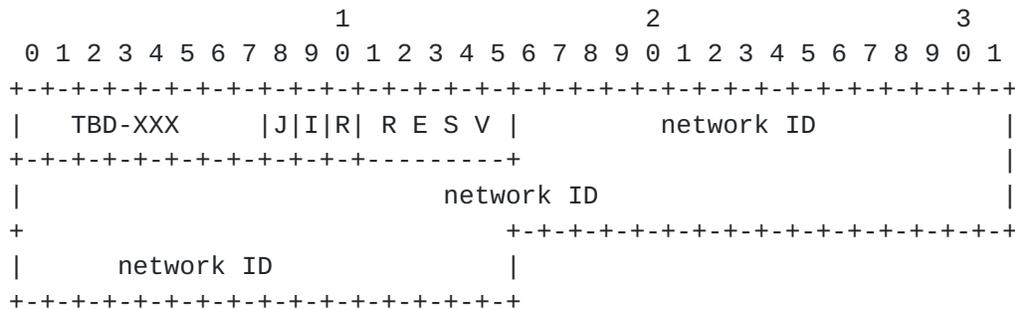
This is a particularly acute issue for the join process for the following reasons:

1. use of a multicast slot by even a non-malicious unauthenticated node for a Router Solicitation may overwhelm that time slot.
2. it may require many seconds of on-time before a new pledge hears a Router Solicitation that it can use.
3. a new pledge may listen to many Enhanced Beacons before it can pick an appropriate network and/or closest Join Assistant to attach to. If it must listen for a RS as well as find the Enhanced Beacon, then the process may take a very long time.

2. Protocol Definition

[I-D.kivinen-802-15-ie] creates a registry for new IETF IE subtypes. This document allocates a new subtype TBD-XXX.

This document documents a new IE subtype structure is as follows. As explained in [I-D.kivinen-802-15-ie] the length of the Sub-Type Content can be calculated from the container, so no length information is necessary.



J the Join Proxy flag is set if the sending node will operate as a Join Proxy according to [I-D.ietf-6tisch-minimal-security].

I the Initiate Join flag is set if this network supports pledges initiating the join process themselves according to [I-D.ietf-6tisch-minimal-security]. If not set, then the pledge should do an NS DAD operation ([RFC6775] section 4.3, explained in [I-D.ietf-6tisch-dtsecurity-secure-join]) and then remain silent, to wait to be contacted.

R the Router Advertisement flag is set if the sending node will act as a Router for host-only nodes that need addressing via unicast Router Solicitation messages.

network ID this is an opaque 16-byte identifier that uniquely identifies this network, potentially among many networks that are operating in the same frequencies in overlapping physical space.

In a 6tisch network, where RPL is used as the mesh routing protocol, the network ID SHOULD be constructed from a SHA256 hash of the DODAGID of the network. The result will be a 32-byte hash, and the lower 16-bytes should be used.

2.1. Protocol Example

Here are three examples of processing.

3. Security Considerations

All of the contents of this Information Element are sent in the clear. The containing Enhanced Beacon is not encrypted, but may be authenticated to nodes which have already received network-wide keying material.

4. Privacy Considerations

The use of a network ID may reveal information about the network. The use of a SHA256 hash of the DODAGID, rather than using the DODAGID directly provides some cover the addresses used within the network. 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 extend of the mesh network.

5. IANA Considerations

Allocate a new number TBD-XXX from Registry IETF IE Sub-type ID. This entry should be called 6tisch-Join-Info.

6. Acknowledgements

Thomas Watteyne provided extensive editorial comments on the document.

7. References

7.1. Normative References

[I-D.ietf-6tisch-architecture]

Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", [draft-ietf-6tisch-architecture-11](#) (work in progress), January 2017.

[I-D.ietf-6tisch-minimal]

Vilajosana, X., Pister, K., and T. Watteyne, "Minimal 6TiSCH Configuration", [draft-ietf-6tisch-minimal-21](#) (work in progress), February 2017.

[I-D.kivinen-802-15-ie]

Kivinen, T. and P. Kinney, "IEEE 802.15.4 Information Element for IETF", [draft-kivinen-802-15-ie-06](#) (work in progress), March 2017.

- [ieee802154]
IEEE Standard, ., "802.15.4-2015 - IEEE Standard for Low-Rate Wireless Personal Area Networks (WPANs)", 2015, <<http://standards.ieee.org/findstds/standard/802.15.4-2015.html>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), DOI 10.17487/RFC2461, December 1998, <<http://www.rfc-editor.org/info/rfc2461>>.
- [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, <<http://www.rfc-editor.org/info/rfc6775>>.
- [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, <<http://www.rfc-editor.org/info/rfc7554>>.

[7.2. Informative References](#)

- [I-D.ietf-6tisch-dtsecurity-secure-join]
Richardson, M., "6tisch Secure Join protocol", [draft-ietf-6tisch-dtsecurity-secure-join-01](#) (work in progress), February 2017.
- [I-D.ietf-6tisch-minimal-security]
Vucinic, M., Simon, J., and K. Pister, "Minimal Security Framework for 6TiSCH", [draft-ietf-6tisch-minimal-security-01](#) (work in progress), February 2017.

[Appendix A. Change history](#)

This is an evolution of an earlier proposal which provided for storing an entire IPv6 Router Advertisement in an Informational Element. It was deemed too general a solution, possibly subject to mis-use. This proposal restricts the use to just the key pieces of information required.

Authors' Addresses

Diego Dujovne (editor)
Universidad Diego Portales
Escuela de Informatica y Telecomunicaciones, Av. Ejercito 441
Santiago, Region Metropolitana
Chile

Phone: +56 (2) 676-8121
Email: diego.dujovne@mail.udp.cl

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

