

6Lo Working Group  
Internet-Draft

Intended status: Standards Track  
Expires: March 31, 2020

C. Gomez  
S. Darroudi  
Universitat Politecnica de Catalunya  
T. Savolainen  
DarkMatter  
M. Spoerk  
Graz University of Technology  
September 28, 2019

IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP  
draft-ietf-6lo-blemesh-06

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 mechanisms that are needed to enable IPv6 mesh over Bluetooth Low Energy links established by using the Bluetooth Internet Protocol Support Profile. This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE links.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 31, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents

(<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
1.1. Terminology and Requirements Language . . . . .	3
2. Bluetooth LE Networks and the IPSP . . . . .	3
3. Specification of IPv6 mesh over Bluetooth LE links . . . . .	4
3.1. Protocol stack . . . . .	4
3.2. Subnet model . . . . .	5
3.3. Link model . . . . .	6
3.3.1. Stateless address autoconfiguration . . . . .	6
3.3.2. Neighbor Discovery . . . . .	6
3.3.3. Header compression . . . . .	7
3.3.4. Unicast and multicast mapping . . . . .	8
4. IANA Considerations . . . . .	9
5. Security Considerations . . . . .	9
6. Contributors . . . . .	9
7. Acknowledgements . . . . .	9
8. Appendix A: Bluetooth LE connection establishment example . .	10
9. Appendix B: Node joining procedure . . . . .	13
10. References . . . . .	13
10.1. Normative References . . . . .	13
10.2. Informative References . . . . .	14
Authors' Addresses . . . . .	15

## 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, the functionality described in RFC 7668 is not

sufficient and would fail to enable an IPv6 mesh over Bluetooth LE links. This document specifies mechanisms that are needed to enable IPv6 mesh over Bluetooth LE links. This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE links.

### 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 (now deprecated) 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 and subsequent Bluetooth versions (e.g. Bluetooth 4.2 [BTCorev4.2] or subsequent), a device may implement both roles simultaneously.

This document assumes a mesh network composed of Bluetooth LE links, where link layer connections are established between neighboring IPv6-enabled devices (see Section 3.3.2, item 3.b)). 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 mesh over 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 links

#### 3.1. Protocol stack

Figure 1 illustrates the protocol stack for IPv6 mesh over Bluetooth LE links. 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 IPv6 mesh over Bluetooth LE") is now adapted for IPv6 mesh over Bluetooth LE links, and b) the protocol stack for IPv6 mesh over Bluetooth LE links includes IPv6 routing functionality.

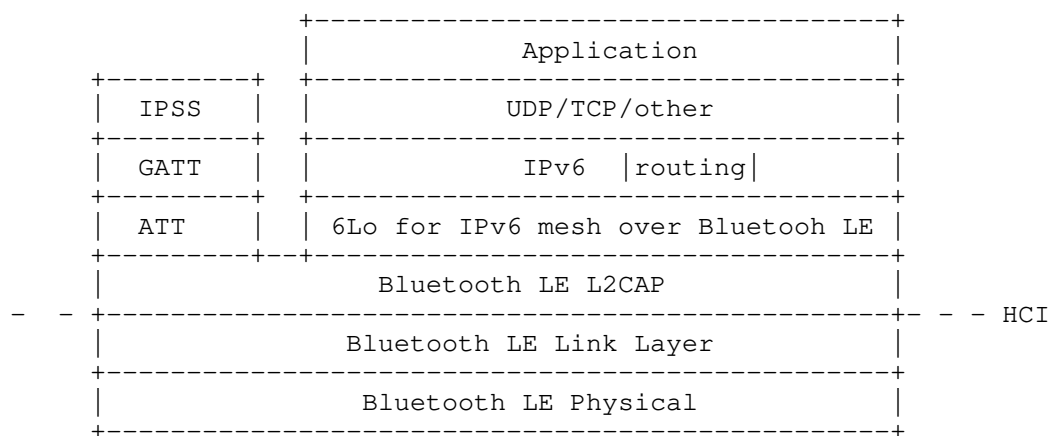


Figure 1: Protocol stack for IPv6 mesh over Bluetooth LE links.

Bluetooth 4.2 defines a default MTU for Bluetooth LE of 251 bytes. Excluding the L2CAP header of 4 bytes, a protocol data unit (PDU) size of 247 bytes is available for the layer above L2CAP. (Note: earlier Bluetooth LE versions offered a maximum amount of 23 bytes for the layer atop L2CAP.) The L2CAP provides a fragmentation and reassembly solution for transmitting or receiving larger PDUs. At each link, the IPSP defines means for negotiating a link-layer connection that provides an MTU of 1280 octets or higher for the IPv6 layer [IPSP]. The link-layer MTU is negotiated separately for each direction. Implementations that require an equal link-layer MTU for the two directions SHALL use the smallest of the possibly different MTU values.

Note that this specification allows using different MTUs in different links. If an implementation requires use of the same MTU on every one of its links, and a new node with a smaller MTU is added to the network, a renegotiation of one or more links can occur. In the

worst case, the renegotiations could cascade network-wide. In that case, implementers need to assess the impact of such phenomenon.

Similarly to RFC 7668, fragmentation functionality from 6LoWPAN standards is not used for IPv6 mesh over Bluetooth LE links. Bluetooth LE's fragmentation support provided by L2CAP is used when necessary.

### 3.2. Subnet model

For IPv6 mesh over Bluetooth LE links, 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].

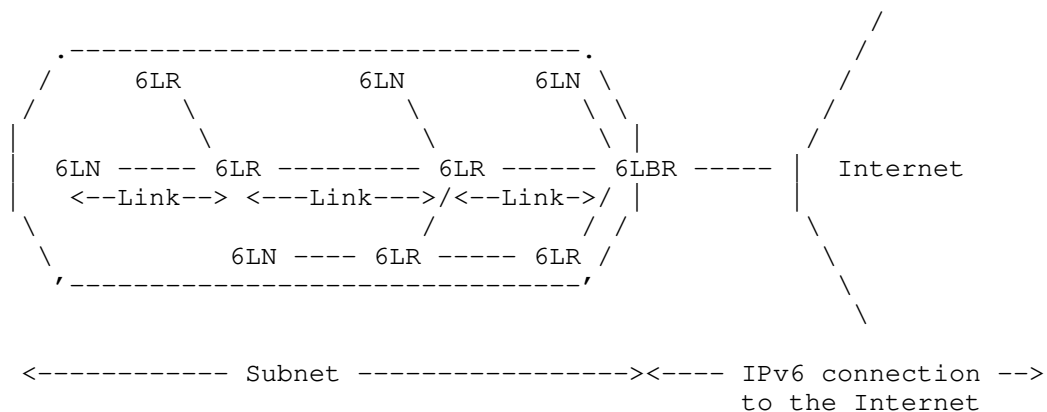


Figure 2: Example of an IPv6 mesh over a Bluetooth LE network connected to the Internet

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

### 3.3. Link model

#### 3.3.1. Stateless address autoconfiguration

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

Multihop DAD functionality as defined in section 8.2 of RFC 6775 and updated by RFC 8505, 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], subsequently updated by 'Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery' [RFC8505], describes the neighbor discovery functionality adapted for use in several 6LoWPAN topologies, including the mesh topology. The route-over functionality of RFC 6775 and RFC 8505 MUST be supported.

The following aspects of the Neighbor Discovery optimizations for 6LoWPAN [RFC6775],[RFC8505] are applicable to Bluetooth LE 6LNs:

1. A Bluetooth LE host MUST register its non-link-local addresses with its routers by sending a Neighbor Solicitation (NS) message with the Extended Address Registration Option (EARO) and process the Neighbor Advertisement (NA) accordingly. The NS with the EARO option MUST be sent irrespective of the method used to generate the IID. The EARO option includes a Registration Ownership Verifier (ROVR) field [RFC8505]. In the case of Bluetooth LE, by default the ROVR field is filled with the 48-bit device address used by the Bluetooth LE node converted into 64-bit Modified EUI-64 format [RFC4291]. Optionally, a cryptographic ID (see [I-D.ietf-6lo-ap-nd]) MAY be placed in the ROVR field. If a cryptographic ID is used, address registration and multihop DAD formats and procedures defined in [I-D.ietf-6lo-ap-nd] MUST be used, unless an alternative mechanism offering equivalent protection is used. As per RFC 8505, a 6LN MUST NOT register its link-local address.

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 hosts MUST, respectively, follow Sections 5.3 and 5.4 of [RFC6775], and Section 5.6 of [RFC8505].

3. The router behavior for 6LRs and 6LBRs is described in Section 6 of RFC 6775, and updated by RFC 8505. However, as per this specification: a) Routers SHALL NOT use multicast NSs to discover other routers' link layer addresses. b) As per section 6.2 of RFC 6775, in a dynamic configuration scenario, a 6LR comes up as a non-router and waits to receive a Router Advertisement for configuring its own interface address first, before setting its interfaces to be advertising interfaces and turning into a router. In order to support such operation in an IPv6 mesh over Bluetooth LE links, a 6LR first uses the IPSP Node role only. Once the 6LR has established a connection with another node previously running as a router, and receives a Router Advertisement from that router, the 6LR configures its own interface address, it turns into a router, and it runs as an IPSP Router. A 6LBR uses the IPSP Router role since the 6LBR is initialized. See an example in the Appendix.

4. Border router behavior is described in Section 7 of RFC 6775, and updated by RFC 8505.

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). RFC 8505 updates those mechanisms and the related message formats. Implementations of this specification MUST support the features described in sections 8.1 and 8.2 of RFC 6775, as updated by RFC 8505, unless some alternative ("substitute") from some other specification is supported by the implementation.

### 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 MAY 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. Note that 6CO is not needed for context-based compression when a single prefix is used in the network.

The specific optimizations of RFC 7668 for header compression, which exploited the star topology and ARO (note that the latter has been updated by EARO as per RFC 8505), cannot be generalized in an IPv6 mesh over Bluetooth LE links. Still, a subset of those optimizations can be applied in some cases in such a network. These cases comprise

link-local interactions, non-link-local packet transmissions originated and performed by a 6LN, and non-link-local packets intended for a 6LN that are originated or forwarded by a neighbor of that 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).

A 6LN SHOULD register its non-link-local address with EARO in the next-hop router. Note that in some cases (e.g. very short-lived connections) it may not be worthwhile for a 6LN to send an NS with EARO for registering its address. When a 6LN transmits a packet, with a non-link-local source address that the 6LN has registered with EARO 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 EARO 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 over Bluetooth LE links requires 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 links, 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.

The ROVR can be derived from the Bluetooth device address. However, such a ROVR can be spoofed, and therefore, any node connected to the subnet and aware of a registered-address-to-ROVR mapping could perform address theft and impersonation attacks. Use of Address Protected Neighbor Discovery [I-D.ietf-6lo-ap-nd] provides protection against such attacks.

#### 6. Contributors

Carlo Alberto Boano (Graz University of Technology) contributed to the design and validation of this document.

#### 7. 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, Martin Turon, Bilhanan Silverajan, Rahul Jadhav and Pascal Thubert 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 projects TEC2012-32531, TEC2016-79988-P and FEDER.

## 8. Appendix A: Bluetooth LE connection establishment example

This appendix provides an example of Bluetooth LE connection establishment and use of IPSP roles in an IPv6 mesh over Bluetooth LE links that uses dynamic configuration. The example follows text in Section 3.3.2, item 3.b).

The example assumes a network with one 6LBR, two 6LRs and three 6LNs, as shown in Figure 3. Connectivity between the 6LNs and the 6LBR is only possible via the 6LRs.

The following text describes the different steps as time evolves, in the example. Note that other sequences of events that may lead to the same final scenario are also possible.

At the beginning, the 6LBR starts running as an IPSP Router, whereas the rest of devices are not yet initialized (Step 1). Next, the 6LRs start running as IPSP Nodes, i.e., they use Bluetooth LE advertisement packets to announce their presence and support of IPv6 capabilities (Step 2). The 6LBR (already running as an IPSP Router) discovers the presence of the 6LRs and establishes one Bluetooth LE connection with each 6LR (Step 3). After establishment of those link layer connections (and after reception of Router Advertisements from the 6LBR), Step 4, the 6LRs start operating as routers, and also initiate the IPSP Router role (note: whether the IPSP Node role is kept running simultaneously is an implementation decision). Then, 6LRs start running the IPSP Node role (Step 5). Finally, the 6LRs discover presence of the 6LNs and establish connections with the latter (Step 6).

Step 1  
\*\*\*\*\*

6LBR  
(IPSP: Router)

6LR	6LR
(not initialized)	(not initialized)

6LN (not initialized)      6LN (not initialized)      6LN (not initialized)

Step 2  
\*\*\*\*\*

6LBR  
(IPSP: Router)

6LR

(IPSP: Node)

6LR

(IPSP: Node)

6LN (not initialized)      6LN (not initialized)      6LN (not initialized)

Step 3  
\*\*\*\*\*

```

Bluetooth LE connection -->
                                6LBR
                                (IPSP: Router)
                               /      \
                              6LR      6LR
                              (IPSP: Node)  (IPSP: Node)

```

6LN (not initialized)      6LN (not initialized)      6LN (not initialized)

Step 4  
\*\*\*\*\*

```

6LBR
(IPSP: Router)
/          \

```

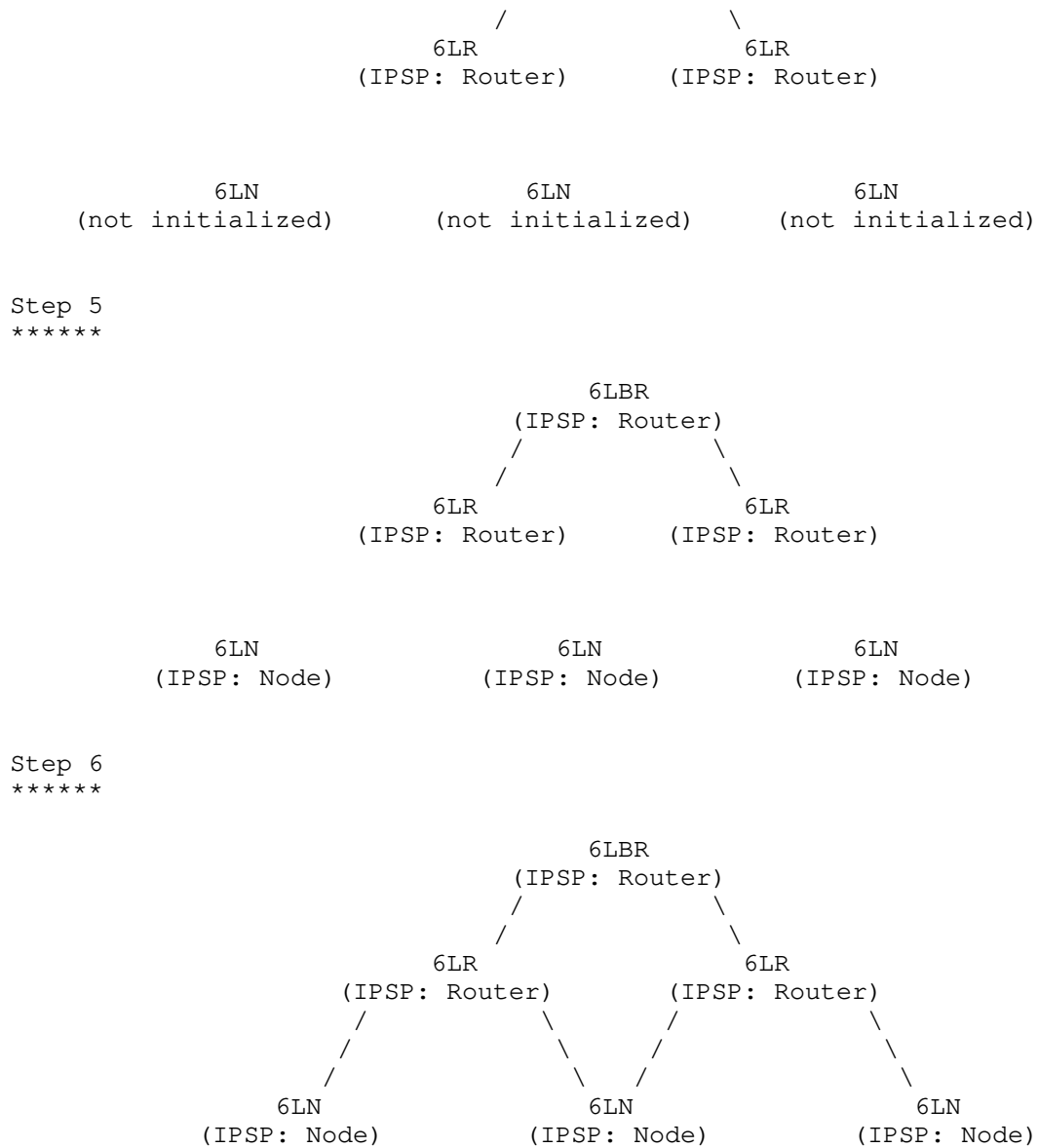


Figure 3: An example of connection establishment and use of IPSP roles in an IPv6 mesh over Bluetooth LE links.

## 9. Appendix B: Node joining procedure

This appendix provides a diagram that illustrates the node joining procedure. First of all, the joining node advertises its presence in order to allow establishing Bluetooth LE connections with neighbors that already belong to a network. The latter typically run as a 6LR or as a 6LBR. After Bluetooth LE connection establishment, the joining node starts acting as a 6LN.

Figure 4 shows the sequence of messages that are exchanged by the 6LN and a neighboring 6LR that already belongs to the network, after the establishment of a Bluetooth LE connection between both devices. Initially, the 6LN sends an RS message (1). Then, the 6LR replies with an RA, which includes the PIO (2). After discovering the non-link-local prefix in use in the network, the 6LN creates its non-link-local address, registers that address with EARO (3) in the 6LR, and multihop DAD is performed (4). The next step is the transmission of the NA message sent by the 6LR in response to the NS previously sent by the 6LN (5). If the non-link-local address of the 6LN has been successfully validated, the 6LN can operate as a member of the network it has joined.

```

(1)          6LN ---- (RS)-----> 6LR
(2)          6LN <--- (RA-PIO)---- 6LR
(3)          6LN ---- (NS-EARO)--> 6LR
(4)          [Multihop DAD procedure]
(5)          6LN <--- (NA)----- 6LR

```

Figure 4: Message exchange diagram for a joining node

## 10. References

### 10.1. Normative References

- [BTCorev4.2] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 4.2", December 2014, <<https://www.bluetooth.com/specifications/archived-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, <<https://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, <<https://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, <<https://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, <<https://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, <<https://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, <<https://www.rfc-editor.org/info/rfc7668>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.

## 10.2. Informative References

- [BTCorev4.1] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 4.1", December 2013, <<https://www.bluetooth.org/en-us/specification/adopted-specifications>>.

[I-D.ietf-6lo-ap-nd]

Thubert, P., Sarikaya, B., Sethi, M., and R. Struik,  
"Address Protected Neighbor Discovery for Low-power and  
Lossy Networks", draft-ietf-6lo-ap-nd-12 (work in  
progress), April 2019.

[RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903,  
DOI 10.17487/RFC4903, June 2007,  
<<https://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,  
<<https://www.rfc-editor.org/info/rfc7416>>.

#### Authors' Addresses

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

Email: [carlesgo@entel.upc.edu](mailto:carlesgo@entel.upc.edu)

Seyed Mahdi Darroudi  
Universitat Politecnica de Catalunya  
C/Esteve Terradas, 7  
Castelldefels 08860  
Spain

Email: [sm.darroudi@entel.upc.edu](mailto:sm.darroudi@entel.upc.edu)

Teemu Savolainen  
DarkMatter LLC

Email: [teemu.savolainen@darkmatter.ae](mailto:teemu.savolainen@darkmatter.ae)

Michael Spoerk  
Graz University of Technology  
Inffeldgasse 16/I  
Graz 8010  
Austria

Email: michael.spoerk@tugraz.at



6lo  
Internet-Draft  
Intended status: Informational  
Expires: March 2, 2020

T. Watteyne, Ed.  
Analog Devices  
C. Bormann  
Universitaet Bremen TZI  
P. Thubert  
Cisco  
August 30, 2019

6LoWPAN Fragment Forwarding  
draft-ietf-6lo-minimal-fragment-04

Abstract

This document provides a simple method to forwarding 6LoWPAN fragments. When employing adaptation layer fragmentation in 6LoWPAN, it may be beneficial for a forwarder not to have to reassemble each packet in its entirety before forwarding it. This has always been possible with the original fragmentation design of RFC4944. This method reduces the latency and increases end-to-end reliability in route-over forwarding. It is the companion to the virtual Reassembly Buffer which is a pure implementation technique.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 2, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Overview of 6LoWPAN Fragmentation . . . . .	2
2. Limits of Per-Hop Fragmentation and Reassembly . . . . .	4
2.1. Latency . . . . .	4
2.2. Memory Management and Reliability . . . . .	4
3. Virtual Reassembly Buffer (VRB) Implementation . . . . .	5
4. Security Considerations . . . . .	6
5. IANA Considerations . . . . .	6
6. Acknowledgments . . . . .	6
7. Informative References . . . . .	7
Authors' Addresses . . . . .	7

## 1. Overview of 6LoWPAN Fragmentation

The original 6LoWPAN fragmentation is defined in [RFC4944] and it is implicitly defined for use over a single IP hop though possibly multiple Layer-2 hops in a meshed 6LoWPAN Network. Although [RFC6282] updates [RFC4944], it does not redefine 6LoWPAN fragmentation.

We use Figure 1 to illustrate 6LoWPAN fragmentation. We assume node A forwards a packet to node B, possibly as part of a multi-hop route between IPv6 source and destination nodes which are neither A nor B.

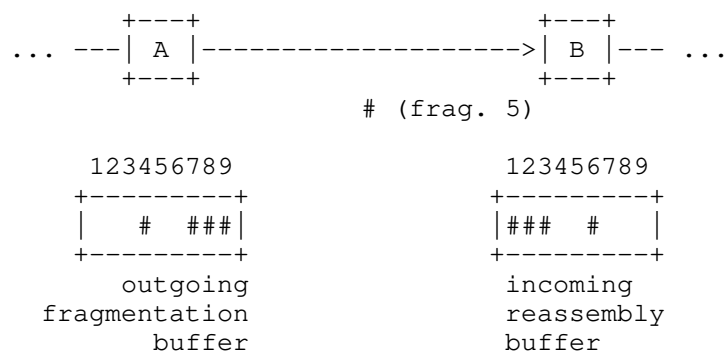


Figure 1: Fragmentation at node A, reassembly at node B.

Node A starts by compacting the IPv6 packet using the header compression mechanism defined in [RFC6282]. If the resulting 6LoWPAN packet does not fit into a single link-layer frame, node A's 6LoWPAN sublayer cuts it into multiple 6LoWPAN fragments, which it transmits as separate link-layer frames to node B. Node B's 6LoWPAN sublayer reassembles these fragments, inflates the compressed header fields back to the original IPv6 header, and hands over the full IPv6 packet to its IPv6 layer.

In Figure 1, a packet forwarded by node A to node B is cut into nine fragments, numbered 1 to 9. Each fragment is represented by the '#' symbol. Node A has sent fragments 1, 2, 3, 5, 6 to node B. Node B has received fragments 1, 2, 3, 6 from node A. Fragment 5 is still being transmitted at the link layer from node A to node B.

The reassembly buffer for 6LoWPAN is indexed in node B by:

- o a unique Identifier of Node A (e.g., Node A's link-layer address)
- o the datagram\_tag chosen by node A for this fragmented datagram

Because it may be hard for node B to correlate all possible link-layer addresses that node A may use (e.g., short vs. long addresses), node A must use the same link-layer address to send all the fragments of a same datagram to node B.

Conceptually, the reassembly buffer in node B contains, assuming that node B is neither the source nor the final destination:

- o a datagram\_tag as received in the incoming fragments, associated to link-layer address of node A for which the received datagram\_tag is unique,
- o the link-layer address that node B uses to forward the fragments
- o the link-layer address of the next hop that is resolved on the first fragment
- o a datagram\_tag that node B uniquely allocated for this datagram and that is used when forwarding the fragments of the datagram
- o the actual packet data from the fragments received so far, in a form that makes it possible to detect when the whole packet has been received and can be processed or forwarded,
- o a datagram\_size,
- o a buffer for the remainder of a previous fragment left to be sent,
- o a timer that allows discarding a partially reassembled packet after some timeout.

A fragmentation header is added to each fragment; it indicates what portion of the packet that fragment corresponds to. Section 5.3 of [RFC4944] defines the format of the header for the first and subsequent fragments. All fragments are tagged with a 16-bit

"datagram\_tag", used to identify which packet each fragment belongs to. Each datagram can be uniquely identified by the sender link-layer addresses of the frame that carries it and the datagram\_tag that the sender allocated for this datagram. Each fragment can be identified within its datagram by the datagram-offset.

Node B's typical behavior, per [RFC4944], is as follows. Upon receiving a fragment from node A with a datagram\_tag previously unseen from node A, node B allocates a buffer large enough to hold the entire packet. The length of the packet is indicated in each fragment (the datagram\_size field), so node B can allocate the buffer even if the first fragment it receives is not fragment 1. As fragments come in, node B fills the buffer. When all fragments have been received, node B inflates the compressed header fields into an IPv6 header, and hands the resulting IPv6 packet to the IPv6 layer.

This behavior typically results in per-hop fragmentation and reassembly. That is, the packet is fully reassembled, then (re)fragmented, at every hop.

## 2. Limits of Per-Hop Fragmentation and Reassembly

There are at least 2 limits to doing per-hop fragmentation and reassembly. See [ARTICLE] for detailed simulation results on both limits.

### 2.1. Latency

When reassembling, a node needs to wait for all the fragments to be received before being able to generate the IPv6 packet, and possibly forward it to the next hop. This repeats at every hop.

This may result in increased end-to-end latency compared to a case where each fragment is forwarded without per-hop reassembly.

### 2.2. Memory Management and Reliability

Constrained nodes have limited memory. Assuming 1 kB reassembly buffer, typical nodes only have enough memory for 1-3 reassembly buffers.

To illustrate this we use the topology from Figure 2, where nodes A, B, C and D all send packets through node E. We further assume that node E's memory can only hold 3 reassembly buffers.

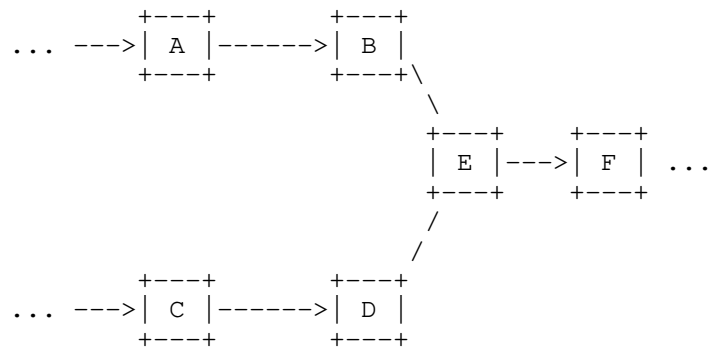


Figure 2: Illustrating the Memory Management Issue.

When nodes A, B and C concurrently send fragmented packets, all 3 reassembly buffers in node E are occupied. If, at that moment, node D also sends a fragmented packet, node E has no option but to drop one of the packets, lowering end-to-end reliability.

### 3. Virtual Reassembly Buffer (VRB) Implementation

Virtual Reassembly Buffer (VRB) is the implementation technique described in [I-D.ietf-lwig-6lowpan-virtual-reassembly] in which a forwarder does not reassemble each packet in its entirety before forwarding it.

VRB overcomes the limits listed in Section 2. Nodes do not wait for the last fragment before forwarding, reducing end-to-end latency. Similarly, the memory footprint of VRB is just the VRB table, reducing the packet drop probability significantly.

There are, however, limits:

**Non-zero Packet Drop Probability:** The abstract data in a VRB table entry contains at a minimum the MAC address of the predecessor and that of the successor, the `datagram_tag` used by the predecessor and the local `datagram_tag` that this node will swap with it. The VRB may need to store a few octets from the last fragment that may not have fit within MTU and that will be prepended to the next fragment. This yields a small footprint that is 2 orders of magnitude smaller compared to needing a 1280-byte reassembly buffer for each packet. Yet, the size of the VRB table necessarily remains finite. In the extreme case where a node is required to concurrently forward more packets than it has entries in its VRB table, packets are dropped.

**No Fragment Recovery:** There is no mechanism in VRB for the node that reassembles a packet to request a single missing fragment.

Dropping a fragment requires the whole packet to be resent. This causes unnecessary traffic, as fragments are forwarded even when the destination node can never construct the original IPv6 packet.

No Per-Fragment Routing: All subsequent fragments follow the same sequence of hops from the source to the destination node as the first fragment, because the IP header is required to route the fragment and is only present in the first fragment. A side effect is that the first fragment must always be forwarded first.

The severity and occurrence of these limits depends on the link-layer used. Whether these limits are acceptable depends entirely on the requirements the application places on the network.

If the limits are present and not acceptable for the application, future specifications may define new protocols to overcome these limits. One example is [I-D.ietf-6lo-fragment-recovery] which defines a protocol which allows fragment recovery.

#### 4. Security Considerations

An attacker can perform a Denial-of-Service (DoS) attack on a node implementing VRB by generating a large number of bogus "fragment 1" fragments without sending subsequent fragments. This causes the VRB table to fill up. Note that the VRB does not need to remember the full datagram as received so far but only possibly a few octets from the last fragment that could not fit in it. It is expected that an implementation protects itself to keep the number of VRBs within capacity, and that old VRBs are protected by a timer of a reasonable duration for the technology and destroyed upon timeout.

Secure joining and the link-layer security that it sets up protects against those attacks from network outsiders.

#### 5. IANA Considerations

No requests to IANA are made by this document.

#### 6. Acknowledgments

The authors would like to thank Yasuyuki Tanaka, for his in-depth review of this document. Also many thanks to Georgios Papadopoulos and Dominique Barthel for their own reviews.

## 7. Informative References

- [ARTICLE] Tanaka, Y., Minet, P., and T. Watteyne, "6LoWPAN Fragment Forwarding", IEEE Communications Standards Magazine , 2019.
- [I-D.ietf-6lo-fragment-recovery]  
Thubert, P., "6LoWPAN Selective Fragment Recovery", draft-ietf-6lo-fragment-recovery-05 (work in progress), July 2019.
- [I-D.ietf-lwig-6lowpan-virtual-reassembly]  
Bormann, C. and T. Watteyne, "Virtual reassembly buffers in 6LoWPAN", draft-ietf-lwig-6lowpan-virtual-reassembly-01 (work in progress), March 2019.
- [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, <<https://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, <<https://www.rfc-editor.org/info/rfc6282>>.

## Authors' Addresses

Thomas Watteyne (editor)  
Analog Devices  
32990 Alvarado-Niles Road, Suite 910  
Union City, CA 94587  
USA

Email: [thomas.watteyne@analog.com](mailto:thomas.watteyne@analog.com)

Carsten Bormann  
Universitaet Bremen TZI  
Postfach 330440  
Bremen D-28359  
Germany

Email: [cabo@tzi.org](mailto:cabo@tzi.org)

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

Email: [pthubert@cisco.com](mailto:pthubert@cisco.com)



6Lo Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 6, 2020

J. Hou  
B. Liu  
Huawei Technologies  
Y-G. Hong  
ETRI  
X. Tang  
SGEPRI  
C. Perkins  
November 3, 2019

Transmission of IPv6 Packets over PLC Networks  
draft-ietf-6lo-plc-01

Abstract

Power Line Communication (PLC), namely using the electric-power lines for indoor and outdoor communications, has been widely applied to support Advanced Metering Infrastructure (AMI), especially smart meters for electricity. The inherent advantage of existing electricity infrastructure facilitates the expansion of PLC deployments, and moreover, a wide variety of accessible devices raises the potential demand of IPv6 for future applications. This document describes how IPv6 packets are transported over constrained PLC networks, such as ITU-T G.9903, IEEE 1901.1 and IEEE 1901.2.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Requirements Notation and Terminology . . . . .	3
3. Overview of PLC . . . . .	4
3.1. Protocol Stack . . . . .	5
3.2. Addressing Modes . . . . .	6
3.3. Maximum Transmission Unit . . . . .	6
3.4. Routing Protocol . . . . .	6
4. IPv6 over PLC . . . . .	7
4.1. Stateless Address Autoconfiguration . . . . .	7
4.2. IPv6 Link Local Address . . . . .	8
4.3. Unicast Address Mapping . . . . .	8
4.3.1. Unicast Address Mapping for IEEE 1901.1 . . . . .	8
4.3.2. Unicast Address Mapping for IEEE 1901.2 and ITU-T G.9903 . . . . .	9
4.4. Neighbor Discovery . . . . .	10
4.5. Header Compression . . . . .	11
4.6. Fragmentation and Reassembly . . . . .	11
5. Internet Connectivity Scenarios and Topologies . . . . .	12
6. IANA Considerations . . . . .	14
7. Security Consideration . . . . .	14
8. Acknowledgements . . . . .	14
9. References . . . . .	15
9.1. Normative References . . . . .	15
9.2. Informative References . . . . .	16
Authors' Addresses . . . . .	17

## 1. Introduction

The idea of using power lines for both electricity supply and communication can be traced back to the beginning of the last century. With the advantage of existing power grid, Power Line Communication (PLC) is a good candidate for supporting various service scenarios such as in houses and offices, in trains and vehicles, in smart grid and advanced metering infrastructure (AMI). The data acquisition devices in these scenarios share common features

such as fixed position, large quantity, low data rate and low power consumption.

Although PLC technology has evolved over several decades, it has not been fully adapted for IPv6 based constrained networks. The 6Lo related scenarios lie in the low voltage PLC networks with most applications in the area of Advanced Metering Infrastructure (AMI), Vehicle-to-Grid communications, in-home energy management and smart street lighting. IPv6 is important for PLC networks, due to its large address space and efficient address auto-configuration. A comparison among various existing PLC standards is provided to facilitate the selection of the most applicable standard in particular scenarios.

This specification provides a brief overview of PLC technologies. Some of them have LLN characteristics, i.e. limited power consumption, memory and processing resources. This specification is focused on the transmission of IPv6 packets over those "constrained" PLC networks. The general approach is to adapt elements of the 6LoWPAN specifications [RFC4944], [RFC6282], and [RFC6775] to constrained PLC networks. Compared to [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks], this document provides a structured and greatly expanded specification of an adaptation layer for IPv6 over PLC (6LoPLC) networks.

## 2. Requirements Notation and 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 often uses the following acronyms and terminologies:

6LoWPAN: IPv6 over Low-Power Wireless Personal Area Network

AMI: Advanced Metering Infrastructure

BBPLC: Broadband Power Line Communication

CID: Context ID

Coordinator: A device capable of relaying messages.

DAD: Duplicate Address Detection

PAN device: An entity follows the PLC standards and implements the protocol stack described in this draft.

EV: Electric Vehicle

IID: IPv6 Interface Identifier

IPHC: IP Header Compression

LAN: Local Area Network

MSDU: MAC Service Data Unit

MTU: Maximum Transmission Unit

NBPLC: Narrowband Power Line Communication

OFDM: Orthogonal Frequency Division Multiplexing

PANC: PAN Coordinator, a coordinator which also acts as the primary controller of a PAN.

PLC: Power Line Communication

PSDU: PHY Service Data Unit

RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks

RA: Router Advertisement

WAN: Wide Area Network

The terminology used in this draft is aligned with IEEE 1901.2

IEEE 1901.2	IEEE 1901.1	ITU-T G.9903
PAN Coordinator	Central Coordinator	PAN Coordinator
Coordinator	Proxy Coordinator	Full-function device
Device	Station	PAN Device

Table 1: Terminology Mapping between PLC standards

### 3. Overview of PLC

PLC technology enables convenient two-way communications for home users and utility companies to monitor and control electric plugged devices such as electricity meters and street lights. Due to the

large range of communication frequencies, PLC is generally classified into two categories: Narrowband PLC (NBPLC) for automation of sensors (which have low frequency band and low power cost), and Broadband PLC (BBPLC) for home and industry networking applications. Various standards have been addressed on the MAC and PHY layers for this communication technology, e.g. BBPLC (1.8-250 MHz) including IEEE 1901 and ITU-T G.hn, and NBPLC (3-500 kHz) including ITU-T G.9902 (G.hnem), ITU-T G.9903 (G3-PLC) [ITU-T\_G.9903], ITU-T G.9904 (PRIME), IEEE 1901.2 [IEEE\_1901.2] (combination of G3-PLC and PRIME PLC) and IEEE 1901.2a [IEEE\_1901.2a] (an amendment to IEEE 1901.2). Moreover, recently a new PLC standard IEEE 1901.1 [IEEE\_1901.1], which aims at the medium frequency band less than 12 MHz, has been published by the IEEE standard for Smart Grid Powerline Communication Working Group (SGPLC WG). IEEE 1901.1 balances the needs for bandwidth versus communication range, and is thus a promising option for 6Lo applications. Currently, this specification is focused on IEEE 1901.1, IEEE 1901.2 and ITU-T G.9903.

### 3.1. Protocol Stack

The protocol stack for IPv6 over PLC is illustrated in Figure 1. The PLC MAC/PHY layer corresponds to IEEE 1901.1, IEEE 1901.2 or ITU-T G.9903. The 6Lo adaptation layer for PLC is illustrated in Section 4. For multihop tree and mesh topologies, a routing protocol is likely to be necessary. The routes can be built in mesh-under mode at layer 2 or in route-over mode at layer 3.

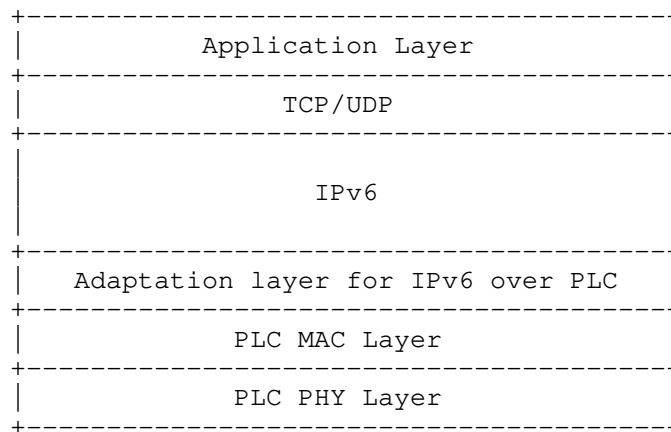


Figure 1: PLC Protocol Stack

### 3.2. Addressing Modes

Each PLC device has a globally unique long address of 48-bit ([IEEE\_1901.1]) or 64-bit ([IEEE\_1901.2], [ITU-T\_G.9903]) and a short address of 12-bit ([IEEE\_1901.1]) or 16-bit ([IEEE\_1901.2], [ITU-T\_G.9903]). The long address is set by the manufacturer according to the IEEE EUI-48 MAC address or the IEEE EUI-64 address. Each PLC device joins the network by using the long address and communicates with other devices by using the short address after joining the network.

### 3.3. Maximum Transmission Unit

The Maximum Transmission Unit (MTU) of the MAC layer determines whether fragmentation and reassembly are needed at the adaptation layer of IPv6 over PLC. IPv6 requires an MTU of 1280 octets or greater; thus for a MAC layer with MTU lower than this limit, fragmentation and reassembly at the adaptation layer are required.

The IEEE 1901.1 MAC supports upper layer packets up to 2031 octets. The IEEE 1901.2 MAC layer supports the MTU of 1576 octets (the original value of 1280 bytes was updated in 2015 [IEEE\_1901.2a]). Though fragmentation and reassembly are not needed in these two technologies, other 6lo functions like header compression are still applicable and useful, particularly in high-noise communication environments.

The MTU for ITU-T G.9903 is 400 octets, insufficient for supporting IPv6's MTU. For this reason, fragmentation and reassembly as per [RFC4944] MUST be enabled for G.9903-based networks.

### 3.4. Routing Protocol

Routing protocols suitable for use in PLC networks include:

- o RPL (Routing Protocol for Low-Power and Lossy Networks) [RFC6550] is a layer 3 routing protocol. AODV-RPL [I-D.ietf-roll-aodv-rpl] updates RPL to include reactive, point-to-point, and asymmetric routing. IEEE 1901.2 specifies Information Elements (IEs) with MAC layer metrics, which can be provided to L3 routing protocol for parent selection. For IPv6-addressable PLC networks, a layer-3 routing protocol such as RPL and/or AODV-RPL SHOULD be supported in the standard.
- o IEEE 1901.1 supports L2 routing. Each PLC node maintains a L2 routing table, in which each route entry comprises the short addresses of the destination and the related next hop. The route entries are built during the network establishment via a pair of

association request/confirmation messages. The route entries can be changed via a pair of proxy change request/confirmation messages. These association and proxy change messages MUST be approved by the central coordinator.

- o LOADng is a reactive protocol operating at layer 2 or layer 3. Currently, LOADng is supported in ITU-T G.9903 [ITU-T\_G.9903], and the IEEE 1901.2 standard refers to ITU-T G.9903 for LOAD-based networks.

#### 4. IPv6 over PLC

6LoWPAN standards [RFC4944], [RFC6775], and [RFC6282] provides useful functionality including link-local IPv6 addresses, stateless address auto-configuration, neighbor discovery and header compression. However, due to the different characteristics of the PLC media, the 6LoWPAN adaptation layer cannot perfectly fulfill the requirements. Besides, some of the features like fragmentation and reassembly are redundant to some PLC technologies. These considerations suggest the need for a dedicated adaptation layer for PLC, which is detailed in the following subsections.

##### 4.1. Stateless Address Autoconfiguration

To obtain an IPv6 Interface Identifier (IID), a PLC device performs stateless address autoconfiguration [RFC4944]. The autoconfiguration can be based on either a long or short link-layer address.

The IID can be based on the device's 48-bit MAC address or its EUI-64 identifier [EUI-64]. A 48-bit MAC address MUST first be extended to a 64-bit Interface ID by inserting 0xFFFE at the fourth and fifth octets as specified in [RFC2464]. The IPv6 IID is derived from the 64-bit Interface ID by inverting the U/L bit [RFC4291].

For IEEE 1901.2 and ITU-T G.9903, a 48-bit "pseudo-address" is formed by the 16-bit PAN ID, 16 zero bits and the 16-bit short address. Then, the 64-bit Interface ID MUST be derived by inserting 16-bit 0xFFFE into as follows:

```
16_bit_PAN:00FF:FE00:16_bit_short_address
```

For the 12-bit short addresses used by IEEE 1901.1, the 48-bit pseudo-address is formed by 24-bit NID (Network Identifier, YYYYYY), 12 zero bits and a 12-bit TEI (Terminal Equipment Identifier, XXX). The 64-bit Interface ID MUST be derived by inserting 16-bit 0xFFFE into this 48-bit pseudo-address as follows:

```
YYYY:YYFF:FE00:0XXX
```

Since the derived Interface ID is not global, the "Universal/Local" (U/L) bit (7th bit) and the Individual/Group bit (8th bit) MUST both be set to zero. In order to avoid any ambiguity in the derived Interface ID, these two bits MUST NOT be used to generate the PANID (for IEEE 1901.2 and ITU-T G.9903) or NID (for IEEE 1901.1). In other words, the PANID or NID MUST always be chosen so that these bits are zeros.

For privacy reasons, the IID derived by the MAC address SHOULD only be used for link-local address configuration. A PLC host SHOULD use the IID derived by the link-layer short address to configure the IPv6 address used for communication with the public network; otherwise, the host's MAC address is exposed.

#### 4.2. IPv6 Link Local Address

The IPv6 link-local address [RFC4291] for a PLC interface is formed by appending the IID, as defined above, to the prefix FE80::/64 (see Figure 2).

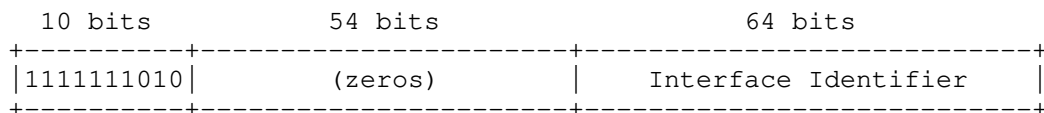


Figure 2: IPv6 Link Local Address for a PLC interface

#### 4.3. Unicast Address Mapping

The address resolution procedure for mapping IPv6 unicast addresses into PLC link-layer addresses follows the general description in section 7.2 of [RFC4861]. [RFC6775] improves this procedure by eliminating usage of multicast NS. The resolution is realized by the NCEs (neighbor cache entry) created during the address registration at the routers. [RFC8505] further improves the registration procedure by enabling multiple LLNs to form an IPv6 subnet, and by inserting a link-local address registration to better serve proxy registration of new devices.

##### 4.3.1. Unicast Address Mapping for IEEE 1901.1

The Source/Target Link-layer Address options for IEEE\_1901.1 used in the Neighbor Solicitation and Neighbor Advertisement have the following form.



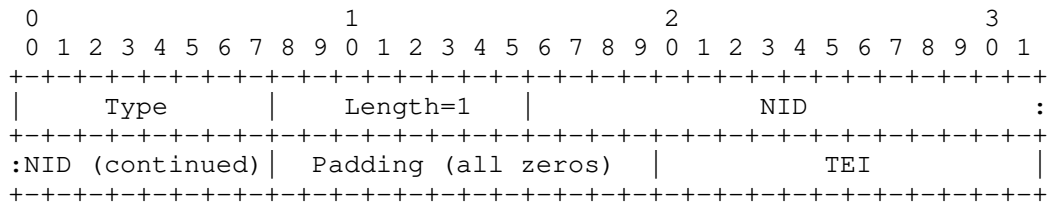


Figure 3: Unicast Address Mapping for IEEE 1901.1

Option fields:

Type: 1 for Source Link-layer Address and 2 for Target Link-layer Address.

Length: The length of this option (including type and length fields) in units of 8 octets. The value of this field is 1 for the 12-bit IEEE 1901.1 PLC short addresses.

NID: 24-bit Network IDentifier

Padding: 12 zero bits

TEI: 12-bit Terminal Equipment Identifier

In order to avoid the possibility of duplicated IPv6 addresses, the value of the NID MUST be chosen so that the 7th and 8th bits of the first byte of the NID are both zero.

#### 4.3.2. Unicast Address Mapping for IEEE 1901.2 and ITU-T G.9903

The Source/Target Link-layer Address options for IEEE\_1901.2 and ITU-T G.9903 used in the Neighbor Solicitation and Neighbor Advertisement have the following form.

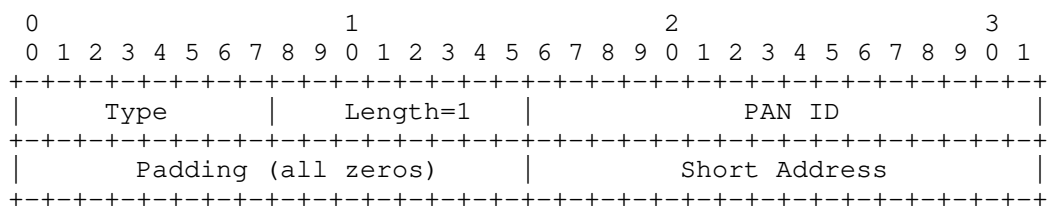


Figure 4: Unicast Address Mapping for IEEE 1901.2

Option fields:

Type: 1 for Source Link-layer Address and 2 for Target Link-layer Address.

Length: The length of this option (including type and length fields) in units of 8 octets. The value of this field is 1 for the 16-bit IEEE 1901.2 PLC short addresses.

PAN ID: 16-bit PAN Identifier

Padding: 16 zero bits

Short Address: 16-bit short address

In order to avoid the possibility of duplicated IPv6 addresses, the value of the PAN ID MUST be chosen so that the 7th and 8th bits of the first byte of the PAN ID are both zero.

#### 4.4. Neighbor Discovery

Neighbor discovery procedures for 6LoWPAN networks are described in Neighbor Discovery Optimization for 6LoWPANs [RFC6775] and [RFC8505]. These optimizations support the registration of sleeping hosts. Although PLC devices are electrically powered, sleeping mode SHOULD still be used for power saving.

For IPv6 address prefix dissemination, Router Solicitations (RS) and Router Advertisements (RA) MAY be used as per [RFC6775]. If the PLC network uses route-over mesh, the IPv6 prefix MAY be disseminated by the layer 3 routing protocol, such as RPL which includes the prefix in the DIO message. In this case, the prefix information option (PIO) MUST NOT be included in the Router Advertisement.

For context information dissemination, Router Advertisements (RA) MUST be used as per [RFC6775]. The 6LoWPAN context option (6CO) MUST be included in the RA to disseminate the Context IDs used for prefix compression.

For address registration in route-over mode, a PLC device MUST register its addresses by sending unicast link-local Neighbor Solicitation to the 6LR. If the registered address is link-local, the 6LR SHOULD NOT further register it to the registrar (6LBR, 6BBR). Otherwise, the address MUST be registered via an ARO or EARO included in the DAR ([RFC6775]) or EDAR ([RFC8505]) messages. For RFC8505 compliant PLC devices, the 'R' flag in the EARO MUST be set when sending Neighbor Solicitations in order to extract the status information in the replied Neighbor Advertisements from the 6LR. If DHCPv6 is used to assign addresses or the IPv6 address is derived by unique long or short link layer address, Duplicate Address Detection

(DAD) MUST NOT be utilized. Otherwise, the DAD MUST be performed at the 6LBR (as per [RFC6775]) or proxied by the routing registrar (as per [RFC8505]). The registration status is feedbacked via the DAC or EDAC message from the 6LBR and the Neighbor Advertisement (NA) from the 6LR.

For address registration in mesh-under mode, since all the PLC devices are the link-local neighbors to the 6LBR, DAR/DAC or EDAR/EDAC messages are not required. A PLC device MUST register its addresses by sending the unicast NS message with an ARO or EARO. The registration status is feedbacked via the NA message from the 6LBR.

#### 4.5. Header Compression

The compression of IPv6 datagrams within PLC MAC frames refers to [RFC6282], which updates [RFC4944]. Header compression as defined in [RFC6282] which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, is included in this document as the basis for IPv6 header compression in PLC. For situations when PLC MAC MTU cannot support the 1280-octet IPv6 packet, headers MUST be compressed according to [RFC6282] encoding formats.

#### 4.6. Fragmentation and Reassembly

PLC differs from other wired technologies in that the communication medium is not shielded; thus, to successfully transmit data through power lines, PLC Data Link layer provides the function of segmentation and reassembly. A Segment Control Field is defined in the MAC frame header regardless of whether segmentation is required. The number of data octets of the PHY payload can change dynamically based on channel conditions, thus the MAC payload segmentation in the MAC sublayer is enabled and guarantees a reliable one-hop data transmission. Fragmentation and reassembly is still required at the adaptation layer, if the MAC layer cannot support the minimum MTU demanded by IPv6, which is 1280 octets.

In IEEE 1901.1 and IEEE 1901.2, since the MAC layer supports payloads of 2031 octets and 1576 octets respectively, fragmentation is not needed for IPv6 packet transmission. The fragmentation and reassembly defined in [RFC4944] SHOULD NOT be used in the 6lo adaptation layer of IEEE 1901.2.

In ITU-T G.9903, the maximum MAC payload size is fixed to 400 octets, so to cope with the required MTU of 1280 octets by IPv6, fragmentation and reassembly at 6lo adaptation layer MUST be provided referring to [RFC4944].

## 5. Internet Connectivity Scenarios and Topologies

The network model can be simplified to two kinds of network devices: PAN Coordinator (PANC) and PAN Device. The PANC is the primary coordinator of the PLC subnet and can be seen as a master node; PAN Devices are typically PLC meters and sensors. The PANC also serves as the Routing Registrar for proxy registration and DAD procedures, making use of the updated registration procedures in [RFC8505]. IPv6 over PLC networks are built as tree, mesh or star according to the use cases. Every network requires at least one PANC to communicate with each PAN Device. Note that the PLC topologies in this section are based on logical connectivity, not physical links.

The star topology is common in current PLC scenarios. In single-hop star topologies, communication at the link layer only takes place between a PAN Device and a PANC. The PANC typically collects data (e.g. a meter reading) from the PAN devices, and then concentrates and uploads the data through Ethernet or LPWAN (see Figure 5). The collected data is transmitted by the smart meters through PLC, aggregated by a concentrator, sent to the utility and then to a Meter Data Management System for data storage, analysis and billing. This topology has been widely applied in the deployment of smart meters, especially in apartment buildings.

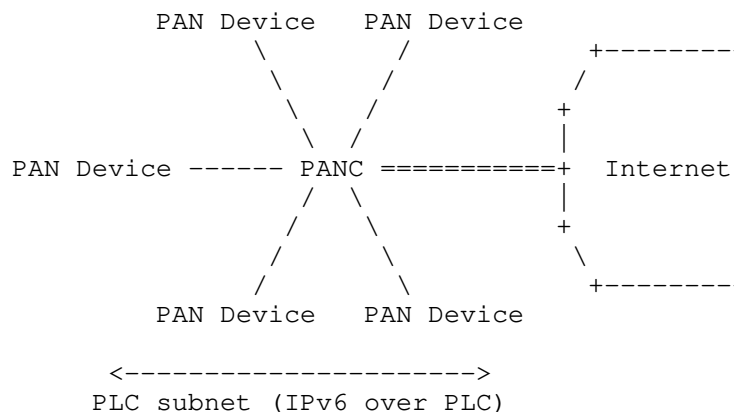


Figure 5: PLC Star Network connected to the Internet

A tree topology is useful when the distance between a device A and PANC is beyond the PLC allowed limit and there is another device B in between able to communicate with both sides. Device B in this case acts both as a PAN Device and a Coordinator. For this scenario, the link layer communications take place between device A and device B, and between device B and PANC. An example of PLC tree network is depicted in Figure 6. This topology can be applied in the smart

street lighting, where the lights adjust the brightness to reduce energy consumption while sensors are deployed on the street lights to provide information such as light intensity, temperature, humidity. Data transmission distance in the street lighting scenario is normally above several kilometers thus the PLC tree network is required. A more sophisticated AMI network may also be constructed into the tree topology which is depicted in [RFC8036]. A tree topology is suitable for AMI scenarios that require large coverage but low density, e.g. the deployment of smart meters in rural areas. RPL is suitable for maintenance of a tree topology in which there is no need for communication directly between PAN devices.

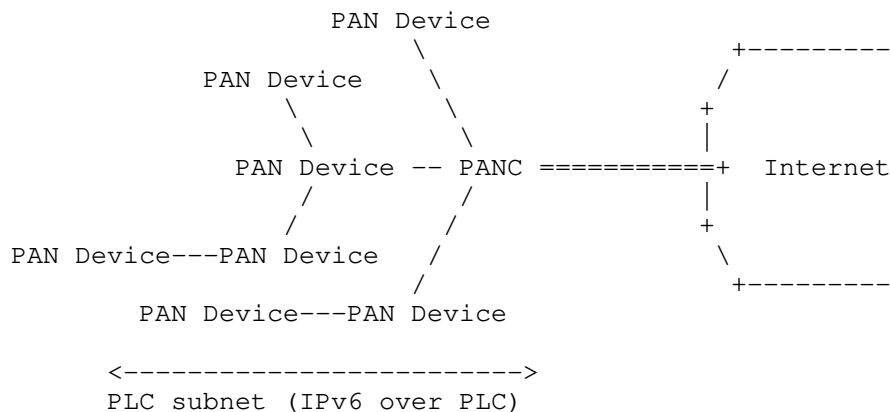


Figure 6: PLC Tree Network connected to the Internet

Mesh networking in PLC is of great potential applications and has been studied for several years. By connecting all nodes with their neighbors in communication range (see Figure 7), mesh topology dramatically enhances the communication efficiency and thus expands the size of PLC networks. A simple use case is the smart home scenario where the ON/OFF state of air conditioning is controlled by the state of home lights (ON/OFF) and doors (OPEN/CLOSE). AODV-RPL enables direct PAN device to PAN device communication, without being obliged to transmit frames through the PANC, which is a requirement often cited for AMI infrastructure.

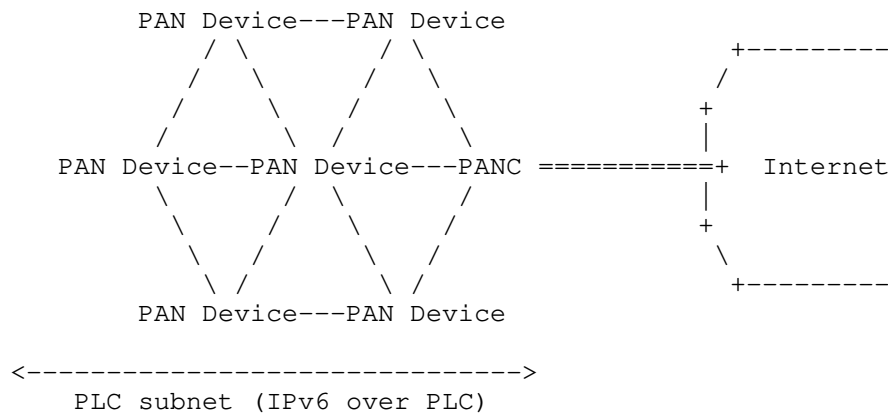


Figure 7: PLC Mesh Network connected to the Internet

## 6. IANA Considerations

There are no IANA considerations related to this document.

## 7. Security Consideration

Due to the high accessibility of power grid, PLC might be susceptible to eavesdropping within its communication coverage, e.g. one apartment tenant may have the chance to monitor the other smart meters in the same apartment building. For security consideration, link layer security is guaranteed in every PLC technology.

IP addresses may be used to track devices on the Internet; such devices can in turn be linked to individuals and their activities. Depending on the application and the actual use pattern, this may be undesirable. To impede tracking, globally unique and non-changing characteristics of IP addresses should be avoided, e.g., by frequently changing the global prefix and avoiding unique link-layer derived IIDs in addresses. [RFC3315], [RFC3972], [RFC4941], [RFC5535], [RFC7217], and [RFC8065] provide valuable information for IID formation with improved privacy, and are RECOMMENDED for IPv6 networks.

## 8. Acknowledgements

We gratefully acknowledge suggestions from the members of the IETF 6lo working group. Great thanks to Samita Chakrabarti and Gabriel Montenegro for their feedback and support in connecting the IEEE and ITU-T sides. Authors thank Scott Mansfield, Ralph Droms, Pat Kinney for their guidance in the liaison process. Authors wish to thank

Stefano Galli, Thierry Lys, Yizhou Li and Yuefeng Wu for their valuable comments and contributions.

## 9. References

### 9.1. Normative References

- [IEEE\_1901.1] IEEE-SA Standards Board, "Standard for Medium Frequency (less than 15 MHz) Power Line Communications for Smart Grid Applications", IEEE 1901.1, May 2018, <<http://sites.ieee.org/sagroups-1901-1>>.
- [IEEE\_1901.2] IEEE-SA Standards Board, "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications", IEEE 1901.2, October 2013, <<https://standards.ieee.org/findstds/standard/1901.2-2013.html>>.
- [ITU-T\_G.9903] International Telecommunication Union, "Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks", ITU-T G.9903, February 2014, <<https://www.itu.int/rec/T-REC-G.9903>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <<https://www.rfc-editor.org/info/rfc2464>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.
- [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, <<https://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, <<https://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, <<https://www.rfc-editor.org/info/rfc6550>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.

## 9.2. Informative References

- [I-D.ietf-roll-aodv-rpl]  
Anamalamudi, S., Zhang, M., Perkins, C., Anand, S., and B. Liu, "Asymmetric AODV-P2P-RPL in Low-Power and Lossy Networks (LLNs)", draft-ietf-roll-aodv-rpl-07 (work in progress), April 2019.
- [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.
- [IEEE\_1901.2a]  
IEEE-SA Standards Board, "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications - Amendment 1", IEEE 1901.2a, September 2015, <<https://standards.ieee.org/findstds/standard/1901.2a-2015.html>>.



- [RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <<https://www.rfc-editor.org/info/rfc3315>>.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <<https://www.rfc-editor.org/info/rfc3972>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <<https://www.rfc-editor.org/info/rfc4941>>.
- [RFC5535] Bagnulo, M., "Hash-Based Addresses (HBA)", RFC 5535, DOI 10.17487/RFC5535, June 2009, <<https://www.rfc-editor.org/info/rfc5535>>.
- [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, <<https://www.rfc-editor.org/info/rfc7217>>.
- [RFC8036] Cam-Winget, N., Ed., Hui, J., and D. Popa, "Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks", RFC 8036, DOI 10.17487/RFC8036, January 2017, <<https://www.rfc-editor.org/info/rfc8036>>.
- [RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <<https://www.rfc-editor.org/info/rfc8065>>.

#### Authors' Addresses

Jianqiang Hou  
Huawei Technologies  
101 Software Avenue,  
Nanjing 210012  
China

Email: [hujianqiang@huawei.com](mailto:hujianqiang@huawei.com)

Bing Liu  
Huawei Technologies  
No. 156 Beiqing Rd. Haidian District,  
Beijing 100095  
China

Email: remy.liubing@huawei.com

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

Email: yghong@etri.re.kr

Xiaojun Tang  
State Grid Electric Power Research Institute  
19 Chengxin Avenue  
Nanjing 211106  
China

Email: itc@sgepri.sgcc.com.cn

Charles E. Perkins

Email: charliep@computer.org

6Lo Working Group  
Internet-Draft  
Intended status: Informational  
Expires: May 7, 2020

Y-G. Hong  
ETRI  
C. Gomez  
UPC  
Y-H. Choi  
ETRI  
AR. Sangi  
Huaiyin Institute of Technology  
T. Aanstoot  
Modio AB  
S. Chakrabarti  
November 4, 2019

IPv6 over Constrained Node Networks (6lo) Applicability & Use cases  
draft-ietf-6lo-use-cases-08

Abstract

This document describes the applicability of IPv6 over constrained node networks (6lo) and provides practical deployment examples. 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, and PLC (IEEE 1901.2) are used as examples. The document targets an audience who like to understand and evaluate running end-to-end IPv6 over the constrained node networks connecting devices to each other or to other devices on the Internet (e.g. cloud infrastructure).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 7, 2020.

## Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions and Terminology . . . . .	4
3. 6lo Link layer technologies . . . . .	4
3.1. ITU-T G.9959 . . . . .	4
3.2. Bluetooth LE . . . . .	4
3.3. DECT-ULE . . . . .	5
3.4. MS/TP . . . . .	5
3.5. NFC . . . . .	6
3.6. PLC . . . . .	7
3.7. Comparison between 6lo Link layer technologies . . . . .	7
4. 6lo Deployment Scenarios . . . . .	8
4.1. G3-PLC usage of 6lo in network layer . . . . .	8
4.2. Netricity usage of 6lo in network layer . . . . .	9
5. Guidelines for adopting IPv6 stack (6lo/6LoWPAN) . . . . .	10
6. 6lo Use Case Examples . . . . .	12
6.1. Use case of ITU-T G.9959: Smart Home . . . . .	12
6.2. Use case of Bluetooth LE: Smartphone-based Interaction . . . . .	13
6.3. Use case of DECT-ULE: Smart Home . . . . .	14
6.4. Use case of MS/TP: Building Automation Networks . . . . .	14
6.5. Use case of NFC: Alternative Secure Transfer . . . . .	15
6.6. Use case of PLC: Smart Grid . . . . .	15
7. IANA Considerations . . . . .	16
8. Security Considerations . . . . .	17
9. Acknowledgements . . . . .	17
10. References . . . . .	17
10.1. Normative References . . . . .	17
10.2. Informative References . . . . .	19
Appendix A. Design Space Dimensions for 6lo Deployment . . . . .	22
Authors' Addresses . . . . .	23

## 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][RFC7228]. For example, some IEEE 802.15.4 link layers[IEEE802154] have a frame size of 127 octets and IPv6 requires the layer below to support an MTU of 1280 bytes, therefore an appropriate fragmentation and reassembly adaptation layer must be provided at the layer below IPv6. Also, the limited size of IEEE 802.15.4 frame and low energy consumption requirements make the need for header compression. The IETF 6LoPWAN (IPv6 over Low powerWPAN) working group published an adaptation layer for sending IPv6 packets over IEEE 802.15.4 [RFC4944], which includes a compression format for IPv6 datagrams over IEEE 802.15.4-based networks [RFC6282], and Neighbor Discovery Optimization for 6LoPWAN [RFC6775].

As IoT (Internet of Things) services become more popular, IPv6 over 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 Power Line Communication (PLC) have been defined at IETF 6lo working group[IETF\_6lo]. IPv6 stacks for constrained node networks use a variation of the 6LoWPAN stack applied to each particular link layer technology.

In the 6LoPWAN 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. Hence, this 6lo applicability document aims to provide guidance to an audience who are new to IPv6-over-low-power networks concept and want to assess if variance of 6LoWPAN stack (6lo) can be applied to the constrained layer two (L2) network of their interest. This 6lo applicability document puts together various design space dimensions such as deployment, network size, power source, connectivity, multi-hop communication, traffic pattern, security level, mobility, and QoS requirements etc. In addition, it describes a few set of 6LoPWAN application scenarios and practical deployment as examples.

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

- o 6lo applicability and use cases MAY be uniquely different from those of 6LoWPAN defined for IEEE 802.15.4.

- o It SHOULD cover various IoT related wire/wireless link layer technologies providing practical information of such technologies.
- o A general guideline on how the 6LoWPAN stack can be modified for a given L2 technology.
- o Example use cases and practical deployment examples.

## 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), and defines physical layer and link layer functionality. Physical layers of 9.6 kbit/s, 40 kbit/s and 100 kbit/s are supported. 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]. The ITU-T G.9959 can be used for smart home applications.

### 3.2. Bluetooth LE

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.

Many Devices such as mobile phones, notebooks, tablets and other handheld computing devices which support Bluetooth 4.0 or subsequent chipsets also support the low-energy variant of Bluetooth. Bluetooth LE is also being 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]. A typical usage of Bluetooth LE is smartphone-based interaction with constrained devices. Bluetooth LE

was originally designed to enable star topology networks. However, recent Bluetooth versions support the formation of extended topologies, and IPv6 support for mesh networks of Bluetooth LE devices is being developed [I-D.ietf-6lo-blemesh]

### 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 [RFC8105]. DECT-ULE can be used for smart metering in a home.

### 3.4. MS/TP

Master-Slave/Token-Passing (MS/TP) is a Medium Access Control (MAC) protocol for the RS-485 [TIA-485-A] physical layer and is used primarily in building automation networks.

An MS/TP device is typically based on a low-cost microcontroller with limited processing power and memory. These constraints, together with low data rates and a small MAC address space, are similar to those faced in 6LoWPAN networks. MS/TP differs significantly from 6LoWPAN in at least three respects: a) MS/TP devices are typically

mains powered, b) all MS/TP devices on a segment can communicate directly so there are no hidden node or mesh routing issues, and c) the latest MS/TP specification provides support for large payloads, eliminating the need for fragmentation and reassembly below IPv6.

MS/TP is designed to enable multidrop networks over shielded twisted pair wiring. It can support network segments up to 1000 meters in length at a data rate of 115.2 kbit/s or segments up to 1200 meters in length at lower bit rates. An MS/TP interface requires only a UART, an RS-485 [TIA-485-A] transceiver with a driver that can be disabled, and a 5 ms resolution timer. The MS/TP MAC is typically implemented in software.

Because of its superior "range" (~1 km) compared to many low power wireless data links, MS/TP may be suitable to connect remote devices (such as district heating controllers) to the nearest building control infrastructure over a single link [RFC8163]. MS/TP can be used for building automation networks.

### 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]. NFC can be used for secure transfer in healthcare services.



### 3.6. PLC

PLC is a data transmission technique that utilizes power conductors as medium. Unlike other dedicated communication infrastructure, power conductors are widely available indoors and outdoors. Moreover, wired technologies are more susceptible to cause interference but are more reliable than their wireless counterparts. PLC is a data transmission technique that utilizes power conductors as medium[I-D.ietf-6lo-plc].

The below table shows some available open standards defining PLC.

PLC Systems	Frequency Range	Type	Data Rate	Distance
IEEE1901	<100MHz	Broadband	200Mbps	1000m
IEEE1901.1	<15MHz	PLC-IoT	10Mbps	2000m
IEEE1901.2	<500kHz	Narrowband	200Kbps	3000m

Table 1: Some Available Open Standards in PLC

[IEEE1901] defines a broadband variant of PLC but is effective within short range. This standard addresses the requirements of applications with high data rate such as: Internet, HDTV, Audio, Gaming etc. Broadband operates on OFDM (Orthogonal Frequency Division Multiplexing) modulation.

[IEEE1901.2] defines a narrowband variant of PLC with less data rate but significantly higher transmission range that could be used in an indoor or even an outdoor environment. It is applicable to typical IoT applications such as: Building Automation, Renewable Energy, Advanced Metering, Street Lighting, Electric Vehicle, Smart Grid etc. Moreover, IEEE 1901.2 standard is based on the 802.15.4 MAC sub-layer and fully endorses the security scheme defined in 802.15.4 [RFC8036]. A typical use case of PLC is smart grid.

### 3.7. Comparison between 6lo Link layer technologies

In above clauses, various 6lo Link layer technologies and a possible candidate are described. The following table shows that dominant parameters of each use case corresponding to the 6lo link layer technology.

	Z-Wave	BLE	DECT-ULE	MS/TP	NFC	PLC
Usage	Home Auto-mation	Interact w/ Smart Phone	Meter Reading	Building Auto-mation	Health-care Service	Smart Grid
Topology & Subnet	L2-mesh or L3-mesh	Star & Mesh	Star No mesh	MS/TP No mesh	P2P L2-mesh	Star Tree Mesh
Mobility Requirement	No	Low	No	No	Moderate	No
Security Requirement	High + Privacy required	Partially	High + Privacy required	High + Authen. required	High	High + Encrypt. required
Buffering Requirement	Low	Low	Low	Low	Low	Low
Latency, QoS Requirement	High	Low	Low	High	High	Low
Data Rate	Infrequent	Infrequent	Infrequent	Frequent	Small	Infrequent
RFC # or Draft	RFC7428	RFC7668	RFC8105	RFC8163	draft-ietf-6lo-nfc	draft-ietf-6lo-plc

Table 2: Comparison between 6lo Link layer technologies

#### 4. 6lo Deployment Scenarios

##### 4.1. G3-PLC usage of 6lo in network layer

G3-PLC [G3-PLC] is a narrow-band PLC technology that is based on ITU-T G.9903 Recommendation [G.9903]. G3-PLC supports multi-hop mesh network, and facilitates highly-reliable, long-range communication. With the abilities to support IPv6 and to cross transformers, G3-PLC is regarded as one of the next-generation NB-PLC technologies.

G3-PLC has got massive deployments over several countries, e.g. Japan and France.

The main application domains targeted by G3-PLC are smart grid and smart cities. This includes, but is not limited to the following applications:

- o Smart Metering
- o Vehicle-to-Grid Communication
- o Demand Response (DR)
- o Distribution Automation
- o Home/Building Energy Management Systems
- o Smart Street Lighting
- o Advanced Metering Infrastructure (AMI) backbone network
- o Wind/Solar Farm Monitoring

In the G3-PLC specification, the 6lo adaption layer utilizes the 6LoWPAN functions (e.g. header compression, fragmentation and reassembly). However, due to the different characteristics of the PLC media, the 6LoWPAN adaptation layer cannot perfectly fulfill the requirements[I-D.ietf-6lo-plc]. The ESC dispatch type is used in the G3-PLC to provide native mesh routing and bootstrapping functionalities[RFC8066].

#### 4.2. Netricity usage of 6lo in network layer

The Netricity program in HomePlug Powerline Alliance [NETRICITY] promotes the adoption of products built on the IEEE 1901.2 Low-Frequency Narrow-Band PLC standard, which provides for urban and long distance communications and propagation through transformers of the distribution network using frequencies below 500 kHz. The technology also addresses requirements that assure communication privacy and secure networks.

The main application domains targeted by Netricity are smart grid and smart cities. This includes, but is not limited to the following applications:

- o Utility grid modernization
- o Distribution automation

- o Meter-to-Grid connectivity
- o Micro-grids
- o Grid sensor communications
- o Load control
- o Demand response
- o Net metering
- o Street Lighting control
- o Photovoltaic panel monitoring

Netricity system architecture is based on the PHY and MAC layers of IEEE 1901.2 PLC standard. Regarding the 6lo adaptation layer and IPv6 network layer, Netricity utilizes IPv6 protocol suite including 6lo/6LoWPAN header compression, DHCPv6 for IP address management, RPL routing protocol, ICMPv6, and unicast/multicast forwarding. Note that the layer 3 routing in Netricity uses RPL in non-storing mode with the MRHOF objective function based on the own defined Estimated Transmission Time (ETT) metric.

#### 5. Guidelines for adopting IPv6 stack (6lo/6LoWPAN)

The following guideline targets new candidate constrained L2 technologies that may be considered for running modified 6LoWPAN stack on top. The modification of 6LoWPAN stack should be based on the following:

- o Addressing Model: Addressing model determines whether the device is capable of forming IPv6 Link-local and global addresses and what is the best way to derive the IPv6 addresses for the constrained L2 devices. Whether the device is capable of forming IPv6 Link-local and global addresses, L2-address-derived IPv6 addresses are specified in [RFC4944], but there exist implications for privacy. For global usage, a unique IPv6 address must be derived using an assigned prefix and a unique interface ID. [RFC8065] provides such guidelines. For MAC derived IPv6 address, please refer to [RFC8163] for IPv6 address mapping examples. Broadcast and multicast support are dependent on the L2 networks. Most low-power L2 implementations map multicast to broadcast networks. So care must be taken in the design when to use broadcast and try to stick to unicast messaging whenever possible.

- o **MTU Considerations:** The deployment SHOULD consider their need for maximum transmission unit (MTU) of a packet over the link layer and should consider if fragmentation and reassembly of packets are needed at the 6LoWPAN layer. For example, if the link layer supports fragmentation and reassembly of packets, then 6LoWPAN layer may skip supporting fragmentation/reassembly. In fact, for most efficiency, choosing a low-power link layer that can carry unfragmented application packets would be optimum for packet transmission if the deployment can afford it. Please refer to 6lo RFCs [RFC7668], [RFC8163], [RFC8105] for example guidance.
- o **Mesh or L3-Routing:** 6LoWPAN specifications do provide mechanisms to support for mesh routing at L2. [RFC6550] defines layer three (L3) routing for low power lossy networks using directed graphs. 6LoWPAN is routing protocol agnostic and other L2 or L3 routing protocols can be run using a 6LoWPAN stack.
- o **Address Assignment:** 6LoWPAN developed a new version of IPv6 Neighbor Discovery[RFC4861][RFC4862] that relies on a proactive registration to avoid the use of multicast. 6LoWPAN Neighbor Discovery[RFC6775][RFC8505] inherits from IPv6 Neighbor Discovery for mechanisms such as Stateless Address Autoconfiguration(SLAAC) and Neighbor Unreachability Detection(NUD), but uses a unicast method for Duplicate Address Detection(DAD), and avoids multicast lookups from all nodes by using non-onlink prefixes. A 6LoWPAN Node is also expected to be an IPv6 host per[RFC8200] which means it should ignore consumed routing headers and Hop-by-Hop options; when operating in a RPL network[RFC6550], it is also beneficial to support IP-in-IP encapsulation [I-D.ietf-roll-useofrplinfo]. The 6LoWPAN Node should also support [RFC8505] and use it as the default Neighbor Discovery method. It is the responsibility of the deployment to ensure unique global IPv6 addresses for the Internet connectivity. For local-only connectivity IPv6 ULA may be used. [RFC6775] specifies the 6LoWPAN border router(6LBR) which is responsible for prefix assignment to the 6lo/6LoWPAN network. 6LBR can be connected to the Internet or Enterprise network via its one of the interfaces. Please refer to [RFC7668] and [RFC8105] for examples of address assignment considerations. In addition, privacy considerations [RFC8065] must be consulted for applicability. In certain scenarios, the deployment may not support autoconfiguration of IPv6 addressing due to regulatory and business reasons and may choose to offer a separate address assignment service.
- o **Header Compression:** IPv6 header compression [RFC6282] is a vital part of IPv6 over low power communication. Examples of header compression for different link-layers specifications are found in

[RFC7668], [RFC8163], [RFC8105]. A generic header compression technique is specified in [RFC7400].

- o Security and Encryption: Though 6LoWPAN basic specifications do not address security at the network layer, the assumption is that L2 security must be present. In addition, application level security is highly desirable. The working groups [IETF\_ace] and [IETF\_core] should be consulted for application and transport level security. 6lo working group is working on address authentication [I-D.ietf-6lo-ap-nd] and secure bootstrapping is also being discussed at IETF. However, there may be different levels of security available in a deployment through other standards such as hardware level security or certificates for initial booting process. Encryption is important if the implementation can afford it.
- o Additional processing: [RFC8066] defines guidelines for ESC dispatch octets use in the 6LoWPAN header. An implementation may take advantage of ESC header to offer a deployment specific processing of 6LoWPAN packets.

## 6. 6lo Use Case Examples

As IPv6 stacks for constrained node networks use a variation of the 6LoWPAN stack applied to each particular link layer technology, various 6lo use cases can be provided. In this clause, various 6lo use cases which are based on each particular link layer technology are described.

### 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 particular 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 within 0.5 seconds [RFC5826].

#### 6.2. Use case of Bluetooth LE: Smartphone-based Interaction

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: Use of 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. Support for extended network topologies (e.g. mesh networks) is being developed as of the writing.

### 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.

### 6.4. Use case of MS/TP: Building Automation Networks

The primary use case for IPv6 over MS/TP (6LoBAC) is in building automation networks. [BACnet] is the open international standard protocol for building automation, and MS/TP is defined in [BACnet] Clause 9. MS/TP was designed to be a low cost multi-drop field bus to inter-connect the most numerous elements (sensors and actuators) of a building automation network to their controllers. A key aspect of 6LoBAC is that it is designed to co-exist with BACnet MS/TP on the same link, easing the ultimate transition of some BACnet networks to native end-to-end IPv6 transport protocols. New applications for 6LoBAC may be found in other domains where low cost, long distance, and low latency are required.

#### Example: Use of 6LoBAC in Building Automation Networks

The majority of installations for MS/TP are for "terminal" or "unitary" controllers, i.e. single zone or room controllers that may connect to HVAC or other controls such as lighting or blinds. The economics of daisy-chaining a single twisted-pair between multiple devices is often preferred over home-run Cat-5 style wiring.



A multi-zone controller might be implemented as an IP router between a traditional Ethernet link and several 6LoBAC links, fanning out to multiple terminal controllers.

The superior distance capabilities of MS/TP (~1 km) compared to other 6lo media may suggest its use in applications to connect remote devices to the nearest building infrastructure. For example, remote pumping or measuring stations with moderate bandwidth requirements can benefit from the low cost and robust capabilities of MS/TP over other wired technologies such as DSL, and without the line-of-site restrictions or hop-by-hop latency of many low cost wireless solutions.

#### 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.

Example: Use of NFC for Secure Transfer 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.

#### 6.6. Use case of PLC: Smart Grid

Smart grid concept is based on numerous operational and energy measuring sub-systems of an electric grid. It comprises of multiple administrative levels/segments to provide connectivity among these numerous components. Last mile connectivity is established over LV segment, whereas connectivity over electricity distribution takes place in HV segment.

Although other wired and wireless technologies are also used in Smart Grid (Advance Metering Infrastructure - AMI, Demand Response - DR, Home Energy Management System - HEMS, Wide Area Situational Awareness - WASA etc), PLC enjoys the advantage of existing (power conductor) medium and better reliable data communication. PLC is a promising wired communication technology in that the electrical power lines are already there and the deployment cost can be comparable to wireless technologies. The 6lo related scenarios lie in the low voltage PLC networks with most applications in the area of Advanced Metering Infrastructure, Vehicle-to-Grid communications, in-home energy management and smart street lighting.

#### Example: Use of PLC for Advanced Metering Infrastructure

Household electricity meters transmit time-based data of electric power consumption through PLC. Data concentrators receive all the meter data in their corresponding living districts and send them to the Meter Data Management System (MDMS) through WAN network (e.g. Medium-Voltage PLC, Ethernet or GPRS) for storage and analysis. Two-way communications are enabled which means smart meters can do actions like notification of electricity charges according to the commands from the utility company.

With the existing power line infrastructure as communication medium, cost on building up the PLC network is naturally saved, and more importantly, labor operational costs can be minimized from a long-term perspective. Furthermore, this AMI application speeds up electricity charge, reduces losses by restraining power theft and helps to manage the health of the grid based on line loss analysis.

#### Example: Use of PLC (IEEE1901.1) for WASA in Smart Grid

Many sub-systems of Smart Grid require low data rate and narrowband variant (IEEE1901.2) of PLC fulfils such requirements. Recently, more complex scenarios are emerging that require higher data rates.

WASA sub-system is an appropriate example that collects large amount of information about the current state of the grid over wide area from electric substations as well as power transmission lines. The collected feedback is used for monitoring, controlling and protecting all the sub-systems.

## 7. IANA Considerations

There are no IANA considerations related to this document.

## 8. Security Considerations

Security considerations are not directly applicable to this document. The use cases will use the security requirements described in the protocol specifications.

## 9. Acknowledgements

Carles Gomez has been funded in part by the Spanish Government through the Jose Castillejo CAS15/00336 grant, and through the TEC2016-79988-P grant. 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.

Thomas Watteyne, Pascal Thubert, Xavier Vilajosana, Daniel Migault, and Jianqiang HOU have provided valuable feedback for this draft.

Das Subir and Michel Veillette have provided valuable information of jupiterMesh and Paul Duffy has provided valuable information of Wi-SUN for this draft. Also, Jianqiang Hou has provided valuable information of G3-PLC and Netricity for this draft. Kerry Lynn and Dave Robin have provided valuable information of MS/TP and practical use case of MS/TP for this draft.

Deoknyong Ko has provided relevant text of LTE-MTC and he shared his experience to deploy IPv6 and 6Lo technologies over LTE MTC in SK Telecom.

## 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, <<https://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, <<https://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, <<https://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, <<https://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, <<https://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, <<https://www.rfc-editor.org/info/rfc6550>>.
- [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, <<https://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, <<https://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, <<https://www.rfc-editor.org/info/rfc7228>>.
- [RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <<https://www.rfc-editor.org/info/rfc7400>>.
- [RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015, <<https://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, <<https://www.rfc-editor.org/info/rfc7668>>.

- [RFC8036] Cam-Winget, N., Ed., Hui, J., and D. Popa, "Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks", RFC 8036, DOI 10.17487/RFC8036, January 2017, <<https://www.rfc-editor.org/info/rfc8036>>.
- [RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <<https://www.rfc-editor.org/info/rfc8065>>.
- [RFC8066] Chakrabarti, S., Montenegro, G., Droms, R., and J. Woodyatt, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines", RFC 8066, DOI 10.17487/RFC8066, February 2017, <<https://www.rfc-editor.org/info/rfc8066>>.
- [RFC8105] Mariager, P., Petersen, J., Ed., Shelby, Z., Van de Logt, M., and D. Barthel, "Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)", RFC 8105, DOI 10.17487/RFC8105, May 2017, <<https://www.rfc-editor.org/info/rfc8105>>.
- [RFC8163] Lynn, K., Ed., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks", RFC 8163, DOI 10.17487/RFC8163, May 2017, <<https://www.rfc-editor.org/info/rfc8163>>.
- [RFC8352] Gomez, C., Kovatsch, M., Tian, H., and Z. Cao, Ed., "Energy-Efficient Features of Internet of Things Protocols", RFC 8352, DOI 10.17487/RFC8352, April 2018, <<https://www.rfc-editor.org/info/rfc8352>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.

## 10.2. Informative References

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

- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [I-D.ietf-6lo-nfc] Choi, Y., Hong, Y., Youn, J., Kim, D., and J. Choi, "Transmission of IPv6 Packets over Near Field Communication", draft-ietf-6lo-nfc-15 (work in progress), July 2019.
- [I-D.ietf-6lo-blemesh] Gomez, C., Darroudi, S., Savolainen, T., and M. Spoerk, "IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP", draft-ietf-6lo-blemesh-06 (work in progress), September 2019.
- [I-D.ietf-6lo-plc] Hou, J., Liu, B., Hong, Y., Tang, X., and C. Perkins, "Transmission of IPv6 Packets over PLC Networks", draft-ietf-6lo-plc-00 (work in progress), February 2019.
- [I-D.ietf-roll-useofrplinfo] Robles, I., Richardson, M., and P. Thubert, "Using RPL Option Type, Routing Header for Source Routes and IPv6-in-IPv6 encapsulation in the RPL Data Plane", draft-ietf-roll-useofrplinfo-31 (work in progress), August 2019.
- [I-D.ietf-6lo-ap-nd] Thubert, P., Sarikaya, B., Sethi, M., and R. Struik, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-12 (work in progress), April 2019.
- [IETF\_6lo] "IETF IPv6 over Networks of Resource-constrained Nodes (6lo) working group", <<https://datatracker.ietf.org/wg/6lo/charter/>>.
- [IETF\_ace] "IETF Authentication and Authorization for Constrained Environments (ace) working group", <<https://datatracker.ietf.org/wg/ace/charter/>>.

- [IETF\_core] "IETF Constrained RESTful Environments (core) working group", <<https://datatracker.ietf.org/wg/core/charter/>>.
- [IEEE802154] IEEE standard for Information Technology, "IEEE Std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks".
- [TIA-485-A] "TIA, "Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems", TIA-485-A (Revision of TIA-485)", March 2003, <[https://global.ihs.com/doc\\_detail.cfm?item\\_s\\_key=00032964](https://global.ihs.com/doc_detail.cfm?item_s_key=00032964)>.
- [G3-PLC] "G3-PLC Alliance", <<http://www.g3-plc.com/home/>>.
- [NETRICITY] "Netricity program in HomePlug Powerline Alliance", <<http://groups.homeplug.org/tech/Netricity>>.
- [G.9959] "International Telecommunication Union, "Short range narrow-band digital radiocommunication transceivers – PHY and MAC layer specifications", ITU-T Recommendation", January 2015.
- [G.9903] "International Telecommunication Union, "Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks", ITU-T Recommendation", August 2017.
- [IEEE1901] "IEEE Standard, IEEE Std. 1901-2010 – IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications", 2010, <<https://standards.ieee.org/findstds/standard/1901-2010.html>>.
- [IEEE1901.2] "IEEE Standard, IEEE Std. 1901.2-2013 – IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications", 2013, <<https://standards.ieee.org/findstds/standard/1901.2-2013.html>>.

[BACnet] "ASHRAE, "BACnet-A Data Communication Protocol for Building Automation and Control Networks", ANSI/ASHRAE Standard 135-2016", January 2016, <[http://www.techstreet.com/ashrae/standards/ashrae-135-2016?product\\_id=1918140#jumps](http://www.techstreet.com/ashrae/standards/ashrae-135-2016?product_id=1918140#jumps)>.

#### Appendix A. Design Space Dimensions for 6lo Deployment

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 [RFC6568], the following design space dimensions are described: Deployment, Network size, Power source, Connectivity, Multi-hop communication, Traffic pattern, Mobility, Quality of Service (QoS). However, in this document, the following design space dimensions are 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: Typically, the link layer technologies of 6lo have low rate of data transmission. But, by adjusting the MTU, it can deliver higher upper layer 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 and Privacy 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 depends on the 6lo use case. If the 6lo nodes can move or moved around, a mobility management mechanism is required.
- 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 [RFC8352]. Readers are expected to be familiar with [RFC7228] terminology.
- o Update firmware requirements: Most 6lo use cases 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.
- o Wired vs. Wireless: Plenty of 6lo link layer technologies are wireless, except MS/TP and PLC. The selection of wired or wireless link layer technology is mainly dependent on the requirement of 6lo use cases and the characteristics of wired/wireless technologies. For example, some 6lo use cases may require easy and quick deployment, whereas others may need a continuous source of power.

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

Abdur Rashid Sangi  
Huaiyin Institute of Technology  
No.89 North Beijing Road, Qinghe District  
Huaian 223001  
P.R. China

Email: sangi\_bahrian@yahoo.com

Take Aanstoot  
Modio AB  
S:t Larsgatan 15, 582 24  
Linkoping  
Sweden

Email: take@modio.se

Samita Chakrabarti  
San Jose, CA  
USA

Email: [samitac.ietf@gmail.com](mailto:samitac.ietf@gmail.com)

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: May 1, 2020

S. Jiang  
Huawei Technologies Co., Ltd  
G. Li  
Huawei Technologies  
B. Carpenter  
Univ. of Auckland  
October 29, 2019

Asymmetric IPv6 for IoT Networks  
draft-jiang-asymmetric-ipv6-02

Abstract

This document describes a new approach to IPv6 header compression for use in scenarios where minimizing packet size is crucial but routing performance must be maximised.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 1, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Proposed Solution . . . . .	3
3. Address Transformation at the Gateway . . . . .	5
4. Routing without Decompression . . . . .	6
5. Address Configuration . . . . .	6
6. Compatibility with Existing Protocols . . . . .	7
7. Relationship to Static Context Header Compression . . . . .	7
8. Security Considerations . . . . .	7
9. IANA Considerations . . . . .	8
10. Acknowledgements . . . . .	8
11. References . . . . .	8
Appendix A. Change log [RFC Editor: Please remove] . . . . .	9
Authors' Addresses . . . . .	10

## 1. Introduction

The large address space of IPv6 is essential for the massive expansion of the network edge that will be caused by "Internet of Things" (IoT) technology over low-power or 5G links. However, the size of a raw IPv6 packet header causes difficulty due to the small maximum transmission units (MTU) allowed by typical low-power, low-cost link layers. For 5G, this aspect is discussed in [I-D.ietf-dmm-5g-uplane-analysis]. Thus header compression, including address compression, is an important issue. This decreases the size of raw packets, but compressed IP addresses are not routeable except by decompressing them completely in every forwarding node. There are two issues here. The first is the extra computation resource needed for compressing or decompressing in constrained IoT nodes. The second is that full-length IPv6 routing will consume more memory to store routing tables and packet queues. Such resource consumption is very undesirable in constrained nodes with limited storage, CPU power, and battery capacity.

To mitigate these issues, here we propose a solution enabling the shortening of IPv6 addresses inside packets, and the routing of packets according to short addresses, without needing the overhead of a decompression step prior to route lookup. Considering that the scale and size of edge networks may vary widely, different lengths of short address can be used in different domains.

As an illustrative example, consider an edge network which is known to never require more than a few hundred nodes, which in most cases will communicate either with each other, or with application layer

gateways to the rest of the Internet. Rather than needing 128-bit addresses, such a network could very well operate with 16-bit addresses. Also, it could very likely operate without needing enhancements such as differentiated services, ECN or flow labels. If only IPv6 is supported, the version number field is pointless. There is no reason for IPv6 packets within such a network to contain 40-byte headers as specified in [RFC8200]. Therefore, the useful information could be carried in 8 bytes (see Figure 1). Furthermore, routers within the edge network can route packets directly on 16-bit addresses, reducing RIB and FIB sizes and the lookup time.

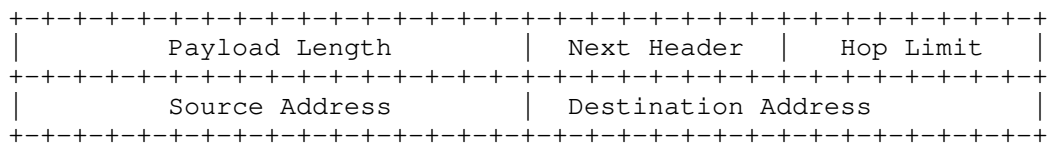


Figure 1

This work is distinct from previous work on address compression [RFC6282] [RFC7400]. Although those solutions tackle the problem of small MTU size, they do not address the problem of decompression overhead.

This work is also distinct from ongoing work on static context header compression [I-D.ietf-lpwan-ipv6-static-context-hc], as discussed in more detail below.

Finally, this work is distinct from the 6LoWPAN Routing Header [RFC8138], which can support truncated addresses in a different way.

## 2. Proposed Solution

The use of IPv6 naturally implies 128-bit addresses for both source and destination. However, this address size is huge by the standards of IoT edge networks. We propose the use of a context parameter to indicate the effective length of the IP address for every node in a local domain. If the effective length is N bits, then all addresses in the domain are assumed to be preceded by a common prefix of 128-N bits, when a full size IPv6 address is needed. Any node in the domain that needs the full address, such as a gateway node to the Internet, can therefore easily synthesize it.

The address length parameter may be needed by every node in the domain. It can be spread by various techniques:

- o Configure the address length in every node.

- o Obtain the address length from a gateway (next hop router) node.
- o Negotiate the address length between neighbors.

The solution operates by shortening IP address fields to save overhead. To enhance this, we propose a new field named Flexible Header Encoding (FHE). It consists of 8 bits, each indicating whether the corresponding IPv6 header field [RFC8200] exists.

Bit 0 indicates the Modified Version field

Bit 1 indicates the Traffic Class field

Bit 2 indicates the Flow Label field.

Bit 3 indicates the Payload Length field.

Bit 4 indicates the Next Header field. (Zero implies "No Next Header", value 59)

Bit 5 indicates the Hop Limit field.

Bit 6 indicates the Source Address field.

Bit 7 indicates the Destination Address field.

The "Version" field is a special case. In the context of FHE, all packets are presumed to be IPv6 so the normal version field has no purpose. The Modified Version field, if present, has the following encoded meanings:

0b0000: The source address (if exist) has pre-determined length inside the domain and the destination address (if exist) uses standard 128-bit IPv6 address. (Outward traffic)

0b0001: The source address (if exist) uses standard 128-bit IPv6 address and the destination address (if exist) has pre-determined length inside the domain. (Inward traffic)

0b0010: The source address and destination address have the same length inside the domain. The address length will be pre-determined.

0b0110: Reserved for IPv6 compatible case.

0b0100: Reserved for IPv4 compatible case.

0b0011~0b1111(except 0b0110, 0b0100): Reserved.

All fields, including the Modified Version field, follow the FHE in the same order as in [RFC8200], with no padding. There are no alignment requirements, but when a packet is decompressed to a normal IPv6 format, padding options as defined in RFC8200 must be inserted.

Compared to the illustrative example in Figure 1, the actual packet size would therefore be 10 bytes, a considerable improvement on the standard 40 bytes.

One implication of the above is that the source and destination addresses may be elided completely if they are implicit. Sourceless packets were originally suggested in [crowcroft].

Figure 2 illustrates an example of the FHE format. In this example the traffic class, flow label and source address are elided, and the destination address is truncated to 16 bits. The modified version field could be 0b0001 or 0b0010.

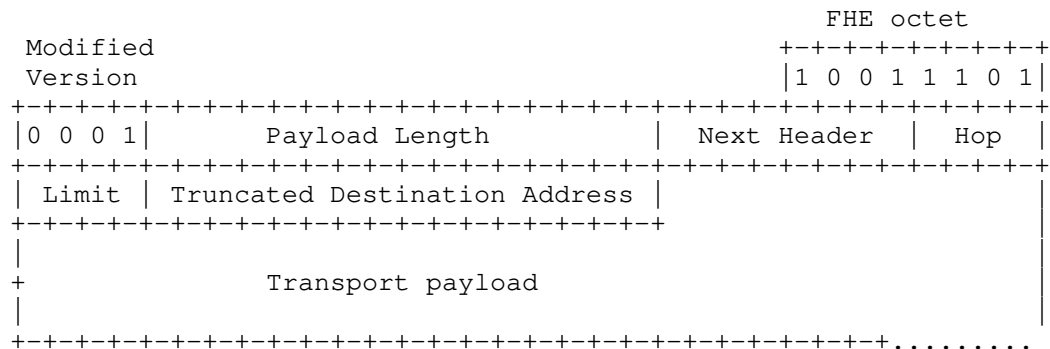


Figure 2

Note that Asymmetric IPv6 does not contain any special handling for IPv6 fragmentation, which will operate exactly as described in [RFC8200], with Asymmetric IPv6 applied to each fragment packet. However, we assume that in IoT deployment scenarios, packets whose length exceeds the IPv6 minimum link MTU before applying Asymmetric IPv6 will be rare. If the underlying link layer cannot carry complete packets even after applying Asymmetric IPv6 compression, an adaptation layer will be necessary exactly as for normal IPv6.

### 3. Address Transformation at the Gateway

Truncated intra-domain addresses will be used to identify nodes inside the domain. When a packet is sent from an IoT node to an external IPv6 host, the node's intra-domain address, which is unique in the domain, will be carried in the source address field. When the



packet is forwarded outside the domain by a gateway, the intra-domain address will be transformed to a complete IPv6 address. To achieve this, the gateway should will maintain a globally routeable prefix for all the nodes in the domain. When a packet with an intra-domain source address is received, the gateway extracts this address and concatenates it to the prefix to form a standard, globally unique IPv6 address. Vice versa, when IPv6 packets are received from the Internet, the prefix will be removed to recover the intra-domain short address.

There are two options for handling the addresses of external hosts within the domain. One is to use their full IPv6 addresses via Modified Version codes 0b0000 and 0b0001. The other is effectively a specialized form of Network Address Translation. Here, the gateway will maintain a dynamic mapping table between synthetic intra-domain addresses and IPv6 addresses. As packets are received, the gateway performs the appropriate mapping. The transformation must be checksum-neutral for the transport layer, so the methods designed for NAT46 should be adapted.

NOTE IN DRAFT: Details and references TBD.

It is an engineering choice whether this method is preferable to carrying full 128-bit addresses on the IOT side.

#### 4. Routing without Decompression

Routing mechanisms may readily be adapted to truncated address sizes. If there is routing with an HFE domain, we assume that the truncated address size will be split into a prefix and an interface identifier, but this will not be at the traditional /64 boundary. If routing between different length addresses is required, a suitably modified Forwarding Information Base (FIB) structure is needed, as for any variable length addressing scheme. A truncated address needs to be virtually expanded to 128 bits at the router's inbound interface, although this may not be the physical implementation.

A possible routing choice for IOT edge networks is RPL [RFC6550], although a more complete survey can be found in [talwar].

#### 5. Address Configuration

The simplest approach to address configuration is simply to run normal IPv6 procedures (SLAAC or DHCPv6), on the argument that this is a rare process and the overhead does not matter. If the truncated address size is less than 64 bits, it will be necessary to use shorter interface identifiers than normal, but this is not a major change. Once a node has acquired an IPv6 address and has learned the

local address length parameter as outlined in Section 2, it can continue in FHE mode.

## 6. Compatibility with Existing Protocols

Although HFE nodes can only talk directly to each other, they are essentially a special form of IPv6 node and they can communicate with the whole IPv6 Internet via gateways. The complexity is not greater than 6LoWPAN. If appropriate, the 6LoWPAN adaptation layer [RFC4944] could be used, with a specific dispatch type.

## 7. Relationship to Static Context Header Compression

Static Context Header Compression (SCHC) [I-D.ietf-lpwan-ipv6-static-context-hc] is a powerful mechanism for reducing IPv6 packet size in an IoT application environment. In particular it includes a profile for UDP over IPv6, and a somewhat modified version of this profile could achieve much of what Asymmetric IPv6 proposes. In addition, SCHC provides support for fragmentation in the case of very small link MTUs. However, SCHC is by design static, and once a context is established the fields to be compressed do not change. Asymmetric IPv6 transmits the FHE and Modified Version bytes with every packet, so it provides dynamic choice as to which header elements are compressed or elided.

In a context where the desirable compression is fixed, e.g. every address is the same length, the flow label is never used, etc., SCHC can be used to the same effect as Asymmetric IPv6. However, if the behavior needs to be dynamic, the signaling power of the FHE and Modified Version bytes in Asymmetric IPv6 is needed.

Further study is needed whether the advantages of the two mechanisms can be combined.

## 8. Security Considerations

HFE is essentially only a non-cryptographic compression technique so it neither adds to nor reduces the intrinsic security of an IPv6 packet. The address length parameter is not a secret, since all nodes in the domain must know it. The mechanism for distributing this parameter must be no less secure than any other configuration mechanism in use.

Address-based privacy issues must be considered in deciding on the address length. If the number of bits available for the interface identifier is significantly less than the 64 currently in use, address traceability and guessability will be affected. However, if the traffic with short addresses is confined to within the edge

network, the privacy issue will be minimized. [RFC7721] and [RFC7217] should be consulted prior to deciding the address length.

## 9. IANA Considerations

This document makes no request of the IANA.

NOTE IN DRAFT: If the solution of a 6LoWPAN dispatch type is adopted, a suitable assignment request will be added.

## 10. Acknowledgements

Useful comments were received from Cheng Li, Pascal Thubert, Laurent Toutain and others.

## 11. References

[crowcroft]

Crowcroft, J. and M. Bagnulo, "SNA: Sourceless Network Architecture", University of Cambridge Computer Laboratory Technical Report UCAM-CL-TR-849, 2014.

[I-D.ietf-dmm-5g-uplane-analysis]

Homma, S., Miyasaka, T., Matsushima, S., and D. Voyer, "User Plane Protocol and Architectural Analysis on 3GPP 5G System", draft-ietf-dmm-5g-uplane-analysis-02 (work in progress), July 2019.

[I-D.ietf-lpwan-ipv6-static-context-hc]

Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and J. Zuniga, "Static Context Header Compression (SCHC) and fragmentation for LPWAN, application to UDP/IPv6", draft-ietf-lpwan-ipv6-static-context-hc-21 (work in progress), July 2019.

[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, <<https://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, <<https://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, <<https://www.rfc-editor.org/info/rfc6550>>.
- [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, <<https://www.rfc-editor.org/info/rfc7217>>.
- [RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <<https://www.rfc-editor.org/info/rfc7400>>.
- [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <<https://www.rfc-editor.org/info/rfc7721>>.
- [RFC8138] Thubert, P., Ed., Bormann, C., Toutain, L., and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header", RFC 8138, DOI 10.17487/RFC8138, April 2017, <<https://www.rfc-editor.org/info/rfc8138>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [talwar] Talwar, M., "ROUTING TECHNIQUES AND PROTOCOLS FOR INTERNET OF THINGS: A SURVEY", Indian J.Sci.Res. 12(1):417-423, 2015.

Appendix A. Change log [RFC Editor: Please remove]

draft-jiang-asymmetric-ipv6-00, 2019-06-03:

Initial version

draft-jiang-asymmetric-ipv6-01, 2019-06-21:

Fixed reference error

draft-jiang-asymmetric-ipv6-02, 2019-10-29:

Added illustrative example

Discussed fragmentation

Discussed relationship to SCHC

Fixed bit pattern errors

#### Authors' Addresses

Sheng Jiang  
Huawei Technologies Co., Ltd  
Q14, Huawei Campus, No.156 Beiqing Road  
Hai-Dian District, Beijing, 100095  
P.R. China

Email: [jiangsheng@huawei.com](mailto:jiangsheng@huawei.com)

Guangpeng Li  
Huawei Technologies  
Q14, Huawei Campus  
No.156 Beiqing Road  
Hai-Dian District, Beijing 100095  
P.R. China

Email: [liguangpeng@huawei.com](mailto:liguangpeng@huawei.com)

Brian Carpenter  
The University of Auckland  
School of Computer Science  
University of Auckland  
PB 92019  
Auckland 1142  
New Zealand

Email: [brian.e.carpenter@gmail.com](mailto:brian.e.carpenter@gmail.com)

6lo Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 7, 2020

A. Minaburo  
Acklio  
L. Toutain  
Institut MINES TELECOM; IMT Atlantique  
November 04, 2019

Comparison of 6lo and SCHC  
draft-toutain-6lo-6lo-and-schc-00

Abstract

6lo and 6lowpan have standardized a stateless IPv6 and UDP compression method for mesh networks. SCHC proposes a generic compression mechanism that can be applied to any protocol stack. The lpwan working group is focusing on star topologies for IPv6, UDP and CoAP header compression and fragmentation.

This document summarizes the differences between 6lo and SCHC and possible combination of SCHC and 6lo.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 7, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Comparison . . . . .	2
2.1. Stateless compression. . . . .	2
2.2. Meshed vs Star . . . . .	2
2.3. Alignment . . . . .	3
3. Uniform vs specific compression rules. . . . .	3
3.1. Bitmap vs Rule ID . . . . .	4
3.2. Fragmentation . . . . .	4
4. Applicability of SCHC in a 6lo network. . . . .	5
5. Normative References . . . . .	5
Authors' Addresses . . . . .	5

## 1. Introduction

6lo and 6lowpan have standardized a stateless IPv6 and UDP compression method for mesh networks. SCHC proposes a generic compression mechanism that can be applied to any protocol stack. The lpwan working group is focusing on star topologies for IPv6, UDP and CoAP header compression and fragmentation.

This document summarizes the differences between 6lo and SCHC and possible combination of SCHC and 6lo.

## 2. Comparison

### 2.1. Stateless compression.

Both compression protocols are stateless regarding the compression/decompression process. Each packet is compressed and decompressed independently of the others and no information is stored during compression or decompression.

The SCHC name comes from the fact that it is a generic mechanism and the context tells how to compress a specific packet.

### 2.2. Meshed vs Star

6lo is defined for meshed network therefore all the node must be able to manipulate any 6lo packet.

SCHC is defined for star network and compression is done at both ends. SCHC offers the possibility to have different compression scheme for each branch of the star. This scheme is described though a context.

If SCHC had to be used in a mesh network, all the intermediary nodes will have to know the rules used in the network.

### 2.3. Alignment

6lo preserves alignment on byte boundary when sending header fields. SCHC is bit oriented and padding can be added when the packet is sent.

### 3. Uniform vs specific compression rules.

6lo focuses mainly on IPv6 header and predefine a compression scheme known by all the nodes in a 6lo network.

SCHC defines a generic compression mechanism based on fields. A field is an abstract notion. A field has several properties:

- o An ID identifying a specific field.
- o A position when a field is repeated several times in a header.
- o A length which can either be a size in bit or a function indicating how the size is computed.
- o A direction which makes sense in a star topology since traffic is originating from a node or is for a node.

The rule contains some functions:

- o Matching Operator: this information is used to select candidate rules for compression. A rule is selected if all the fields in the packets matches all the fields in the rule. Current MO are:
  - \* "ignore" (any value is possible),
  - \* "equal",
  - \* "MSB" (Most Significant Bits) or
  - \* "Matching".



- o Compression Decompression Action: if a compression rule is selected, then compression action tells how to compress header fields into residues. Current CDA are:
  - \* Not-sent: the field is elided. This behavior is found also in 6lo as elided.
  - \* Value-sent: the field is sent. If the field was defined as variable, the length can be sent before the residue. This behavior is found also in 6lo, but only for well-known length fields.
  - \* LSB (Less Significant Bit): the less significant bits are sent.
  - \* Matching-sent: an index is sent instead of the value. 6lo has something similar for hop-limit. 3 well-known values are defined.

### 3.1. Bitmap vs Rule ID

6lo defines a dispatch indicating the nature of the 6lo packet and for IPHC defines a bitmap to indicate the nature of the header compression.

SCHC uses a rule ID to identify the nature of the SCHC packet. Rule ID have a variable length, most frequent rules may use shorter values. The rule ID space is split between compression and decompression rules. The rule ID refers to a context which contains the nature of the rule and associated parameters.

In a sense the combination dispatch and bitmap for compression are equivalent to the rule ID, the main difference is that the rules are implicit in 6lo and the same rules are shared by all the node and explicit in SCHC. Context synchronization is needed between both ends.

### 3.2. Fragmentation

SCHC implement a fragmentation mechanisms dedicated to LPWAN networks. 3 modes exists:

- o NoAck mode is an optimisitic mode, a RCS (rassembly Check Sequence) is added in the last fragment. unvalid received messages are discarded. No retransmission is done.
- o Ack Always is base on a "jumping window", sender must received a acknowledgement to jump to the next window.

- o Ack on Error is more efficient. The message is cut into tiles of a specific length. Tiles are regrouped into windows. Tiles are sent into fragments. Fragment size may vary during transmission. Receiver generate

#### 4. Applicability of SCHC in a 6lo network.

To apply SCHC in a 6lo meshed network, the following requirements are needed:

- o A SCHC dispatch to indicate that a SCHC rule ID follows,
- o A context synchronization among all the 6lo nodes to share the context, or predefined rules,
- o The rule should not contain a direction indicator.

#### 5. Normative References

[I-D.ietf-lpwan-ipv6-static-context-hc]

Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and J. Zuniga, "Static Context Header Compression (SCHC) and fragmentation for LPWAN, application to UDP/IPv6", draft-ietf-lpwan-ipv6-static-context-hc-22 (work in progress), October 2019.

[rfc2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

#### Authors' Addresses

Ana Minaburo  
Acklio  
1137A avenue des Champs Blancs  
35510 Cesson-Sevigne Cedex  
France

Email: [ana@ackl.io](mailto:ana@ackl.io)

Laurent Toutain  
Institut MINES TELECOM; IMT Atlantique  
2 rue de la Chataigneraie  
CS 17607  
35576 Cesson-Sevigne Cedex  
France

Email: [Laurent.Toutain@imt-atlantique.fr](mailto:Laurent.Toutain@imt-atlantique.fr)

6Lo Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 19 April 2020

A. Wachter  
Graz University of Technology  
17 October 2019

IPv6 over Controller Area Network  
draft-wachter-6lo-can-00

Abstract

Controller Area Network (CAN) is a fieldbus initially designed for automotive applications. It is a multi-master bus with 11-bit or 29-bit frame identifiers. The CAN standard (ISO 11898 series) defines the physical and data-link layer. This document describes how to transfer IPv6 packets over CAN using ISO-TP, a dedicated addressing scheme, and IP header compression (IPHC).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 April 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
1.1. Terminology . . . . .	3
1.2. Controller Area Network Overview . . . . .	3
1.3. ISO-TP Overview . . . . .	3
2. Addressing . . . . .	4
2.1. Unicast . . . . .	5
2.2. Multicast . . . . .	5
2.3. Address Generation . . . . .	6
3. Link-Layer Duplicate Address Detection . . . . .	6
4. Stateless Address Autoconfiguration . . . . .	7
5. IPv6 Link-Local Address . . . . .	8
6. ISO-TP . . . . .	8
6.1. Multicast . . . . .	8
6.2. Unicast . . . . .	9
6.3. Frame Format . . . . .	10
6.4. Single-Frame . . . . .	11
6.5. First-Frame . . . . .	11
6.6. Consecutive-Frame . . . . .	12
6.7. Flow-Control-Frame . . . . .	12
7. Frame Format . . . . .	13
8. Ethernet Border Translator . . . . .	14
9. IANA Considerations . . . . .	16
10. Security Considerations . . . . .	16
11. Reference Implementation . . . . .	16
12. Normative References . . . . .	16
Author's Address . . . . .	17

## 1. Introduction

Controller Area Network (CAN) is mostly known for its use in the automotive domain. However, it is also used in industrial applications as CANopen, building automation and many more.

It is a two-wire wired-AND multi-master bus that uses CSMA/CR in its arbitration field. CAN uses 11-bit (standard ID) and 29-bit (extended ID) identifiers to identify frames. The maximum payload data size is 8 octets for classical CAN and 64 octets for CAN-FD.

The minimal MTU of IPv6 is 1280 octets, and therefore, a mechanism to support a larger payload is needed. This document uses a slightly modified version of the ISO-TP protocol to transfer data up to 4095 octets per packet. Mapping addresses to identifiers uses an addressing scheme with a 14-bit source address, a 14-bit destination address, and a multicast bit. This scheme uses extended identifiers only.

To make data transfer more efficient IPHC [RFC6282] is used.

Due to the limited address space of 14 bits, random address generation would generate duplicate addresses with an unacceptably high probability. For this reason, a link-layer duplicate address detection is introduced to resolve address conflicts.

An Ethernet border translator is designed to connect a 6LoCAN bus segment to other networks.

### 1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

### 1.2. Controller Area Network Overview

This section provides a brief overview of Controller Area Network (CAN), as specified in [ISO 11898-1:2015]. CAN has two wires, CAN High and CAN Low, where CAN High is tied to 5V and CAN Low to 0V when transmitting a dominant (0) bit. Both wires are at the same level (approximately 2.5V) when transmitting a recessive (1) bit. Because of the wired-AND structure, a dominant bit overrides a recessive bit.

To resolve collisions in the arbitration field, a CAN controller checks for overridden recessive bits. The sender that was sending the recessive bit then stops the transmission. Therefore an identifier with all zeros has the highest priority.

CAN controllers are usually able to filter frames by identifiers and only pass frames where the filter matches. The identifiers can be masked in order to define which bits of the identifier must match and which ones are ignored.

### 1.3. ISO-TP Overview

A subset of ISO-TP (ISO 15765-2) is used to fragment and reassemble the packets. This subset of ISO-TP can send packets with a payload size of up to 4095 octets, enough for IPv6 minimum MTU size of 1280 octets. ISO-TP is designed for CAN and its small payload data size and therefore preferred over [RFC4944] fragmentation.

The 6LoWPAN fragmentation would use more than the half of the available payload for the fragmentation headers. This fact prevents 6LoWPAN fragmentation from being used for 6LoCAN.

## 2. Addressing

This section provides information about the 14-bit node address to CAN identifier mapping.

Because CAN uses identifiers to identify the frame's content, an addressing scheme is introduced to map node addresses to identifiers. Every node has a unique 14-bit address. This address is assigned either statically or randomly. The addressing scheme uses the 29-bit extended identifier only. It is a combination of a source address, a destination address, and a multicast bit.

The address 0x3DFE is reserved for link-layer duplicate address detection, and address 0x3DF0 is reserved for the Ethernet border translator. Addresses from 0x0100 to 0x3DEF are used as node addresses. Other addresses (0x0000 to 0x00FF and 0x3DF0 to 0x3FFF) are reserved or used for special purposes. Note that a lower address number has a higher priority on the bus.

6LoCAN does not use the 11-bit standard identifiers. They may be used for other purposes.

Address	Description
0x3DFE - 0x3FFF	Reserved
0x3DFE	LLDAD
0x3DF1 - 0x3DFD	Reserved
0x3DF0	Ethernet Translator
0x0100 - 0x3DEF	Node addresses
0x0000 - 0x00FF	Reserved

Table 1: Address ranges

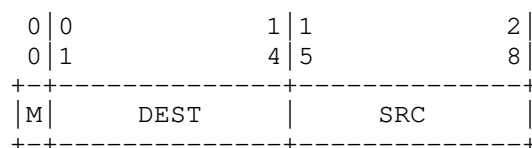


Figure 1: Addressing Scheme

M : Multicast.

DEST : Destination Address (14 bits).

SRC : Source Address (14 bits).

For example, a destination of 0x3055 and source address of 0x3AAF result in the following identifier:

0	1	2
0	4	8
0	1	1
0	1	5
-----		
0	11000001010101	11101010101111
-----		

Figure 2: Unicast identifier example

A multicast group of 1 and a source address of 0x3AAF result in the following identifier:

0	1	2
0	4	8
0	1	1
0	1	5
-----		
1	0000000000000001	11101010101111
-----		

Figure 3: Multicast identifier example

## 2.1. Unicast

For unicast packets, the multicast bit is set to zero, and the 14-bit source address is the address of the sender. The 14-bit destination address of the receiver is discovered by IPv6 NDP defined in [RFC4861]. Every node MUST be able to receive all frames targeting its address as the destination address.

## 2.2. Multicast

For multicast packets, the multicast bit is set to one, and the 14-bit source address is the address of the sender. The 14-bit destination address is the last 14 bits of the multicast group. Every node MUST be able to receive all frames matching the last 14 bits of all joined multicast groups as the destination address.



### 2.3. Address Generation

Every node has a 14-bit address. This address **MUST** be unique within the CAN bus segment. The address can either be statically defined or assigned randomly. For the random address assignment, the node tries randomly chosen addresses until the link-layer duplicate address detection succeeds. The link-layer duplicate address detection prevents nodes from assigning an address already in use.

### 3. Link-Layer Duplicate Address Detection

This section provides information about how to perform link-layer duplicate address detection (LLDAD).

LLDAD is introduced to prevent collisions of CAN identifiers and makes it possible to use random address assignment with only 14 bits of address space. To perform an LLDAD, a LLDAD-request is sent. If there is no DAD-response sent back, the DAD is considered successful. The node **MUST** wait for a response for at least 100ms.

LLDAD-requests are remote transmission request (RTR) frames with the desired address as the destination and 14 bits entropy as the source address. The entropy prevents identifier collisions when nodes are trying to get the same address at the same time.

DAD-responses are data-frames sent to the LLDAD address (0x3DFE) with the responder's address as the source address. Both LLDAD-request and DAD-response have a data length of zero.

The node **MUST** be configured to receive RTR frames with the desired address as the destination address before the LLDAD-request is sent and frames with the LLDAD address as long as the LLDAD is in progress. This prevents from assigning the same address to more than one node when sending the LLDAD-request at the same time. The ability to receive RTR frames with the desired address as the destination address **MUST** be kept as long as the node uses the address. The response to LLDAD-requests that matches the node address **MUST** be sent before the requesting node stops waiting for the response, which is 100ms.

Figure 4 shows a DAD Fail example where node A performs a LLDAD-request on address 0x3055 where this address is already in use by node B.

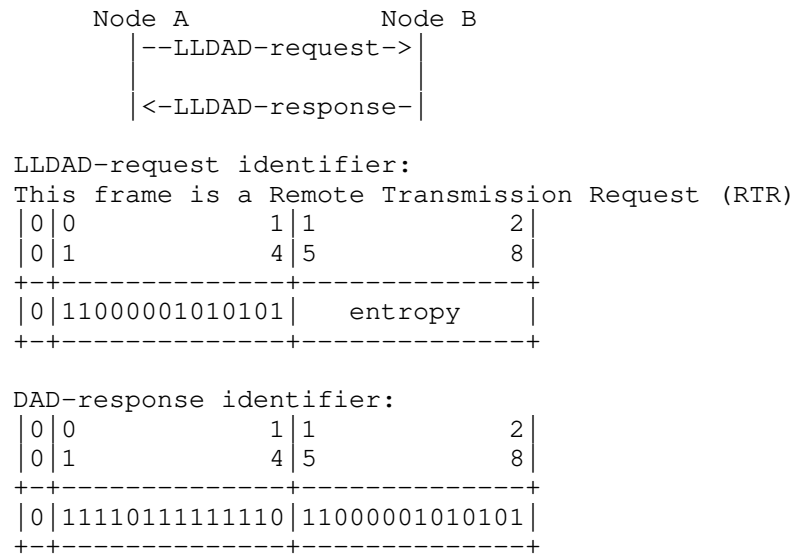


Figure 4: DAD Fail example

#### 4. Stateless Address Autoconfiguration

This section defines how to obtain an IPv6 Interface Identifier.

It is RECOMMENDED to form an IID derived from the node's address. IIDs generated from the node address result in most efficient IPHC header compression. However, IIDs MAY also be generated from other sources. The general procedure for creating an IID is described in Appendix A of [RFC4291], "Creating Modified EUI-64 Format Interface Identifiers", as updated by [RFC7136].

The Interface Identifier for link-local addresses SHOULD be formed by concatenating the node's 14-bit address to the six octets 0x00, 0x00, 0x00, 0xFF, 0xFE, 0x00 and two bits 0b00. For example, an address of hexadecimal value 0x3AAF results in the following IID:

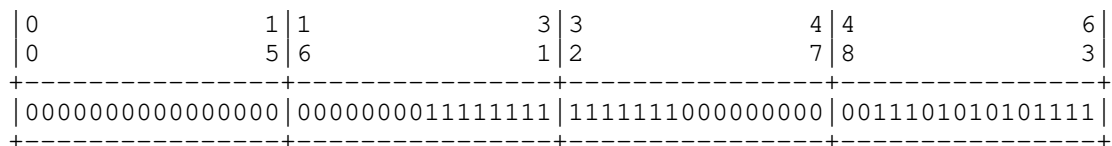


Figure 5: IID from Address 0x3AAF

## 5. IPv6 Link-Local Address

The IPv6 link-local address [RFC4291] for a 6LoCAN interface is formed by appending the Interface Identifier, as defined above, to the prefix FE80::/64.

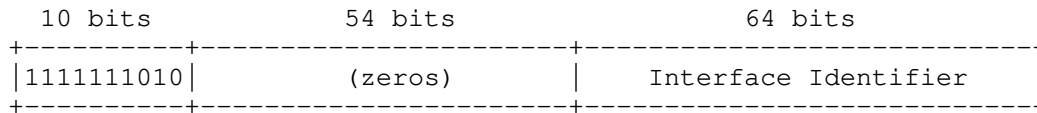


Figure 6: Link-Local address from IID

## 6. ISO-TP

This section provides information about the use of ISO-TP (ISO 15765-2) in this document. Parts of ISO-TP are used to provide a reliable way for sending up to 4095 octets as a packet. It includes a flow-control mechanism for unicast-packets and timeouts.

Multicast packets do not use any flow-control mechanism and are therefore not covered by the ISO-TP standard. However, the fragmentation and reassembly mechanism is still used for multicast packets.

ISO-TP defines four different types of frames: Single-Frames (SF), First-Frames (FF), Consecutive-Frames (CF), and Flow Control Frames (FC). Single-Frames are used when the payload data size is small enough to fit into a single CAN frame. For larger payload data sizes, a First-Frame indicates the start of the message, Consecutive-Frames carry the payload data and Flow Control Frames steer the transmission. Network address extension and packet size larger than 4095 octets defined by ISO 15765-2 MUST NOT be used for 6LoCAN. Single-Frame packets are only useful for CAN-FD because the eight octets of classical CAN are too small for any IPv6 header.

### 6.1. Multicast

Multicast packets MUST be transferred in a Single-Frame when the packet fits in a single frame. Multicast packets that are too big for Single-Frames start with a First-Frame (FF). The FF contains information about the entire payload data size and payload data bytes to fill the rest of the remaining frame. The First-Frame is followed by a break of 1 millisecond to allow the receivers to prepare for the data reception. Consecutive-Frames carry the rest of the payload data and a 4-bit sequence number to detect missing or out of order frames. The number of Consecutive-Frames depends on the CAN frame data size and the payload data size. Consecutive-Frames SHALL have

the maximum possible CAN data size. The last Consecutive-Frame may have to include padding at the end.

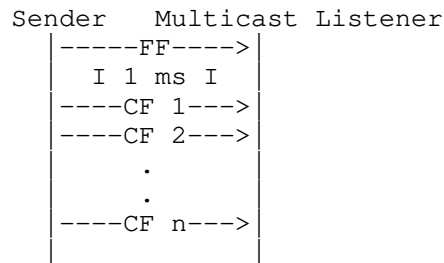


Figure 7: Multicast packet sequence

## 6.2. Unicast

Unicast transfers use the same format for First-Frames and Consecutive-Frames as the multicast transfer does. In contrast to multicast, unicast transfers use Flow-Control-Frames to steer the sender's behavior and signalize readiness.

The receiver can choose a block size and a minimum separation time (ST min).

The block size (BS) defines how many frames are transmitted before the sender MUST wait for another FC Frame. A zero BS is allowed and denotes that the sender MUST NOT wait for another FC Frame. ST min defines the minimal pause between the end of the previous frame and the start of the next frame. The receiver MAY change BS and ST min for following FC Frames.

The receiver MUST answer a FF within 1 second. After this timeout the sender SHOULD abort and stop waiting for an FC frame. CF frames MUST have a separation time less than or equal to one second. After this timeout, a receiver SHOULD abort and stop waiting for CF. Receivers and sender SHOULD handle more than one packet reception from different peers at the same time.

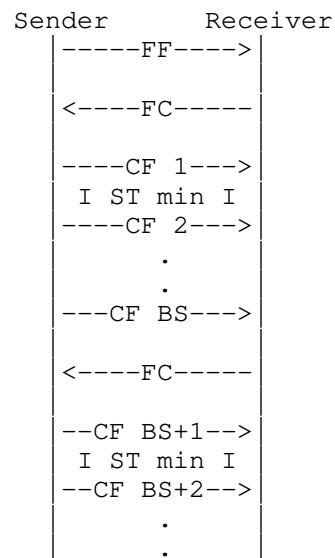


Figure 8: Unicast packet sequence.

### 6.3. Frame Format

The frame format of ISO-TP is described in this section.

The first 4 bits denote the Protocol Control Information (PCI). This information is used to distinguish the different frame types.

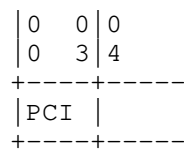


Figure 9: ISO-TP Frame format

Number	Description
0	Single-Frame
1	First-Frame
2	Consecutive-Frame
3	Flow-Control-Frame
4-15	Reserved

Table 2: PCI Numbers

#### 6.4. Single-Frame

The Single-Frame PCI is 0, and the rest of the octet is padded with 0. This format is compatible with ISO-TP with data size greater than 16 octets.

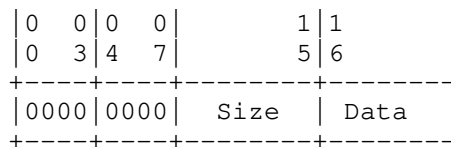


Figure 10: Single-Frame Format

Size : Number of payload data octets.

#### 6.5. First-Frame

The First-Frame PCI is 1, and the remaining 4-bit nibble of the first byte carries the upper 4-bit nibble of the payload data length. The second byte contains the lower byte of the payload data length. The rest of the frame is filled with payload data. The First-Frame MUST have a data length of the maximum CAN data length. For example, classic CAN has a maximum data length of 8 octets, and therefore six payload bytes are included in the FF.

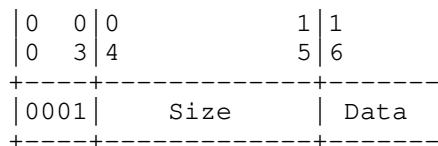


Figure 11: First-Frame Format

Size : Number of payload data octets

#### 6.6. Consecutive-Frame

The Consecutive-Frame PCI is two, and the remaining 4-bit nibble of the first byte carries an index. This index starts with one for the first CF and wraps around at 16. Then it starts at 0 again. The index is used to check for lost or out of order frames. When the index is not sequential, the reception MUST be aborted. The last Consecutive-Frame may have to include padding at the end to obtain a valid data length for CAN-FD frames. The RECOMMENDED padding value is 0xCC.

```

| 0  0 | 0  0 | 0
| 0  3 | 4  7 | 8
+-----+-----+-----+
| 0010 | Idx  | Data
+-----+-----+-----+
```

Figure 12: Consecutive-Frame Format

#### 6.7. Flow-Control-Frame

The Flow-Control-Frame PCI is three, and the remaining 4-bit nibble of the first byte carries a Flow-State (FS). The second byte is the block size, and the third byte is the ST min. The Flow-States are:

Number	Description
0	CTS (Continue To Send)
1	WAIT
2	OVFLW (Overflow)

Table 3: Flow-State

CTS advises the sender to continue sending CF frames.

WAIT resets the timeout for receiving an FC frame on the sender side. The sender SHOULD only accept a limited number of wait states and silently abort when reaching the limit.

OVFLW is sent when the receiver is running out of resources and can't handle the packet. The sender MUST abort when receiving an OVFLW Flow-State.

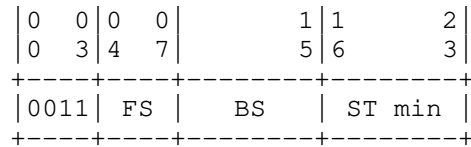


Figure 13: Flow-Control-Frame Format

FS : Frame State

BS : Block Size

ST min : Minimal Separation Time

## 7. Frame Format

This section provides information about data arrangement in the frame data field.

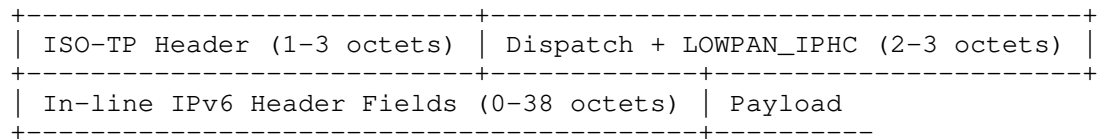


Figure 14: 6LoCAN Frame Format

Packets with a destination or source address of the 0x3DF0 (Translator address) carry the Ethernet MAC address inline directly after the ISO-TP Header. For packets destined for the translator, it is the destination MAC address, and for packets originated by the translator, it is the source MAC address.

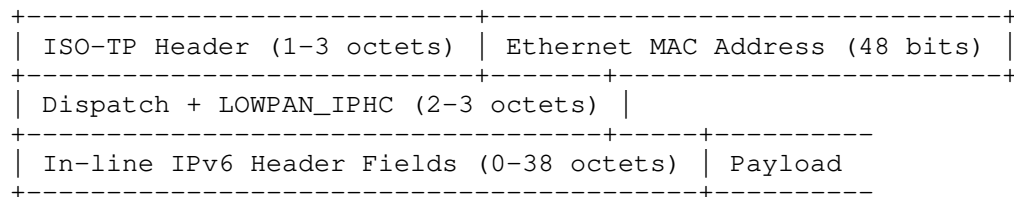


Figure 15: 6LoCAN Translator Frame Format



## 8. Ethernet Border Translator

This section provides information about translating 6LoCAN packets to Ethernet frames.

The Ethernet Border Translator connects 6LoCAN bus-segments either to other 6LoCAN bus-segments or other technologies. Ethernet is a widely used technology that provides enough bandwidth to connect several 6LoCAN segments. A mechanism like the 6LBR is not necessary because there is no routing on 6LoCAN segments. To provide routing or switching capabilities, the Ethernet Border Translator connects a 6LoCAN network to such devices via Ethernet.

Bus segments **MUST NOT** have more than one translator. The translator has a fixed node address (0x3DF0) and a range of Ethernet MAC addresses. Every packet sent to this node address or any multicast address is forwarded to Ethernet. Every Ethernet frame matching the MAC address range and every multicast Ethernet frame is forwarded to the 6LoCAN bus-segment.

For translating a 6LoCAN packet to an Ethernet frame, the source address is extended with the first 34 bits of the translator MAC address and the IPHC compressed headers are decompressed. The destination MAC is carried in-line before the compressed IPv6 header (see Section 7, Figure 15). ICMPv6 messages **MUST** be checked for Link-Layer Address Options (LLAO), and if an LLAO is present, it **MUST** be changed to the extended link-layer address. For translating Ethernet frames to 6LoCAN packets, the source MAC address is carried in-line, the destination node address is the last 14 bits of the MAC address, and the IPv6 headers are compressed using IPHC.

For multicast Ethernet frames, the last 14 bits of the multicast group is the destination address, and the multicast bit is set. The destination address **MAY** also be reconstructed from the destination multicast address. The destination Ethernet MAC address is formed from the destination IP address as described in [RFC2464] section 7.

If the translator includes a network stack, the translator **MUST NOT** use a MAC address within the ranges used for translation, with the following exception: The translator **MAY** use the extended MAC address that corresponds to the translator node address.

Figure 18 shows an example setup of a 6LoCAN segment connected to an Ethernet network.

Figure 16 shows a translation from Ethernet MAC to CAN identifier. The source (src) MAC address is carried in-line in the CAN frame

data. The translator MAC address for this example is 02:00:5E:10:3D:F0.

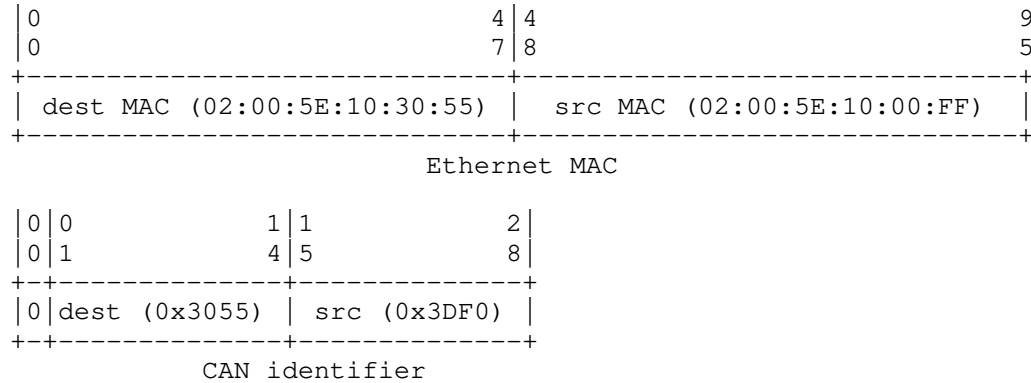


Figure 16: Example address translation from Ethernet MAC to CAN identifier.

Figure 17 shows a translation from a multicast Ethernet MAC to CAN identifier. The source MAC address is carried in-line in the CAN frame data.

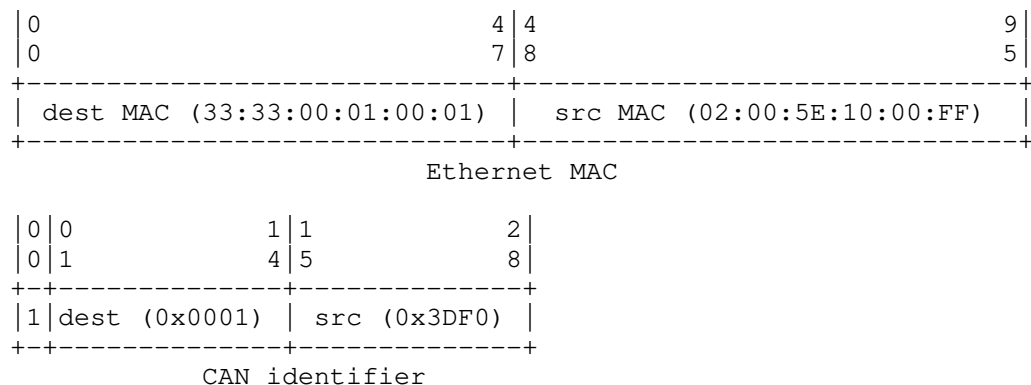


Figure 17: Example address translation from Ethernet to CAN for multicast Frames.

Section 8 shows a translation CAN identifier to Ethernet MAC. The destination (dest) MAC address is carried inline in the CAN frame data. The translator MAC address for this example is 02:00:5E:10:3D:F0.

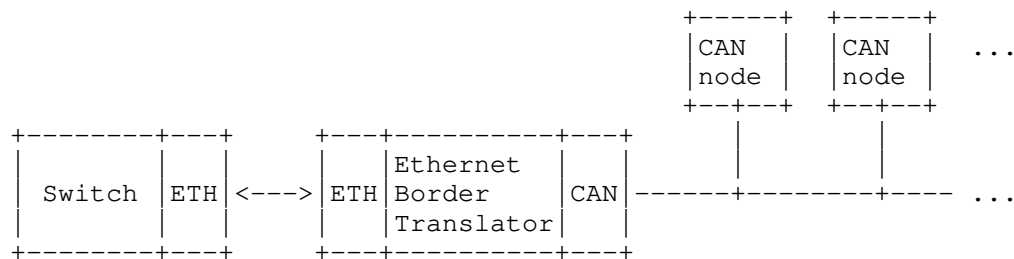
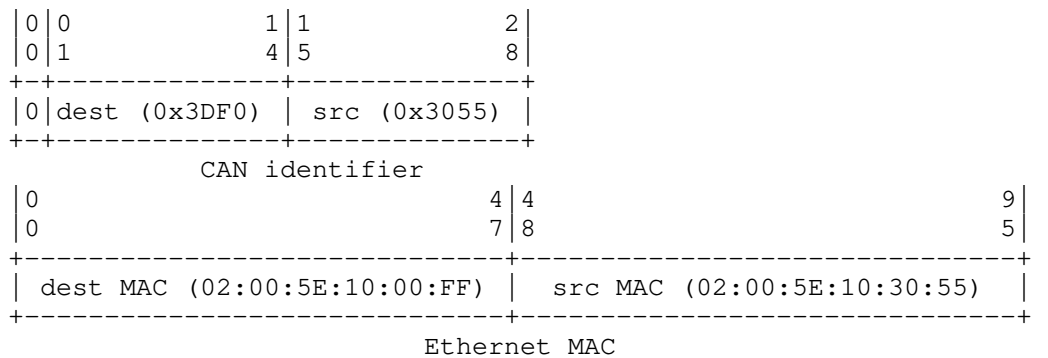


Figure 18: Example setup with Ethernet Border Translator

## 9. IANA Considerations

The MAC addresses generated by extending the node's address may be randomly generated and, therefore, MUST NOT set the UAA-bit.

## 10. Security Considerations

This document doesn't provide any security mechanisms. Traffic on the bus can be intersected, spoofed, or destroyed. For confidentiality and integrity, mechanisms like TLS or IPsec need to be applied.

The small 14-bit node address space makes it hard to track nodes globally and therefore has inherent privacy properties.

## 11. Reference Implementation

As a reference, this standard proposal is implemented in the Zephyr RTOS from version 2.0 ongoing. This implementation can be tested with the overlay-6locan.conf on echo\_server and echo\_client application.

## 12. 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, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <<https://www.rfc-editor.org/info/rfc2464>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://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, <<https://www.rfc-editor.org/info/rfc4861>>.
- [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, <<https://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, <<https://www.rfc-editor.org/info/rfc6282>>.
- [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <<https://www.rfc-editor.org/info/rfc7136>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

## Author's Address

Alexander Wachter  
Graz University of Technology

Email: [alexander@wachter.cloud](mailto:alexander@wachter.cloud)