

6lo Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: January 11, 2022

C. Gomez  
UPC  
A. Minaburo  
Acklio  
July 10, 2021

Transmission of SCHC-compressed packets over IEEE 802.15.4 networks  
draft-gomez-6lo-schc-15dot4-00

Abstract

A framework called Static Context Header Compression and fragmentation (SCHC) has been designed with the primary goal of supporting IPv6 over Low Power Wide Area Network (LPWAN) technologies [RFC8724]. One of the SCHC components is a header compression mechanism. If used properly, SCHC header compression allows a greater compression ratio than that achievable with traditional 6LoWPAN header compression [RFC6282]. For this reason, it may make sense to use SCHC header compression in some 6LoWPAN environments, including IEEE 802.15.4 networks. This document specifies how a SCHC-compressed packet can be carried over IEEE 802.15.4 networks.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <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 January 11, 2022.

Copyright Notice

Copyright (c) 2021 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. Terminology . . . . .	3
2.1. Requirements language . . . . .	3
2.2. Background on SCHC . . . . .	4
3. Architecture . . . . .	4
3.1. Network topologies . . . . .	4
3.2. Protocol stack . . . . .	4
4. Frame Format . . . . .	5
4.1. SCHC Dispatch . . . . .	6
4.2. Padding . . . . .	6
5. SCHC compression for IPv6, UDP, and CoAP headers . . . . .	6
6. Fragmentation and reassembly . . . . .	7
7. IANA Considerations . . . . .	7
8. Security Considerations . . . . .	7
9. Acknowledgments . . . . .	7
10. References . . . . .	7
10.1. Normative References . . . . .	7
10.2. Informative References . . . . .	8
Authors' Addresses . . . . .	8

## 1. Introduction

RFC 6282 is the main specification for IPv6 over Low power Wireless Personal Area Network (6LoWPAN) IPv6 header compression [RFC6282]. This RFC was designed assuming IEEE 802.15.4 as the layer below the 6LoWPAN adaptation layer, and it has also been reused (with proper adaptations) for IPv6 header compression over many other technologies relatively similar to IEEE 802.15.4 in terms of characteristics such as physical layer bit rate, layer 2 maximum payload size, etc. Examples of such technologies comprise BLE, DECT-ULE, ITU G.9959, MS/TP, NFC, and PLC. RFC 6282 provides additional functionality, such as a mechanism for UDP header compression.

In the best cases, RFC 6282 allows to compress a 40-byte IPv6 header down to a 2-byte compressed header (for link-local interactions) or a 3-byte compressed header (when global IPv6 addresses are used). On the other hand, an RFC 6282 compressed UDP header has a typical size of 4 bytes. Therefore, in advantageous conditions, a 48-byte uncompressed IPv6/UDP header may be compressed down to a 6-byte

format (when using link-local addresses) or a 7-byte format (for global interactions) by using RFC 6282.

Recently, a framework called Static Context Header Compression (SCHC) has been designed with the primary goal of supporting IPv6 over Low Power Wide Area Network (LPWAN) technologies [RFC8724]. SCHC comprises header compression and fragmentation functionality tailored to the extraordinary constraints of LPWAN technologies, which are more severe than those exhibited by IEEE 802.15.4 or other relatively similar technologies. SCHC header compression allows a greater compression ratio than that of RFC 6282. If used properly, SCHC allows to compress an IPv6/UDP header down to e.g. a single byte. In addition, SCHC can be used to compress Constrained Application Protocol (CoAP) headers as well [RFC7252][RFC8824], which further increases the achievable performance improvement of using SCHC header compression, since there is no 6LoWPAN header compression defined for CoAP. Therefore, it may make sense to use SCHC header compression in some 6LoWPAN environments [I-D.toutain-6lo-6lo-and-schc], including IEEE 802.15.4 networks, considering its greater efficiency.

If SCHC header compression is added to the panoply of header compression mechanisms used in 6LoWPAN environments, then there is a need to signal when a packet header has been compressed by using SCHC. To this end, in its current form, the present document specifies a 6LoWPAN Dispatch Type for SCHC header compression, based on exploiting RFC 8025 Dispatch type space [RFC8025].

This document specifies how a SCHC-compressed packet can be carried over IEEE 802.15.4 networks. Note that, as per this document, and while SCHC defines fragmentation mechanisms as well, 6LoWPAN/6Lo fragmentation is used when necessary to transport SCHC-compressed packets over IEEE 802.15.4 networks [RFC4944][RFC8931].

TO-DO: indicate here any specific updates of RFC 8724 for IEEE 802.15.4.

## 2. Terminology

### 2.1. Requirements language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP14 [RFC2119], [RFC8174], when, and only when, they appear in all capitals, as shown here.

## 2.2. Background on SCHC

The reader is expected to be familiar with the terms and concepts defined in the specification of SCHC (RFC 8724).

## 3. Architecture

### 3.1. Network topologies

IEEE 802.15.4 supports two main network topologies: the star topology, and the peer-to-peer (i.e., mesh) topology.

SCHC has been designed for LPWAN technologies, which are typically based on a star topology where constrained devices (e.g., sensors) communicate with a less constrained, central network gateway [RFC 8376]. However, as stated in [draft-ietf-lpwan-architecture], SCHC is generic and it can also be used in networking environments beyond the ones originally considered for SCHC.

SCHC compression is applicable to both star topology and mesh topology IEEE 802.15.4 networks.

### 3.2. Protocol stack

The traditional 6LoWPAN-based protocol stack for constrained devices (Figure 1, left) places the 6LoWPAN adaptation layer between IPv6 and an underlying technology such as IEEE 802.15.4. Suitable upper layer protocols include CoAP [RFC7252] and UDP. (Note that, while CoAP has also been specified over TCP, and TCP may play a significant role in IoT environments [RFC9006], 6LoWPAN header compression has not been defined for TCP.)

6LoWPAN can be envisioned as a set of two main sublayers, where the upper one provides header compression, while the lower one offers fragmentation.

This document defines an alternative approach for packet header compression over IEEE 802.15.4, which leads to a modified protocol stack (Figure 1, right).

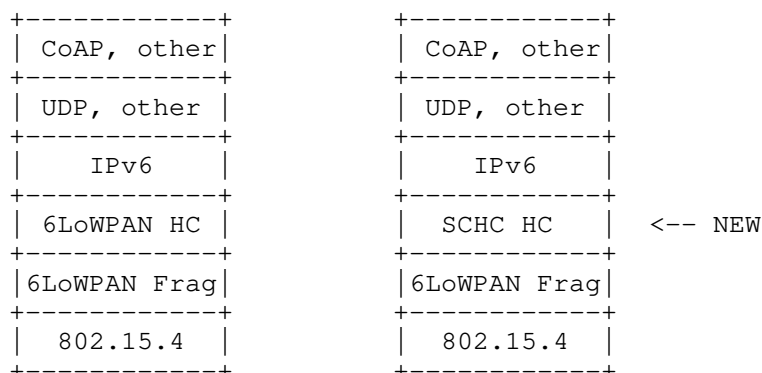


Figure 1: Traditional 6LoWPAN-based protocol stack over IEEE 802.15.4 (left) and alternative protocol stack using SCHC for header compression (right). HC and Frag stand for Header Compression and Fragmentation, respectively.

SCHC header compression may be applied to the headers of different protocols or sets of protocols. Some examples include: i) IPv6 packet headers, ii) joint IPv6 and UDP packet headers, iii) joint IPv6, UDP and CoAP packet headers, etc.

#### 4. Frame Format

This document defines the frame format to be used when a SCHC-compressed packet is carried over IEEE 802.15.4. Such format is carried as IEEE 802.15.4 frame payload. The format comprises a SCHC Dispatch Type, a SCHC Packet (i.e. a SCHC-compressed packet (RFC 8724), and Padding bits, if any). Figure 2 illustrates the described frame format.

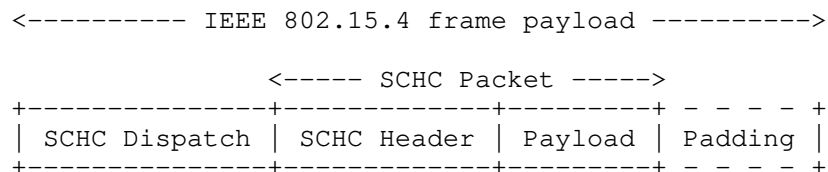


Figure 2: Encapsulated, SCHC-compressed packet. Padding bits are added if needed.

#### 4.1. SCHC Dispatch

Adding SCHC header compression to the panoply of header compression mechanisms used in 6LoWPAN/6Lo environments creates the need to signal when a packet header has been compressed by using SCHC. To this end, the present document specifies the SCHC Dispatch. The SCHC Dispatch indicates that the next field in the frame format is a SCHC-compressed header. The latter corresponds to a packet header that has been compressed by using SCHC. As defined in [RFC8724], the SCHC Header comprises a RuleID, and a compression residue.

This document defines the SCHC Dispatch as a 6LoWPAN Dispatch Type for SCHC header compression, based on exploiting RFC 8025 Dispatch type space and the concept of "pages" [RFC8025]. With the aim to minimize overhead, the present document allocates a whole page (Page 2) for the SCHC Dispatch Type:

SCHC Dispatch Type bit pattern: 11110010 (Page 2) (Note: to be confirmed by IANA))

TO-DO: RuleID discussion

#### 4.2. Padding

If SCHC header compression leads to a SCHC Packet size of a non-integer number of bytes, padding bits of value equal to zero MUST be appended to the SCHC Packet as appropriate to align to an octet boundary.

#### 5. SCHC compression for IPv6, UDP, and CoAP headers

SCHC header compression may be applied to the headers of different protocols or sets of protocols. Some examples include: i) IPv6 packet headers, ii) joint IPv6 and UDP packet headers, iii) joint IPv6, UDP and CoAP packet headers, etc.

IPv6 and UDP header fields MUST be compressed as per Section 10 of RFC 8724.

TO-DO: adaptation of DevIID and AppIID in 802.15.4 environments

CoAP header fields MUST be compressed as per Sections 4 to 6 of RFC 8824.

TO-DO: provide examples for IPv6-only, IPv6/UDP and IPv6/UDP/CoAP.

## 6. Fragmentation and reassembly

After applying SCHC header compression to a packet intended for transmission, if the size of the resulting frame format (Section 4) exceeds the IEEE 802.15.4 frame payload space available, such frame format MUST be fragmented, carried and reassembled by means of 6LoWPAN fragmentation and reassembly [RFC4944][RFC8931].

## 7. IANA Considerations

This document requests the allocation of the Dispatch Type Field bit pattern 11110010 (Page 2) as SCHC Dispatch Type.

## 8. Security Considerations

TBD

## 9. Acknowledgments

Ana Minaburo and Laurent Toutain suggested for the first time the use of SCHC in environments where 6LoWPAN has traditionally been used. Laurent Toutain made comments that helped shape this document.

Carles Gomez has been funded in part by the Spanish Government through project PID2019-106808RA-I00, and by Secretaria d'Universitats i Recerca del Departament d'Empresa i Coneixement de la Generalitat de Catalunya 2017 through grant SGR 376.

## 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>>.
- [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>>.

- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <<https://www.rfc-editor.org/info/rfc7252>>.
- [RFC8025] Thubert, P., Ed. and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch", RFC 8025, DOI 10.17487/RFC8025, November 2016, <<https://www.rfc-editor.org/info/rfc8025>>.
- [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>>.
- [RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <<https://www.rfc-editor.org/info/rfc8724>>.
- [RFC8824] Minaburo, A., Toutain, L., and R. Andreasen, "Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)", RFC 8824, DOI 10.17487/RFC8824, June 2021, <<https://www.rfc-editor.org/info/rfc8824>>.
- [RFC8931] Thubert, P., Ed., "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Selective Fragment Recovery", RFC 8931, DOI 10.17487/RFC8931, November 2020, <<https://www.rfc-editor.org/info/rfc8931>>.

## 10.2. Informative References

- [I-D.toutain-6lo-6lo-and-schc] Minaburo, A. and L. Toutain, "Comparison of 6lo and SCHC", draft-toutain-6lo-6lo-and-schc-00 (work in progress), November 2019.
- [RFC9006] Gomez, C., Crowcroft, J., and M. Scharf, "TCP Usage Guidance in the Internet of Things (IoT)", RFC 9006, DOI 10.17487/RFC9006, March 2021, <<https://www.rfc-editor.org/info/rfc9006>>.

Authors' Addresses



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

Email: carlesgo@entel.upc.edu

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

Email: ana@ackl.io

6Lo Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 13, 2022

Y-G. Hong  
Daejeon University  
C. Gomez  
UPC  
Y-H. Choi  
ETRI  
AR. Sangi  
Huaiyin Institute of Technology  
S. Chakrabarti  
July 12, 2021

IPv6 over Constrained Node Networks (6Lo) Applicability & Use cases  
draft-ietf-6lo-use-cases-11

## Abstract

This document describes the applicability of IPv6 over constrained node networks (6Lo) and provides practical deployment examples. In addition to IEEE Std 802.15.4, various link layer technologies such as ITU-T G.9959 (Z-Wave), Bluetooth Low Energy, DECT-ULE, MS/TP, NFC, and PLC are used as examples. The document targets an audience who would like to understand and evaluate running end-to-end IPv6 over the constrained node networks for local or Internet connectivity.

## 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 January 13, 2022.

## Copyright Notice

Copyright (c) 2021 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. 6lo Link layer technologies . . . . .	4
2.1. ITU-T G.9959 . . . . .	4
2.2. Bluetooth LE . . . . .	4
2.3. DECT-ULE . . . . .	5
2.4. MS/TP . . . . .	5
2.5. NFC . . . . .	6
2.6. PLC . . . . .	6
2.7. Comparison between 6lo link layer technologies . . . . .	8
3. Guidelines for adopting IPv6 stack (6lo) . . . . .	9
4. 6lo Deployment Scenarios . . . . .	11
4.1. Wi-SUN usage of 6lo in network layer . . . . .	11
4.2. Thread usage of 6lo in network layer . . . . .	12
4.3. G3-PLC usage of 6lo in network layer . . . . .	13
4.4. Netricity usage of 6lo in network layer . . . . .	14
5. 6lo Use Case Examples . . . . .	15
5.1. Use case of ITU-T G.9959: Smart Home . . . . .	15
5.2. Use case of Bluetooth LE: Smartphone-based Interaction . . . . .	16
5.3. Use case of DECT-ULE: Smart Home . . . . .	16
5.4. Use case of MS/TP: Building Automation Networks . . . . .	17
5.5. Use case of NFC: Alternative Secure Transfer . . . . .	18
5.6. Use case of PLC: Smart Grid . . . . .	18
6. IANA Considerations . . . . .	19
7. Security Considerations . . . . .	19
8. Acknowledgements . . . . .	20
9. Informative References . . . . .	20
Appendix A. Design Space Dimensions for 6lo Deployment . . . . .	26
Authors' Addresses . . . . .	27

## 1. Introduction

Running IPv6 on constrained node networks presents challenges, due to the characteristics of these networks such as small packet size, low power, low bandwidth, low cost, and large number of devices, among others [RFC4919][RFC7228]. For example, many IEEE Std 802.15.4 variants [IEEE802154] exhibit a frame size of 127 octets, whereas

IPv6 requires its underlying layer to support an MTU of 1280 bytes. Furthermore, those IEEE Std 802.15.4 variants do not offer fragmentation and reassembly functionality. (It is noted that IEEE Std 802.15.9-2016 provides multiplexing and fragmentation layer for the IEEE Std 802.15.4[IEEE802159].) Therefore, an appropriate adaptation layer supporting fragmentation and reassembly must be provided below IPv6. Also, the limited IEEE Std 802.15.4 frame size and low energy consumption requirements motivate the need for packet header compression. The IETF IPv6 over Low-Power WPAN (6LoWPAN) working group published a suite of specification that provide an adaptation layer to support IPv6 over IEEE Std 802.15.4 comprising the following functionality:

- o Fragmentation and reassembly, address autoconfiguration, and a frame format [RFC4944],
- o IPv6 (and UDP) header compression [RFC6282],
- o Neighbor Discovery Optimization for 6LoWPAN [RFC6775][RFC8505].

As Internet of Things (IoT) services become more popular, the IETF 6lo working group [IETF\_6lo] has defined adaptation layer functionality to support IPv6 over various link layer technologies other than IEEE Std 802.15.4, 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). The 6lo adaptation layers use a variation of the 6LoWPAN stack applied to each particular link layer technology.

The 6LoWPAN working group produced the document entitled "Design and Application Spaces for 6LoWPANs" [RFC6568], which describes potential application scenarios and use cases for low-power wireless personal area networks. The present document aims to provide guidance to an audience who are new to the IPv6 over constrained node networks (6lo) concept and want to assess its application to the constrained node network of their interest. This 6lo applicability document describes a few sets of practical 6lo deployment scenarios and use cases examples. In addition, it considers various network design space dimensions such as deployment, network size, power source, connectivity, multi-hop communication, traffic pattern, security level, mobility, and QoS requirements etc.

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

- o It covers various IoT-related wired/wireless link layer technologies providing practical information of such technologies.

- o It provides a general guideline on how the 6LoWPAN stack can be modified for a given L2 technology.
- o Various 6lo use cases and practical deployment examples are described.

## 2. 6lo Link layer technologies

### 2.1. ITU-T G.9959

The ITU-T G.9959 Recommendation [G.9959] targets low-power Wireless Personal Area Networks (WPANs), 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.

### 2.2. Bluetooth LE

Bluetooth LE was introduced in Bluetooth 4.0, enhanced in Bluetooth 4.1, and developed further in successive versions. Bluetooth SIG has also published the 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 versions 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. 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]

### 2.3. 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 physical layer operating at frequencies in the dedicated 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 Medium Access Control (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.

### 2.4. MS/TP

MS/TP is a 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 Universal Asynchronous Receiver-Transmitter (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].

## 2.5. 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).

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.

## 2.6. PLC

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

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	<12MHz	PLC-IoT	10Mbps	2000m
IEEE1901.2	<500kHz	Narrowband	200kbps	3000m
G3-PLC	<500kHz	Narrowband	234kbps	3000m

Table 1: Some Available Open Standards in PLC

IEEE Std 1901 [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 Orthogonal Frequency Division Multiplexing (OFDM) modulation.

IEEE Std 1901.1 [IEEE1901.1] defines a medium frequency band (less than 12 MHz) broadband PLC technology for smart grid applications based on OFDM. By achieving an extended communication range with medium speeds, this standard can be applied both in indoor and outdoor scenarios, such as Advanced Metering Infrastructure (AMI), street lighting, electric vehicle charging, smart city etc.

IEEE Std 1901.2 [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 Std 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.

G3-PLC [G3-PLC] is a narrowband PLC technology that is based on the ITU-T G.9903 Recommendation [G.9903]. The ITU-T G.9903 Recommendation contains the physical layer and data link layer specification for the G3-PLC narrowband OFDM power line communication transceivers, for communications via alternating current and direct current electric power lines over frequencies below 500 kHz.



## 2.7. Comparison between 6lo link layer technologies

In above clauses, various 6lo link layer technologies are described. The following table shows 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, ietf-6lo-blemesh	RFC8105	RFC8163	draft-ietf-6lo-nfc	draft-ietf-6lo-plc

Table 2: Comparison between 6lo link layer technologies

### 3. Guidelines for adopting IPv6 stack (6lo)

6lo aims at reusing and/or adapting existing 6LoWPAN functionality in order to efficiently support IPv6 over a variety of IoT L2 technologies. The following guideline targets new candidate constrained L2 technologies that may be considered for running a 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. 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 addresses, 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 packet maximum transmission unit (MTU) needs 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 the 6LoWPAN layer may not need to support 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 provide mechanisms to support mesh routing at L2, a configuration called mesh-under [RFC6606]. It is also possible to use an L3 routing protocol in 6LoWPAN, an approach known as route-over. [RFC6550] defines RPL, a L3 routing protocol for low power and lossy networks using directed acyclic graphs. 6LoWPAN is routing-protocol-agnostic and does not specify any particular L2 or L3 routing protocol to use with a 6LoWPAN stack.
- o Address Assignment: 6LoWPAN developed a new version of IPv6 Neighbor Discovery [RFC4861][RFC4862]. 6LoWPAN Neighbor Discovery [RFC6775][RFC8505] inherits from IPv6 Neighbor Discovery for mechanisms such as Stateless Address Autoconfiguration (SLAAC) and Neighbor Unreachability Detection (NUD). 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 [RFC9008]. 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 Internet connectivity. For local-only connectivity IPv6 Unique Local Address (ULA) may be used. [RFC6775][RFC8505] specifies the 6LoWPAN border router (6LBR), which is responsible for prefix assignment to the 6LoWPAN network. A 6LBR can be connected to the Internet or to an enterprise network via 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 IPv6 address autoconfiguration due to regulatory and business reasons and may choose to offer a separate address assignment service. Address Protection for 6LoWPAN Neighbor Discovery (AP-ND) [RFC8928] enables Source Address Validation [RFC6620] and protects the address ownership against impersonation attacks.

- o **Broadcast Avoidance:** 6LoWPAN Neighbor Discovery aims at reducing the amount of multicast traffic of classical Neighbor Discovery, since IP-level multicast translates into L2 broadcast in many L2 technologies. 6LoWPAN Neighbor Discovery relies on a proactive registration to avoid the use of multicast for address resolution. It also uses a unicast method for Duplicate Address Detection (DAD), and avoids multicast lookups from all nodes by using non-onlink prefixes. Router Advertisements (RAs) are also sent in unicast, in response to Router Solicitations (RSs)
- o **Host-to-Router interface:** 6lo has defined registration extensions for 6LoWPAN Neighbor Discovery [RFC8505]. This effort provides a host-to-router interface by which a host can request its router to ensure reachability for the address registered with the router. Note that functionality has been developed to ensure that such a host can benefit from routing services in a RPL network [RFC9010]
- o **Proxy Neighbor Discovery:** Further functionality also allows a device (e.g. an energy-constrained device that needs to sleep most of the time) to request proxy Neighbor Discovery services from a 6LoWPAN Backbone Router (6BBR) [RFC8505][RFC8929]. The latter federates a number of links into a multilink subnet.
- o **Header Compression:** IPv6 header compression [RFC6282] is a vital part of IPv6 over low power communication. Examples of header compression over different link-layer specifications are found in

[RFC7668], [RFC8163], [RFC8105]. A generic header compression technique is specified in [RFC7400]. For 6LoWPAN networks where RPL is the routing protocol, there exist 6LoWPAN header compression extensions which allow to compress also the RPL artifacts used when forwarding packets in the route-over mesh [RFC8138] [RFC9035]

- 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 [RFC8928] 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.

#### 4. 6lo Deployment Scenarios

##### 4.1. Wi-SUN usage of 6lo in network layer

Wireless Smart Ubiquitous Network (Wi-SUN) [Wi-SUN] is a technology based on the IEEE Std 802.15.4g standard. Wi-SUN networks support star and mesh topologies, as well as hybrid star/mesh deployments, but these are typically laid out in a mesh topology where each node relays data for the network to provide network connectivity. Wi-SUN networks are deployed on both powered and battery-operated devices [RFC8376].

The main application domains targeted by Wi-SUN are smart utility and smart city networks. This includes, but is not limited to the following applications:

- o Advanced Metering Infrastructure
- o Distribution Automation
- o Home Energy Management
- o Infrastructure Management

- o Intelligent Transportation Systems
- o Smart Street Lighting
- o Agriculture
- o Structural health (bridges, buildings)
- o Monitoring and Asset Management
- o Smart Thermostats, Air Conditioning and Heat Controls
- o Energy Usage Information Displays

The Wi-SUN Alliance Field Area Network (FAN) covers primarily outdoor networks, and its specification is oriented towards meeting the more rigorous challenges of these environments. It has the following features:

- o Open standards based on IEEE802, IETF, TIA, ETSI
- o Architecture based on an IPv6 frequency hopping wireless mesh network with enterprise-level security
- o Simple infrastructure of low cost, low complexity
- o Enhanced network robustness, reliability, and resilience to interference, due to high redundancy and frequency hopping
- o Enhanced scalability, long range, and energy friendliness
- o Supports multiple global license-exempt sub-GHz bands
- o Multi-vendor interoperability
- o Very low power modes in development permitting long term battery operation of network nodes

The Wi-SUN FAN specification defines an IPv6-based protocol suite including TCP/UDP, IPv6, 6lo adaptation layer, DHCPv6 for IPv6 address management, RPL, and ICMPv6.

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

Thread is an IPv6-based networking protocol stack built on open standards, designed for smart home environments, and based on low-power IEEE Std 802.15.4 mesh networks. Because of its IPv6 foundation, Thread can support existing popular application layers

and IoT platforms, provide end-to-end security, ease development and enable flexible and future-proof designs [Thread].

The Thread specification uses the IEEE Std 802.15.4 [IEEE802154] physical and MAC layers operating at 250 kbps in the 2.4 GHz band.

Thread devices use 6LoWPAN, as defined in [RFC4944][RFC6282], for transmission of IPv6 Packets over IEEE Std 802.15.4 networks. Header compression is used within the Thread network and devices transmitting messages compress the IPv6 header to minimize the size of the transmitted packet. The mesh header is supported for link-layer (i.e., mesh under) forwarding. The mesh header as used in Thread also allows efficient end-to-end fragmentation of messages rather than the hop-by-hop fragmentation specified in [RFC4944]. Mesh under routing in Thread is based on a distance vector protocol in a full mesh topology.

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

G3-PLC [G3-PLC] is a narrowband PLC technology that is based on the ITU-T G.9903 Recommendation [G.9903]. G3-PLC supports multi-hop mesh network topology, 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 narrowband 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
- 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].

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

The Netricity program in HomePlug Powerline Alliance [NETRICITY] promotes the adoption of products built on the IEEE Std 1901.2 low-frequency narrowband 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 physical and MAC layers of IEEE Std 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 L3 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. 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 section, various 6lo use cases which are based on different link layer technologies are described.

### 5.1. 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. turning off a light). 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].



## 5.2. 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. 6lo enables this use case by providing efficient end-to-end IPv6 support. 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.

## 5.3. 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. Since DECT-ULE uses dedicated bandwidth, it avoids the coexistence issues suffered by other technologies that use e.g. ISM frequency bands.

#### 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.

#### 5.4. 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. Note that BACnet comprises various networking solutions other than MS/TP, including the recently emerged BACnet IP. However, the latter is based on high speed Ethernet infrastructure, and thus it falls outside of the constrained node network scope.

#### 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-sight restrictions or hop-by-hop latency of many low cost wireless solutions.

#### 5.5. Use case of NFC: Alternative Secure Transfer

In different applications, a variety of secured data can be handled and transferred. Depending on the security level of the data, different transfer methods 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. A 6LBR 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. Hidden hackers can overhear the data based on the LTE connection, but they cannot gather the personal data over the NFC connection.

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

The smart grid concept is based on deploying numerous operational and energy measuring sub-systems in an electricity grid system. It comprises multiple administrative levels/segments to provide connectivity among these numerous components. Last mile connectivity is established over the Low Voltage (LV) segment, whereas connectivity over electricity distribution takes place in the High Voltage (HV) segment. Smart grid systems include Advanced Metering Infrastructure (AMI), Demand Response (DR), Home Energy Management System (HEMS), Wide Area Situational Awareness (WASA), among others.

Although other wired and wireless technologies are also used in Smart Grid, PLC enjoys the advantage of reliable data communication over electrical power lines that are already present, and the deployment cost can be comparable to wireless technologies. The 6lo-related scenarios for PLC mainly lie in the LV 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 (IEEE Std 1901.1) for WASA in Smart Grid

Many sub-systems of Smart Grid require low data rate and narrowband variants (e.g., IEEE Std 1901.1) of PLC fulfill 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.

## 6. IANA Considerations

There are no IANA considerations related to this document.

## 7. Security Considerations

Security considerations are not directly applicable to this document. For the use cases, the security requirements described in the protocol specifications apply.

## 8. Acknowledgements

Carles Gomez has been funded in part by the Spanish Government through the Jose Castillejo CAS15/00336 grant, the TEC2016-79988-P grant, and the PID2019-106808RA-I00 grant, and by Secretaria d'Universitats i Recerca del Departament d'Empresa i Coneixement de la Generalitat de Catalunya 2017 through grant SGR 376. 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, Jianqiang Hou, Kerry Lynn, S.V.R. Anand, and Seyed Mahdi Darroudi 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. Take Aanstoot, 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.

## 9. Informative References

- [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)>.
- [G.9903] "International Telecommunication Union, "Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks", ITU-T Recommendation", August 2017.
- [G.9959] "International Telecommunication Union, "Short range narrow-band digital radiocommunication transceivers - PHY and MAC layer specifications", ITU-T Recommendation", January 2015.
- [G3-PLC] "G3-PLC Alliance", <<http://www.g3-plc.com/home/>>.

- [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>>.
- [IEEE1901.1]  
"IEEE Standard, IEEE Std 1901.1-2018 - IEEE Standard for Medium Frequency (less than 12 MHz) Power Line Communications for Smart Grid Applications", 2018,  
<<https://ieeexplore.ieee.org/document/8360785>>.
- [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>>.
- [IEEE802154]  
IEEE standard for Information Technology, "IEEE Standard for Low-Rate Wireless Networks".
- [IEEE802159]  
IEEE standard for Information Technology, "IEEE Std 802.15.9-2016 - IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams".
- [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-10 (work in progress), April 2021.
- [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-17 (work in progress),  
August 2020.
- [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-06 (work in progress), April 2021.

- [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/>>.
- [Wi-SUN] "Wi-SUN Alliance", <<http://www.wi-sun.org>>.
- [Thread] "Thread Group", <<https://www.threadgroup.org/Support>>.
- [NETRICITY] "Netricity program in HomePlug Powerline Alliance",  
<<http://groups.homeplug.org/tech/Netricity>>.
- [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>>.
- [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>>.
- [RFC6606] Kim, E., Kaspar, D., Gomez, C., and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing", RFC 6606, DOI 10.17487/RFC6606, May 2012, <<https://www.rfc-editor.org/info/rfc6606>>.
- [RFC6620] Nordmark, E., Bagnulo, M., and E. Levy-Abegnoli, "FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses", RFC 6620, DOI 10.17487/RFC6620, May 2012, <<https://www.rfc-editor.org/info/rfc6620>>.
- [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. Poppa, "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>>.
- [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>>.
- [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>>.
- [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>>.

- [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>>.
- [RFC8376] Farrell, S., Ed., "Low-Power Wide Area Network (LPWAN) Overview", RFC 8376, DOI 10.17487/RFC8376, May 2018, <<https://www.rfc-editor.org/info/rfc8376>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.
- [RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November 2020, <<https://www.rfc-editor.org/info/rfc8928>>.
- [RFC8929] Thubert, P., Ed., Perkins, C., and E. Levy-Abegnoli, "IPv6 Backbone Router", RFC 8929, DOI 10.17487/RFC8929, November 2020, <<https://www.rfc-editor.org/info/rfc8929>>.
- [RFC9008] Robles, M., Richardson, M., and P. Thubert, "Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane", RFC 9008, DOI 10.17487/RFC9008, April 2021, <<https://www.rfc-editor.org/info/rfc9008>>.
- [RFC9010] Thubert, P., Ed. and M. Richardson, "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves", RFC 9010, DOI 10.17487/RFC9010, April 2021, <<https://www.rfc-editor.org/info/rfc9010>>.
- [RFC9035] Thubert, P., Ed. and L. Zhao, "A Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration Option for the 6LoWPAN Routing Header", RFC 9035, DOI 10.17487/RFC9035, April 2021, <<https://www.rfc-editor.org/info/rfc9035>>.
- [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)>.

## 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  
Daejeon University  
62 Daehak-ro, Dong-gu  
Daejeon 34520  
Korea

Phone: +82 42 280 4841  
Email: yonggeun.hong@gmail.com

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 34129  
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

Samita Chakrabarti  
San Jose, CA  
USA

Email: samitac.ietf@gmail.com

Internet Area Working Group  
Internet-Draft  
Intended status: Experimental  
Expires: 11 January 2022

G. Li  
Huawei  
10 July 2021

Native Short Address for Internet Expansion  
draft-li-native-short-address-00

Abstract

This document specifies mechanisms of NSA (Native Short Address) that enables IP packet transmission over links where the transmission of a full length address may be wasteful. All descriptions will focus on carrying IP packets across LLN (Low power and Lossy Networks), those LLNs positioned as limited domains. The specifications include NSA allocation, routing with NSA, header format design including length-variable fields, and how to access full IPv6 networks.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <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 11 January 2022.

Copyright Notice

Copyright (c) 2021 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 . . . . .	4
3. Overview . . . . .	4
4. NSA Allocation . . . . .	5
5. Routing in a NSA Network . . . . .	6
5.1. Routing within the NSA limited domain . . . . .	6
5.2. Routing between NSA and IPv6 domains . . . . .	7
6. NSA Header Format . . . . .	7
7. IANA Considerations . . . . .	9
8. Security Considerations . . . . .	9
9. References . . . . .	9
9.1. Normative References . . . . .	9
9.2. Informative References . . . . .	10
Author's Address . . . . .	10

## 1. Introduction

There is an ongoing massive expansion of the network edge that is driven by the "Internet of Things" (IoT) technology, especially over low-power links which often, in the past, didn't support IP packet transmission. Particularly driven by the requirements stemming from Industry 4.0 and Smart City deployments, more and more devices/things need to connect to each other and the Internet. Comparing with traditional scenarios, scalability of the (edge) network along with lower power consumption are key technical requirements. Moreover, large-scale LLN expect optimization for IP packet transmission over its low-power links, together with an efficient access to IPv6 domains.

The work in [SIXLOWPAN]/[SIXLO]/[LPWAN] Working Groups addresses many foundational issues for those type of deployments. These deployments can be considered an instantiation of what [RFC8799] calls "limited domains". For instance, the 6lowpan compression technology ([RFC4944] and [RFC6282]) addresses the problem of IPv6 transmission over low-power packet loss networks, making it possible to connect IoT networks to Internet via IPv6. For routing, [RFC8138] introduces a framework for implementing multi-hop routing on an LLN

using compressed routing headers and RPLs. This technique enables the ability to route IPv6 packets within the domain without decompressing it. In addition, SCHC [RFC8724] utilizes a context mechanism to make headers very small through compression.

On the basis of this previous work, the NSA technique would optimize networking of devices within IoT and towards the Internet. It is independent from stateless address assignment that depends on specific link-layer conventions. Also, it is different from stateful address allocation that requires all nodes to obtain addresses from a centralized DHCPv6 server, which would lead to long network startup time and consumption of extra bandwidth resources. Comparing to RPL-based routing [RFC6550], NSA will avoid the extra overhead of RPI (RPL Information) encapsulation. NSA routing does not need to spread routing messages to establish the node-local routing table; such diffusion action would consume too much network resources, thus not being suitable for large networks that consist of many nodes.

Moreover, NSA is a context-independent mechanism. Thus, it is possible to support simpler, dynamic, and efficient forwarding. In the best case, the NSA packet header size is smaller than LOWPAN\_IPHC's 7 octets, see Figure 1. Considering context-based and stateless address configuration is not appropriate for this the scenario proposed in this document, 7 octets is the smallest size that LOWPAN\_IPHC can achieve without those conditions, instead of 3 octets.

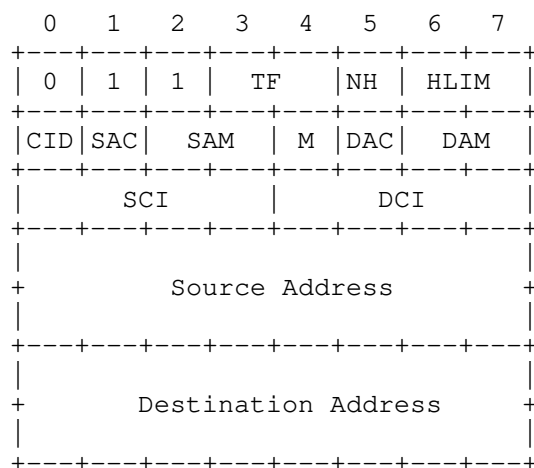


Figure 1: Best case of LOWPAN\_IPHC header.



## 2. Requirements Notation

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] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. Overview

Native Short Address (NSA) is a distributed assigned network layer identifier for efficient routing in a limited domain. It is normally locally assigned, using a smaller address space than IPv6. The architecture of NSA network is showed in Figure 2.

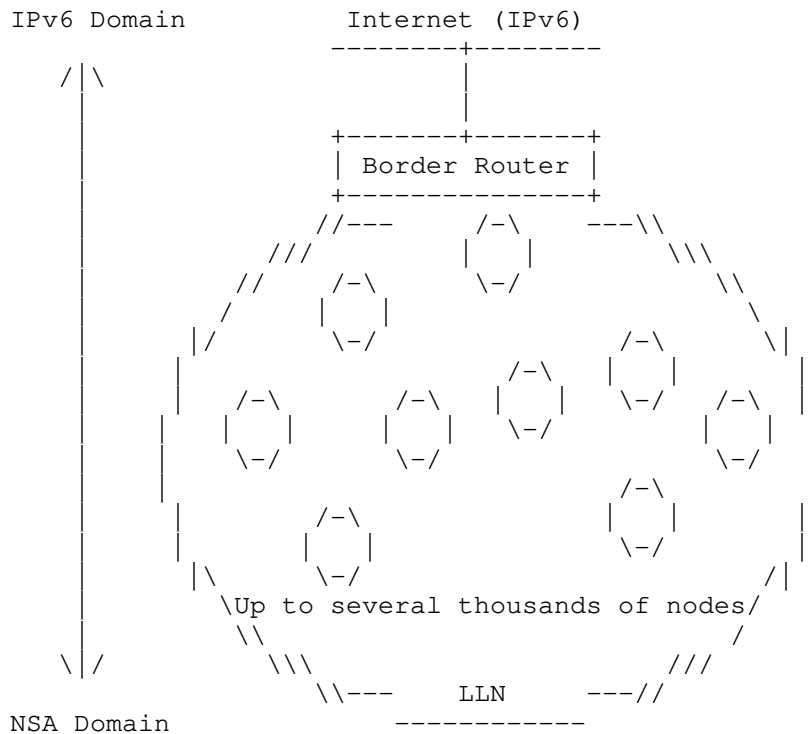


Figure 2: The architecture of general NSA networks.

Our overall design objective is centered on how to minimize the packet overhead and message exchange to achieve energy saving, while being suitable for a large-scale IoT network. This determines the key technologies of NSA in a limited domain, namely (i) the native short address allocation (see Section 4), (ii) the mechanisms for native table-free routing (see Section 5), and (iii) a compact header format design (see Section 6) that avoids context and compression.

#### 4. NSA Allocation

In an NSA network, there are 3 roles for nodes, namely: \* Root \* Forwarder \* Leaf

The basic aspects of allocation include: \* Root's address will always be '1'. \* Forwarder's address will always end with '0' (least significative bit = 0). \* Leaf's address will always end with '1' (least significative bit = 1).

Normally, the root role is assigned to the border router when the LLN bootstraps. All child nodes' addresses will strictly start with their parent's address. An example is showed in Figure 3.

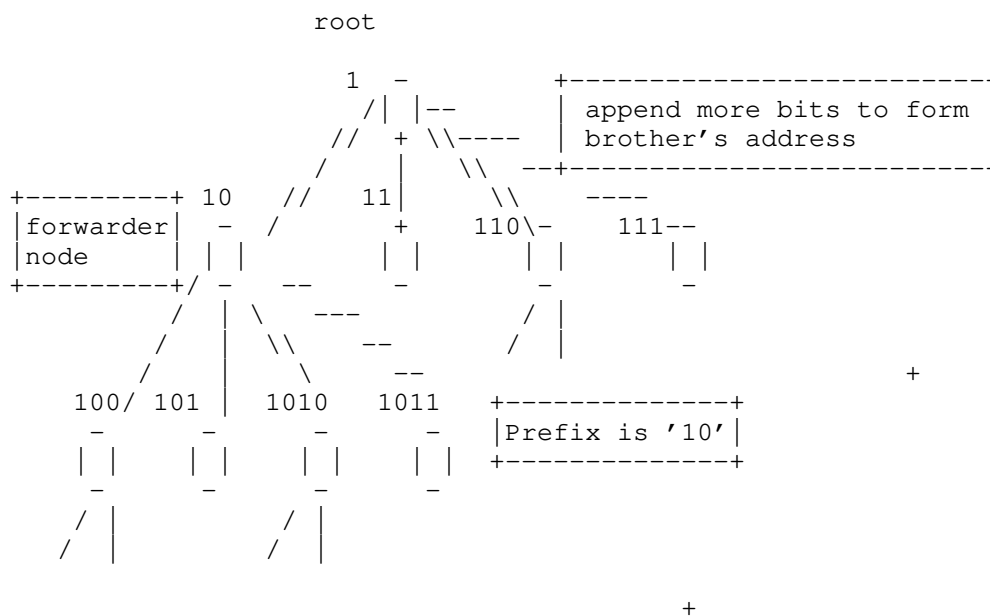


Figure 3: An example of NSA addresses allocation.

Each node that wants to acquire a native short address needs to send an Address Request (AR) message to its link layer neighbors and wait for the response. In the AR message, node needs to designate a 'role' value (forwarder or leaf) and 'nodeid'. If neighbor has not been configured with forwarder address and is not root, it will drop the message silently. Or, the neighbor should pick up an address according to 'role' parameter in the AR message. The allocation function  $A(\text{role}, i)$  is defined as shown in Figure 4. Every forwarder node should maintain separate index value for leaf and forwarder childs.

```
A(role, i) = 'root/forwarder address'
            + (i-1)*'1'
            + (role == leaf?'1':'0'),
in which, i is index of leaf/forwarder at this layer.
```

Figure 4: Definition of the allocation function of forwarder/root nodes.

After neighbor forwarder node assigned an address for node n, it assigns the suffix of that address as the interface id from which receiving the AR message. Then, it generates a response message of AR and sends it to the request node.

When node n successfully acquires an address from its neighbor, it will become child of that neighbor. Once a node received a valid response of AR, it uses that native short address for its own network layer address and ignores replies from other neighbors. If node doesn't receive any response after an interval, it will send the AR message again.

## 5. Routing in a NSA Network

### 5.1. Routing within the NSA limited domain

When a packet arrives at or is generated in a NSA node, the node will perform one of the following actions, depending on which condition holds:

1. If the destination equals the current node's address, the packet is delivered to the upper layers.
2. If the node is originating the packet and it is a leaf node, it sends packet to its parent.
3. If node is a forwarder and its address is in the same prefix of the Destination Address (DA), it makes the following calculation. It checks the bit values from bit next to the prefix, skip '1'

until the first '0' to find a new longer prefix. This prefix should be direct child of current node. If there are only '1's following, DA should be the direct leaf child of current node.

4. If the node is not root, it sends packet to parent

## 5.2. Routing between NSA and IPv6 domains

For downlink traffic (Internet toward NSA domain):

1. The border router (i.e., the root node) can construct IPv6 address for nodes by concatenating IPv6 prefix and native short address. The IPv6 prefix can be obtained by configuration. The border router can keep IPv6 addresses for all nodes in the domain.
2. The root will get native short address from those IPv6 addresses, while native table free routing will be used for packet transmission (cf., previous section).

For uplink traffic (NSA domain toward the Internet):

1. Border router maintains a table that maps IPv6 destinations to native short addresses, which will be seen as index of IPv6 address table.
2. Packet carries an index of table item when transmitting in the domain. Border router will look up real IPv6 destination before sending the packets to IPv6 domain.

## 6. NSA Header Format

As per Section 4, the address field would be variable in length. In this section, we outline the design of the header format partially based on the format of 6lowpan, accommodating the variable length fields in the packet. The header format is shown in Figure 5.

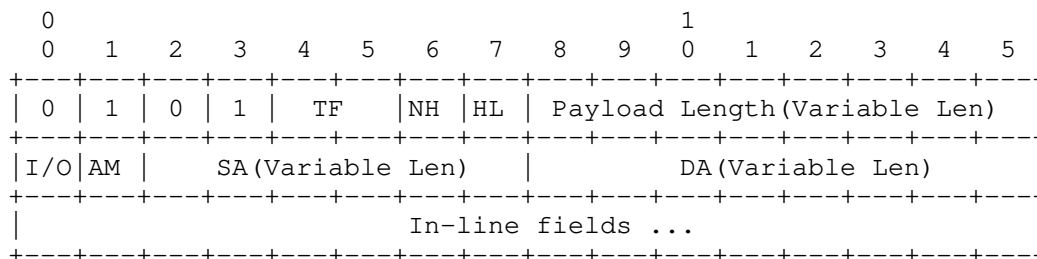


Figure 5: Header format of NSA packets

The first 4 bits would be new dispatch type that will be introduced in Section 7.

- \* TF: Same definition as in [RFC6282] Section 3.1.1.
- \* NH: Same definition as in [RFC6282] Section 3.1.1.
- \* HL: This field indicates the hop limit. When HL is 0, a hop limit field defined in [RFC2460] locates in in-line fields, while HL is 1 means no hop limit header in packet.
- \* Payload length is a variable length field. It normally occupies an octet assuming most packets are smaller than 252 bytes. For larger packets, payload length may expand to 2 to 3 octets. The encoding method is defined as follows. When the first octet has value of:
  - 0~252: Indicates how many octets the payload consist of.
  - 253: Indicates that there is an extra octet for payload length, with the actual length value equal to the last byte value plus 252.
  - 254: Indicates that there is an extra two octets for payload length, with the actual length value equal to the value of the second byte multiple 256 plus value of the last byte plus 252.
  - 255: Reserved.
- \* I/O: Indicates whether this packet belongs to uplink or downlink traffic, where the former means from an NSA node to IPv6 destination in the Internet, while the latter means opposite direction. This field is meaningless when the traffic is inside the NSA domain.
- \* AM: Indicates the address mode. When it is '0', the SA of downlink packets or DA of uplink packets is a full IPv6 address, while if it is '1', the SA of downlink packets or DA of uplink packets is a native short address that indexes the full IPv6 address on root node. This field is meaningless when the traffic is inside the NSA domain.

For length variable native short address encoding, for both Source Address (SA) and Destination Address (DA), the definition is:

- \* 0~252: if the address value locates in this interval, one octet is used to encode the value

- \* 253: indicates that the address is encoded in 2 octets.
- \* 254: indicates that the following 4 octets encode the address.
- \* 255: indicates that the following octet defines the length of address in octets, followed by the address value octets.

## 7. IANA Considerations

This document requires IANA to assign the range 0101000 to 0101111 of the "Dispatch Type Field" registry as follows:

0101TTNH	LOWPAN NSA IP (LOWPAN_NIP)	[This Document]
----------	----------------------------	-----------------

Figure 6: LOWPAN Dispatch Type Field requested allocation

## 8. Security Considerations

An extended security analysis will be provided in future revision of this document. As of this point we consider that the security considerations of [RFC4944], [RFC6282] apply.

## 9. References

## 9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <<https://www.rfc-editor.org/info/rfc2460>>.
- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <<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>>.

- [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>>.

## 9.2. Informative References

- [LPWAN] "IPv6 over Low Power Wide-Area Networks (lpwan) WG", n.d., <<https://datatracker.ietf.org/wg/lpwan/about/>>.
- [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>>.
- [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>>.
- [RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zúñiga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <<https://www.rfc-editor.org/info/rfc8724>>.
- [RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <<https://www.rfc-editor.org/info/rfc8799>>.
- [SIXLO] "IPv6 over Networks of Resource-constrained Nodes (6lo) WG", n.d., <<https://datatracker.ietf.org/wg/6lo/about/>>.
- [SIXLOWPAN] "IPv6 over Low power WPAN (6lowpan) - Concluded WG", n.d., <<https://datatracker.ietf.org/wg/6lowpan/about/>>.

## Author's Address

Guangpeng Li  
Huawei Technologies  
Beiqing Road, Haidian District  
Beijing  
100095  
China

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