

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 4, 2017

C. Gomez
S. Darroudi
UPC/i2cat
T. Savolainen
Nokia
October 31, 2016

IPv6 Mesh over Bluetooth(R) Low Energy using IPSP
draft-gomez-6lo-blemesh-02

Abstract

RFC 7668 describes the adaptation of 6LoWPAN techniques to enable IPv6 over Bluetooth low energy networks that follow the star topology. However, recent Bluetooth specifications allow the formation of extended topologies as well. This document specifies the mechanisms needed to enable IPv6 over mesh networks composed of Bluetooth low energy links established by using the Bluetooth Internet Protocol Support Profile.

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 May 4, 2017.

Copyright Notice

Copyright (c) 2016 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 and Requirements Language	3
2. Bluetooth LE Networks and the IPSP	3
3. Specification of IPv6 mesh over Bluetooth LE networks	3
3.1. Protocol stack	4
3.2. Subnet model	4
3.3. Link model	5
3.3.1. Stateless address autoconfiguration	5
3.3.2. Neighbor Discovery	5
3.3.3. Header compression	6
3.3.4. Unicast and multicast mapping	7
4. IANA Considerations	8
5. Security Considerations	8
6. Acknowledgements	8
7. References	8
7.1. Normative References	9
7.2. Informative References	9
Authors' Addresses	10

1. Introduction

Bluetooth low energy (hereinafter, Bluetooth LE) was first introduced in the Bluetooth 4.0 specification. Bluetooth LE (which has been marketed as Bluetooth Smart) is a low-power wireless technology designed for short-range control and monitoring applications. Bluetooth LE is currently implemented in a wide range of consumer electronics devices, such as smartphones and wearable devices. Given the high potential of this technology for the Internet of Things, the Bluetooth Special Interest Group (Bluetooth SIG) and the IETF have produced specifications in order to enable IPv6 over Bluetooth LE, such as the Internet Protocol Support Profile (IPSP) [IPSP], and RFC 7668, respectively. Bluetooth 4.0 only supports Bluetooth LE networks that follow the star topology. In consequence, RFC 7668 was specifically developed and optimized for that type of network topology. However, subsequent Bluetooth specifications allow the formation of extended topologies [BTCorev4.1], such as the mesh topology. The functionality described in RFC 7668 is not sufficient and would fail to enable IPv6 over mesh networks composed of Bluetooth LE links. This document specifies the mechanisms needed to enable IPv6 over mesh networks composed of Bluetooth LE links. This specification also allows to run IPv6 over Bluetooth LE star topology

networks, albeit without all the topology-specific optimizations contained in RFC 7668.

1.1. Terminology and Requirements Language

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].

The terms 6LoWPAN Node (6LN), 6LoWPAN Router (6LR) and 6LoWPAN Border Router (6LBR) are defined as in [RFC6775], with an addition that Bluetooth LE central and Bluetooth LE peripheral (see Section 2) can both be adopted by a 6LN, a 6LR or a 6LBR.

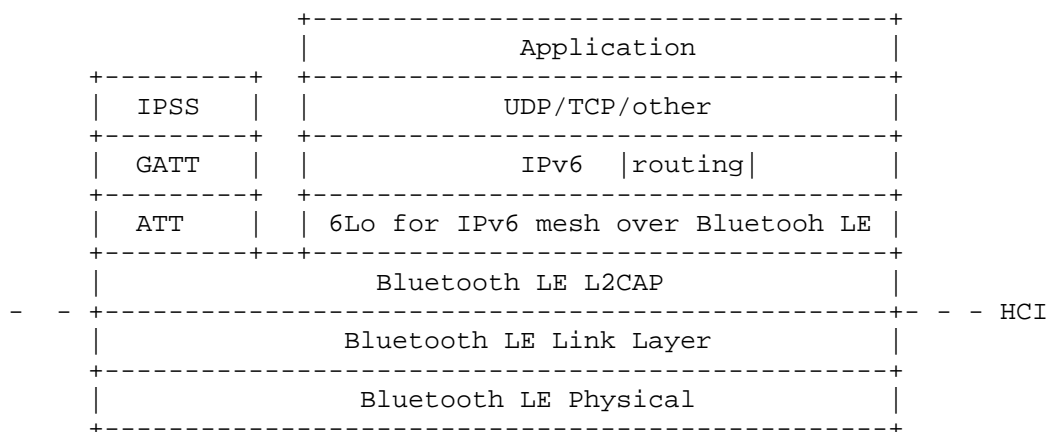
2. Bluetooth LE Networks and the IPSP

Bluetooth LE defines two Generic Access Profile (GAP) roles of relevance herein: the Bluetooth LE central role and the Bluetooth LE peripheral role. A device in the central role, which is called central from now on, has traditionally been able to manage multiple simultaneous connections with a number of devices in the peripheral role, called peripherals hereinafter. Bluetooth 4.1 introduced the possibility for a peripheral to be connected to more than one central simultaneously, therefore allowing extended topologies beyond the star topology for a Bluetooth LE network. In addition, a device may simultaneously be a central in a set of link layer connections, as well as a peripheral in others. On the other hand, the IPSP enables discovery of IP-enabled devices and the establishment of a link layer connection for transporting IPv6 packets. The IPSP defines the Node and Router roles for devices that consume/originate IPv6 packets and for devices that can route IPv6 packets, respectively. Consistently with Bluetooth 4.1, a device may implement both roles simultaneously.

This document assumes a mesh network composed of Bluetooth LE links, where link layer connections have been established between neighboring IPv6-enabled devices. The IPv6 forwarding devices of the mesh have to implement both Node and Router roles, while simpler leaf-only nodes can implement only the Node role. In an IPv6-enabled mesh of Bluetooth LE links, a node is a neighbor of another node, and vice versa, if a link layer connection has been established between both by using the IPSP functionality for discovery and link layer connection establishment for IPv6 packet transport.

3. Specification of IPv6 mesh over Bluetooth LE networks

Figure 1 illustrates the protocol stack for IPv6 mesh over Bluetooth LE networks. There are two main differences with the IPv6 over Bluetooth LE stack in RFC 7668: a) the adaptation layer below IPv6 (labelled as "6Lo for mesh of Bluetooth LE") is now adapted for mesh networks of Bluetooth LE links, and b) the protocol stack for IPv6 mesh networks of Bluetooth LE links includes IPv6 routing functionality.



3.2. Subnet model

For IPv6 mesh over Bluetooth LE, a multilink model has been chosen, as further illustrated in Figure 2. As IPv6 over Bluetooth LE is intended for constrained nodes, and for Internet of Things use cases and environments, the complexity of implementing a separate subnet on each peripheral-central link and routing between the subnets appears to be excessive. In this specification, the benefits of treating the collection of point-to-point links between a central and its connected peripherals as a single multilink subnet rather than a multiplicity of separate subnets are considered to outweigh the multilink model's drawbacks as described in [RFC4903].

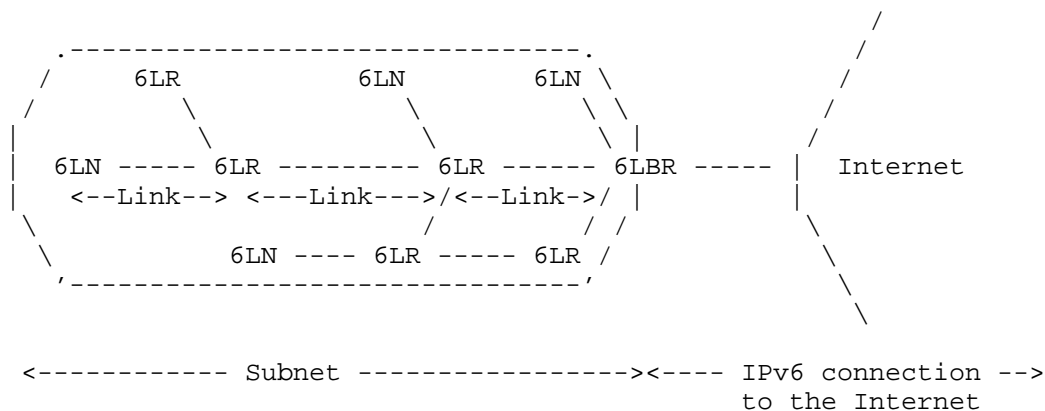


Figure 2: Example of an IPv6 mesh over a Bluetooth LE network connected to the Internet

One or more 6LBRs are connected to the Internet. 6LNs are connected to the network through a 6LR or a 6LBR. A prefix is used on the whole subnet.

IPv6 mesh networks over Bluetooth LE MUST follow a route-over approach. This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE.

3.3. Link model

3.3.1. Stateless address autoconfiguration

6LN, 6LR and 6LBR IPv6 addresses in an IPv6 mesh over Bluetooth LE are configured as per section 3.2.2 of RFC 7668.

Multihop DAD functionality as defined in section 8.2 of RFC 6775, or some substitute mechanism (see section 3.3.2), MUST be supported.

3.3.2. Neighbor Discovery

'Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)' [RFC6775] describes the neighbor discovery approach as adapted for use in several 6LoWPAN topologies, including the mesh topology. The route-over functionality of RFC 6775 MUST be supported.

The following aspects of the Neighbor Discovery optimizations [RFC6775] are applicable to Bluetooth LE 6LNs:

1. A Bluetooth LE 6LN MUST NOT register its link-local address. A Bluetooth LE 6LN MUST register its non-link-local addresses with its routers by sending a Neighbor Solicitation (NS) message with the Address Registration Option (ARO) and process the Neighbor Advertisement (NA) accordingly. The NS with the ARO option MUST be sent irrespective of the method used to generate the IID. The ARO option requires use of an EUI-64 identifier [RFC6775]. In the case of Bluetooth LE, the field SHALL be filled with the 48-bit device address used by the Bluetooth LE node converted into 64-bit Modified EUI-64 format [RFC4291].

If the 6LN registers for a same compression context multiple addresses that are not based on Bluetooth device address, the header compression efficiency will decrease.

2. For sending Router Solicitations and processing Router Advertisements the Bluetooth LE 6LNs MUST, respectively, follow Sections 5.3 and 5.4 of the [RFC6775].

3. The router behavior for 6LRs and 6LBRs is described in Section 6 of RFC 6775. However, as per this specification, routers SHALL NOT use multicast NSs to discover other routers' link layer addresses.

4. Border router behavior is described in Section 7 of RFC 6775.

RFC 6775 defines substitutable mechanisms for distributing prefixes and context information (section 8.1 of RFC 6775), as well as for Duplicate Address Detection across a route-over 6LoWPAN (section 8.2 of RFC 6775). Implementations of this specification MUST support the features described in sections 8.1 and 8.2 of RFC 6775 unless some alternative ("substitute") from some other specification is supported.

3.3.3. Header compression

Header compression as defined in RFC 6282 [RFC6282], which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, is REQUIRED as the basis for IPv6 header compression on top of Bluetooth LE. All headers MUST be compressed according to RFC 6282 [RFC6282] encoding formats.

To enable efficient header compression, when the 6LBR sends a Router Advertisement it MUST include a 6LoWPAN Context Option (6CO) [RFC6775] matching each address prefix advertised via a Prefix Information Option (PIO) [RFC4861] for use in stateless address autoconfiguration.

The specific optimizations of RFC 7668 for header compression, which exploit the star topology and ARO, cannot be generalized in a mesh network composed of Bluetooth LE links. Still, a subset of those optimizations can be applied in some cases in such a network. In particular, the latter comprise link-local interactions, non-link-local packet transmissions originated and performed by a 6LN, and non-link-local packet transmissions originated by a 6LN neighbor and sent to a 6LN. For the rest of packet transmissions, context-based compression MAY be used.

When a device transmits a packet to a neighbor, the sender MUST fully elide the source IID if the source IPv6 address is the link-local address based on the sender's Bluetooth device address (SAC=0, SAM=11). The sender also MUST fully elide the destination IPv6 address if it is the link-local-address based on the neighbor's Bluetooth device address (DAC=0, DAM=11).

When a 6LN transmits a packet, with a non-link-local source address that the 6LN has registered with ARO in the next-hop router for the indicated prefix, the source address MUST be fully elided if it is the latest address that the 6LN has registered for the indicated prefix (SAC=1, SAM=11). If the source non-link-local address is not the latest registered by the 6LN, then the 64-bits of the IID SHALL be fully carried in-line (SAC=1, SAM=01) or if the first 48-bits of the IID match with the latest address registered by the 6LN, then the last 16-bits of the IID SHALL be carried in-line (SAC=1, SAM=10).

When a router transmits a packet to a neighboring 6LN, with a non-link-local destination address, the router MUST fully elide the destination IPv6 address if the destination address is the latest registered by the 6LN with ARO for the indicated context (DAC=1, DAM=11). If the destination address is a non-link-local address and not the latest registered, then the 6LN MUST either include the IID part fully in-line (DAM=01) or, if the first 48-bits of the IID match to the latest registered address, then elide those 48-bits (DAM=10).

3.3.4. Unicast and multicast mapping

The Bluetooth LE Link Layer does not support multicast. Hence, traffic is always unicast between two Bluetooth LE neighboring nodes. If a node needs to send a multicast packet to several neighbors, it has to replicate the packet and unicast it on each link. However, this may not be energy efficient, and particular care must be taken if the node is battery powered. A router (i.e. a 6LR or a 6LBR) MUST keep track of neighboring multicast listeners, and it MUST NOT forward multicast packets to neighbors that have not registered as listeners for multicast groups the packets belong to.

4. IANA Considerations

There are no IANA considerations related to this document.

5. Security Considerations

The security considerations in RFC 7668 apply.

IPv6 mesh networks over Bluetooth LE require a routing protocol to find end-to-end paths. Unfortunately, the routing protocol may generate additional opportunities for threats and attacks to the network.

RFC 7416 [RFC 7416] provides a systematic overview of threats and attacks on the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), as well as countermeasures. In that document, described threats and attacks comprise threats due to failures to authenticate, threats due to failure to keep routing information, threats and attacks on integrity, and threats and attacks on availability. Reported countermeasures comprise confidentiality attack, integrity attack, and availability attack countermeasures.

While this specification does not state the routing protocol to be used in IPv6 mesh over Bluetooth LE networks, the guidance of RFC 7416 is useful when RPL is used in such scenarios. Furthermore, such guidance may partly apply for other routing protocols as well.

6. Acknowledgements

The Bluetooth, Bluetooth Smart and Bluetooth Smart Ready marks are registered trademarks owned by Bluetooth SIG, Inc.

The authors of this document are grateful to all RFC 7668 authors, since this document borrows many concepts (albeit, with necessary extensions) from RFC 7668.

The authors also thank Alain Michaud, Mark Powell and Martin Turon for their comments, which helped improve the document.

Carles Gomez has been supported in part by the Spanish Government Ministerio de Economia y Competitividad through project TEC2012-32531, and FEDER.

7. References

7.1. Normative References

- [BTCorev4.1] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 4.1", December 2013, <<https://www.bluetooth.org/en-us/specification/adopted-specifications>>.
- [IPSP] Bluetooth Special Interest Group, "Bluetooth Internet Protocol Support Profile Specification Version 1.0.0", December 2014, <<https://www.bluetooth.org/en-us/specification/adopted-specifications>>.
- [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>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<http://www.rfc-editor.org/info/rfc4291>>.
- [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, <<http://www.rfc-editor.org/info/rfc4861>>.
- [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, <<http://www.rfc-editor.org/info/rfc6282>>.
- [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>>.
- [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <<http://www.rfc-editor.org/info/rfc7668>>.

7.2. Informative References

- [RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, DOI 10.17487/RFC4903, June 2007, <<http://www.rfc-editor.org/info/rfc4903>>.

[RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015, <<http://www.rfc-editor.org/info/rfc7416>>.

Authors' Addresses

Carles Gomez
Universitat Politecnica de Catalunya/Fundacio i2cat
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: carlesgo@entel.upc.edu

Sayed Mahdi Darroudi
Universitat Politecnica de Catalunya/Fundacio i2cat
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: sm.darroudi@entel.upc.edu

Teemu Savolainen
Nokia Technologies
Hatanpaan valtatie 30
Tampere 33100
Finland

Email: teemu.savolainen@nokia.com

6lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 26, 2017

C. Gomez
J. Paradells
UPC/i2CAT
J. Crowcroft
University of Cambridge
October 23, 2016

Optimized 6LoWPAN Fragmentation Header
draft-gomez-6lo-optimized-fragmentation-header-00

Abstract

RFC 4944 specifies 6LoWPAN fragmentation, in order to support the IPv6 MTU requirement over IEEE 802.15.4-2003 networks. The 6LoWPAN fragmentation header format comprises a 4-byte format for the first fragment, and a 5-byte format for subsequent fragments. This specification defines a more efficient 3-byte, optimized 6LoWPAN fragmentation header for all fragments.

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 April 26, 2017.

Copyright Notice

Copyright (c) 2016 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. Conventions used in this document	3
2. 6LoFH rules and format	3
3. Changes from RFC 4944 fragmentation header and rationale . .	4
4. IANA Considerations	5
5. Security Considerations	5
6. Acknowledgments	6
7. Annex A. Quantitative performance comparison of RFC 4944 fragmentation header with 6LoFH	7
8. References	7
8.1. Normative References	7
8.2. Informative References	8
Authors' Addresses	8

1. Introduction

IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) was originally designed as an adaptation layer intended to enable IPv6 over IEEE 802.15.4- 2003 networks [RFC4944]. One of the 6LoWPAN protocol suite components is fragmentation, which fulfills the IPv6 MTU requirement of 1280 bytes [RFC2460] over a radio interface with a layer two (L2) payload size around 100 bytes (in the best case) and without fragmentation support [RFC4944].

RFC 4944 defines the 6LoWPAN fragmentation header format, which comprises a 4-byte format for the first fragment, and a 5-byte format for subsequent fragments. This specification defines a more efficient 3-byte, optimized 6LoWPAN Fragmentation Header (6LoFH). The benefits of using 6LoFH are the following:

- Reduced overhead for transporting an IPv6 packet that requires fragmentation (see Annex A). This decreases consumption of energy and bandwidth, which are typically limited resources in the scenarios where 6LoWPAN fragmentation is used.

- Because the datagram offset can be expressed in increments of a single octet, 6LoFH enables the transport of IPv6 packets over L2 data units with a maximum payload size as small as only 4 bytes in the most extreme case. Note that RFC 4944 fragmentation can only be used over L2 technologies with a maximum L2 payload size of at least 13 bytes.

In comparison with the 6LoWPAN fragmentation header, parsing of the 6loFH format is also simplified, as the format has a constant size, and a 'symmetric' shape for both the first fragment and subsequent fragments. However, receiver buffer management will involve greater complexity as explained in Section 3.

1.1. Conventions used in this document

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 [RFC2119]

2. 6LoFH rules and format

If an entire payload (e.g., IPv6) datagram fits within a single L2 data unit, it is unfragmented and a fragmentation header is not needed. If the datagram does not fit within a single L2 data unit, it SHALL be broken into fragments. The first fragment SHALL contain the first fragment header as defined in Figure 1.

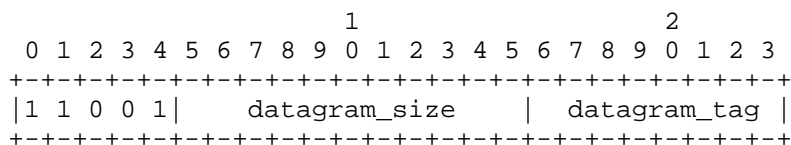


Figure 1: First Fragment

The second and subsequent fragments (up to and including the last) SHALL contain a fragmentation header that conforms to the format shown in Figure 2.

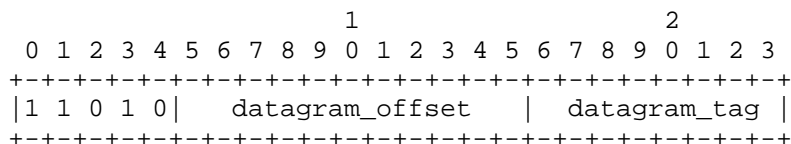


Figure 2: Subsequent Fragments

datagram_size: This 11-bit field encodes the size of the entire IP packet before link-layer fragmentation (but after IP layer fragmentation). For IPv6, the datagram size SHALL be 40 octets (the size of the uncompressed IPv6 header) more than the value of Payload Length in the IPv6 header [RFC4944] of the packet. Note that this

packet may already be fragmented by hosts involved in the communication, i.e., this field needs to encode a maximum length of 1280 octets (the required by IPv6).

datagram_tag: The value of `datagram_tag` (datagram tag) SHALL be the same for all fragments of a payload (e.g., IPv6) datagram. The sender SHALL increment `datagram_tag` for successive, fragmented datagrams. The incremented value of `datagram_tag` SHALL wrap from 255 back to zero. This field is 8 bits long, and its initial value is not defined.

datagram_offset: This field is present only in the second and subsequent fragments and SHALL specify the offset, in increments of 1 octet, of the fragment from the beginning of the payload datagram. The first octet of the datagram (e.g., the start of the IPv6 header) has an offset of zero; the implicit value of `datagram_offset` in the first fragment is zero. This field is 11 bits long.

The recipient of link fragments SHALL use (1) the sender's L2 source address, (2) the destination's L2 address, (3) `datagram_size`, and (4) `datagram_tag` to identify all the fragments that belong to a given datagram.

Upon receipt of a link fragment, the recipient starts constructing the original unfragmented packet whose size is `datagram_size`. It uses the `datagram_offset` field to determine the location of the individual fragments within the original unfragmented packet. For example, it may place the data payload (except the encapsulation header) within a payload datagram reassembly buffer at the location specified by `datagram_offset`. The size of the reassembly buffer SHALL be determined from `datagram_size`.

If a fragment recipient disassociates from its L2 network, the recipient MUST discard all link fragments of all partially reassembled payload datagrams, and fragment senders MUST discard all not yet transmitted link fragments of all partially transmitted payload (e.g., IPv6) datagrams. Similarly, when a node first receives a fragment with a given `datagram_tag`, it starts a reassembly timer. When this time expires, if the entire packet has not been reassembled, the existing fragments MUST be discarded and the reassembly state MUST be flushed. The reassembly timeout MUST be set to a maximum of TBD seconds).

3. Changes from RFC 4944 fragmentation header and rationale

The main changes introduced in this specification to the fragmentation header format defined in RFC 4944 are listed below, together with their rationale:

-- The datagram size field is only included in the first fragment.
Rationale: In the RFC 4944 fragmentation header, the datagram size was included in all fragments to ease the task of reassembly at the receiver, since in an IEEE 802.15.4 mesh network, the fragment that arrives earliest to a destination is not necessarily the first fragment transmitted by the source. Nevertheless, the fragmentation format defined in this document supports reordering, at the expense of additional complexity in this regard.

-- The datagram tag size is reduced from 2 bytes to 1 byte.
Rationale: Given the low bit rate, as well as the relatively low message rate in IEEE 802.15.4 scenarios, ambiguities due to datagram tag wrapping events are unlikely despite the reduced tag space.

-- The datagram offset size is increased from 8 bits to 11 bits.
Rationale: This allows to express the datagram offset in single-octet increments.

4. IANA Considerations

This document allocates the following sixteen RFC 4944 Dispatch type values:

11001 000

through

11001 111

and

11010 000

through

11010 111

5. Security Considerations

6LoWPAN fragmentation attacks have been analyzed in the literature. Countermeasures to these have been proposed as well [HHWH].

A node can perform a buffer reservation attack by sending a first fragment to a target. Then, the receiver will reserve buffer space for the whole packet on the basis of the datagram size announced in that first fragment. Other incoming fragmented packets will be dropped while the reassembly buffer is occupied during the reassembly timeout. Once that timeout expires, the attacker can repeat the same

procedure, and iterate, thus creating a denial of service attack. The (low) cost to mount this attack is linear with the number of buffers at the target node. However, the cost for an attacker can be increased if individual fragments of multiple packets can be stored in the reassembly buffer. To further increase the attack cost, the reassembly buffer can be split into fragment-sized buffer slots. Once a packet is complete, it is processed normally. If buffer overload occurs, a receiver can discard packets based on the sender behavior, which may help identify which fragments have been sent by an attacker.

In another type of attack, the malicious node is required to have overhearing capabilities. If an attacker can overhear a fragment, it can send a spoofed duplicate (e.g. with random payload) to the destination. A receiver cannot distinguish legitimate from spoofed fragments. Therefore, the original IPv6 packet will be considered corrupt and will be dropped. To protect resource-constrained nodes from this attack, it has been proposed to establish a binding among the fragments to be transmitted by a node, by applying content-chaining to the different fragments, based on cryptographic hash functionality. The aim of this technique is to allow a receiver to identify illegitimate fragments.

Further attacks may involve sending overlapped fragments (i.e. comprising some overlapping parts of the original datagram) or announcing a datagram size in the first fragment that does not reflect the actual amount of data carried by the fragments. Implementers should make sure that correct operation is not affected by such events.

6. Acknowledgments

In section 2, the authors have reused extensive parts of text available in section 5.3 of RFC 4944, and would like to thank the authors of RFC 4944.

The authors would like to thank Carsten Bormann, Tom Phinney, Ana Minaburo and Laurent Toutain for valuable comments that helped improve the document.

Carles Gomez has been funded in part by the Spanish Government (Ministerio de Educacion, Cultura y Deporte) through the Jose Castillejo grant CAS15/00336. Part of his contribution to this work has been carried out during his stay as a visiting scholar at the Computer Laboratory of the University of Cambridge.

7. Annex A. Quantitative performance comparison of RFC 4944 fragmentation header with 6LoFH

	IPv6 datagram size (bytes)							
	40		100		640		1280	
L2 payload (bytes)	4944	6LoFH	4944	6LoFH	4944	6LoFH	4944	6LoFH
10	----	18	----	45	----	276	----	549
20	19	9	59	18	394	114	794	228
40	0	0	19	9	99	54	199	105
60	0	0	9	6	69	36	134	69
80	0	0	9	6	44	27	89	51
100	0	0	0	0	39	21	74	42

Figure 3: Adaptation layer fragmentation overhead (in bytes) required to transport an IPv6 datagram

Note 1: while IEEE 802.15.4-2003 allows a maximum L2 payload size between 81 and 102 bytes, a range of L2 payload size between 10 and 100 bytes is considered in the study to illustrate the performance of 6LoFH also for other potential L2 technologies with short payload size and without fragmentation support.

Note 2: with the RFC 4944 fragmentation header it is not possible to transport IPv6 datagrams of the considered sizes over a 10-byte payload L2 technology.

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <<http://www.rfc-editor.org/info/rfc2460>>.

- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <<http://www.rfc-editor.org/info/rfc4944>>.
- [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, <<http://www.rfc-editor.org/info/rfc6282>>.

8.2. Informative References

- [HHWH] Hummen et al, R., "6LoWPAN fragmentation attacks and mitigation mechanisms", 2013.
- [I-D.minaburo-lpwan-gap-analysis] Minaburo, A., Gomez, C., Toutain, L., Paradells, J., and J. Crowcroft, "LPWAN Survey and GAP Analysis", draft-minaburo-lpwan-gap-analysis-02 (work in progress), October 2016.

Authors' Addresses

Carles Gomez
UPC/i2CAT
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: carlesgo@entel.upc.edu

Josep Paradells
UPC/i2CAT
C/Jordi Girona, 1-3
Barcelona 08034
Spain

Email: josep.paradells@entel.upc.edu

Jon Crowcroft
University of Cambridge
JJ Thomson Avenue
Cambridge, CB3 0FD
United Kingdom

Email: jon.crowcroft@cl.cam.ac.uk

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2017

Y-G. Hong
ETRI
C. Gomez
UPC/i2cat
Y-H. Choi
ETRI
D-Y. Ko
SKtelecom
October 30, 2016

IPv6 over Constrained Node Networks(6lo) Applicability & Use cases
draft-hong-6lo-use-cases-03

Abstract

This document describes the applicability of IPv6 over constrained node networks (6lo) and use cases. It describes the practical deployment scenarios of 6lo technologies with the consideration of 6lo link layer technologies and identifies the requirements. In addition to IEEE 802.15.4, various link layer technologies such as ITU-T G.9959 (Z-Wave), BLE, DECT-ULE, MS/TP, NFC, LTE MTC, and IEEE 802.15.4e(6tisch) are widely used at constrained node networks for typical services. Based on these link layer technologies, IPv6 over networks of resource-constrained nodes has various and practical use cases. To efficiently implement typical services, the applicability and consideration of several design space dimensions are described.

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 May 3, 2017.

Copyright Notice

Copyright (c) 2016 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	3
2. Conventions and Terminology	4
3. 6lo Link layer technologies	4
3.1. ITU-T G.9959	4
3.2. Bluetooth Low Energy	4
3.3. DECT-ULE	5
3.4. Master-Slave/Token-Passing	5
3.5. NFC	6
3.6. LTE MTC	6
3.7. IEEE 802.15.4e	7
4. 6lo Deployment Scenarios	8
5. Design Space	8
6. 6lo Use Cases	10
6.1. Use case of ITU-T G.9959: Smart Home	10
6.2. Use case of Bluetooth Low Energy: Smartphone-Based Interaction with Constrained Devices	11
6.3. Use case of DECT-ULE: Smart Home	13
6.4. Use case of MS/TP:	14
6.5. Use case of NFC: Alternative Secure Transfer	14
6.6. Use case of LTE MTC	16
6.7. Use case of IEEE 802.15.4e:	18
7. IANA Considerations	18
8. Security Considerations	18
9. Acknowledgements	18
10. References	19
10.1. Normative References	19
10.2. Informative References	20
Authors' Addresses	21

1. Introduction

Running IPv6 on constrained node networks has different features from general node networks due to the characteristics of constrained node networks such as small packet size, short link-layer address, low bandwidth, network topology, low power, low cost, and large number of devices [RFC4919]. For example, because some IEEE 802.15.4 link layers have a frame size of 127 octets and IPv6 requires the layer below to support an MTU of 1280 bytes, an appropriate fragmentation and reassembly adaptation layer must be provided at the layer of below IPv6. Also, the limited size of IEEE 802.15.4 frame and low energy consumption requirements make the need for header compression. IETF 6lowpan (IPv6 over Low powerWPAN) working group published, an adaptation layer for sending IPv6 packets over IEEE 802.15.4 [RFC4944], compression format for IPv6 datagrams over IEEE 802.15.4-based networks [RFC6282], and Neighbor Discovery Optimization for 6lowpan [RFC6775].

As IoT (Internet of Things) services become more popular, various link layer technologies such as Bluetooth Low Energy (Bluetooth LE), ITU-T G.9959 (Z-Wave), Digital Enhanced Cordless Telecommunications - Ultra Low Energy (DECT-ULE), Master-Slave/Token Passing (MS/TP), Near Field Communication (NFC), and LTE Machine Type Communication are actively used. And the transmission of IPv6 packets over these link layer technologies is required. A number of IPv6-over-foo documents have been developed in the IETF 6lo (IPv6 over Networks of Resource-constrained Nodes) and 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) working groups.

In the 6lowpan working group, the [RFC6568], "Design and Application Spaces for 6LoWPANs" was published and it describes potential application scenarios and use cases for low-power wireless personal area networks. In this document, various design space dimensions such as deployment, network size, power source, connectivity, multi-hop communication, traffic pattern, security level, mobility, and QoS were analyzed. And it described a fundamental set of 6lowpan application scenarios and use cases: Industrial monitoring-Hospital storage rooms, Structural monitoring-Bridge safety monitoring, Connected home-Home Automation, Healthcare-Healthcare at home by tele-assistance, Vehicle telematics-telematics, and Agricultural monitoring-Automated vineyard.

Even though the [RFC6568] describes some potential application scenarios and use cases and it lists the design space in the context of 6lowpan, it does not cover the different use cases and design space in the context of the 6lo working group. The RFC6568 assumed that the link layer technology is the IEEE802.15.4 and the described application scenarios and use cases were based on the IEEE 802.15.4

technologies. Due to various link layer technologies such as ITU-T G.9959 (Z-Wave), BLE, DECT-ULE, MS/TP, NFC, LTE MTC, and IEEE 802.15.4e(6tisch), potential application scenarios and use cases of 6lo will go beyond the RFC6568.

This document provides the applicability and use cases of 6lo, considering the following:

- o 6lo applicability and use cases MAY be uniquely different from those of 6lowpan.
- o 6lo applicability and use cases SHOULD cover various IoT related wire/wireless link layer technologies providing practical information of such technologies.
- o 6lo applicability and use cases SHOULD describe characteristics and typical use cases of each link layer technology, and then 6lo use cases's applicability.

2. Conventions 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 [RFC2119].

3. 6lo Link layer technologies

3.1. ITU-T G.9959

The ITU-T G.9959 recommendation [G.9959] targets low-power Personal Area Networks (PANs). G.9959 defines how a unique 32-bit HomeID network identifier is assigned by a network controller and how an 8-bit NodeID host identifier is allocated to each node. NodeIDs are unique within the network identified by the HomeID. The G.9959 HomeID represents an IPv6 subnet that is identified by one or more IPv6 prefixes [RFC7428].

3.2. Bluetooth Low Energy

Bluetooth LE was introduced in Bluetooth 4.0, enhanced in Bluetooth 4.1, and developed even further in successive versions. Bluetooth SIG has also published Internet Protocol Support Profile (IPSP). The IPSP enables discovery of IP-enabled devices and establishment of link-layer connection for transporting IPv6 packets. IPv6 over Bluetooth LE is dependent on both Bluetooth 4.1 and IPSP 1.0 or newer.

Devices such as mobile phones, notebooks, tablets and other handheld computing devices which will include Bluetooth 4.1 chipsets will probably also have the low-energy variant of Bluetooth. Bluetooth LE will also be included in many different types of accessories that collaborate with mobile devices such as phones, tablets and notebook computers. An example of a use case for a Bluetooth LE accessory is a heart rate monitor that sends data via the mobile phone to a server on the Internet [RFC7668].

3.3. DECT-ULE

DECT ULE is a low power air interface technology that is designed to support both circuit switched services, such as voice communication, and packet mode data services at modest data rate.

The DECT ULE protocol stack consists of the PHY layer operating at frequencies in the 1880 - 1920 MHz frequency band depending on the region and uses a symbol rate of 1.152 Mbps. Radio bearers are allocated by use of FDMA/TDMA/TDD techniques.

In its generic network topology, DECT is defined as a cellular network technology. However, the most common configuration is a star network with a single Fixed Part (FP) defining the network with a number of Portable Parts (PP) attached. The MAC layer supports traditional DECT as this is used for services like discovery, pairing, security features etc. All these features have been reused from DECT.

The DECT ULE device can switch to the ULE mode of operation, utilizing the new ULE MAC layer features. The DECT ULE Data Link Control (DLC) provides multiplexing as well as segmentation and re-assembly for larger packets from layers above. The DECT ULE layer also implements per-message authentication and encryption. The DLC layer ensures packet integrity and preserves packet order, but delivery is based on best effort.

The current DECT ULE MAC layer standard supports low bandwidth data broadcast. However the usage of this broadcast service has not yet been standardized for higher layers [I-D.ietf-6lo-dect-ule].

3.4. Master-Slave/Token-Passing

MS/TP is a contention-free access method for the RS-485 physical layer, which is used extensively in building automation networks.

An MS/TP device is typically based on a low-cost microcontroller with limited processing power and memory. Together with low data rates and a small address space, these constraints are similar to those

faced in 6LoWPAN networks and suggest some elements of that solution might be leveraged. MS/TP differs significantly from 6LoWPAN in at least three respects: a) MS/TP devices typically have a continuous source of power, b) all MS/TP devices on a segment can communicate directly so there are no hidden node or mesh routing issues, and c) recent changes to MS/TP provide support for large payloads, eliminating the need for link-layer fragmentation and reassembly.

MS/TP is designed to enable multidrop networks over shielded twisted pair wiring. It can support a data rate of 115,200 baud on segments up to 1000 meters in length, or segments up to 1200 meters in length at lower baud rates. An MS/TP link requires only a UART, an RS-485 transceiver with a driver that can be disabled, and a 5ms resolution timer. These features make MS/TP a cost-effective field bus for the most numerous and least expensive devices in a building automation network [I-D.ietf-6lo-6lobac].

3.5. NFC

NFC technology enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and it enables a consumer to utilize one device across different systems.

Extending the capability of contactless card technology, NFC also enables devices to share information at a distance that is less than 10 cm with a maximum communication speed of 424 kbps. Users can share business cards, make transactions, access information from a smart poster or provide credentials for access control systems with a simple touch.

NFC's bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch. In addition to the easy connection and quick transactions, simple data sharing is also available [I-D.ietf-6lo-nfc].

3.6. LTE MTC

LTE category defines the overall performance and capabilities of the UE (User Equipment). For example, the maximum down rate of category 1 UE and category 2 UE are 10.3 Mbit/s and 51.0 Mbit/s respectively. There are many categories in LTE standard. 3GPP standards defined the category 0 to be used for low rate IoT service in release 12. Since

category 1 and category 0 could be used for low rate IoT service, these categories are called LTE MTC (Machine Type Communication) [LTE_MTC].

LTE MTC have the advantages compared to above category 2 to be used for low rate IoT service such as low power and low cost.

The below figure shows the primary characteristics of LTE MTC.

Category	Max. Data Rate Down	Max. Data Rate Up
Category 0	1.0 Mbit/s	1.0 Mbit/s
Category 1	10.3 Mbit/s	5.2 Mbit/s

Table 1: Primary characteristics of LTE MTC

3.7. IEEE 802.15.4e

The Timeslotted Channel Hopping (TSCH) mode was introduced in the IEEE 802.15.4-2015 standard. In a TSCH network, all nodes are synchronized. Time is sliced up into timeslots. The duration of a timeslot, typically 10ms, is large enough for a node to send a full-sized frame to its neighbor, and for that neighbor to send back an acknowledgment to indicate successful reception. Timeslots are grouped into one of more slotframes, which repeat over time.

All the communication in the network is orchestrated by a communication schedule which indicates to each node what to do in each of the timeslots of a slotframe: transmit, listen or sleep. The communication schedule can be built so that the right amount of link-layer resources (the cells in the schedule) are scheduled to satisfy the communication needs of the applications running on the network, while keeping the energy consumption of the nodes very low. Cells can be scheduled in a collision-free way, introducing a high level of determinism to the network.

A TSCH network exploits channel hopping: subsequent packets exchanged between neighbor nodes are done so on a different frequency. This means that, if a frame isn't received, the transmitter node will re-transmitt the frame on a different frequency. The resulting "channel hopping" efficiently combats external interference and multi-path fading.

The main benefits of IEEE 802.15.4 TSCH are:

- ultra high reliability. Off-the-shelf commercial products offer over 99.999% end-to-end reliability.

- ultra low-power consumption. Off-the-shelf commercial products offer over a decade of battery lifetime.

4. 6lo Deployment Scenarios

In this clause, we will describe some 6lo deployment scenarios such as Smart Grid activity in WiSun

[TBD]

5. Design Space

The [RFC6568] lists the dimensions used to describe the design space of wireless sensor networks in the context of the 6LoWPAN working group. The design space is already limited by the unique characteristics of a LoWPAN (e.g., low power, short range, low bit rate). In the RFC 6568, the following design space dimensions are described; Deployment, Network size, Power source, Connectivity, Multi-hop communication, Traffic pattern, Mobility, Quality of Service (QoS).

The design space dimensions of 6lo are a little different from those of the RFC 6568 due to the different characteristics of 6lo link layer technologies. The following design space dimensions can be considered.

- o Deployment/Bootstrapping: 6lo nodes can be connected randomly, or in an organized manner. The bootstrapping has different characteristics for each link layer technology.
- o Topology: Topology of 6lo networks may inherently follow the characteristics of each link layer technology. Point-to-point, star, tree or mesh topologies can be configured, depending on the link layer technology considered.
- o L2-Mesh or L3-Mesh: L2-mesh and L3-mesh may inherently follow the characteristics of each link layer technology. Some link layer technologies may support L2-mesh and some may not support.
- o Multi-link subnet, single subnet: The selection of multi-link subnet and single subnet depends on connectivity and the number of 6lo nodes.

- o Data rate: Originally, the link layer technologies of 6lo have low rate of data transmission. But, by adjusting the MTU, it can deliver higher data rate.
- o Buffering requirements: Some 6lo use case may require more data rate than the link layer technology support. In this case, a buffering mechanism to manage the data is required.
- o Security Requirements: Some 6lo use case can involve transferring some important and personal data between 6lo nodes. In this case, high-level security support is required.
- o Mobility across 6lo networks and subnets: The movement of 6lo nodes is dependent on the 6lo use case. If the 6lo nodes can move or moved around, it requires a mobility management mechanism.
- o Time synchronization requirements: The requirement of time synchronization of the upper layer service is dependent on the 6lo use case. For some 6lo use case related to health service, the measured data must be recorded with exact time and must be transferred with time synchronization.
- o Reliability and QoS: Some 6lo use case requires high reliability, for example real-time service or health-related services.
- o Traffic patterns: 6lo use cases may involve various traffic patterns. For example, some 6lo use case may require short data length and random transmission. Some 6lo use case may require continuous data and periodic data transmission.
- o Security Bootstrapping: Without the external operations, 6lo nodes must have the security bootstrapping mechanism.
- o Power use strategy: to enable certain use cases, there may be requirements on the class of energy availability and the strategy followed for using power for communication [RFC7228]. Each link layer technology defines a particular power use strategy which may be tuned [I-D.ietf-lwig-energy-efficient]. Readers are expected to be familiar with RFC 7228 terminology.
- o Update firmware requirements: Most 6lo uses case will need a mechanism for updating firmware. In these cases support for over the air updates are required, probably in a broadcast mode when bandwidth is low and the number of identical devices is high.

6. 6lo Use Cases

6.1. Use case of ITU-T G.9959: Smart Home

Z-Wave is one of the main technologies that may be used to enable smart home applications. Born as a proprietary technology, Z-Wave was specifically designed for this use case. Recently, the Z-Wave radio interface (physical and MAC layers) has been standardized as the ITU-T G.9959 specification.

Example: Use of ITU-T G.9959 for Home Automation

Variety of home devices (e.g. light dimmers/switches, plugs, thermostats, blinds/curtains and remote controls) are augmented with ITU-T G.9959 interfaces. A user may turn on/off or may control home appliances by pressing a wall switch or by pressing a button in a remote control. Scenes may be programmed, so that after a given event, the home devices adopt a specific configuration. Sensors may also periodically send measurements of several parameters (e.g. gas presence, light, temperature, humidity, etc.) which are collected at a sink device, or may generate commands for actuators (e.g. a smoke sensor may send an alarm message to a safety system).

The devices involved in the described scenario are nodes of a network that follows the mesh topology, which is suitable for path diversity to face indoor multipath propagation issues. The multihop paradigm allows end-to-end connectivity when direct range communication is not possible. Security support is required, specially for safety-related communication. When a user interaction (e.g. a button press) triggers a message that encapsulates a command, if the message is lost, the user may have to perform further interactions to achieve the desired effect (e.g. a light is turned off). A reaction to a user interaction will be perceived by the user as immediate as long as the reaction takes place after less than 0.5 seconds [RFC5826].

Dominant parameters in home automation scenarios with ITU-T G.9959:

- o Deployment/Bootstrapping: Pre-planned.
- o Topology: Mesh topology.
- o L2-mesh or L3-mesh: ITU-T G.9959 provides support for L2-mesh, and L3-mesh can also be used (the latter requires an IP-based routing protocol).
- o Multi-link subnet, single subnet: Multi-link subnet.
- o Data rate: Small data rate, infrequent transmissions.

- o Buffering requirements: Low requirement.
 - o Security requirements: Data privacy and security must be provided. Encryption is required.
 - o Mobility: Most devices are static. A few devices (e.g. remote control) are portable.
 - o Time Synchronization: TBD.
 - o Reliability and QoS: Moderate to high level of reliability support. Actions as a result of human-generated traffic should occur after less than 0.5 seconds.
 - o Traffic patterns: Periodic (sensor readings) and aperiodic (user-triggered interaction).
 - o Security Bootstrapping: Required.
 - o Power use strategy: Mix of P1 (Low-power) devices and P9 (Always-on) devices.
 - o Update firmware requirements: TBD.
- 6.2. Use case of Bluetooth Low Energy: Smartphone-Based Interaction with Constrained Devices

The key feature behind the current high Bluetooth LE momentum is its support in a large majority of smartphones in the market. Bluetooth LE can be used to allow the interaction between the smartphone and surrounding sensors or actuators. Furthermore, Bluetooth LE is also the main radio interface currently available in wearables. Since a smartphone typically has several radio interfaces that provide Internet access, such as Wi-Fi or 4G, the smartphone can act as a gateway for nearby devices such as sensors, actuators or wearables. Bluetooth LE may be used in several domains, including healthcare, sports/wellness and home automation.

Example: Bluetooth LE-based Body Area Network for fitness

A person wears a smartwatch for fitness purposes. The smartwatch has several sensors (e.g. heart rate, accelerometer, gyrometer, GPS, temperature, etc.), a display, and a Bluetooth LE radio interface. The smartwatch can show fitness-related statistics on its display. However, when a paired smartphone is in the range of the smartwatch, the latter can report almost real-time measurements of its sensors to the smartphone, which can forward the data to a cloud service on the Internet. In addition, the smartwatch can receive notifications

(e.g. alarm signals) from the cloud service via the smartphone. On the other hand, the smartphone may locally generate messages for the smartwatch, such as e-mail reception or calendar notifications.

The functionality supported by the smartwatch may be complemented by other devices such as other on-body sensors, wireless headsets or head-mounted displays. All such devices may connect to the smartphone creating a star topology network whereby the smartphone is the central component.

Dominant parameters in fitness scenarios with Bluetooth LE:

- o Deployment/Bootstrapping: Pre-planned.
- o Topology: Star topology.
- o L2-mesh or L3-mesh: No.
- o Multi-link subnet, single subnet: Multi-link subnet.
- o Data rate: TBD.
- o Buffering requirements: Low requirement.
- o Security requirements: For health-critical information, data privacy and security must be provided. Encryption is required. Some types of notifications sent by the smartphone may not need.
- o Mobility: Low.
- o Time Synchronization: the link layer, which is based on TDMA, provides a basis for time synchronization.
- o Reliability and QoS: a relatively low ratio of message losses is acceptable for periodic sensor readings. End-to-end latency of sensor readings should be low for critical notifications or alarms, generated by either the smartphone or an Internet cloud service.
- o Traffic patterns: periodic (sensor readings) and aperiodic (smartphone-generated notifications).
- o Security Bootstrapping: Required.
- o Power use strategy: P1 (Low-power) devices.
- o Update firmware requirements: TBD.

6.3. Use case of DECT-ULE: Smart Home

DECT is a technology widely used for wireless telephone communications in residential scenarios. Since DECT-ULE is a low-power variant of DECT, DECT-ULE can be used to connect constrained devices such as sensors and actuators to a Fixed Part, a device that typically acts as a base station for wireless telephones. Therefore, DECT-ULE is specially suitable for the connected home space in application areas such as home automation, smart metering, safety, healthcare, etc.

Example: use of DECT-ULE for Smart Metering

The smart electricity meter of a home is equipped with a DECT-ULE transceiver. This device is in the coverage range of the Fixed Part of the home. The Fixed Part can act as a router connected to the Internet. This way, the smart meter can transmit electricity consumption readings through the DECT-ULE link with the Fixed Part, and the latter can forward such readings to the utility company using Wide Area Network (WAN) links. The meter can also receive queries from the utility company or from an advanced energy control system controlled by the user, which may also be connected to the Fixed Part via DECT-ULE.

Dominant parameters in smart metering scenarios with DECT-ULE:

- o Deployment/Bootstrapping: Pre-planned.
- o Topology: Star topology.
- o L2-mesh or L3-mesh: No.
- o Multi-link subnet, single subnet: Multi-link subnet.
- o Data rate: Small data rate, infrequent transmissions.
- o Buffering requirements: Low requirement.
- o Security requirements: Data privacy and security must be provided. Encryption is required.
- o Mobility: No.
- o Time Synchronization: TBD.
- o Reliability and QoS: bounded latency, stringent reliability service agreements [I-D.ietf-roll-applicability-ami].

- o Traffic patterns: Periodic (meter reading notifications sent by the meter) and aperiodic (user- or company-triggered queries to the meter, and messages triggered by local events such as power outage or leak detection [I-D.ietf-roll-applicability-ami]).
- o Security Bootstrapping: required.
- o Power use strategy: P0 (Normally-off) for devices with long sleep intervals (i.e. greater than ~10 seconds) which then may need to resynchronize again, and P1 (Low-power) for short sleep intervals. P9 (Always-on) for the Fixed Part (FP), which is the central node in the star topology.
- o Update firmware requirements: TBD.

6.4. Use case of MS/TP:

[TBD]

Example: [TBD]

- o Power use strategy: P9 (Always-on).

6.5. Use case of NFC: Alternative Secure Transfer

According to applications, various secured data can be handled and transferred. Depending on security level of the data, methods for transfer can be alternatively selected. The personal data having serious issues should be transferred securely, but data transfer by using Wi-Fi and Bluetooth connections cannot always be secure because of their a little long radio frequency range. Hackers can overhear the personal data transfer behind hidden areas. Therefore, methods need to be alternatively selected to transfer secured data. Voice and video data, which are not respectively secure and requires long transmission range, can be transferred by 3G/4G technologies, such as WCDMA, GSM, and LTE. Big size data, which are not secure and requires high speed and broad bandwidth, can be transferred by Wi-Fi and wired network technologies. However, the personal data, which pose serious issues if mishandled while transferred in wireless domain, can be securely transferred by NFC technology. It has very short frequency range - nearly single touch communication.

Example: Secure Transfer by Using NFC in Healthcare Services with Tele-Assistance

A senior citizen who lives alone wears one to several wearable 6lo devices to measure heartbeat, pulse rate, etc. The 6lo devices are densely installed at home for movement detection. An LoWPAN Border

Router (LBR) at home will send the sensed information to a connected healthcare center. Portable base stations with LCDs may be used to check the data at home, as well. Data is gathered in both periodic and event-driven fashion. In this application, event-driven data can be very time-critical. In addition, privacy also becomes a serious issue in this case, as the sensed data is very personal.

While the senior citizen is provided audio and video healthcare services by a tele-assistance based on LTE connections, the senior citizen can alternatively use NFC connections to transfer the personal sensed data to the tele-assistance. At this moment, hidden hackers can overhear the data based on the LTE connection, but they cannot gather the personal data over the NFC connection.

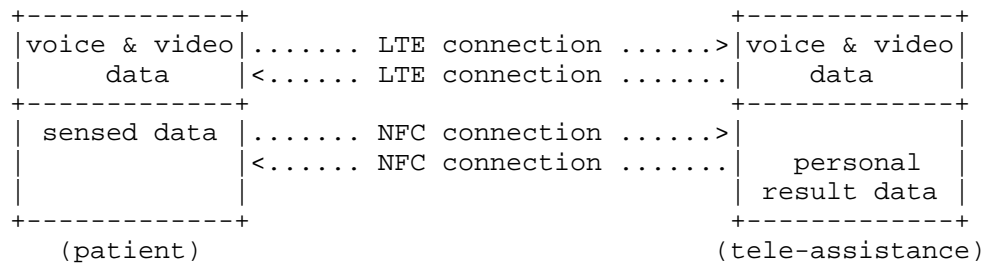


Figure 1: Alternative Secure Transfer in Healthcare Services

Dominant parameters in secure transfer by using NFC in healthcare services:

- o Deployment/Bootstrapping: Pre-planned. MP2P/P2MP (data collection), P2P (local diagnostic).
- o Topology: Small, NFC-enabled device connected to the Internet.
- o L2-mesh or L3-mesh: NFC does not support L2-mesh, L3-mesh can be configured.
- o Multi-link subnet, single subnet: a single hop for gateway; patient's body network is mesh topology.
- o Data rate: Small data rate.
- o Buffering requirements: Low requirement.
- o Security requirements: Data privacy and security must be provided. Encryption is required.

- o Mobility: Moderate (patient's mobility).
- o Time Synchronization: Highly required.
- o Reliability and QoS: High level of reliability support (life-or-death implication), role-based.
- o Traffic patterns: Short data length and periodic (randomly).
- o Security Bootstrapping: Highly required.
- o Other Issues: Plug-and-play configuration is required for mainly non-technical end-users. Real-time data acquisition and analysis are important. Efficient data management is needed for various devices that have different duty cycles, and for role-based data control. Reliability and robustness of the network are also essential.
- o Power use strategy: TBD.
- o Update firmware requirements: TBD.

6.6. Use case of LTE MTC

Wireless link layer technologies can be divided into short range connectivity and long range connectivity. BLE, ITU-T G.9959 (Z-Wave), DECT-ULE, MS/TP, NFC are used for short range connectivity. LTE MTC is used for long range connectivity. And there is another long range connectivity technology. It is LPWAN (Low Power Wide Area Network) technology such as LoRa, Sigfox, etc. Therefore, the use case of LTE MTC could be used in LPWAN.

Example: Use of wireless backhaul for LoRa gateway

LoRa is one of the most promising technologies of LPWAN. LoRa network architecture has a star of star topology. LoRa gateway relay the messages from LoRa end device to application server and vice versa. LoRa gateway can has two types of backhaul, wired and wireless backhaul.

If LoRa gateway has wireless backhaul, it should have LTE modem. Since the modem cost of LTE MTC is cheaper than the modem cost of above LTE category 2, it is helpful to design to use LTE MTC. Since the maximum data rate of LoRa end device is 50kbps, it is sufficient to use LTE MTC without using category 2.

Dominant parameters in LoRa gateway scenarios with above example:

- o Deployment/Bootstrapping: Pre-planned.
- o Topology: Star topology.
- o L2-mesh or L3-mesh: No.
- o Multi-link subnet, single subnet: Single subnet.
- o Data rate: depends on 3GPP specification.
- o Buffering requirements: High requirement.
- o Security requirements: No, because data security is already provided in LoRa specification.
- o Mobility: Static.
- o Time Synchronization: Highly required.
- o Reliability and QoS: TBD.
- o Traffic patterns: Random.
- o Security Bootstrapping: required.
- o Power use strategy: P9 (Always-on).
- o Update firmware requirements: TBD.

Example: Use of controlling car

Car sharing services are becoming more popular. Customers wish to control the car with smart phone application. For example, customers wish to lock/unlock the car door with smart phone application, because customers may not have a car key. Customers wish to blow with smart phone application to locate the car easily.

Therefore, rental car should have a long range connectivity capable modem such as LoRa end device and LTE UE. However, LoRa may not be used because LoRa has low reliability and may not be supported in an indoor environment such as a basement parking lot. And since message size for car control is very small, it is sufficient to use LTE MTC but category 2.

Dominant parameters in controlling car scenarios with above example:

- o Deployment/Bootstrapping: Pre-planned.

- o Topology: Star topology.
- o L2-mesh or L3-mesh: No.
- o Multi-link subnet, single subnet: Single subnet.
- o Data rate: depends on 3GPP specification.
- o Buffering requirements: High requirement.
- o Security requirements: High requirement.
- o Mobility: Always dynamic .
- o Time Synchronization: Highly required.
- o Reliability and QoS: TBD.
- o Traffic patterns: Random.
- o Security Bootstrapping: required.
- o Power use strategy: P1 (Low-power).

6.7. Use case of IEEE 802.15.4e:

[TBD]

Example: [TBD]

7. IANA Considerations

There are no IANA considerations related to this document.

8. Security Considerations

[TBD]

9. Acknowledgements

Carles Gomez has been funded in part by the Spanish Government (Ministerio de Educacion, Cultura y Deporte) through the Jose Castillejo grant CAS15/00336. His contribution to this work has been carried out in part during his stay as a visiting scholar at the Computer Laboratory of the University of Cambridge.

Samita Chakrabarti, Thomas Watteyne, Pascal Thubert, Abdur Rashid Sangi, Xavier Vilajosana, Daniel Migault, and Take Aanstoot have provided valuable feedback for this draft.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [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, <<http://www.rfc-editor.org/info/rfc4919>>.
- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <<http://www.rfc-editor.org/info/rfc4944>>.
- [RFC5826] Brandt, A., Buron, J., and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5826, DOI 10.17487/RFC5826, April 2010, <<http://www.rfc-editor.org/info/rfc5826>>.
- [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, <<http://www.rfc-editor.org/info/rfc6282>>.
- [RFC6568] Kim, E., Kaspar, D., and JP. Vasseur, "Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6568, DOI 10.17487/RFC6568, April 2012, <<http://www.rfc-editor.org/info/rfc6568>>.
- [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>>.

- [RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <<http://www.rfc-editor.org/info/rfc7228>>.
- [RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015, <<http://www.rfc-editor.org/info/rfc7428>>.
- [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <<http://www.rfc-editor.org/info/rfc7668>>.

10.2. Informative References

- [I-D.ietf-6lo-dect-ule]
Mariager, P., Petersen, J., Shelby, Z., Logt, M., and D. Barthel, "Transmission of IPv6 Packets over DECT Ultra Low Energy", draft-ietf-6lo-dect-ule-07 (work in progress), October 2016.
- [I-D.ietf-6lo-6lobac]
Lynn, K., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over MS/TP Networks", draft-ietf-6lo-6lobac-05 (work in progress), June 2016.
- [I-D.ietf-6lo-nfc]
Choi, Y., Youn, J., and Y. Hong, "Transmission of IPv6 Packets over Near Field Communication", draft-ietf-6lo-nfc-05 (work in progress), October 2016.
- [I-D.ietf-lwig-energy-efficient]
Gomez, C., Kovatsch, M., Tian, H., and Z. Cao, "Energy-Efficient Features of Internet of Things Protocols", draft-ietf-lwig-energy-efficient-05 (work in progress), October 2016.
- [I-D.ietf-roll-applicability-ami]
Cam-Winget, N., Hui, J., and D. Popa, "Applicability Statement for the Routing Protocol for Low Power and Lossy Networks (RPL) in AMI Networks", draft-ietf-roll-applicability-ami-15 (work in progress), October 2016.

- [G.9959] "International Telecommunication Union, "Short range narrow-band digital radiocommunication transceivers - PHY and MAC layer specifications", ITU-T Recommendation", January 2015.
- [LTE_MTC] "3GPP TS 36.306 V13.0.0, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities (Release 13)", December 2015.

Authors' Addresses

Yong-Geun Hong
ETRI
161 Gajeong-Dong Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 6557
Email: yghong@etri.re.kr

Carles Gomez
Universitat Politecnica de Catalunya/Fundacio i2cat
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: carlesgo@entel.upc.edu

Younghwan Choi
ETRI
218 Gajeongno, Yuseong
Daejeon 305-700
Korea

Phone: +82 42 860 1429
Email: yhc@etri.re.kr

Deoknyong Ko
SKtelecom
9-1 Byundang-gu Sunae-dong, Seongnam-si
Gyeonggi-do 13595
Korea

Phone: +82 10 3356 8052
Email: engineer@sk.com

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 14, 2017

Y-H. Choi
Y-G. Hong
ETRI
J-S. Youn
Dongueui Univ
D-K. Kim
KNU
J-H. Choi
Samsung Electronics Co.,
October 11, 2016

Transmission of IPv6 Packets over Near Field Communication
draft-ietf-6lo-nfc-05

Abstract

Near field communication (NFC) is a set of standards for smartphones and portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than 10 cm. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum. The NFC technology has been widely implemented and available in mobile phones, laptop computers, and many other devices. This document describes how IPv6 is transmitted over NFC using 6LowPAN techniques.

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 April 14, 2017.

Copyright Notice

Copyright (c) 2016 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	3
2. Conventions and Terminology	3
3. Overview of Near Field Communication Technology	4
3.1. Peer-to-peer Mode of NFC	4
3.2. Protocol Stacks of NFC	4
3.3. NFC-enabled Device Addressing	6
3.4. NFC MAC PDU Size and MTU	6
4. Specification of IPv6 over NFC	7
4.1. Protocol Stacks	7
4.2. Link Model	7
4.3. Stateless Address Autoconfiguration	8
4.4. IPv6 Link Local Address	9
4.5. Neighbor Discovery	9
4.6. Dispatch Header	9
4.7. Header Compression	10
4.8. Fragmentation and Reassembly	11
4.9. Unicast Address Mapping	11
4.10. Multicast Address Mapping	12
5. Internet Connectivity Scenarios	12
5.1. NFC-enabled Device Connected to the Internet	12
5.2. Isolated NFC-enabled Device Network	13
6. IANA Considerations	13
7. Security Considerations	13
8. Acknowledgements	14
9. References	14
9.1. Normative References	14
9.2. Informative References	15
Authors' Addresses	15

1. Introduction

NFC is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is possible, provided both devices are powered. NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only. It has been used in devices such as mobile phones, running Android operating system, named with a feature called "Android Beam". In addition, it is expected for the other mobile phones, running the other operating systems (e.g., iOS, etc.) to be equipped with NFC technology in the near future.

Considering the potential for exponential growth in the number of heterogeneous air interface technologies, NFC would be widely used as one of the other air interface technologies, such as Bluetooth Low Energy (BT-LE), Wi-Fi, and so on. Each of the heterogeneous air interface technologies has its own characteristics, which cannot be covered by the other technologies, so various kinds of air interface technologies would co-exist together. Therefore, it is required for them to communicate with each other. NFC also has the strongest ability (e.g., secure communication distance of 10 cm) to prevent a third party from attacking privacy.

When the number of devices and things having different air interface technologies communicate with each other, IPv6 is an ideal internet protocols owing to its large address space. Also, NFC would be one of the endpoints using IPv6. Therefore, this document describes how IPv6 is transmitted over NFC using 6LoWPAN techniques.

RFC4944 [1] specifies the transmission of IPv6 over IEEE 802.15.4. The NFC link also has similar characteristics to that of IEEE 802.15.4. Many of the mechanisms defined in RFC 4944 [1] can be applied to the transmission of IPv6 on NFC links. This document specifies the details of IPv6 transmission over NFC links.

2. Conventions 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 [2].

3. Overview of Near Field Communication Technology

NFC technology enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and it enables a consumer to utilize one device across different systems.

Extending the capability of contactless card technology, NFC also enables devices to share information at a distance that is less than 10 cm with a maximum communication speed of 424 kbps. Users can share business cards, make transactions, access information from a smart poster or provide credentials for access control systems with a simple touch.

NFC's bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch. In addition to the easy connection and quick transactions, simple data sharing is also available.

3.1. Peer-to-peer Mode of NFC

NFC-enabled devices are unique in that they can support three modes of operation: card emulation, peer-to-peer, and reader/writer. Peer-to-peer mode enables two NFC-enabled devices to communicate with each other to exchange information and share files, so that users of NFC-enabled devices can quickly share contact information and other files with a touch. Therefore, an NFC-enabled device can securely send IPv6 packets to any corresponding node on the Internet when an NFC-enabled gateway is linked to the Internet.

3.2. Protocol Stacks of NFC

IP can use the services provided by the Logical Link Control Protocol (LLCP) in the NFC stack to provide reliable, two-way transport of information between the peer devices. Figure 1 depicts the NFC P2P protocol stack with IPv6 bindings to LLCP.

For data communication in IPv6 over NFC, an IPv6 packet SHALL be passed down to LLCP of NFC and transported to an Information Field in Protocol Data Unit (I PDU) of LLCP of the NFC-enabled peer device. LLCP does not support fragmentation and reassembly. For IPv6 addressing or address configuration, LLCP SHALL provide related information, such as link layer addresses, to its upper layer. The

LLCP to IPv6 protocol binding SHALL transfer the SSAP and DSAP value to the IPv6 over NFC protocol. SSAP stands for Source Service Access Point, which is a 6-bit value meaning a kind of Logical Link Control (LLC) address, while DSAP means an LLC address of the destination NFC-enabled device.

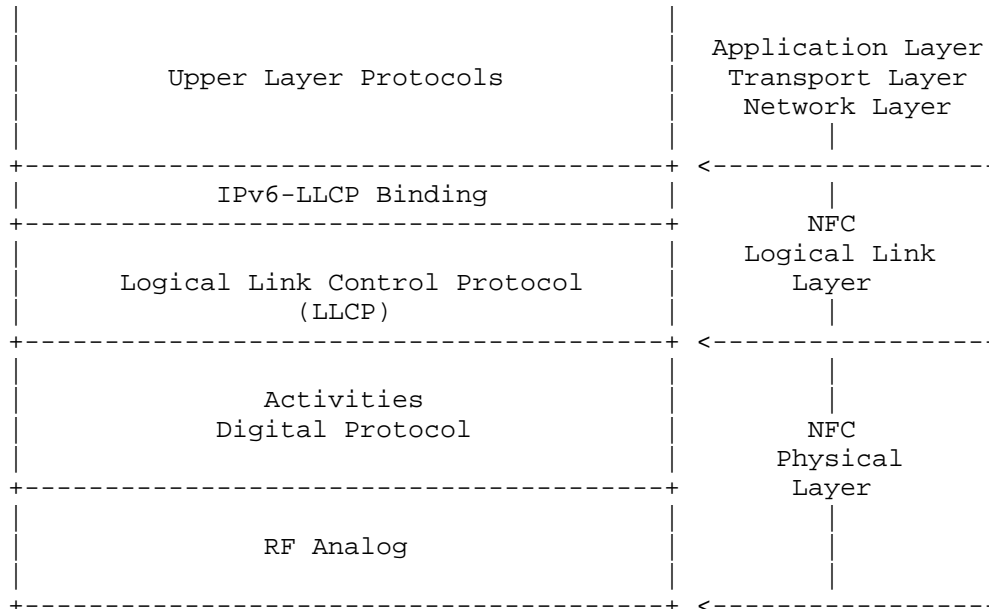


Figure 1: Protocol Stacks of NFC

The LLCP consists of Logical Link Control (LLC) and MAC Mapping. The MAC Mapping integrates an existing RF protocol into the LLCP architecture. The LLC contains three components, such as Link Management, Connection-oriented Transport, and Connection-less Transport. The Link Management component is responsible for serializing all connection-oriented and connection-less LLC PDU (Protocol Data Unit) exchanges and for aggregation and disaggregation of small PDUs. This component also guarantees asynchronous balanced mode communication and provides link status supervision by performing the symmetry procedure. The Connection-oriented Transport component is responsible for maintaining all connection-oriented data exchanges including connection set-up and termination. The Connectionless Transport component is responsible for handling unacknowledged data exchanges.

3.3. NFC-enabled Device Addressing

According to NFCForum-TS-LLCP_1.3 [3], NFC-enabled devices have two types of 6-bit addresses (i.e., SSAP and DSAP) to identify service access points. The several service access points can be installed on a NFC device. However, the SSAP and DSAP can be used as identifiers for NFC link connections with the IPv6 over NFC adaptation layer. Therefore, the SSAP can be used to generate an IPv6 interface identifier. Address values between 00h and 0Fh of SSAP and DSAP are reserved for identifying the well-known service access points, which are defined in the NFC Forum Assigned Numbers Register. Address values between 10h and 1Fh SHALL be assigned by the local LLC to services registered by local service environment. In addition, address values between 20h and 3Fh SHALL be assigned by the local LLC as a result of an upper layer service request. Therefore, the address values between 20h and 3Fh can be used for generating IPv6 interface identifiers.

3.4. NFC MAC PDU Size and MTU

As mentioned in Section 3.2, an IPv6 packet SHALL be passed down to LLC of NFC and transported to an Unnumbered Information Protocol Data Unit (UI PDU) and an Information Field in Protocol Data Unit (I PDU) of LLC of the NFC-enabled peer device.

The information field of an I PDU SHALL contain a single service data unit. The maximum number of octets in the information field is determined by the Maximum Information Unit (MIU) for the data link connection. The default value of the MIU for I PDUs SHALL be 128 octets. The local and remote LLCs each establish and maintain distinct MIU values for each data link connection endpoint. Also, an LLC MAY announce a larger MIU for a data link connection by transmitting an MIUX extension parameter within the information field. If no MIUX parameter is transmitted, the default MIU value of 128 SHALL be used. Otherwise, the MTU size in NFC LLC SHALL calculate the MIU value as follows:

$$\text{MIU} = 128 + \text{MIUX}.$$

When the MIUX parameter is encoded as a TLV, the TLV Type field SHALL be 0x02 and the TLV Length field SHALL be 0x02. The MIUX parameter SHALL be encoded into the least significant 11 bits of the TLV Value field. The unused bits in the TLV Value field SHALL be set to zero by the sender and SHALL be ignored by the receiver. However, a maximum value of the TLV Value field can be 0x7FF, and a maximum size of the MTU in NFC LLC is 2176 bytes.

4. Specification of IPv6 over NFC

NFC technology also has considerations and requirements owing to low power consumption and allowed protocol overhead. 6LoWPAN standards RFC 4944 [1], RFC 6775 [4], and RFC 6282 [5] provide useful functionality for reducing overhead which can be applied to NFC. This functionality consists of link-local IPv6 addresses and stateless IPv6 address auto-configuration (see Section 4.3), Neighbor Discovery (see Section 4.5) and header compression (see Section 4.7).

4.1. Protocol Stacks

Figure 2 illustrates IPv6 over NFC. Upper layer protocols can be transport layer protocols (TCP and UDP), application layer protocols, and others capable running on top of IPv6.

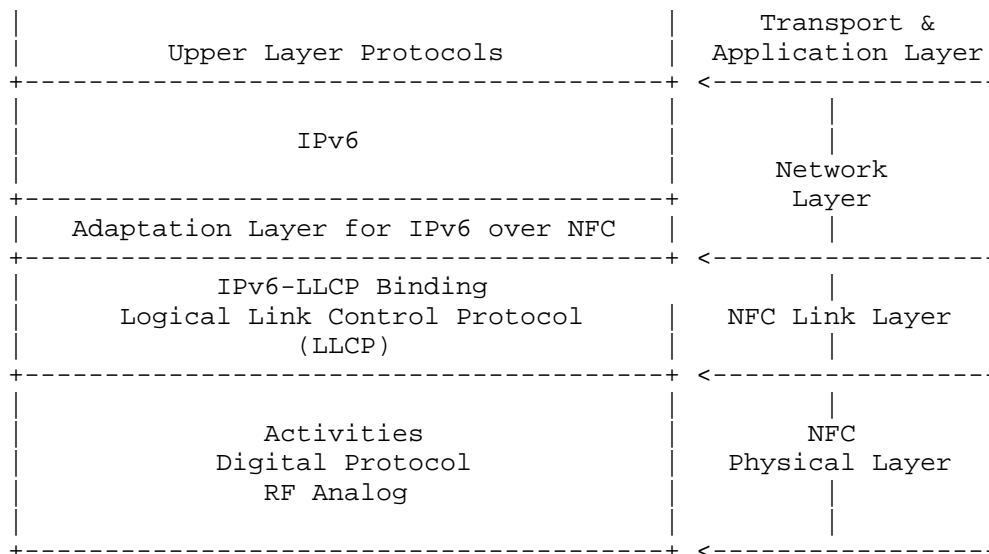


Figure 2: Protocol Stacks for IPv6 over NFC

The adaptation layer for IPv6 over NFC SHALL support neighbor discovery, stateless address auto-configuration, header compression, and fragmentation & reassembly.

4.2. Link Model

In the case of BT-LE, the Logical Link Control and Adaptation Protocol (L2CAP) supports fragmentation and reassembly (FAR) functionality; therefore, the adaptation layer for IPv6 over BT-LE does not have to conduct the FAR procedure. The NFC LLCP, in

contrast, does not support the FAR functionality, so IPv6 over NFC needs to consider the FAR functionality, defined in RFC 4944 [1]. However, the MTU on an NFC link can be configured in a connection procedure and extended enough to fit the MTU of IPv6 packet (see Section 4.8).

The NFC link between two communicating devices is considered to be a point-to-point link only. Unlike in BT-LE, an NFC link does not support a star topology or mesh network topology but only direct connections between two devices. Furthermore, the NFC link layer does not support packet forwarding in link layer. Due to this characteristics, 6LoWPAN functionalities, such as addressing and auto-configuration, and header compression, need to be specialized into IPv6 over NFC.

4.3. Stateless Address Autoconfiguration

An NFC-enabled device (i.e., 6LN) performs stateless address autoconfiguration as per RFC 4862 [6]. A 64-bit Interface identifier (IID) for an NFC interface is formed by utilizing the 6-bit NFC LLCP address (see Section 3.3). In the viewpoint of address configuration, such an IID SHOULD guarantee a stable IPv6 address because each data link connection is uniquely identified by the pair of DSAP and SSAP included in the header of each LLC PDU in NFC.

Following the guidance of RFC 7136 [10], interface identifiers of all unicast addresses for NFC-enabled devices are 64 bits long and constructed in a modified EUI-64 format as shown in Figure 3.

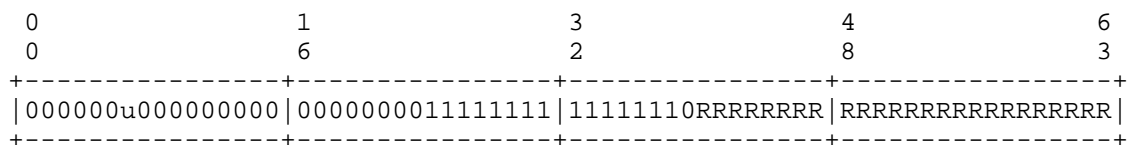


Figure 3: Formation of IID from NFC-enabled device address

The 'R' bits are random values which MAY be created by mechanisms like hash function with the SSAP as an input value because the 6-bit address of SSAP is easy and short to be targeted by attacks of third party (e.g., address scanning). In addition, the "Universal/Local" bit (i.e., the 'u' bit) of an NFC-enabled device address MUST be set to 0 RFC 4291 [7].

4.4. IPv6 Link Local Address

Only if the NFC-enabled device address is known to be a public address, the "Universal/Local" bit be set to 1. The IPv6 link-local address for an NFC-enabled device is formed by appending the IID, to the prefix FE80::/64, as depicted in Figure 4.

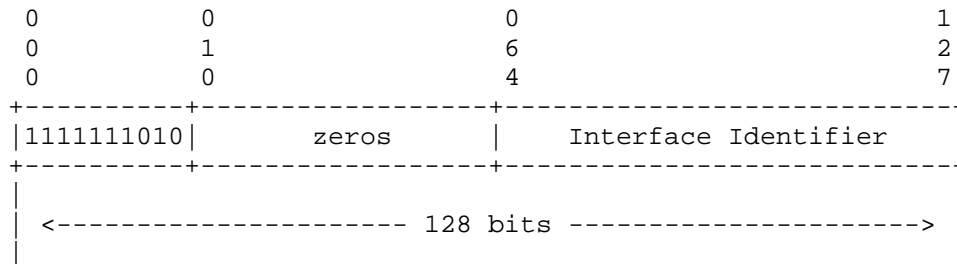


Figure 4: IPv6 link-local address in NFC

The tool for a 6LBR to obtain an IPv6 prefix for numbering the NFC network is can be accomplished via DHCPv6 Prefix Delegation (RFC 3633 [8]).

4.5. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs (RFC 6775 [4]) describes the neighbor discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC does not support a complicated mesh topology but only a simple multi-hop network topology or directly connected peer-to-peer network. Therefore, the following aspects of RFC 6775 are applicable to NFC:

1. In a case that an NFC-enabled device (6LN) is directly connected to a 6LBR, an NFC 6LN MUST register its address with the 6LBR by sending a Neighbor Solicitation (NS) message with the Address Registration Option (ARO) and process the Neighbor Advertisement (NA) accordingly. In addition, if DHCPv6 is used to assign an address, Duplicate Address Detection (DAD) MAY not be required.
2. For sending Router Solicitations and processing Router Advertisements the NFC 6LNs MUST follow Sections 5.3 and 5.4 of RFC 6775.

4.6. Dispatch Header

All IPv6-over-NFC encapsulated datagrams are prefixed by an encapsulation header stack consisting of a Dispatch value followed by zero or more header fields. The only sequence currently defined for

IPv6-over-NFC is the LOWPAN_IPHC header followed by payload, as depicted in Figure 5.

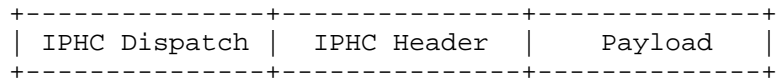


Figure 5: A IPv6-over-NFC Encapsulated 6LOWPAN_IPHC Compressed IPv6 Datagram

The dispatch value may be treated as an unstructured namespace. Only a single pattern is used to represent current IPv6-over-NFC functionality.

Pattern	Header Type	Reference
01 1xxxxx	6LOWPAN_IPHC	[RFC6282]

Figure 6: Dispatch Values

Other IANA-assigned 6LoWPAN Dispatch values do not apply to this specification.

4.7. Header Compression

Header compression as defined in RFC 6282 [5], which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, is REQUIRED in this document as the basis for IPv6 header compression on top of NFC. All headers MUST be compressed according to RFC 6282 encoding formats.

Therefore, IPv6 header compression in RFC 6282 [5] MUST be implemented. Further, implementations MAY also support Generic Header Compression (GHC) of RFC 7400 [11].

If a 16-bit address is required as a short address, it MUST be formed by padding the 6-bit NFC link-layer (node) address to the left with zeros as shown in Figure 7.

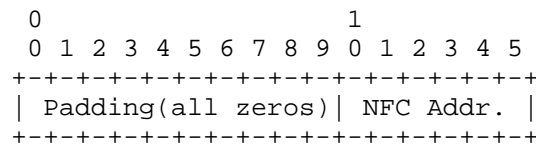


Figure 7: NFC short address format

4.8. Fragmentation and Reassembly

NFC provides fragmentation and reassembly (FAR) for payloads from 128 bytes up to 2176 bytes as mentioned in Section 3.4. The MTU of a general IPv6 packet can fit into a single NFC link frame. Therefore, the FAR functionality as defined in RFC 4944, which specifies the fragmentation methods for IPv6 datagrams on top of IEEE 802.15.4, MAY NOT be required as the basis for IPv6 datagram FAR on top of NFC. The NFC link connection for IPv6 over NFC MUST be configured with an equivalent MIU size to fit the MTU of IPv6 Packet. If NFC devices support extension of the MTU, the MIUX value is 0x480 in order to fit the MTU (1280 bytes) of a IPv6 packet.

4.9. Unicast Address Mapping

The address resolution procedure for mapping IPv6 non-multicast addresses into NFC link-layer addresses follows the general description in Section 7.2 of RFC 4861 [9], unless otherwise specified.

The Source/Target link-layer Address option has the following form when the addresses are 6-bit NFC link-layer (node) addresses.

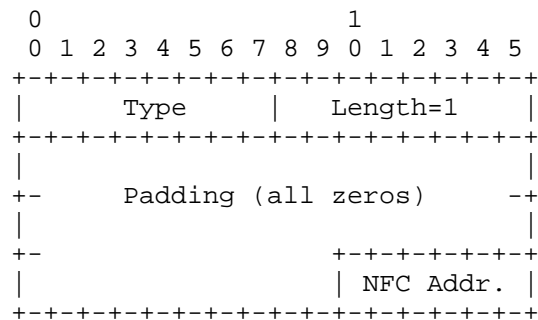


Figure 8: Unicast address mapping

Option fields:

Type:

1: for Source Link-layer address.

2: for Target Link-layer address.

Length:

This is the length of this option (including the type and length fields) in units of 8 octets. The value of this field is 1 for 6-bit NFC node addresses.

NFC address:

The 6-bit address in canonical bit order. This is the unicast address the interface currently responds to.

4.10. Multicast Address Mapping

All IPv6 multicast packets MUST be sent to NFC Destination Address, 0x3F (broadcast) and be filtered at the IPv6 layer. When represented as a 16-bit address in a compressed header, it MUST be formed by padding on the left with a zero. In addition, the NFC Destination Address, 0x3F, MUST NOT be used as a unicast NFC address of SSAP or DSAP.

```

      0                               1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---+---+---+---+---+---+---+---+
| Padding(all zeros) | 1 1 1 1 1 1 |
+---+---+---+---+---+---+---+---+

```

Figure 9: Multicast address mapping

5. Internet Connectivity Scenarios

As two typical scenarios, the NFC network can be isolated and connected to the Internet.

5.1. NFC-enabled Device Connected to the Internet

One of the key applications of using IPv6 over NFC is securely transmitting IPv6 packets because the RF distance between 6LN and 6LBR is typically within 10 cm. If any third party wants to hack into the RF between them, it must come to nearly touch them. Applications can choose which kinds of air interfaces (e.g., BT-LE, Wi-Fi, NFC, etc.) to send data depending on the characteristics of the data.

Figure 10 illustrates an example of an NFC-enabled device network connected to the Internet. The distance between 6LN and 6LBR is typically 10 cm or less. If there is any laptop computers close to a user, it will become the a 6LBR. Additionally, when the user mounts an NFC-enabled air interface adapter (e.g., portable NFC dongle) on the close laptop PC, the user's NFC-enabled device (6LN) can communicate with the laptop PC (6LBR) within 10 cm distance.

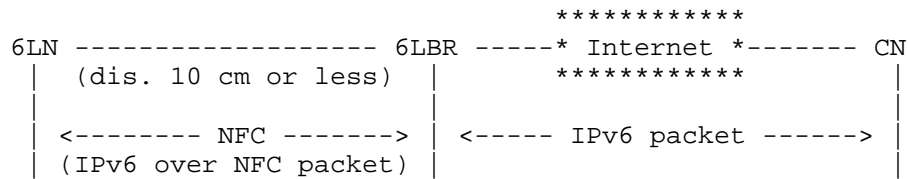


Figure 10: NFC-enabled device network connected to the Internet

5.2. Isolated NFC-enabled Device Network

In some scenarios, the NFC-enabled device network may transiently be a simple isolated network as shown in the Figure 11.

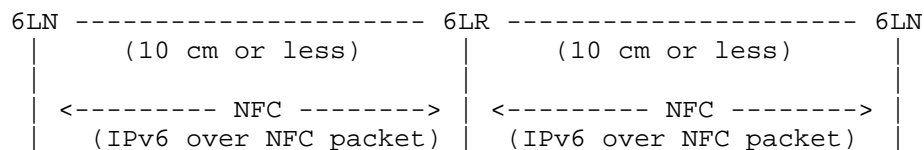


Figure 11: Isolated NFC-enabled device network

In mobile phone markets, applications are designed and made by user developers. They may image interesting applications, where three or more mobile phones touch or attach each other to accomplish outstanding performance.

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

When interface identifiers (IIDs) are generated, devices and users are required to consider mitigating various threats, such as correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning.

IPv6-over-NFC is, in practice, not used for long-lived links for big size data transfer or multimedia streaming, but used for extremely short-lived links (i.e., single touch-based approaches) for ID verification and mobile payment. This will mitigate the threat of correlation of activities over time.

IPv6-over-NFC uses an IPv6 interface identifier formed from a "Short Address" and a set of well-known constant bits (such as padding with '0's) for the modified EUI-64 format. However, the short address of NFC link layer (LLC) is not generated as a physically permanent value

but logically generated for each connection. Thus, every single touch connection can use a different short address of NFC link with an extremely short-lived link. This can mitigate address scanning as well as location tracking and device-specific vulnerability exploitation.

However, malicious tries for one connection of a long-lived link with NFC technology are not secure, so the method of deriving interface identifiers from 6-bit NFC Link layer addresses is intended to preserve global uniqueness when it is possible. Therefore, it requires a way to protect from duplication through accident or forgery and to define a way to include sufficient bit of entropy in the IPv6 interface identifier, such as random EUI-64.

8. Acknowledgements

We are grateful to the members of the IETF 6lo working group.

Michael Richardson, Suresh Krishnan, Pascal Thubert, Carsten Bormann, and Alexandru Petrescu have provided valuable feedback for this draft.

9. References

9.1. Normative References

- [1] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <<http://www.rfc-editor.org/info/rfc4944>>.
- [2] 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>>.
- [3] "NFC Logical Link Control Protocol version 1.3", NFC Forum Technical Specification , March 2016.
- [4] 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>>.

- [5] 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, <<http://www.rfc-editor.org/info/rfc6282>>.
- [6] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<http://www.rfc-editor.org/info/rfc4862>>.
- [7] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<http://www.rfc-editor.org/info/rfc4291>>.
- [8] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, DOI 10.17487/RFC3633, December 2003, <<http://www.rfc-editor.org/info/rfc3633>>.
- [9] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<http://www.rfc-editor.org/info/rfc4861>>.
- [10] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <<http://www.rfc-editor.org/info/rfc7136>>.
- [11] 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, <<http://www.rfc-editor.org/info/rfc7400>>.

9.2. Informative References

- [12] "Near Field Communication - Interface and Protocol (NFCIP-1) 3rd Ed.", ECMA-340 , June 2013.

Authors' Addresses

Younghwan Choi
Electronics and Telecommunications Research Institute
218 Gajeongno, Yuseong
Daejeon 305-700
Korea

Phone: +82 42 860 1429
Email: yhc@etri.re.kr

Yong-Geun Hong
Electronics and Telecommunications Research Institute
161 Gajeong-Dong Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 6557
Email: yghong@etri.re.kr

Joo-Sang Youn
DONG-EUI University
176 Eomgwangno Busan_jin_gu
Busan 614-714
Korea

Phone: +82 51 890 1993
Email: joosang.youn@gmail.com

Dongkyun Kim
Kyungpook National University
80 Daehak-ro, Buk-gu
Daegu 702-701
Korea

Phone: +82 53 950 7571
Email: dongkyun@knu.ac.kr

JinHyouk Choi
Samsung Electronics Co.,
129 Samsung-ro, Youngdong-gu
Suwon 447-712
Korea

Phone: +82 2 2254 0114
Email: jinchoe@samsung.com

6lo
Internet-Draft
Intended status: Standards Track
Expires: May 1, 2017

Lijo Thomas
C-DAC
P. Akshay
Indian Institute of Science
Satish Anamalamudi
Individual Contributor
S.V.R.Anand
Malati Hegde
Indian Institute of Science
C. Perkins
Futurewei
October 28, 2016

Packet expiration time in 6LoWPAN Routing Header
draft-lijo-6lo-expiration-time-00

Abstract

This document specifies a new type to the 6LoWPAN Dispatch Page 1 [I-D.ietf-roll-routing-dispatch] for carrying the expiration time of data packets within the 6LoWPAN routing header. The expiration time is useful in making forwarding and scheduling decisions for time critical IoT M2M applications that need deterministic delay guarantees over constrained networks and operate within time-synchronized networks.

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 May 1, 2017.

Copyright Notice

Copyright (c) 2016 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
2. Terminology	3
3. 6LoRHC Header Format	3
4. Timestamp-6LoRH header	3
5. Timestamp-6LoRH Header in Heterogeneous Network Scenarios . .	5
6. IANA Considerations	8
7. Security Considerations	8
8. Acknowledgements	9
9. References	9
9.1. Normative References	9
9.2. Informative References	10
Authors' Addresses	10

1. Introduction

Low Power and Lossy Networks (LLNs) could be employed for implementing real time industrial applications that require end-to-end delay guarantees [I-D.grossman-detnet-use-cases]. The Deterministic Network requires that data packets generated by the senders have to reach the receivers within strict time bounds. Including an expiration time information in the packets enables intermediate nodes to make appropriate packet forwarding and scheduling decisions to meet this requirement.

The draft [I-D.ietf-roll-routing-dispatch] specifies the 6LoWPAN Routing Header (6LoRH), compression schemes for RPL routing (source routing) operation [RFC6554], header compression of RPI field [RFC6553], and IP-in-IP encapsulation. This document specifies a new Timestamp-6LoRH type to the 6LoWPAN Dispatch Page 1 for including the expiration time of data packets within the 6LoWPAN routing header. In addition, this specification specifies handling of the expiration

time when packets traverse through time-synchronized networks operating in different timezones and distinct reference clocks.

2. 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 [RFC2119].

3. 6LoRHC Header Format

The generic header format of the 6LoRHC header is specified in [I-D.ietf-roll-routing-dispatch]. Figure 1 describes the generic header format for the 6LoRHC header.

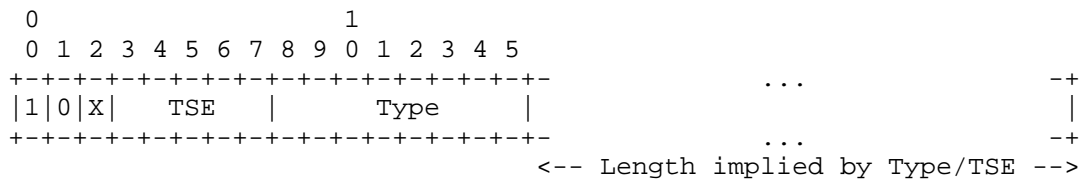


Figure 1: 6LoRHC header format

1. X bit: In Figure 1, if 'X' is 0 then it is a critical header. If 'X' is 1, then it is a elective header.
 2. TSE: Type Specific Extension. The meaning depends on the Type, which must be known to all the nodes. The interpretation of the TSE depends on the Type field that follows. For instance, it may be used to transport control bits, the number of elements in an array, or the length of the remainder of 6LoRHC expressed in a unit other than bytes.
 3. Type: Type of the 6LoRHC.
 4. Length: variable
- ## 4. Timestamp-6LoRH header

The Timestamp-6LoRH header (see Figure 2) is an elective 6LoRH header that provides a compressed form of expiration time for an IPv6 datagram. All nodes within the network SHOULD support the Timestamp-6LoRH header in order to support delay-sensitive deterministic applications. In this specification, the packet origination time is represented in microseconds. In the case of 6tisch networks which is

explained below, the origination time is the current ASN
[I-D.vilajosana-6tisch-minimal] converted into microseconds.

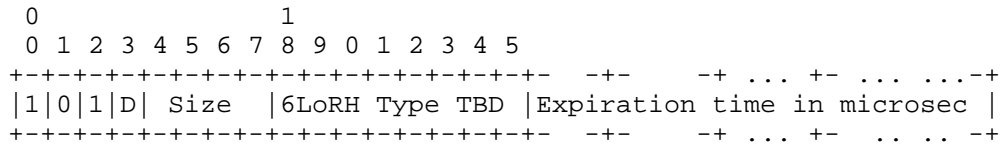


Figure 2: Timestamp-6LoRH header format

D flag (1 bit): The 'D' flag, set by the Sender, indicates the action that needs to be taken when an 6LR detects expiration time is elapsed. If 'D' bit is 1, then the 6LR SHOULD drop the packet if the expiration time is elapsed. If 'D' bit is 0, then the 6LR can choose to ignore the expiration time and forward it.

Size (4 bits): Size represents the total length of expiration time measured in octets. In this specification, the maximum length of the expiration time is 8 octets (64 bits).

For example, Size = 0001 means the expiration time in the 6LoRHC timestamp header is 1 octet (8 bits) long. Likewise, Size = 1000 means the expiration time in the 6LoRHC timestamp header is 8 octet (64 bits) long.

6LoRH Type: In this specification, Type value for the Timestamp-6LoRH is TBD.

Expiration time: This field describes the time limit before which the packet SHOULD be delivered to the Receiver:

$$\text{expiration_time} = \text{packet_origination_time} + \text{max_allowable_transmission_delay}.$$

Whenever the Sender initiates the IP datagram, it includes the Timestamp-6LoRH header along with other 6LoRH routing header information. The 6LoRH timestamp contains the expiration time as given in the above expression. Since the maximum allowable transmission delay is specific to each application, the expiration time is of variable length.

Example: In a 6TiSCH network let the time-slot length be 10ms. If the packet_origination_time = Current ASN is 200, and the max_allowable_delay is 1 second, then:

$$\begin{aligned} \text{expiration_time} &= \text{packet_origination_time} + \text{max_allowable_delay} \\ &= 200 * 10\text{ms} + 1 \text{ second} \end{aligned}$$

$$= 3 * 10^6 \text{ microseconds}$$

This expiration time requires 22 bits, or 3 octets, in length. The Size is represented as x0011.

5. Timestamp-6LoRH Header in Heterogeneous Network Scenarios

In this section, Timestamp-6LoRH header operation is described for 3 different network scenarios. Figure 3 depicts a constrained time-synchronized LLN that has two subnets N1 and N2, connected through BBRs [I-D.ietf-6lo-backbone-router] with different reference clock times T1 and T2.

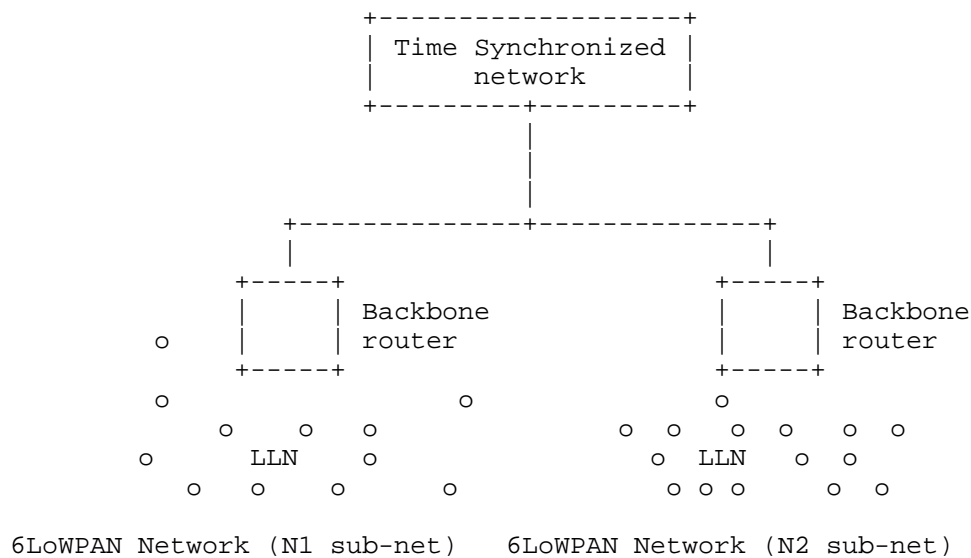


Figure 3: Intra-network Timezone Scenario

Case 1: Endpoints in the same DODAG(N1 sub-net) in non-storing mode.

Let us consider the scenario, as shown in Figure 4, where the Sender 'S' has an IP datagram to be routed to a Receiver 'R' within the same DODAG. For the route segment from Sender to 6LBR, the Sender includes a Timestamp-6LoRH header. Subsequently, 6LR will perform hop-by-hop operation to forward the packet towards the 6LBR. Once the IP datagram reaches 6LBR, it generates IPv6-in-IPv6 encapsulated packet when sending the packet downwards to the Receiver [I-D.ietf-roll-useofrplinfo]. The 6LBR copies the Timestamp-6LoRH header from the Sender originated IP header to the outer IP header. The Timestamp-6LoRH header contained in the inner IP header is elided.

At the tunnel endpoint of IPv6-in-IPv6 encapsulation, the Timestamp-6LoRH header is copied back from the outer header to inner header, and the inner IP packet is handed over to 'R'.

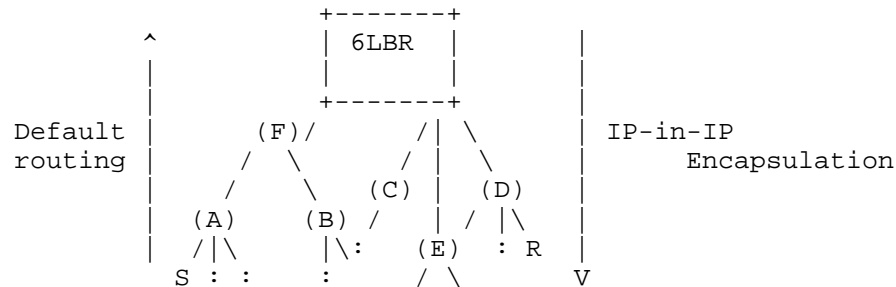


Figure 4: End points within same DODAG(N1 sub-net)

Case 2: Packet transmission in Heterogeneous Deterministic Networks (Heterogeneous L2 Technologies)

Let us consider the scenario, as shown in Figure 5, where the Sender 'S' (belonging to DODAG 1) has IP datagram to be routed to a Receiver 'R' over a time-synchronized IPv6 network. For the route segment from 'S' to 6LBR, 'S' includes a Timestamp-6LoRH header.

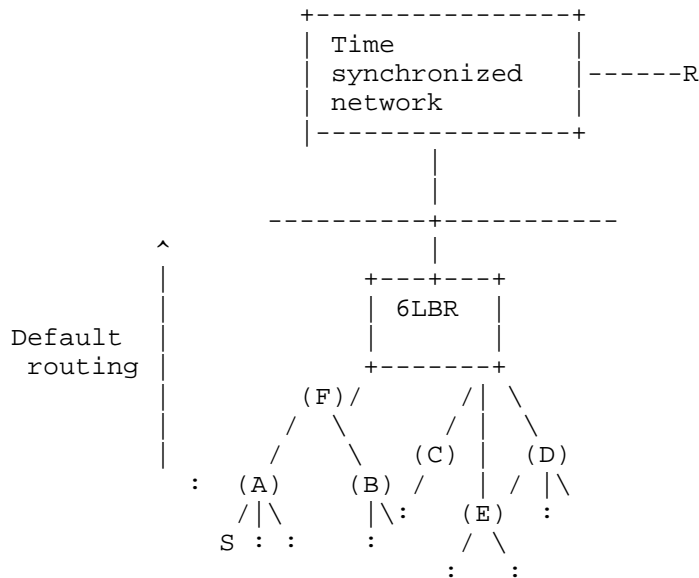


Figure 5: Packet transmission in different Deterministic Networks or Internet

Subsequently, 6LR will perform hop-by-hop operation to forward the packet towards the 6LBR. Once the IP datagram reaches 6LBR of DODAG1, it performs the following operation. It computes the remaining time by subtracting the elapsed time from the expiration time. The Timestamp-6LoRH header is updated with the remaining time. This value can then be encoded into In-band OAM Edge to Edge option [I-D.brockners-inband-oam-data] and handed over to IPv6 layer for further routing. Since the IP datagram is routed to another time synchronized deterministic network following its own distinct reference clock, the expiration time in In-band OAM is updated by adding the remaining time to the current time according to the time synchronization of the network of the outgoing interface.

Case 3: Packet transmission across different DODAGs (N1 to N2)

Let us consider the scenario, as shown in Figure 6, where the Sender 'S' (belonging to DODAG 1) has an IP datagram to be sent to Receiver 'R' belonging to another DODAG (DODAG 2). For the route segment from 'S' to 6LBR, 'S' includes the Timestamp-6LoRH header. Subsequently, each 6LR will perform hop-by-hop operation to forward the packet towards the 6LBR. Once the IP datagram reaches 6LBR of DODAG1, it performs the following operation. It computes the remaining time by subtracting the elapsed time from the expiration time. The expiration time in the Timestamp-6LoRH header is updated with the remaining time. It will then forward the packet to 6LBR of DODAG2. Once the IP datagram reaches 6LBR of DODAG2, it updates the Timestamp-6LoRH header by adding the current time of DODAG2. Further, it generates IPv6-in-IPv6 encapsulated packet when sending the packet downwards to the Receiver [I-D.ietf-roll-useofrplinfo].

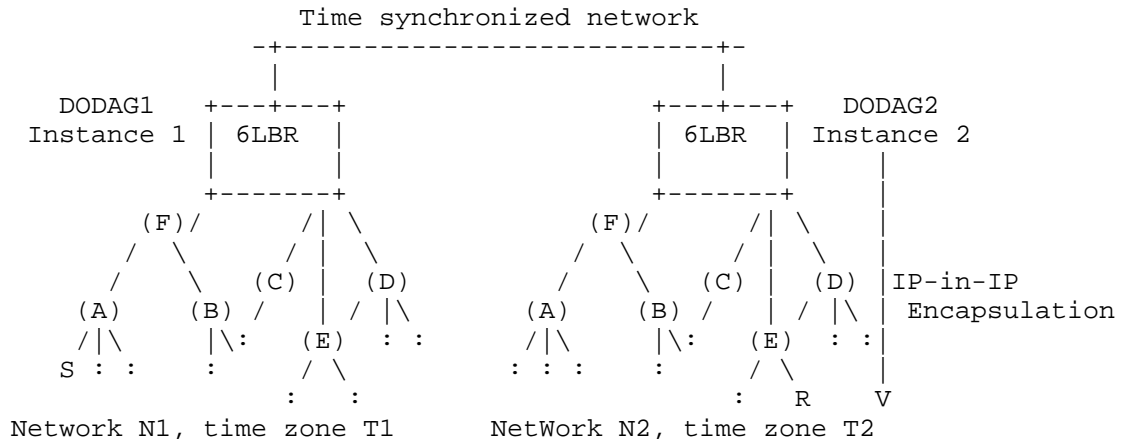


Figure 6: Packet transmission in different DODAGs(N1 to N2)

Let us consider an example of a 6TiSCH network where S in DODAG1 generates the packet at ASN 200 to R in DODAG2. Let the maximum allowable delay be 1 second. The time-slot length in DODAG1 and DODAG2 is assumed to be 10ms. Once the expiration time is encoded in Timestamp-6LoRH header, the packet is forwarded to LBR of DODAG1. Let us say the packet reaches LBR of DODAG1 at ASN 250.

```
current_time = ASN at LBR * slot_length_value.
```

```
remaining_time = expiration_time - current_time.
```

```
= ((packet_origination_time + max_allowable_transmission_delay) -
current time)
```

```
= (200*10 ms + 1 second) - 2.5 seconds
```

```
= 0.5 second
```

```
= 5 * 10^5 microseconds.
```

The remaining time is encoded in In-Band OAM (see Case 2) and forwarded to LBR2 over a different L2-interface, typically wired. Once the packet reaches LBR2, the expiration time in Timestamp-6LoRH header is re-calculated by adding to it the current ASN, before forwarding the packet to its connected 6TiSCH network.

6. IANA Considerations

This document defines a new 6LoWPAN Timestamp Header Type, and assigned a value of TBD from the 6LoWPAN Dispatch Page1 number space.

6LoRH Type	Value
Timestamp-6LoRH	TBD

Figure 7: Timestamp-6LoRH header type

7. Security Considerations

The security considerations of [RFC4944], [RFC6282] and [RFC6553] apply. Using a compressed format as opposed to the full in-line format is logically equivalent and does not create an opening for a new threat when compared to [RFC6550], [RFC6553] and [RFC6554].

8. Acknowledgements

The authors thank Pascal Thubert for suggesting the idea and encouraging the work. Thanks to Shwetha Bhandari's suggestions which were instrumental in extending the timing information to heterogeneous networks. The authors acknowledge the 6TiSCH WG members for their inputs on the mailing list. Special thanks to Jerry Daniel J for his support and valuable feedback.

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <<http://www.rfc-editor.org/info/rfc4944>>.
- [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, <<http://www.rfc-editor.org/info/rfc6282>>.
- [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, <<http://www.rfc-editor.org/info/rfc6550>>.
- [RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, DOI 10.17487/RFC6553, March 2012, <<http://www.rfc-editor.org/info/rfc6553>>.
- [RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, DOI 10.17487/RFC6554, March 2012, <<http://www.rfc-editor.org/info/rfc6554>>.

9.2. Informative References

[I-D.brockners-inband-oam-data]

Brockners, F., Bhandari, S., Pignataro, C., Gredler, H., Leddy, J., and S. Youell, "Data Formats for In-band OAM", draft-brockners-inband-oam-data-01 (work in progress), July 2016.

[I-D.grossman-detnet-use-cases]

Grossman, E., Gunther, C., Thubert, P., Wetterwald, P., Raymond, J., Korhonen, J., Kaneko, Y., Das, S., and Y. Zha, "Deterministic Networking Use Cases", draft-grossman-detnet-use-cases-01 (work in progress), November 2015.

[I-D.ietf-6lo-backbone-router]

Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-02 (work in progress), September 2016.

[I-D.ietf-roll-routing-dispatch]

Thubert, P., Bormann, C., Toutain, L., and R. Cragie, "6LoWPAN Routing Header", draft-ietf-roll-routing-dispatch-05 (work in progress), October 2016.

[I-D.ietf-roll-useofrplinfo]

Robles, I., Richardson, M., and P. Thubert, "When to use RFC 6553, 6554 and IPv6-in-IPv6", draft-ietf-roll-useofrplinfo-09 (work in progress), October 2016.

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

Vilajosana, X. and K. Pister, "Minimal 6TiSCH Configuration", draft-vilajosana-6tisch-minimal-00 (work in progress), October 2013.

Authors' Addresses

Lijo Thomas
C-DAC
Trivandrum 695033
India

Email: lijo@cdac.in

P.M. Akshay
Indian Institute of Science
Bangalore 560012
India

Email: akshaypm@ece.iisc.ernet.in

Satish Anamalamudi
Individual Contributor

Email: satishnaidu80@gmail.com

S.V.R Anand
Indian Institute of Science
Bangalore 560012
India

Email: anand@ece.iisc.ernet.in

Malati Hegde
Indian Institute of Science
Bangalore 560012
India

Email: malati@ece.iisc.ernet.in

Charles E. Perkins
Futurewei
2330 Central Expressway
Santa Clara 95050
Unites States

Email: charliep@computer.org

6lo
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2017

AR. Sangi
M. Chen
Huawei Technologies
C. Perkins
Futurewei
October 30, 2016

Designating 6LBR for IID Assignment
draft-rashid-6lo-iid-assignment-02

Abstract

In IPv6 Stateless Address Autoconfiguration (SLAAC), randomizing the interface identifier (IID) is a common practice to promote privacy. If there are a very large number of nodes, as has been discussed in several use cases, the effect will to proportionately increase the number of IIDs. A duplicate address detection (DAD) cycle is needed for each configured IID, introducing more and more overhead into the network. Each failed DAD requires the initiating node to regenerate a new IID and undergo the DAD cycle again. This document proposes an optimized approach when higher privacy is required by given network by allowing 6LBR (6LoWPAN Border Router) to provide a unique IID, avoiding the potential duplication. Such practice also prevent probable failure of time-critical application by enabling 6LBR to suggest unique IID, in case of address collision.

Additionally, further optimizations are suggested to enable multiple concurrent DAD cycles and to return the suggested IID from 6LBR to 6LN in a space-efficient manner.

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 May 3, 2017.

Copyright Notice

Copyright (c) 2016 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
2. Terminology	3
3. Likelihood of Address Collision	4
4. IID Assignment by 6LBR	4
4.1. Advantages of suggested algorithm	5
4.2. Extended Request/Confirmation Message	6
4.3. Extended Address Registration Option	7
5. Concurrent DAD	8
6. Aggregation Approach	8
7. IANA Considerations	9
7.1. EDAR and EDAC Messages, and EARO Option	9
7.2. Additions to Status Field	9
8. Security Considerations	10
9. References	10
9.1. Normative References	10
9.2. Informative References	10
Authors' Addresses	11

1. Introduction

IPv6 addresses in SLAAC are formed by concatenating a network prefix, acquired from Router Advertisement (RA) messages, with a locally generated IID [RFC4862], [RFC2464]. Since the best method for generating IIDs depends on the nature of networks, none of the proposed mechanisms [RFC4941], [RFC7217] is considered a default mechanism. Using neighbour discovery (ND), the uniqueness of newly generated IID is verified [RFC6775]. 6LBR performs DAD, and replies with a status. A failed DAD would require the initiating 6LN (6LoWPAN node) to regenerate an IID and wait for another DAD cycle, until the 6LN successfully registers a unique address [RFC6775].

A locally generated IID can be derived either from an embedded IEEE identifier [RFC4941], or randomly (based on a few variables) [RFC7217]. Since MAC reuse is unfortunately far more common than usually assumed [RFC7217], IIDs derived from MAC address are likely to cause more than the expected number of DAD failures. As soon as the 6LN generates an IID, it sends the NS (Neighbor Solicitation) message to 6LR (LLN Router). Then 6LR proceeds to send an ICMPv6 based DAR (Duplicate Address Request) message to 6LBR. An LN sends out a NS after checking its local cache for duplication; before proceeding with DAR, the 6LR also protects against address duplication within a locally maintained Neighbor Cache Entry (NCE) [RFC7217].

Use cases including huge numbers of nodes and vast scale networks are discussed in [RFC5548], [RFC5827]. The use of arbitrary IIDs can resolve privacy concerns for a participating node, but a simple NS intended to be targeted to a small group of nodes can pollute all the wireless bandwidth [I-D.vyncke-6man-mcast-not-efficient]. Multicast NS and NA are much more frequent in large scale radio environment with mobile devices [I-D.thubert-6lo-backbone-router]. Since the IIDs may be sporadically changed for privacy, the probability increases that a duplicate IIDs would result in DAD failure and repeated DAD cycles.

On the other hand, waiting for 6LN to regenerate another IID due to a failed DAD might lead to failure of time-critical application.

This document describes optimizations to 6LoWPAN ND which enable 6LBR to grant a unique IID for failed DAD, to undergo concurrent DAD and to return an IID to 6LN in a space-efficient manner.

2. 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 [RFC2119]. This document uses terminology from [RFC6775], [RFC2464], [I-D.ietf-6man-default-iids], and [I-D.ietf-6man-ipv6-address-generation-privacy].

SLLAO: Stateless Link-Local Address Option

RID: Random IDentifier

PRF: Pseudo Random Function

IID: Interface IDentifier

This document also uses the following terms:

EARO: Extended Address Registration Option

EDAR: Extended Duplicate Address Request

EDAC: Extended Duplicate Address Confirmation

LSB: Least Significant Bit

3. Likelihood of Address Collision

Following are several reasons to support necessity of this proposal:

- o Manufacturer may not follow a fine grained randomness in MAC addresses,
- o Shorter than 64 bits MAC addresses are used in numerous constrained technologies, and
- o Frequency of an IID being changed, depends on the degree of privacy that a particular application requires.

It depends on the way an IID is generated using MAC address and with shorter MAC addresses, it is more likely to face address collision.

4. IID Assignment by 6LBR

MAC driven IIDs [RFC2464] reduce or eliminate the need for DAD, but in practice such IID generation is discouraged ([I-D.ietf-6man-default-iids], [I-D.ietf-6man-ipv6-address-generation-privacy]), as common privacy concerns still persist, for instance:

- o Network activity correlation,
- o Location tracking,
- o Address scanning, and
- o Device-specific vulnerability exploitation.

Moreover, multiple approaches are proposed to suit different network constraints. Mechanisms such as specified in [RFC4941], which is mainly based on MAC address or an appropriate simple random number generation algorithm can be considered to generate IID.

Considering the scalability of a network and enabling 6LBR to suggest an IID, the method for IID generation specified in [RFC7217] SHOULD be used as this method is appropriate to support periodically changing IIDs.

```

RID (Random Identifier) :=
|Prefix|Interface Index|N/W ID|DAD Counter|Randomized Secret Key|
  \      \      \      /      /
    \      \      /      /
      +-----+-----+-----+
      |             Hash Function             |
      +-----+-----+-----+
    /      /      \      \
  /      /      \      \
                        Extract 64 LSBs

```

Figure 1: Using RFC7217 to generate IID

If DAD fails, the 6LBR will use public values for Prefix, Interface Index, and Network ID; the remaining two variables (DAD Counter, Randomized Secret Key) are local values. Neighbor solicitation using link-local address cannot be avoided, but only the newly generated IID needs to be forwarded to the LN.

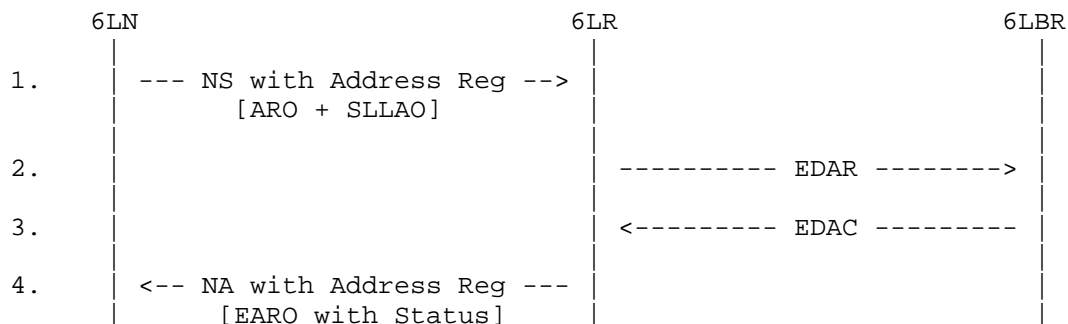


Figure 2: DAD cycle when 6LBR generates an IID

The approach in this draft is reactive rather than proactive; 6LBR only replies with a locally generated IID when DAD fails.

4.1. Advantages of suggested algorithm

Reference to [RFC7217] the resulting IID fulfils following main advantages:

- o For a given interface, same prefix and subnet would always result in same IID,
- o It would always be a different IID generated when a different prefix is used, and
- o DAD_Counter is another parameter that is used in this algorithm. In case of address collision, this parameter is incremented and the resulting address would be different than the previous address.

4.2. Extended Request/Confirmation Message

The Prefix is the same throughout each LoWPAN network. This draft uses that feature to reduce the size of the DAR:

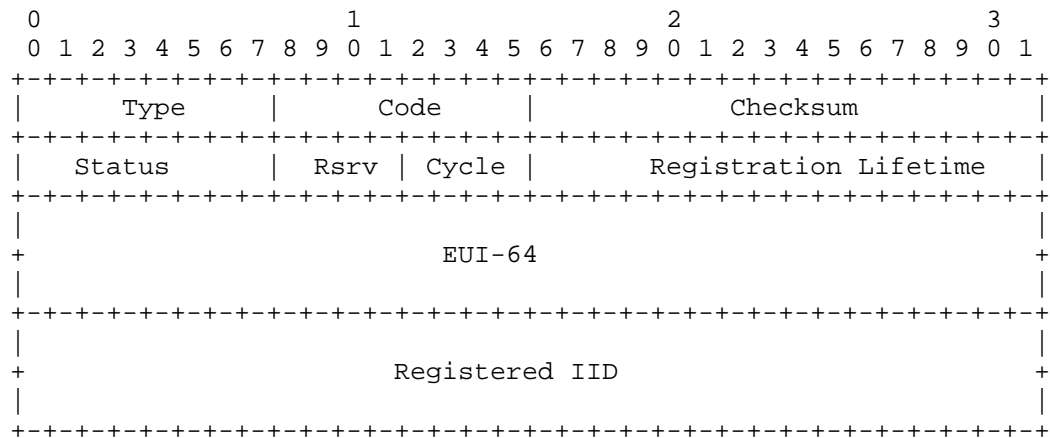


Figure 3: Extended Duplication Address Request

The fields are similar to DAR in [RFC6775] except:

Type: 159 (TBD)

Cycle: 4 out of 8 reserved bits to identify the DAD cycle between given 6LR and 6LBR. The reference is used later by 6LR to extract IID suggested by 6LBR.

Unlike the DAR, the Registered IID (64 bit) is returned instead of Registered Address (128 bit).

EDAC reduces the space needed for returning the EUI-64:

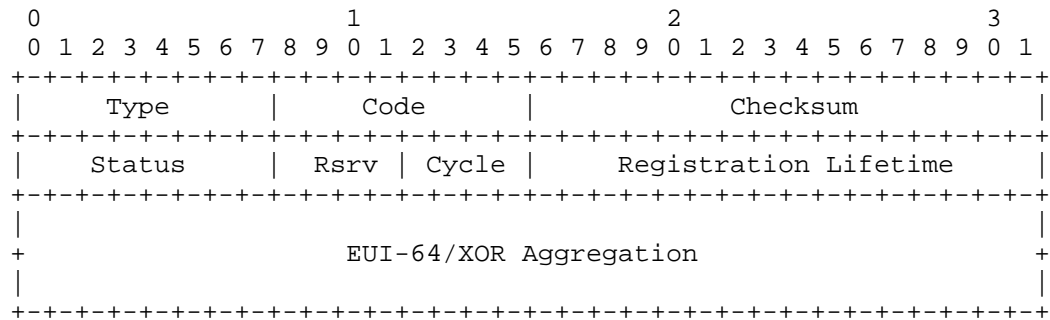


Figure 4: Extended Duplication Address Confirmation

The fields are similar to DAC in [RFC6775] except:

Type: 160 (TBD)

Cycle: 4 out of 8 reserved bits identify the DAD cycle between the 6LR and 6LBR. The reference is used later by 6LR to extract the IID suggested by 6LBR.

In case of a failed DAD, a 6LBR-generated IID is aggregated using XOR with EUI-64; otherwise the same EUI-64 occupies the 64 bits.

4.3. Extended Address Registration Option

ARO and EARO can ONLY be initiated by host and 6LR, respectively. [RFC6775] expects the reply of a host initiated ARO from 6LR with the same ARO except for changing the status bit to indicate the duplication detection. EARO is introduced in this document; 6LR can send out this option if it receives EDAC instead of DAC from 6LBR.

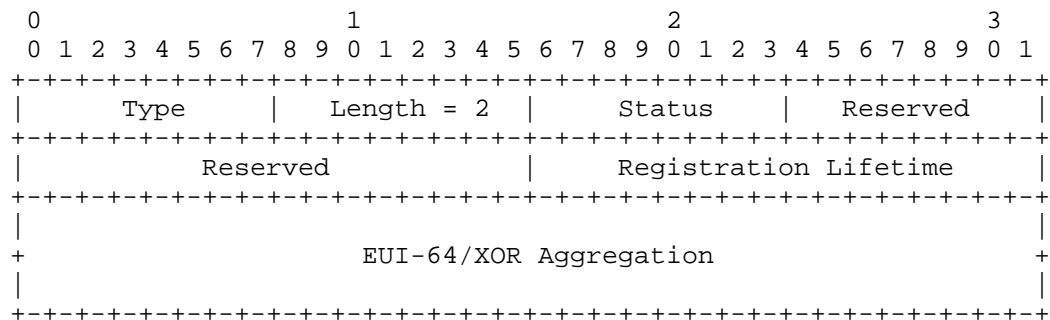


Figure 5: Extended Address Registration Option

The fields are similar to ARO in [RFC6775] except:

Type: 36 (TBD)

EUI-64/XOR Aggregation: a 64 bit IID generated by 6LBR is XOR'ed with EUI-64.

5. Concurrent DAD

In [RFC6775], 6LN is expected to generate an IID; so 6LR only acts on the first unique IID claim and silently discards any later claims for the same IID. In contrast, this document enables 6LBR to assign a unique IID in case of a duplicate IID claim by 6LR. For this purpose, a "Cycle" field is introduced to enable concurrency that will be helpful for large-scale networks [RFC5548]. See Figure 3 and Figure 4 for the format of the Cycle field.

6. Aggregation Approach

Each iteration of DAR and DAC [RFC6775] carries the entire 128 bit Registered Address during the DAD routine, even though the network Prefix is the same throughout each LoWPAN. This document enables eliding the network prefix part of the Registered Address as well in EDAC and EARO using simple XOR aggregation. The aggregated 64 bit field carries EUI-64 and suggested IID. See Figure 4 and Figure 5 for the format of the EUI-64/XOR Aggregation.

Under the proposed arrangement, 6LBR would only aggregate values, 6LN would only extract values and 6LR would do both.

At 6LR before sending EDAR to 6LBR:

- o 6LR would use the 4 out of 8 Reserved "Cycle" bits of EDAR to keep track of multiple DAD cycles. These iterations are recorded at 6LR and that information is used to extract IID/EUI-64 from EDAC to be forwarded to the appropriate 6LN.

At 6LBR before sending to 6LR:

- o If Status = 0 (Success), then 6LBR returns EDAC using all the values as received from EDAR.

- o If Status = 1 (Duplicate), then 6LBR generates IID and XORs it with EUI-64 to return in the EDAC to 6LR.

At 6LR before sending to 6LN:

- o If Status = 0 (Success) then keep the claimed address of 6LN as Destination Address for ARO to 6LN.

o If Status = 1 (Duplicate), then match the "Cycle" bits of EDAC to extract (using XOR) the EUI-64 address and use the extracted address as the Destination Address for EARO to 6LN.

Finally, at 6LN:

o If Status = 0 (Success), 6LN starts using the address that it claimed.

o If Status = 1 (Duplicate) then 6LN XORs the received EUI-64 address with its claimed EUI-64, which results in the newly generated IID sent by 6LBR.

7. IANA Considerations

7.1. EDAR and EDAC Messages, and EARO Option

The document requires two new ICMPv6 type numbers under the subregistry 'ICMPv6 "type" Numbers':

- o Extended Duplicate Address Request (159)
- o Extended Duplicate Address Confirmation (160)

This document requires a new ND option type under the subregistry "IPv6 Neighbor Discovery Option Formats":

- o Extended Address Registration Option (36)

7.2. Additions to Status Field

One new value is required for the "Address Registration Option Status Values" sub-registry under the "IPv6 Neighbor Discovery Option Formats":

Status	Description
0	Success
1	Duplicate Address
2	Neighbor Cache Full
3	6LBR generated IID
4-255	Allocated using Standards Action [RFC5226]

Addition to Status bits

8. Security Considerations

TBD

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <<http://www.rfc-editor.org/info/rfc2464>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<http://www.rfc-editor.org/info/rfc4862>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <<http://www.rfc-editor.org/info/rfc4941>>.
- [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>>.
- [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <<http://www.rfc-editor.org/info/rfc7217>>.

9.2. Informative References

- [I-D.ietf-6man-default-iids] Gont, F., Cooper, A., Thaler, D., and S. LIU, "Recommendation on Stable IPv6 Interface Identifiers", draft-ietf-6man-default-iids-16 (work in progress), September 2016.

- [I-D.ietf-6man-ipv6-address-generation-privacy]
Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-08 (work in progress), September 2015.
- [I-D.thubert-6lo-backbone-router]
Thubert, P., "IPv6 Backbone Router", draft-thubert-6lo-backbone-router-03 (work in progress), November 2015.
- [I-D.vyncke-6man-mcast-not-efficient]
Vyncke, E., Thubert, P., Levy-Abegnoli, E., and A. Yourtchenko, "Why Network-Layer Multicast is Not Always Efficient At Datalink Layer", draft-vyncke-6man-mcast-not-efficient-01 (work in progress), February 2014.
- [RFC5548] Dohler, M., Ed., Watteyne, T., Ed., Winter, T., Ed., and D. Barthel, Ed., "Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, DOI 10.17487/RFC5548, May 2009, <<http://www.rfc-editor.org/info/rfc5548>>.
- [RFC5827] Allman, M., Avrachenkov, K., Ayesta, U., Blanton, J., and P. Hurtig, "Early Retransmit for TCP and Stream Control Transmission Protocol (SCTP)", RFC 5827, DOI 10.17487/RFC5827, May 2010, <<http://www.rfc-editor.org/info/rfc5827>>.

Authors' Addresses

Abdur Rashid Sangi
Huawei Technologies
No.156 Beiqing Rd. Haidian District
Beijing 100095
P.R. China

Email: rashid.sangi@huawei.com

Mach(Guoyi) Chen
Huawei Technologies
No.156 Beiqing Rd. Haidian District
Beijing 100095
P.R. China

Email: mach.chen@huawei.com

Charles E. Perkins
Futurewei
2330 Central Expressway
Santa Clara 95050
USA

Email: charliep@computer.org

6lo
Internet-Draft
Updates: 6775 (if approved)
Intended status: Standards Track
Expires: April 29, 2017

P. Thubert, Ed.
cisco
E. Nordmark
Arista Networks
S. Chakrabarti
Ericsson
October 26, 2016

An Update to 6LoWPAN ND
draft-thubert-6lo-rfc6775-update-01

Abstract

This specification updates 6LoWPAN Neighbor Discovery (RFC6775), to clarify the role of the protocol as a registration technique, simplify the registration operation in 6LoWPAN routers, and provide enhancements to the registration capabilities, in particular for the registration to a backbone router for proxy ND operations.

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 April 29, 2017.

Copyright Notice

Copyright (c) 2016 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
2. Terminology	3
3. Updating RFC 6775	4
3.1. Extended Address Registration Option	4
3.2. Registering the Target Address	5
3.3. Link-local Addresses and Registration	5
4. Applicability and Requirements Served	7
5. The Enhanced Address Registration Option (EARO)	7
6. Backward Compatibility	11
6.1. Legacy 6LoWPAN Node	11
6.2. Legacy 6LoWPAN Router	11
6.3. Legacy 6LoWPAN Border Router	12
7. Security Considerations	12
8. IANA Considerations	13
9. Acknowledgments	13
10. References	13
10.1. Normative References	13
10.2. Informative References	14
10.3. External Informative References	16
Appendix A. Requirements	17
A.1. Requirements Related to Mobility	17
A.2. Requirements Related to Routing Protocols	17
A.3. Requirements Related to the Variety of Low-Power Link types	18
A.4. Requirements Related to Proxy Operations	19
A.5. Requirements Related to Security	20
A.6. Requirements Related to Scalability	21
Authors' Addresses	21

1. Introduction

The scope of this draft is an IPv6 Low Power Lossy Network (LLN), which can be a simple star or a more complex mesh topology. The LLN may be anchored at an IPv6 Backbone Router (6BBR). The Backbone Routers interconnect the LLNs over a Backbone Link and emulate that the LLN nodes are present on the Backbone using proxy-ND operations.

IPv6 Neighbor Discovery (ND) Optimization for IPv6 over Low-Power Wireless Personal Area Networks(6LoWPANs) [RFC6775] introduced a proactive registration mechanism to IPv6 ND services for nodes belonging to a LLN.

This specification modifies and extends the behaviour and protocol elements of [RFC6775] to enable additional capabilities, in particular the registration to a 6BBR for proxy ND operations [I-D.ietf-6lo-backbone-router].

2. 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 [RFC2119].

Readers are expected to be familiar with all the terms and concepts that are discussed in "Neighbor Discovery for IP version 6" [RFC4861], "IPv6 Stateless Address Autoconfiguration" [RFC4862], "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919], Neighbor Discovery Optimization for Low-power and Lossy Networks [RFC6775] and "Multi-link Subnet Support in IPv6" [I-D.ietf-ipv6-multilink-subnets].

Additionally, this document uses terminology from "Terms Used in Routing for Low-Power and Lossy Networks" [RFC7102] and [I-D.ietf-6tisch-terminology], as well as this additional terminology:

Backbone This is an IPv6 transit link that interconnects 2 or more Backbone Routers. It is expected to be deployed as a high speed backbone in order to federate a potentially large set of LLNS. Also referred to as a LLN backbone or Backbone network.

Backbone Router An IPv6 router that federates the LLN using a Backbone link as a backbone. A 6BBR acts as a 6LoWPAN Border Routers (6LBR) and an Energy Aware Default Router (NEAR).

Extended LLN This is the aggregation of multiple LLNs as defined in [RFC4919], interconnected by a Backbone Link via Backbone Routers, and forming a single IPv6 MultiLink Subnet.

Registration The process during which a wireless Node registers its address(es) with the Border Router so the 6BBR can proxy ND for it over the backbone.

Binding The state in the 6BBR that associates an IP address with a MAC address, a port and some other information about the node that owns the IP address.

Registered Node The node for which the registration is performed, which owns the fields in the EARO option.

Registering Node The node that performs the registration to the 6BBR, either for one of its own addresses, in which case it is Registered Node and indicates its own MAC Address as SLLA in the NS(ARO), or on behalf of a Registered Node that is reachable over a LLN mesh. In the latter case, if the Registered Node is reachable from the 6BBR over a Mesh-Under mesh, the Registering Node indicates the MAC Address of the Registered Node as SLLA in the NS(ARO). Otherwise, it is expected that the Registered Device is reachable over a Route-Over mesh from the Registering Node, in which case the SLLA in the NS(ARO) is that of the Registering Node, which causes it to attract the packets from the 6BBR to the Registered Node and route them over the LLN.

Registered Address The address owned by the Registered Node node that is being registered.

3. Updating RFC 6775

The support of this specification is signaled in Router Advertisement (RA) messages by 6LoWPAN Router (6LR) (how: tbd). Support for this specification can also be inferred from the update of the ARO option in the ND exchanges

. A Registering Node that supports this specification will favor registering to a 6LR that indicates support for this specification over that of [RFC6775].

3.1. Extended Address Registration Option

This specification extends the Address Registration Option (ARO) used for the process of address registration. The new ARO is referred to as Extended ARO (EARO), and its semantics are modified as follows:

The address that is being registered with a Neighbor Solicitation (NS) with an EARO is now the Target Address, as opposed to the Source Address as specified in [RFC6775]. This change enables a 6LBR to use an address of his as source to the proxy-registration of an address that belongs to a LLN Node to a 6BBR. This also limits the use of an address as source address before it is registered and the associated Duplicate Address Detection (DAD) is complete.

The Unique ID in the EARO option does no more have to be a MAC address. A new TLV format is introduced and a IANA registry is created for the type (TBD). This enables in particular the use of a Provable Temporary UID (PT-UID) as opposed to burn-in MAC address, the PT-UID providing a trusted anchor by the 6LR and 6LBR to protect the state associated to the node.

The specification introduces a Transaction ID (TID) field in the EARO. The TID MUST be provided by a node that supports this specification and a new T flag MUST be set to indicate so. The T bit can be used to determine whether the peer supports this specification.

3.2. Registering the Target Address

One of the requirements that this specification serves is the capability by a router such as a RPL root to proxy-register an address to a 6BBR on behalf of a 6LN, as discussed in Appendix A.4. In order to serve that requirement, this specification changes the behaviour of the 6LN and the 6LR so that the Registered Address is found in the Target Address field of the NS and NA messages as opposed to the Source Address.

With this convention, a TLLA option would indicate the link-layer address of the 6LN that owns the address, whereas the SLLA Option in a NS message indicates that of the Registering Node, which can be the owner device, or a proxy.

Since the Registering Node is the one that has reachability with the 6LR, and is the one expecting packets for the 6LN, it makes sense to maintain compatibility with [RFC6775], and it is REQUIRED that an SLLA Option is always placed in a registration NS(EARO) message.

3.3. Link-local Addresses and Registration

Considering that LLN nodes are often not wired and may move, there is no guarantee that a link-local address stays unique between a potentially variable and unbounded set of neighboring nodes. Compared to [RFC6775], this specification only requires that a link-local address is unique from the perspective of the peering nodes. This simplifies the Duplicate Address Detection (DAD) for link-local addresses, and there is no DAR/DAC exchange between the 6LR and a 6LBR for link-local addresses.

Additionally, [RFC6775] requires that a 6LoWPAN Node (6LN) uses an address being registered as the source of the registration message. This generates complexities in the 6LR to be able to cope with a potential duplication, in particular for global addresses. To simplify this, a 6LN and a 6LR that conform this specification always use link-local addresses as source and destination addresses for the registration NS/NA exchange. As a result, the registration is globally faster, and some of the complexity is removed.

In more details:

An exchange between two nodes using link-local addresses implies that they are reachable over one hop and that at least one of the 2 nodes acts as a 6LR. A node MUST register a link-local address to a 6LR in order to obtain reachability from that 6LR beyond the current exchange, and in particular to use the link-local address as source address to register other addresses, e.g. global addresses. If there is no collision with an address previously registered to this 6LR by another 6LN, then, from the standpoint of this 6LR, this link-local address is unique and the registration is acceptable. Conversely, it may possibly happen that two different 6LRs expose a same link-local address but different link-layer addresses. In that case, a 6LN may only interact with one of the 6LR so as to avoid confusion in the 6LN neighbor cache.

The DAD process between the 6LR and a 6LoWPAN Border Router (6LBR), which is based on a Duplicate Address Request (DAR) / Duplicate Address Confirmation (DAC) exchange as described in [RFC6775], does not need to take place for link-local addresses.

It is desired that a 6LR does not need to modify its state associated to the Source Address of an NS(EARO) message. For that reason, when possible, it is RECOMMENDED to use an address that is already registered with a 6LR

When registering to a 6LR that conforms this specification, a node MUST use a link-local address as the source address of the registration, whatever the type of IPv6 address that is being registered. That link-local Address MUST be either already registered, or the address that is being registered.

When a Registering Node does not have an already-registered address, it MUST register a link-local address, using it as both the Source and the Target Address of an NS(EARO) message. In that case, it is RECOMMENDED to use a link-local address that is (expected to be) globally unique, e.g. derived from a burn-in MAC address. An EARO option in the response NA indicates that the 6LR supports this specification.

Since there is no DAR/DAC exchange for link-local addresses, the 6LR may answer immediately to the registration of a link-local address, based solely on its existing state and the Source Link-Layer Option that MUST be placed in the NS(EARO) message as required in [RFC6775].

A node needs to register its IPv6 Global Unicast IPv6 Addresses (GUA) to a 6LR in order to obtain a global reachability for these addresses via that 6LR. As opposed to a node that complies to [RFC6775], a Registering Node registering a GUA does use that GUA as Source Address for the registration to a 6LR that conforms this

specification. The DAR/DAC exchange MUST take place for non-link-local addresses as prescribed by [RFC6775].

4. Applicability and Requirements Served

This specification extends 6LoWPAN ND to sequence the registration and serves the requirements expressed Appendix A.1 by enabling the mobility of devices from one LLN to the next based on the complementary work in [I-D.ietf-6lo-backbone-router].

In the context of the the TimeSlotted Channel Hopping (TSCH) mode of [IEEE802154], the 6TiSCH architecture [I-D.ietf-6tisch-architecture] introduces how a 6LoWPAN ND host could connect to the Internet via a RPL mesh Network, but this requires additions to the 6LoWPAN ND protocol to support mobility and reachability in a secured and manageable environment. This specification details the new operations that are required to implement the 6TiSCH architecture and serves the requirements listed in Appendix A.2.

The term LLN is used loosely in this specification to cover multiple types of WLANs and WPANs, including Low-Power Wi-Fi, BLUETOOTH(R) Low Energy, IEEE802.11AH and IEEE802.15.4 wireless meshes, so as to address the requirements discussed in Appendix A.3

This specification can be used by any wireless node to associate at Layer-3 with a 6BBR and register its IPv6 addresses to obtain routing services including proxy-ND operations over the backbone, effectively providing a solution to the requirements expressed in Appendix A.4.

Efficiency aware IPv6 Neighbor Discovery Optimizations [I-D.chakrabarti-nordmark-6man-efficient-nd] suggests that 6LoWPAN ND [RFC6775] can be extended to other types of links beyond IEEE802.15.4 for which it was defined. The registration technique is beneficial when the Link-Layer technique used to carry IPv6 multicast packets is not sufficiently efficient in terms of delivery ratio or energy consumption in the end devices, in particular to enable energy-constrained sleeping nodes. The value of such extension is especially apparent in the case of mobile wireless nodes, to reduce the multicast operations that are related to classical ND ([RFC4861], [RFC4862]) and plague the wireless medium. This serves scalability requirements listed in Appendix A.6.

5. The Enhanced Address Registration Option (EARO)

With the ARO option defined in 6LoWPAN ND [RFC6775], the address being registered and its owner can be uniquely identified and matched with the Binding Table entries of each Backbone Router.

The Enhanced Address Registration Option (EARO) is intended to be used as a replacement to the ARO option within Neighbor Discovery NS and NA messages between a LLN node and its 6LoWPAN Router (6LR), as well as in Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC) messages between 6LRs and 6LBRs in LLNs meshes such as 6TiSCH networks.

An NS message with an EARO option is a registration if and only if it also carries an SLLAO option. The AERO option also used in NS and NA messages between Backbone Routers over the backbone link to sort out the distributed registration state, and in that case, it does not carry the SLLAO option and is not confused with a registration.

The EARO extends the ARO and is recognized by the setting of the TID bit. A node that supports this specification MUST always use an EARO as a replacement to an ARO in its registration to a router. This is harmless since the TID bit and fields are reserved in [RFC6775] are ignored by a legacy router. A router that supports this specification answers to an ARO with an ARO and to an EARO with an EARO.

This specification changes the behavior of the peers in a registration flows. To enable backward compatibility, a node that registers to a router that is not known to support this specification MUST behave as prescribed by [RFC6775]. Once the router is known to support this specification, the node MUST obey this specification.

When using the EARO option, the address being registered is found in the Target Address field of the NS and NA messages. This differs from 6LoWPAN ND [RFC6775] which specifies that the address being registered is the source of the NS.

The reason for this change is to enable proxy-registrations on behalf of other nodes in Route-Over meshes, for instance to enable that a RPL root registers addresses on behalf LLN nodes that are deeper in a 6TiSCH mesh. In that case, the Registering Node MUST indicate its own address as source of the ND message and its MAC address in the Source Link-Layer Address Option (SLLAO), since it still expects to get the packets and route them down the mesh. But the Registered Address belongs to another node, the Registered Node, and that address is indicated in the Target Address field of the NS message.

One way of achieving all the above is for a node to first register an address that it owns in order to validate that the router supports this specification, placing the same address in the Source and Target Address fields of the NS message. The node may for instance register an address that is based on EUI-64. For such address, DAD is not

required and using the SLLAO option in the NS is actually more amenable with older ND specifications such as ODAD [RFC4429].

Once that first registration is complete, the node knows from the setting of the TID in the response whether the router supports this specification. If this is verified, the node may register other addresses that it owns, or proxy-register addresses on behalf some another node, indicating those addresses being registered in the Target Address field of the NS messages, while using one of its own, already registered, addresses as source.

The format of the EARO option is as follows:

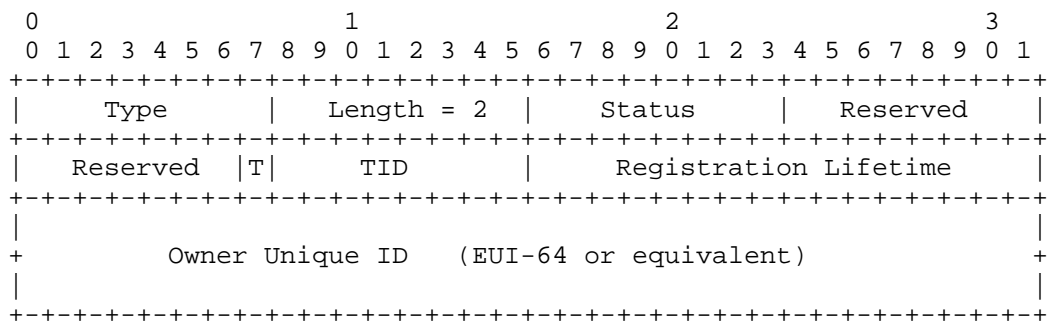


Figure 1: EARO

Option Fields

Type:

Length: 2

Status:

Value	Description
0..2	See [RFC6775]. Note that a Status of 1 "Duplicate Address" applies to the Registered Address. If the Source Address conflicts with an existing registration, "Duplicate Source Address" should be used instead
3	Moved: The registration fails because it is not the freshest
4	Removed: The binding state was removed. This may be placed in an asynchronous NS(ARO) message, or as the rejection of a proxy registration to a Backbone Router
5	Proof requested: The registering node is challenged for owning the registered address or for being an acceptable proxy for the registration
6	Duplicate Source Address: The address used as source of the NS(ARO) conflicts with an existing registration.
7	Administrative Rejection: The address being registered is reserved for another use by an administrative decision (e.g. placed in a DHCPv6 pool); The Registering Node is requested to form a different address and retry
8	Invalid Registered Address: The address being registered is not usable on this link, e.g. it is not topologically correct
9	Invalid Source Address: The address used as source of the NS(ARO) is not usable on this link, e.g. it is not topologically correct

Table 1

Reserved: This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

T: One bit flag. Set if the next octet is a used as a TID.

TID: 1-byte integer; a transaction id that is maintained by the node and incremented with each transaction. it is recommended that the node maintains the TID in a persistent storage.

Registration Lifetime: 16-bit integer; expressed in minutes. 0 means that the registration has ended and the state should be removed.

Owner Unique Identifier (OUI): A globally unique identifier for the node associated. This can be the EUI-64 derived IID of an interface, or some provable ID obtained cryptographically.

New status values are introduced, their values to be confirmed by IANA:

Moved: This status indicates that the registration is rejected because another more recent registration was done, as indicated by a same OUI and a more recent TID. One possible cause is a stale registration that has progressed slowly in the network and was passed by a more recent one. It could also indicate a OUI collision.

Removed: This status is expected in asynchronous messages from a registrar (6LR, 6LBR, 6BBR) to indicate that the registration state is removed, for instance due to time out of a lifetime, or a movement. It is used for instance by a 6BBR in a NA(ARO) message to indicate that the ownership of the proxy state on the backbone was transferred to another 6BBR, which is indicative of a movement of the device. The receiver of the NA is the device that has performed a registration that is now stale and it should clean up its state.

6. Backward Compatibility

6.1. Legacy 6LoWPAN Node

A legacy 6LN will use the registered address as source and will not use an EARO option. In order to be backward compatible, an updated 6LR needs to accept that registration if it is valid per [RFC3972], and manage the binding cache accordingly.

The main difference with [RFC3972] is that DAR/DAC exchange for DAD may be avoided for link-local addresses. Additionally, the 6LR SHOULD use an EARO in the reply, and may use all the status codes defined in this specification.

6.2. Legacy 6LoWPAN Router

The first registration by a an updated 6LN is for a link-local address, using that link-local address as source. A legacy 6LN will not makes a difference and accept -or reject- that registration as if the 6LN was a legacy node.

An updated 6LN will always use an EARO option in the registration NS message, whereas a legacy 6LN will always areply with an ARO option in the NA message. So from that first registration, the updated 6LN can figure whether the 6LR supports this specification or not.

When facing a legacy 6LR, an updated 6LN may attempt to find an alternate 6LR that is updated. In order to be backward compatible, based on the discovery that a 6LR is legacy, the 6LN needs to fallback to legacy behaviour and source the packet with the registrered address.

The main difference is that the updated 6LN SHOULD use an EARO in the request regardless of the type of 6LN, legacy or updated

6.3. Legacy 6LoWPAN Border Router

With this specification, the DAR/DAC transports an EARO option as opposed to an ARO option. As described for the NS/NA exchange, devices that support this specification always use an EARO option and all the associated behaviour.

7. Security Considerations

This specification expects that the link layer is sufficiently protected, either by means of physical or IP security for the Backbone Link or MAC sublayer cryptography. In particular, it is expected that the LLN MAC provides secure unicast to/from the Backbone Router and secure Broadcast from the Backbone Router in a way that prevents tempering with or replaying the RA messages.

The use of EUI-64 for forming the Interface ID in the link-local address prevents the usage of Secure ND ([RFC3971] and [RFC3972]) and address privacy techniques. This specification RECOMMENDS the use of additional protection against address theft such as provided by [I-D.sarikaya-6lo-ap-nd], which guarantees the ownership of the OUID.

When the ownership of the OUID cannot be assessed, this specification limits the cases where the OUID and the TID are multicasted, and obfuscates them in responses to attempts to take over an address.

The LLN nodes depend on the 6LBR and the 6BBR for their operation. A trust model must be put in place to ensure that the right devices are acting in these roles, so as to avoid threats such as black-holing, or bombing attack whereby an impersonated 6LBR would destroy state in the network by using the "Removed" status code.

8. IANA Considerations

This document requires the following additions:

Address Registration Option Status Values Registry

Status	Description
3	Moved
4	Removed
5	Proof requested
6	Invalid Source Address
7	Administrative Rejection

IANA is required to change the registry accordingly

Table 2: New ARO Status values

9. Acknowledgments

Kudos to Eric Levy-Abegnoli who designed the First Hop Security infrastructure at Cisco.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <<http://www.rfc-editor.org/info/rfc4429>>.
- [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, <<http://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, <<http://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, <<http://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, <<http://www.rfc-editor.org/info/rfc6775>>.

10.2. Informative References

- [I-D.chakrabarti-nordmark-6man-efficient-nd]
Chakrabarti, S., Nordmark, E., Thubert, P., and M. Wasserman, "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", draft-chakrabarti-nordmark-6man-efficient-nd-07 (work in progress), February 2015.
- [I-D.delcarpio-6lo-wlanah]
Vega, L., Robles, I., and R. Morabito, "IPv6 over 802.11ah", draft-delcarpio-6lo-wlanah-01 (work in progress), October 2015.
- [I-D.ietf-6lo-6lobac]
Lynn, K., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over MS/TP Networks", draft-ietf-6lo-6lobac-05 (work in progress), June 2016.
- [I-D.ietf-6lo-backbone-router]
Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-02 (work in progress), September 2016.
- [I-D.ietf-6lo-dect-ule]
Mariager, P., Petersen, J., Shelby, Z., Logt, M., and D. Barthel, "Transmission of IPv6 Packets over DECT Ultra Low Energy", draft-ietf-6lo-dect-ule-07 (work in progress), October 2016.

- [I-D.ietf-6lo-nfc]
Choi, Y., Youn, J., and Y. Hong, "Transmission of IPv6 Packets over Near Field Communication", draft-ietf-6lo-nfc-05 (work in progress), October 2016.
- [I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-10 (work in progress), June 2016.
- [I-D.ietf-6tisch-terminology]
Palattella, M., Thubert, P., Watteyne, T., and Q. Wang, "Terminology in IPv6 over the TSCH mode of IEEE 802.15.4e", draft-ietf-6tisch-terminology-07 (work in progress), March 2016.
- [I-D.ietf-bier-architecture]
Wijnands, I., Rosen, E., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast using Bit Index Explicit Replication", draft-ietf-bier-architecture-04 (work in progress), July 2016.
- [I-D.ietf-ipv6-multilink-subnets]
Thaler, D. and C. Huitema, "Multi-link Subnet Support in IPv6", draft-ietf-ipv6-multilink-subnets-00 (work in progress), July 2002.
- [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks]
Popa, D. and J. Hui, "6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks", draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00 (work in progress), March 2014.
- [I-D.sarikaya-6lo-ap-nd]
Sethi, M., Thubert, P., and B. Sarikaya, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-sarikaya-6lo-ap-nd-04 (work in progress), August 2016.
- [RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <<http://www.rfc-editor.org/info/rfc3810>>.
- [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <<http://www.rfc-editor.org/info/rfc3971>>.

- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <<http://www.rfc-editor.org/info/rfc3972>>.
- [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, <<http://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, <<http://www.rfc-editor.org/info/rfc6282>>.
- [RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <<http://www.rfc-editor.org/info/rfc7102>>.
- [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <<http://www.rfc-editor.org/info/rfc7217>>.
- [RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015, <<http://www.rfc-editor.org/info/rfc7428>>.
- [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <<http://www.rfc-editor.org/info/rfc7668>>.

10.3. External Informative References

- [IEEE80211]
IEEE standard for Information Technology, "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".

[IEEE802151]

IEEE standard for Information Technology, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)".

[IEEE802154]

IEEE standard for Information Technology, "IEEE Standard for Local and metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)".

Appendix A. Requirements

This section lists requirements that were discussed at 6lo for an update to 6LoWPAN ND. This specification meets most of them, but those listed in Appendix A.5 which are deferred to a different specification such as [I-D.sarikaya-6lo-ap-nd].

A.1. Requirements Related to Mobility

Due to the unstable nature of LLN links, even in a LLN of immobile nodes a 6LN may change its point of attachment to a 6LR, say 6LR-a, and may not be able to notify 6LR-a. Consequently, 6LR-a may still attract traffic that it cannot deliver any more. When links to a 6LR change state, there is thus a need to identify stale states in a 6LR and restore reachability in a timely fashion.

Req1.1: Upon a change of point of attachment, connectivity via a new 6LR MUST be restored timely without the need to de-register from the previous 6LR.

Req1.2: For that purpose, the protocol MUST enable to differentiate between multiple registrations from one 6LoWPAN Node and registrations from different 6LoWPAN Nodes claiming the same address.

Req1.3: Stale states MUST be cleaned up in 6LRs.

Req1.4: A 6LoWPAN Node SHOULD also be capable to register its Address to multiple 6LRs, and this, concurrently.

A.2. Requirements Related to Routing Protocols

The point of attachment of a 6LN may be a 6LR in an LLN mesh. IPv6 routing in a LLN can be based on RPL, which is the routing protocol that was defined at the IETF for this particular purpose. Other

routing protocols than RPL are also considered by Standard Defining Organizations (SDO) on the basis of the expected network characteristics. It is required that a 6LoWPAN Node attached via ND to a 6LR would need to participate in the selected routing protocol to obtain reachability via the 6LR.

Next to the 6LBR unicast address registered by ND, other addresses including multicast addresses are needed as well. For example a routing protocol often uses a multicast address to register changes to established paths. ND needs to register such a multicast address to enable routing concurrently with discovery.

Multicast is needed for groups. Groups MAY be formed by device type (e.g. routers, street lamps), location (Geography, RPL sub-tree), or both.

The Bit Index Explicit Replication (BIER) Architecture [I-D.ietf-bier-architecture] proposes an optimized technique to enable multicast in a LLN with a very limited requirement for routing state in the nodes.

Related requirements are:

Req2.1: The ND registration method SHOULD be extended in such a fashion that the 6LR MAY advertise the Address of a 6LoWPAN Node over the selected routing protocol and obtain reachability to that Address using the selected routing protocol.

Req2.2: Considering RPL, the Address Registration Option that is used in the ND registration SHOULD be extended to carry enough information to generate a DAO message as specified in [RFC6550] section 6.4, in particular the capability to compute a Path Sequence and, as an option, a RPLInstanceID.

Req2.3: Multicast operations SHOULD be supported and optimized, for instance using BIER or MPL. Whether ND is appropriate for the registration to the 6BBR is to be defined, considering the additional burden of supporting the Multicast Listener Discovery Version 2 [RFC3810] (MLDv2) for IPv6.

A.3. Requirements Related to the Variety of Low-Power Link types

6LoWPAN ND [RFC6775] was defined with a focus on IEEE802.15.4 and in particular the capability to derive a unique Identifier from a globally unique MAC-64 address. At this point, the 6lo Working Group is extending the 6LoWPAN Header Compression (HC) [RFC6282] technique to other link types ITU-T G.9959 [RFC7428], Master-Slave/Token-Passing [I-D.ietf-6lo-6lobac], DECT Ultra Low Energy

[I-D.ietf-6lo-dect-ule], Near Field Communication [I-D.ietf-6lo-nfc], IEEE802.11ah [I-D.delcarpio-6lo-wlanah], as well as IEEE1901.2 Narrowband Powerline Communication Networks [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks] and BLUETOOTH(R) Low Energy [RFC7668].

Related requirements are:

Req3.1: The support of the registration mechanism SHOULD be extended to more LLN links than IEEE 802.15.4, matching at least the LLN links for which an "IPv6 over foo" specification exists, as well as Low-Power Wi-Fi.

Req3.2: As part of this extension, a mechanism to compute a unique Identifier should be provided, with the capability to form a Link-Local Address that SHOULD be unique at least within the LLN connected to a 6LBR discovered by ND in each node within the LLN.

Req3.3: The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of unique Identifier.

Req3.4: The Neighbour Discovery should specify the formation of a site-local address that follows the security recommendations from [RFC7217].

A.4. Requirements Related to Proxy Operations

Duty-cycled devices may not be able to answer themselves to a lookup from a node that uses classical ND on a backbone and may need a proxy. Additionally, the duty-cycled device may need to rely on the 6LBR to perform registration to the 6BBR.

The ND registration method SHOULD defend the addresses of duty-cycled devices that are sleeping most of the time and not capable to defend their own Addresses.

Related requirements are:

Req4.1: The registration mechanism SHOULD enable a third party to proxy register an Address on behalf of a 6LoWPAN node that may be sleeping or located deeper in an LLN mesh.

Req4.2: The registration mechanism SHOULD be applicable to a duty-cycled device regardless of the link type, and enable a 6BBR to operate as a proxy to defend the registered Addresses on its behalf.

Req4.3: The registration mechanism SHOULD enable long sleep durations, in the order of multiple days to a month.

A.5. Requirements Related to Security

In order to guarantee the operations of the 6LoWPAN ND flows, the spoofing of the 6LR, 6LBR and 6BBRs roles should be avoided. Once a node successfully registers an address, 6LoWPAN ND should provide energy-efficient means for the 6LBR to protect that ownership even when the node that registered the address is sleeping.

In particular, the 6LR and the 6LBR then should be able to verify whether a subsequent registration for a given Address comes from the original node.

In a LLN it makes sense to base security on layer-2 security. During bootstrap of the LLN, nodes join the network after authorization by a Joining Assistant (JA) or a Commissioning Tool (CT). After joining nodes communicate with each other via secured links. The keys for the layer-2 security are distributed by the JA/CT. The JA/CT can be part of the LLN or be outside the LLN. In both cases it is needed that packets are routed between JA/CT and the joining node.

Related requirements are:

Req5.1: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR, 6LBR and 6BBR to authenticate and authorize one another for their respective roles, as well as with the 6LoWPAN Node for the role of 6LR.

Req5.2: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR and the 6LBR to validate new registration of authorized nodes. Joining of unauthorized nodes MUST be impossible.

Req5.3: 6LoWPAN ND security mechanisms SHOULD lead to small packet sizes. In particular, the NS, NA, DAR and DAC messages for a re-registration flow SHOULD NOT exceed 80 octets so as to fit in a secured IEEE802.15.4 frame.

Req5.4: Recurrent 6LoWPAN ND security operations MUST NOT be computationally intensive on the LoWPAN Node CPU. When a Key hash calculation is employed, a mechanism lighter than SHA-1 SHOULD be preferred.

Req5.5: The number of Keys that the 6LoWPAN Node needs to manipulate SHOULD be minimized.

Req5.6: The 6LoWPAN ND security mechanisms SHOULD enable CCM* for use at both Layer 2 and Layer 3, and SHOULD enable the reuse of security code that has to be present on the device for upper layer security such as TLS.

Req5.7: Public key and signature sizes SHOULD be minimized while maintaining adequate confidentiality and data origin authentication for multiple types of applications with various degrees of criticality.

Req5.8: Routing of packets should continue when links pass from the unsecured to the secured state.

Req5.9: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR and the 6LBR to validate whether a new registration for a given address corresponds to the same 6LoWPAN Node that registered it initially, and, if not, determine the rightful owner, and deny or clean-up the registration that is duplicate.

A.6. Requirements Related to Scalability

Use cases from Automatic Meter Reading (AMR, collection tree operations) and Advanced Metering Infrastructure (AMI, bi-directional communication to the meters) indicate the needs for a large number of LLN nodes pertaining to a single RPL DODAG (e.g. 5000) and connected to the 6LBR over a large number of LLN hops (e.g. 15).

Related requirements are:

Req6.1: The registration mechanism SHOULD enable a single 6LBR to register multiple thousands of devices.

Req6.2: The timing of the registration operation should allow for a large latency such as found in LLNs with ten and more hops.

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis 06254
FRANCE

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

Erik Nordmark
Arista Networks
Santa Clara, CA
USA

Email: nordmark@arista.com

Samita Chakrabarti
Ericsson
San Jose, CA
USA

Email: samita.chakrabarti@ericsson.com