6Lo Working Group
Internet-Draft
Intended Status: Standards Track
Expires: May 3, 2018

J. Hou
Huawei Technologies
Y-G. Hong
ETRI
X. Tang
SGEPRI

October 30, 2017

Transmission of IPv6 Packets over PLC Networks
draft-hou-6lo-plc-02

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 the 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. As part of this technology, Narrowband PLC (NBPLC) is focused on the low-bandwidth and low-power scenarios that includes current standards such as IEEE 1901.2 and ITU-T G.9903. This document describes how IPv6 packets are transported over constrained PLC networks.

Status of this Memo

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

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

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

This Internet-Draft will expire on May 3, 2018.

Table of Contents

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, 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). Such applications cover the smart meters for electricity, gas and water that share the common features like fixed position, large quantity, low data rate, and long life time.

Although PLC technology has an evolution history of several decades,

the adaptation of PLC for IPv6 based constrained networks is not fully developed. 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. It is of great importance to deploy IPv6 for PLC devices for its large address space and quick addressing. In addition, due to various existing PLC standards, a comparison among them is needed to facilitate the selection of the most applicable PLC standard in certain using scenarios.

The following sections provide a brief overview of PLC, then describe transmission of IPv6 packets over PLC networks. The general approach is to adapt elements of the 6LoWPAN specifications [RFC4944], [RFC6282], and [RFC6775] to constrained PLC networks. Similar 6LoPLC adaptation layer was previously proposed in [draft-popa-6lo-6loplc], however, with the same purpose, this document provides more updated, structured and instructive information for the deployment of IPv6 over PLC 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].

Below are the terms used in this document:

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

AMI: Advanced Metering Infrastructure

BBPLC: Broadband Power Line Communication

CID: Context ID

EV: Electric Vehicle

HDPLC: High Definition Power Line Communication

IID: Interface Identifier

IPHC: IP Header Compression

LAN: Local Area Network

LOADng: Lightweight On-demand Ad-hoc Distance-vector Routing Protocol Next Generation

MSDU: MAC Service Data Unit

MTU: Maximum Transmission Unit

NBPLC: Narrowband Power Line Communication

OFDM: Orthogonal Frequency Division Multiplexing

PCO: PAN Coordinator

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

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, 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. IEEE 1901 and ITU-T G.hn for BBPLC (1.8-250 MHz), IEEE 1901.2, ITU-T G.9902 (G.hnem), ITU-T G.9903 (G3-PLC) and ITU-T G.9904 (PRIME) for NBPLC (3-500 kHz) and the recent proposal for the IEEE 1901.1 standard aiming at the frequency band of 2-12 MHz.

Narrowband PLC is a very important branch of PLC technology due to its low frequency band and low power cost. So far the recent PLC standards, ITU-T G.9903 (G3-PLC) and IEEE 1901.2, are dominating as two of the most robust schemes available. Different networking methods exist in different NBPLC standards. There are 2 routing algorithms used in PLC networks for AMI applications:

- LOADng (Lightweight On-demand Ad-hoc Distance-vector Routing Protocol Next Generation) is a reactive protocol, operating in layer 2 or layer 3.

- RPL (Routing Protocol for Low-Power and Lossy Networks) is a proactive protocol operating only in layer 3.

LOADng is supported in G.9903 and 1901.2. IEEE 1901.2 specifies additionally Information Elements (IEs) which carry metrics from PHY layer to IP layer and the IE content is user-defined. These IEs enable RPL to be used as the routing algorithm in 1901.2 networks.

The IEEE 1901.1 WG is currently working on a new PLC standard, IEEE 1901.1, which focuses on the frequency band of 2-12 MHz [IEEE 1901.1]. This promising medium-frequency PLC standard, known as PLC-IoT, is suitable for 6lo applications thus mentioned in this document. Details on this standard is to be determined.

3.1. Protocol Stack

The protocol stack for IPv6 over PLC is illustrated in Figure 1 that contains the following elements from bottom to top: PLC PHY Layer, PLC MAC Layer, Adaptation layer for IPv6 over PLC, IPv6 Layer, TCP/UDP Layer and Application Layer. The PLC MAC/PHY layer corresponds to a certain PLC standard such as IEEE 1901.2 or ITU-T G.9903. Details of the 6lo adaptation layer for PLC are illustrated in section 4. Routing protocol like RPL on Network layer is optional according to the specified PLC standard, e.g. IEEE 1901.2.

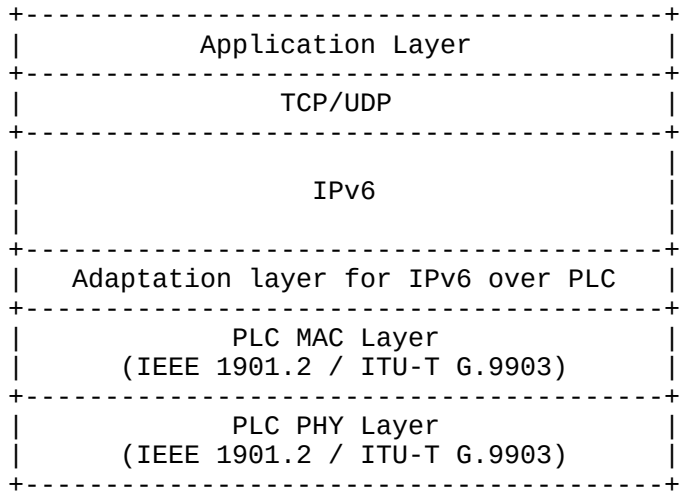

Figure 1: PLC Protocol Stack

3.2. Addressing Modes

Each PLC device has a globally unique 64-bit long address and a 16-bit short address. The long address is set by manufacturers according to 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

Maximum Transmission Unit (MTU) of MAC layer is an important parameter that determines the applicability of fragmentation and reassembly at the adaptation layer of IPv6 over PLC. An IPv6 packet require that every link in the Internet have 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 1901.2 MAC layer supports the MTU of 1576 octets (the original value 1280 byte was updated in 2015 [IEEE 1901.2a]). The MTU for ITU-T G.9903 is 400 octets, insufficient for supporting complete IPv6 packets. For this concern, fragmentation and reassembly in [RFC4944] are enabled for the G.9903-based scenarios (details can be found in section 4.2.6).

4. Specification of IPv6 over Narrowband PLC

Due to the narrow bandwidth and low data rate in NBPLC, a 6lo adaptation layer is needed to support the transmission of IPv6 packets. 6LoWPAN standards [RFC4944], [RFC6775], and [RFC6282] provides useful functionality including link-local IPv6 addresses, stateless address auto-configuration, neighbor discovery and header compression. These standards are referred in the specifications of the 6lo adaptation layer which is illustrated in the following subsections.

4.1. Stateless Address Autoconfiguration

PLC devices perform stateless address autoconfiguration according to [RFC4944] so as to obtain an IPv6 Interface Identifier (IID). The 64-bit IID is derived by insert 16-bit "FFEE" into a "pseudo 48-bit address" which is formed by the 16-bit PAN ID, 16-bit zero and the 16-bit short address as follows:

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

Considering that this derived IID is not globally unique, the "Universal/Local" (U/L) bit (7th bit) shall be set to zero.

4.2. IPv6 Link Local Address

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

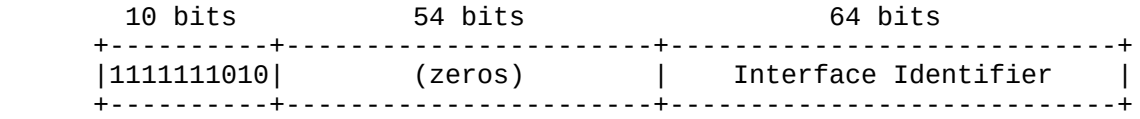

Figure 2: IPv6 Link Local Address in PLC

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], unless otherwise specified.

The Source/Target Link-layer Address option has the following form and the addresses are 16-bit short addresses. Since the 64-bit long address is only used in the joining process, no long address option is included the unicast address mapping.

Figure 3: Unicast Address Mapping

Option fields:

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

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

* Note that the format of Source/Target Link-layer Address option illustrated in Figure 3 is not used when sending RS/RA in G.9903 PLC networks. G.9903 specifies its SLLAO format for sending RS/RA. Details can be found in the Annex E of [ITU-T G.9903]. This inconsistency of SLLAO format has been informed to ITU-T SG15/Q15 and will be solved in future.

4.4. Neighbor Discovery

* No detailed specification of IPv6 neighbor discovery is defined in current PLC standards, and this section provides a guidance for the use of [RFC6775] in PLC networks.

Neighbor Discovery Optimization for 6LoWPANs [RFC6775] describes the neighbor discovery approach in several 6LoWPAN topologies including the mesh topology. In the route-over RPL-based network, the neighbor discovery process is recommended to refer to [RFC6775]. PLC devices may follow Sections 5.3 and 5.4 of [RFC6775] for sending Router Solicitations and processing Router Advertisements. Note that although PLC devices are electrically powered, the sleeping mode is still applicable for power saving. In addition, if DHCPv6 is used to assign addresses, Duplicate Address Detection (DAD) is not needed. In the mesh-under LOADng-based network, since there is a defined PAN bootstrapping protocol, the address registration defined in [RFC6775] is not used. An implementation for mesh-under operation could use [RFC6775] mechanisms for managing IPv6 prefixes and corresponding header compression context information [RFC6282].

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 can 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 functionality of segmentation and reassembly. A Segment Control Field is defined in the MAC frame header regardless of whether segmentation is required. This process segments a MAC layer datagram into multiple fragments and provides a reliable one-hop transfer of the resulting fragments. To minimize redundant fragmentation and reassembly (FAR) on the 6lo adaptation layer, similar functions defined in [RFC4944] should only be used when necessary. This document gives a requirement of the use of 6LoWPAN FAR in PLC networks as below:

* In PLC networks, if Layer-2 segmentation and reassembly is supported while the MAC layer supports MTU size of 1280 octets or greater, then 6LoWPAN fragmentation and reassembly as defined in

[RFC4944] is not needed and should not be used.

In IEEE 1901.2, since the MAC layer supports a payload of 1280 octets, which is the minimum MTU required by IPv6 packets, there is no need of fragmentation for the IPv6 packet transmission, thus the fragmentation and reassembly defined in [RFC4944] is not recommended 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 are provided referring to [RFC4944].

4.7. Extension at 6lo Adaptation Layer

Apart from the 6lo headers specified in [RFC4944], an additional Command Frame Header is defined for the mesh routing procedure in LOADng protocol. Figure 4 illustrates the format of the Command Frame Header [RFC8066]: The ESC dispatch type (01000000b) indicates an ESC extension type follows (see [RFC4944] and [RFC6282]). Then this 1-octet dispatch field is used as the Command Frame Header and filled with the Command ID. The Command ID can be classified into 4 types:

- LOADng message (0x01)

- LoWPAN bootstrapping protocol message (0x02)

- Reserved by ITU-T (0x03-0x0F)

- CMSR protocol messages (0X10-0X1F)

The LOADng message is used to provide the default routing protocol LOADng while the LoWPAN bootstrapping protocol message is for the LoWPAN bootstrap procedure. The CMSR protocol messages are specified for the Centralized metric-based source routing [ITU-T G.9905] which is out of the scope of this draft.

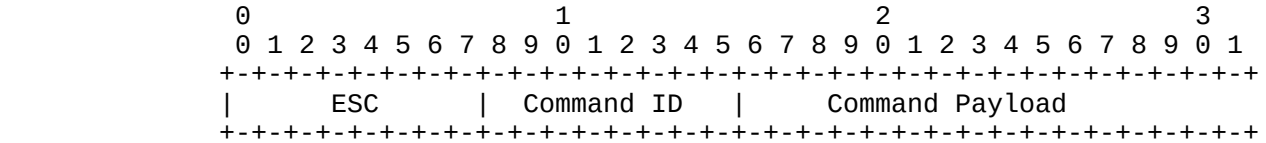

Figure 4: Command Frame Header Format of ITU-T G.9903

Command Frame Header appears in the last position if more than one header is present in the 6LoWPAN frame [ITU-T G.9903]. On the other

hand, this Command Frame Header must appear before the LoWPAN_IPHC dispatch type as per [RFC8066].

* Regarding the order of the command frame header, the inconsistency between G.9903 and RFC8066 still exists and is being solved in ITU-T SG15/Q15.

Following these two requirements of header order mentioned above, an example of the header order is illustrated in Figure 5 including the Fragmentation type, Fragmentation header, ESC dispatch type, ESC Extension Type (Command ID), ESC Dispatch Payload (Command Payload), LOWPAN_IPHC Dispatch Type, LOWPAN_IPHC header, and Payload.

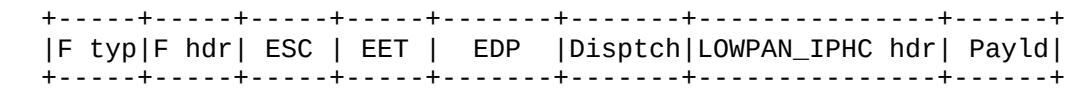

Figure 5: A 6LoWPAN packet including the Command Frame Header

5. Internet Connectivity Scenarios and Topologies

The network model can be simplified to two kinds of network devices: PAN Coordinator (PCO) and PAN Device. PCO is the coordinator of the PLC subnet and can be seen as a master node while PAN Devices are typically PLC meters and sensors. The IPv6 over PLC networks are built as tree, mesh or star according to the specified using scenarios. Every network requires at least one PCO to communicate with each PAN Device. Note that the PLC topologies included in this section are based on the logical connectivity, not physical links.

One common topology in the current PLC scenarios is star. In this case, the communication at the link layer only takes place between a PAN Device and a PCO. The PCO collects data (e.g. smart meter reading) from different nodes, and then concentrates and uploads the data through Ethernet or LPWAN (see Figure 6). 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. Such topology has been widely applied in the deployment of smart meters, especially in apartment buildings.

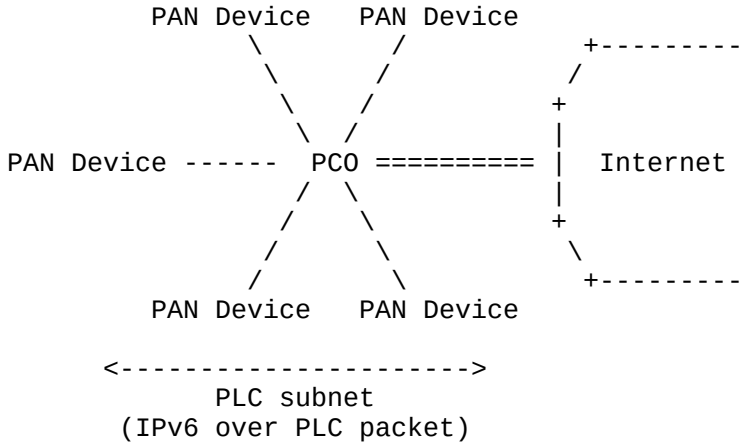

Figure 6: PLC Star Network connected to the Internet

Tree topology is used when the distance between a device A and PCO is beyond the PLC allowed limit while 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 Proxy Coordinator. For this scenario, the link layer communications take place between device A and device B, and between device B and PCO. An example of PLC tree network is depicted in Figure 7. 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 as depicted in [RFC8036]. Tree topology is suitable for the AMI scenarios that require large coverage but low density, e.g. the deployment of smart meters in rural areas.

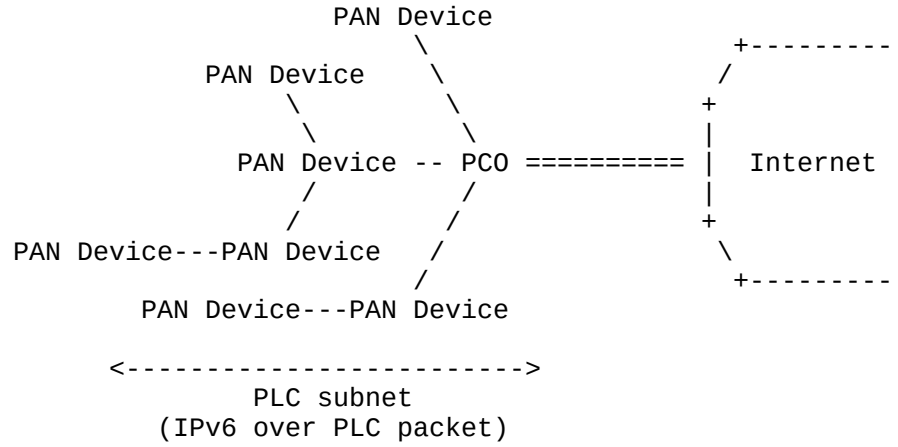

Figure 7: PLC Tree Network connected to the Internet

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 8), 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). LOADng enables direct pan device to pan devices (without being obliged to get through the pan coordinator) which significantly improves performances in typical use cases like charging station to electric vehicle (EV) communications.

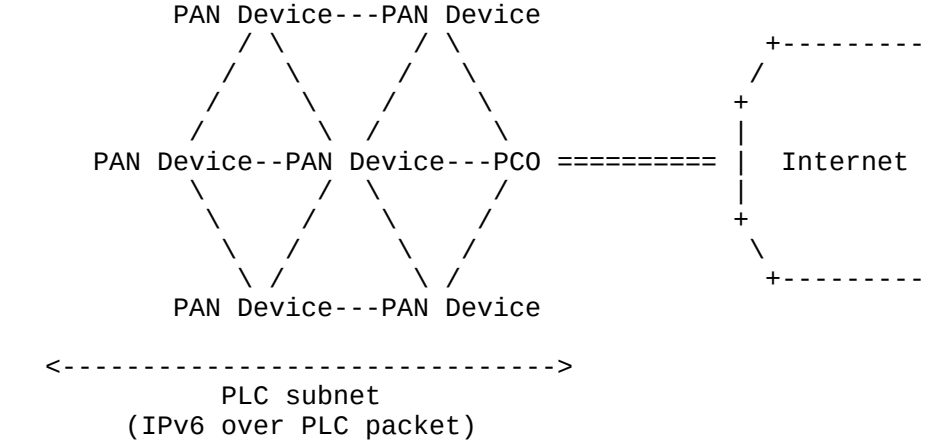

Figure 8: PLC Mesh Network connected to the Internet

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 privacy consideration, link layer security is guaranteed in every PLC technology.

8. Acknowledgements

We are grateful to the members of the IETF 6LoWPAN 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 1901.2] 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998, <http://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, <http://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, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC6282] Hui, J. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011, <http://www.rfc-editor.org/info/rfc6282>.

[RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012, <http://www.rfc-editor.org/info/rfc6775>.

9.2. Informative References

[draft-ietf-6lo-ap-nd-02] Sarikaya, B., Thubert, P. and M. Sethi, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-02, May 2017, <https://tools.ietf.org/html/draft-ietf-6lo-ap-nd-02>.

[draft-popa-6lo-6loplc] Popa, D. and J.H. Hui, "6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks", draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00, March 2014, <https://tools.ietf.org/html/draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00>.

[draft-rashid-6lo-iid-assignment-03] Sangi, AR., Chen, M. and C. Perkins, "Designating 6LBR for IID Assignment", draft-rashid-6lo-iid-assignment-03, March 2017, <https://tools.ietf.org/html/draft-rashid-6lo-iid-assignment-03>.

[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, work in progress, <http://sites.ieee.org/sagroups-1901-1>.

[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>.

[ITU-T G.9960] International Telecommunication Union, "Unified high-speed wireline-based home networking transceivers - System architecture and physical layer specification", ITU-T G.9960, December 2011, <https://www.itu.int/rec/T-REC-G.9960>.

[ITU-T G.9961] International Telecommunication Union, "Unified high-speed wireline-based home networking transceivers - Data link layer specification", ITU-T G.9961, June 2010, <https://www.itu.int/rec/T-REC-G.9961>.

[RFC8036] Cam-Winget, N., 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, January 2017, <http://www.rfc-editor.org/info/rfc8036>.

[RFC8065] D. Thaler, " Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, Februray 2017, <http://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, Februray 2017, <http://www.rfc-editor.org/info/rfc8066>.

Authors' Addresses

Jianqiang Hou
Huawei Technologies
101 Software Avenue,
Nanjing 210012
China

Phone: +86 15852944235
Email: houjianqiang@huawei.com

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

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

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

Phone: +86-25-81098508
Email: itc@sgepri.sgcc.com.cn

6lo
Internet-Draft
Updates: 6775 (if approved)
Intended status: Standards Track
Expires: March 25, 2018

B. Sarikaya

P. Thubert
Cisco

M. Sethi
Ericsson

September 21, 2017

Address Protected Neighbor Discovery for Low-power and Lossy Networks
draft-ietf-6lo-ap-nd-03

Abstract

This document defines an extension to 6LoWPAN Neighbor Discovery RFC 6775. Nodes supporting this extension compute a cryptographic Owner Unique Interface ID and associate it with one or more of their Registered Addresses. Once an address is registered with a Cryptographic ID, only the owner of that ID can modify the anchor state information of the Registered Address, and Source Address Validation can be enforced.

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 25, 2018.

Copyright Notice

Table of Contents

1. Introduction

"Neighbor Discovery Optimizations for 6LoWPAN networks" [RFC6775] (6LoWPAN ND) adapts the classical IPv6 ND protocol [RFC4861][RFC4862] (IPv6 ND) for operations over a constrained low-power and lossy network (LLN). In particular, 6LoWPAN ND introduces a unicast host address registration mechanism that contributes to reduce the use of multicast messages that are present in the classical IPv6 ND protocol. 6LoWPAN ND defines a new Address Registration Option (ARO) that is carried in the unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages between the 6LoWPAN Node (6LN) and the 6LoWPAN Router (6LR). Additionally, it also defines the Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages between the 6LR and the 6LoWPAN Border Router (6LBR). In LLN networks, the 6LBR is the central repository of all the registered addresses in its domain.

The registration mechanism in 6LoWPAN ND [RFC6775] prevents the use of an address if that address is already present in the subnet (first come first serve). In order to validate address ownership, the registration mechanism enables the 6LR and 6LBR to validate claims for a registered address with an associated Owner Unique Interface IDentifier (OUID). 6LoWPAN ND specifies that the OUID is derived from the MAC address of the device (EUI-64), which can be spoofed. Therefore, any node connected to the subnet and aware of a registered-address-to-OUID mapping could effectively fake the OUID, steal the address and redirect traffic for that address towards a different 6LN. The "Update to 6LoWPAN ND" [I-D.ietf-6lo-rfc6775-update] defines an Extended ARO (EARO) option that allows to transport alternate forms of OUIDs, and is a prerequisite for this specification.

According to this specification, a 6LN generates a cryptographic ID (Crypto-ID) and places it in the OUID field in the registration of one (or more) of its addresses with the 6LR(s) that the 6LN uses as default router(s). Proof of ownership of the cryptographic ID (Crypto-ID) is passed with the first registration to a given 6LR, and enforced at the 6LR, in a new Crypto-ID Parameters Option (CIPO). The 6LR validates ownership of the cryptographic ID upon the creation of a registration state, or a change in the anchor information, such as Link-Layer Address and associated Layer-2 cryptographic material.

The protected address registration protocol proposed in this document enables the enforcement of Source Address Validation (SAVI) [RFC7039], which ensures that only the correct owner uses a registered address in the source address field in IPv6 packets. Consequently, a 6LN that sources a packet has to use a 6LR to which the source address of the packet is registered to forward the packet. The 6LR maintains state information for the registered addressed, including the MAC address, and a link-layer cryptographic key associated with the 6LN. In SAVI-enforcement mode, the 6LR allows only packets from a connected Host if the connected Host owns the registration of the source address of the packet.

The 6lo adaptation layer framework ([RFC4944], [RFC6282]) expects that a device forms its IPv6 addresses based on Layer-2 address, so as to enable a better compression. This is incompatible with "Secure Neighbor Discovery (SEND)" [RFC3971] and "Cryptographically Generated Addresses (CGAs)" [RFC3972], which derive the Interface ID (IID) in the IPv6 addresses from cryptographic material. "Privacy Considerations for IPv6 Address Generation Mechanisms" [RFC7721] places additional recommendations on the way addresses should be formed and renewed.

This document specifies that a device may form and register addresses at will, without a constraint on the way the address is formed or the number of addresses that are registered in parallel. It enables to protect multiple addresses with a single cryptographic material and to send the proof only once to a given 6LR for multiple addresses and refresher registrations.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Readers are expected to be familiar with all the terms and concepts that are discussed in [RFC3971], [RFC3972], [RFC4861], [RFC4919], [RFC6775], and [I-D.ietf-6lo-backbone-router] which proposes an evolution of [RFC6775] for wider applicability.

This document defines Crypto-ID as an identifier of variable size which in most cases is 64 bits long. It is generated using cryptographic means explained later in this document Section 4.1.

The document also conforms to the terms and models described in [RFC5889] and uses the vocabulary and the concepts defined in [RFC4291] for the IPv6 Architecture. Finally, common terminology related to Low power And Lossy Networks (LLN) defined in [RFC7102] is also used.

3. Updating RFC 6775

This specification defines a cryptographic identifier (Crypto-ID) that can be used as a replacement to the MAC address in the OUID field of the EARO option; the computation of the Crypto-ID is detailed in Section 4.1. A node in possession of the necessary cryptographic material SHOULD use Crypto-ID by default as OUID in its registration. Whether a OUID is a Crypto-ID is indicated by a new "C" flag in the NS(EARO) message.

This specification introduces a new option, the CIPO, that is used to prove ownership of the Crypto-ID. A node that registers for the first time to a 6LR SHOULD place a CIPO option in its registration. However, it is not expected to place the option in the periodic refresher registrations for that address, or to register other addresses with the same OUID. When a 6LR receives a NS(EARO) registration with a new Crypto-ID as a OUID, it SHOULD challenge by responding with a NA(EARO) with a status of "Validation Requested". This process of validation MAY be skipped in networks where there is no mobility.

The challenge MUST also be triggered in the case of a registration for which the Source Link-Layer Address is not consistent with a state that already exists either at the 6LR or the 6LBR. In the latter case, the 6LBR returns a status of "Validation Requested" in the DAR/DAC exchange, which is echoed by the 6LR in the NA (EARO) back to the registering node. This flow should not alter a preexisting state in the 6LR or the 6LBR.

Upon receiving a NA(EARO) with a status of "Validation Requested", the registering node SHOULD retry its registration with a CIPO option that proves its ownership of the Crypto-ID.

If the 6LR cannot validate the CIPO, it responds with a status of "Validation Failed". After receiving a NA(EARO) with a status of "Validation Failed", the registering node MUST NOT use this Crypto-ID for registering with that 6LR.

4. New Fields and Options

4.1. New Crypto-ID

Elliptic Curve Cryptography (ECC) is used to calculate the Crypto-ID. Each 6LN using a Crypto-ID for registration MUST have a public/ private key pair. The digital signature is constructed by using the 6LN’s private key over its EUI-64 (MAC) address. The signature value is computed using the ECDSA signature algorithm and the hash function used is SHA-256 [RFC6234]. Public Key is the most important parameter in CGA Parameters (sent by 6LN in an NS message). ECC Public Key could be in uncompressed form or in compressed form where the first octet of the OCTET STRING is 0x04 and 0x02 or 0x03, respectively. Point compression can further reduce the key size by about 32 octets.

The Crypto-ID is computed as follows:

1. the modifier is set to a random or pseudo-random 128-bit value

2. the modifier, 9 zero octets and the ECC public key are concatenated from left to right.

3. the SHA-256 algorithm is applied on the concatenation

4. the 112 leftmost bits of the hash value are retained

5. the modifier value, the subnet prefix and the encoded public key are concatenated from left to right

6. NIST P-256 is executed on the concatenation

7. the leftmost bits of the result are used as the Crypto-ID.

With this specification, the last 64 bits are retained, but it could be expanded to more bits in the future by increasing the size of the OUID field.

To support cryptographic algorithm agility [RFC7696], Curve25519 [RFC7748] can also be used instead of NIST P-256. This is indicated by 6LN using the Crypto Type field in the CIPO option. The document currently only defines two possible values for the Crypto Type field. A value of 0 indicates that NIST P-256 is used for the signature operation and SHA-256 as the hash algorithm. A value of 1 indicates that Curve25519 is used for the signature operation and SHA-256 as the hash algorithm. New values for the Crypto Type maybe defined in the future for new curves.

4.2. Updated EARO

This specification updates the EARO option as follows:

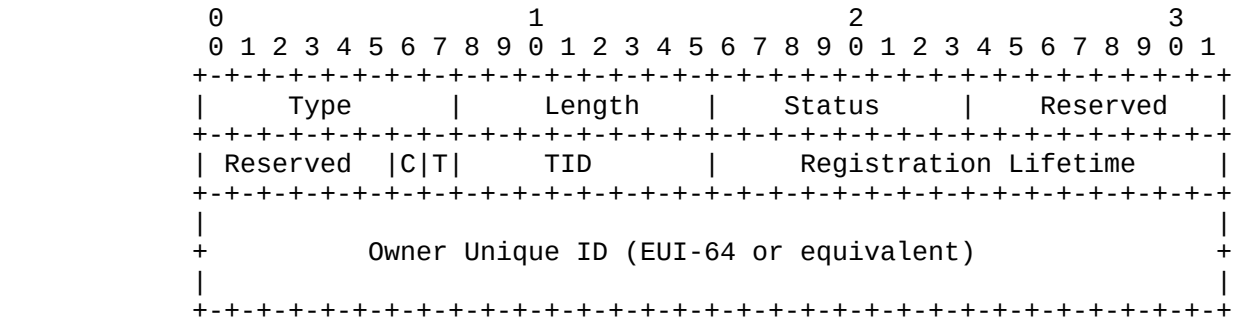

Figure 1: Enhanced Address Registration Option

Type: 33

Length: 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 bytes.

Status: 8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. This specification uses values introduced in the update to 6LoWPAN ND [I-D.ietf-6lo-rfc6775-update], such as "Validation Requested" and "Validation Failed". No additional value is defined.

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

C: This "C" flag is set to indicate that the Owner Unique ID field contains a Crypto-ID.

T and TID: Defined in [I-D.ietf-6lo-rfc6775-update].

Owner Unique ID: When the "C" flag is set, this field contains a Crypto-ID.

4.3. New Crypto-ID Parameters Option

This specification introduces a new option, the Crypto-ID Parameters Option (CIPO), that carries the proof of ownership of a crypto-ID.

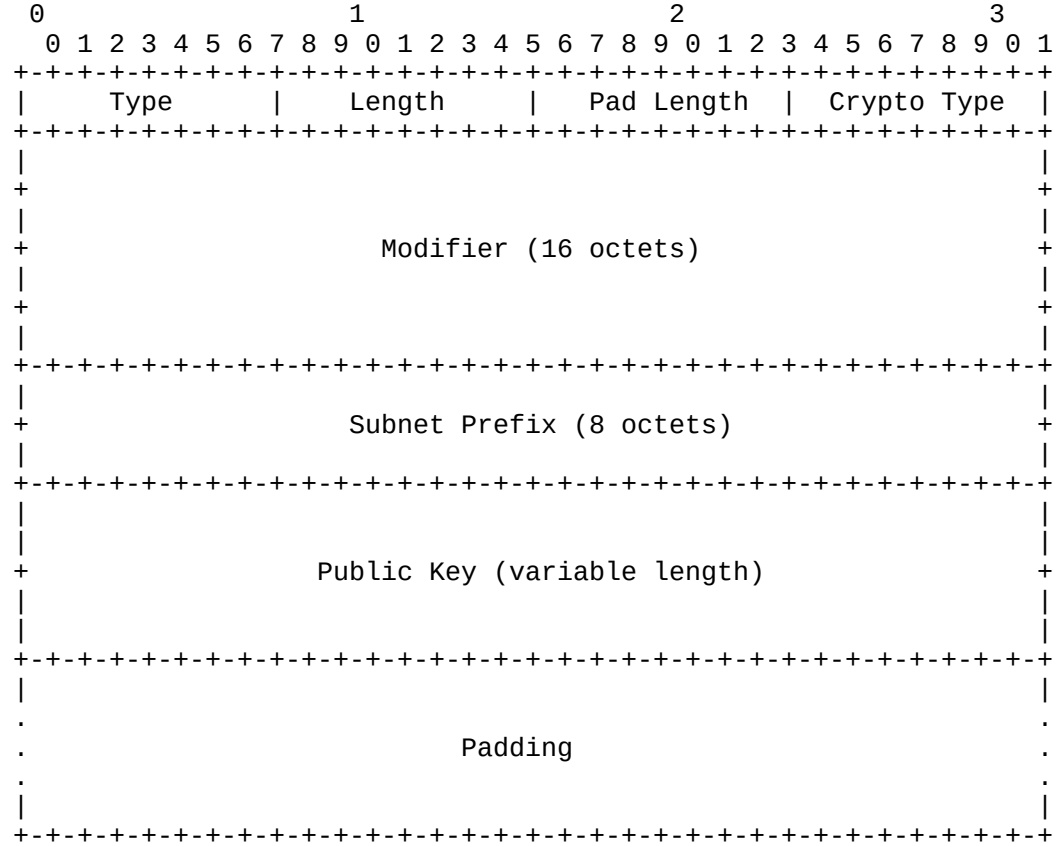

Figure 2: Crypto-ID Parameters Option

Type: CIPO, to be assigned by IANA.

Length: The length of the option in units of 8 octets.

Pad Length: The length of the Padding field.

Crypto Type: The type of cryptographic algorithm used in calculation Crypto-ID. Default value of all zeros indicate NIST P-256. A value of 1 is assigned for Curve25519. New values may be defined later.

Modifier: 128 bit random value.

Subnet Prefix: 64 bit subnet prefix.

Public Key: ECC public key of 6LN.

Padding: A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

5. Protocol Overview

5.1. Protocol Scope

The scope of the present work is a 6LoWPAN Low Power Lossy Network (LLN), typically a stub network connected to a larger IP network via a Border Router called a 6LBR per [RFC6775].

The 6LBR maintains a registration state for all devices in the attached LLN, and, in conjunction with the first-hop router (the 6LR), is in a position to validate uniqueness and grant ownership of an IPv6 address before it can be used in the LLN. This is a fundamental difference with a classical network that relies on IPv6 address auto-configuration [RFC4862], where there is no guarantee of ownership from the network, and any IPv6 Neighbor Discovery packet must be individually secured [RFC3971].

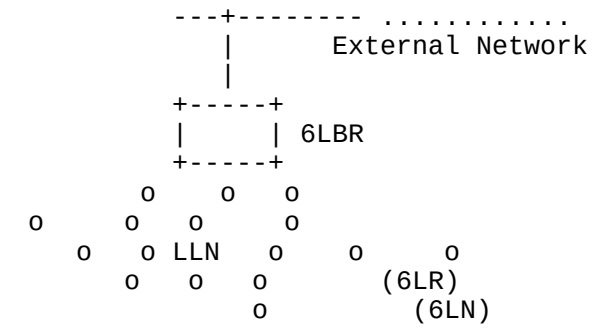

Figure 3: Basic Configuration

In a mesh network, the 6LR is directly connected to the host device. This specification expects that the peer-wise layer-2 security is deployed so that all the packets from a particular host are securely identifiable by the 6LR. The 6LR may be multiple hops away from the 6LBR. Packets are routed between the 6LR and the 6LBR via other 6LRs. This specification expects that a chain of trust is established so that a packet that was validated by the first 6LR can be safely routed by the next 6LRs to the 6LBR.

5.2. Protocol Flows

Figure 4 illustrates a registration flow all the way to a 6LowPAN Backbone Router (6BBR).

A new device that joins the network auto-configures an address and performs an initial registration to an on-link 6LR with an NS message that carries an Address Registration Option (EARO) [RFC6775]. The 6LR validates the address with the central 6LBR using a DAR/DAC exchange, and the 6LR confirms (or denies) the address ownership with an NA message that also carries an Address Registration Option.

In a multihop 6LoWPAN, the registration with Crypto-ID is propagated to 6LBR as described in Section 5.3. If a chain of trust is present between the 6LR and the 6LBR, then there is no need to propagate the proof of ownership to the 6LBR. All the 6LBR needs to know is that this particular OUID is randomly generated, so as to enforce that any update via a different 6LR is also random.

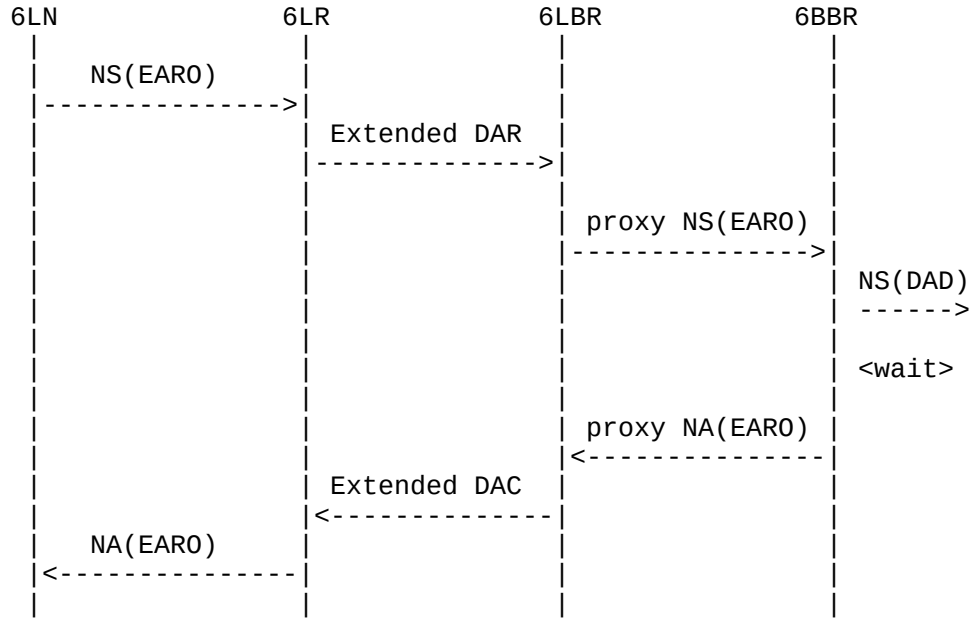

Figure 4: (Re-)Registration Flow

On-link (local) protocol interactions are shown in Figure 5. Crypto-ID and ARO are passed to and stored by the 6LR on the first NS and not sent again in the next NS. The operation starts with 6LR sending a Router Advertisement (RA) message to 6LN.

The 6LR/6LBR ensures first-come/first-serve by storing the ARO and the Crypto-ID correlated to the node being registered. The node is free to claim any address it likes as long as it is the first to make such a claim. After a successful registration, the node becomes the owner of the registered address and the address is bound to the Crypto-ID in the 6LR/6LBR registry. This binding can be verified later, which prevents other nodes from stealing the address and trying to attract traffic for that address or use it as their source address.

A node may use multiple IPv6 addresses at the same time. The node may use the same Crypto-ID to protect multiple IPv6 addresses. The separation of the address and the Crypto-ID avoids the constrained device to compute multiple keys for multiple addresses. The registration process allows the node to bind all of its addresses to the same Crypto-ID.

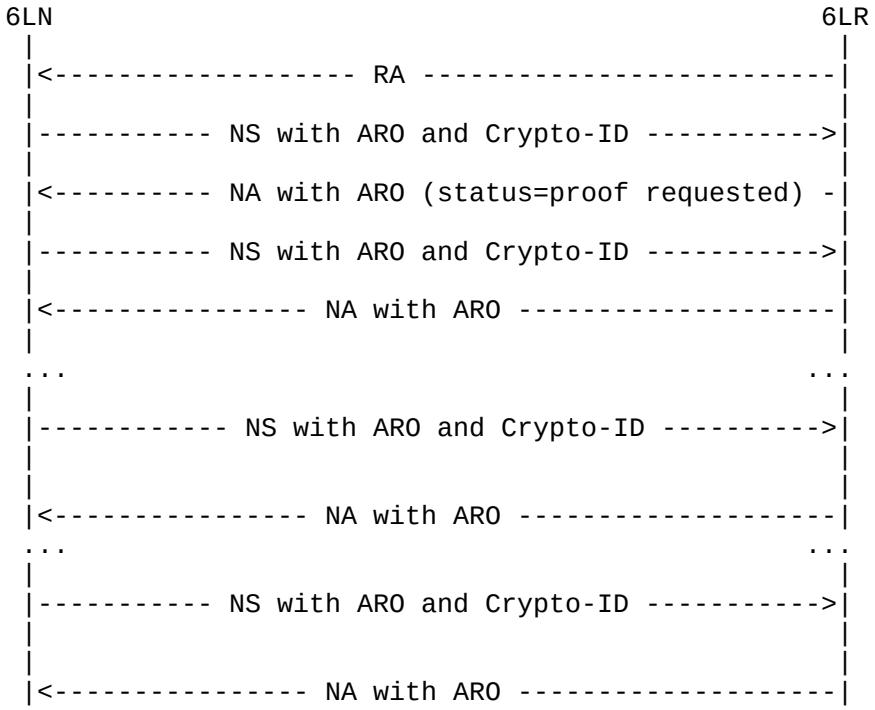

Figure 5: On-link Protocol Operation

5.3. Multihop Operation

In a multihop 6LoWPAN, a 6LBR sends RAs with prefixes downstream and the 6LR receives and relays them to the nodes. 6LR and 6LBR communicate using ICMPv6 Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages. The DAR and DAC use the same message format as NS and NA, but have different ICMPv6 type values.

In ND-PAR we extend DAR/DAC messages to carry cryptographically generated OUID. In a multihop 6LoWPAN, the node exchanges the messages shown in Figure 4. The 6LBR must identify who owns an address (EUI-64) to defend it, if there is an attacker on another 6LR. Because of this the content that the source signs and the signature needs to be propagated to the 6LBR in the DAR message. For this purpose the DAR message sent by 6LR to 6LBR MUST contain the CIPO option. The DAR message also contains ARO.

Occasionally, a 6LR might miss the node’s OUID (that it received in ARO). 6LR should be able to ask for it again. This is done by restarting the exchanges shown in Figure 5. The result enables 6LR

to refresh the information that was lost. The 6LR MUST send DAR message with ARO to 6LBR. The 6LBR replies with a DAC message with the information copied from the DAR, and the Status field is set to zero. With this exchange, the 6LBR can (re)validate and store the information to make sure that the 6LR is not a fake.

In some cases, the 6LBR may use a DAC message to solicit a Crypto-ID from a 6LR and also requests 6LR to verify the EUI-64 6LR received from 6LN. This may happen when a 6LN node is compromised and a fake node is sending the Crypto-ID as if it is the node's EUI-64. Note that the detection in this case can only be done by 6LBR not by 6LR.

6. Security Considerations

The observations regarding the threats to the local network in [RFC3971] also apply to this specification.

The threats discussed in 6LoWPAN ND [RFC6775] and its update [I-D.ietf-6lo-rfc6775-update] also apply here. Compared with SeND, this specification saves about 1Kbyte in every NS/NA message. Also, this specification separates the cryptographic identifier from the registered IPv6 address so that a node can have more than one IPv6 address protected by the same cryptographic identifier. SeND forces the IPv6 address to be cryptographic since it integrates the CGA as the IID in the IPv6 address. This specification frees the device to form its addresses in any fashion, so as to enable the classical 6LoWPAN compression which derives IPv6 addresses from Layer-2 addresses, as well as privacy addresses. The threats discussed in Section 9.2 of [RFC3971] are countered by the protocol described in this document as well.

Collisions of Owner Unique Interface IDentifier (OUID) (which is the Crypto-ID in this specification) is a possibility that needs to be considered. The formula for calculating the probability of a collision is 1 - e^{-k^2/(2n)} where n is the maximum population size (2^64 here, 1.84E19) and K is the actual population (number of nodes). If the Crypto-ID is 64-bit long, then the chance of finding a collision is 0.01% when the network contains 66 million nodes. It is important to note that the collision is only relevant when this happens within one stub network (6LBR). A collision of Crypto-ID is a rare event. In the case of a collision, an attacker may be able to claim the registered address of an another legitimate node. However for this to happen, the attacker would also need to know the address which was registered by the legitimate node. This registered address is however never broadcasted on the network and therefore it provides an additional entropy of 64-bits that an attacker must correctly guess. To prevent such a scenario, it is RECOMMENDED that nodes derive the address being registered independently of the OUID.

7. IANA considerations

IANA is requested to assign two new option type values for the CIPO under the subregistry "IPv6 Neighbor Discovery Option Formats".

7.1. Crypto Type Registry

The following Crypto Type values are defined in this document:

Crypto Type value	Algorithms
0	NIST P-256, SHA-256 [RFC6234]
1	Curve25519 [RFC7748], SHA-256 [RFC6234]

Table 1: Crypto Types

Assignment of new values for new Crypto Type MUST be done through IANA with "Specification Required" and "IESG Approval" as defined in [RFC8126].

8. Acknowledgements

Special thanks to Charlie Perkins for his in-depth review and constructive suggestions. We are also grateful to Rene Struik and Robert Moskowitz for their comments that lead to many improvements to this document.

9. Change Log

- submitted version -00 as a working group draft after adoption, and corrected the order of authors
- submitted version -01 with no changes
- submitted version -02 with these changes: Moved Requirements to Appendix A, Section 4.2 moved to Section 3, New section 4 on New Fields and Options, Section 4 changed to Protocol Overview as Section 5 with Protocol Scope and Flows subsections.
- submitted version -03 addressing Charlie Perkins’ comments

10. References

10.1. Normative References

[I-D.ietf-6lo-rfc6775-update]
Thubert, P., Nordmark, E., and S. Chakrabarti, "An Update to 6LoWPAN ND", draft-ietf-6lo-rfc6775-update-09 (work in progress), September 2017.

[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>.

[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>.

[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>.

10.2. Informative references

[I-D.ietf-6lo-backbone-router]
Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-04 (work in progress), July 2017.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/info/rfc3972>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <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>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <https://www.rfc-editor.org/info/rfc5889>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[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>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <https://www.rfc-editor.org/info/rfc7039>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <https://www.rfc-editor.org/info/rfc7102>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015, <https://www.rfc-editor.org/info/rfc7696>.

[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>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Appendix A. Requirements Addressed in this Document

In this section we state requirements of a secure neighbor discovery protocol for low-power and lossy networks.

- The protocol MUST be based on the Neighbor Discovery Optimization for Low-power and Lossy Networks protocol defined in [RFC6775]. RFC6775 utilizes optimizations such as host-initiated interactions for sleeping resource-constrained hosts and elimination of multicast address resolution.

- New options to be added to Neighbor Solicitation messages MUST lead to small packet sizes, especially compared with existing protocols such as SEcure Neighbor Discovery (SEND). Smaller packet sizes facilitate low-power transmission by resource-constrained nodes on lossy links.

- The support for this registration mechanism SHOULD be extensible to more LLN links than IEEE 802.15.4 only. Support for at least the LLN links for which a 6lo "IPv6 over foo" specification exists, as well as Low-Power Wi-Fi SHOULD be possible.

- As part of this extension, a mechanism to compute a unique Identifier should be provided with the capability to form a Link Local Address that SHOULD be unique at least within the LLN connected to a 6LBR.

- The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of Unique Interface IDentifier.

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

Authors' Addresses

Behcet Sarikaya
Plano, TX
USA

Email: sarikaya@ieee.org

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

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

Mohit Sethi
Ericsson
Hirsalantie
Jorvas 02420

Email: mohit@piuha.net

6lo
Internet-Draft
Intended status: Standards Track
Expires: January 18, 2018

P. Thubert, Ed.
cisco

July 17, 2017

IPv6 Backbone Router
draft-ietf-6lo-backbone-router-04

Abstract

This specification proposes an update to IPv6 Neighbor Discovery, to enhance the operation of IPv6 over wireless links that exhibit lossy multicast support, and enable a large degree of scalability by splitting the broadcast domains. A broadcast-efficient backbone running classical IPv6 Neighbor Discovery federates multiple wireless links to form a large MultiLink Subnet, but the broadcast domain does not need to extend to the wireless links for the purpose of ND operation. Backbone Routers placed at the wireless edge of the backbone proxy the ND operation and route packets from/to registered nodes, and wireless nodes register or are proxy-registered to the Backbone Router to setup proxy services in a fashion that is essentially similar to a classical Layer-2 association.

Table of Contents

1. Introduction

One of the key services provided by IEEE std. 802.1 [IEEEstd8021] Ethernet Bridging is an efficient and reliable broadcast service, and multiple applications and protocols have been built that heavily depends on that feature for their core operation. But a wide range of wireless networks do not provide the solid and cheap broadcast capabilities of Ethernet Bridging, and protocols designed for bridged networks that rely on broadcast often exhibit disappointing behaviours when applied unmodified to a wireless medium.

IEEE std. 802.11 [IEEEstd80211] Access Points (APs) deployed in an Extended Service Set (ESS) effectively act as bridges, but, in order to ensure a solid connectivity to the devices and protect the medium against harmful broadcasts, they refrain from relying on broadcast-intensive protocols such as Transparent Bridging on the wireless side. Instead, an association process is used to register proactively the MAC addresses of the wireless device (STA) to the AP, and then the APs proxy the bridging operation and cancel the broadcasts.

Classical IPv6 [RFC8200] Neighbor Discovery [RFC4862] Protocol (NDP) operations are reactive and rely heavily on multicast operations to locate an on-link correspondent and ensure address uniqueness, which is a pillar that sustains the whole IP architecture. When the Duplicate Address Detection [RFC4862] (DAD) mechanism was designed, it was a natural match with the efficient broadcast operation of Ethernet Bridging, but with the unreliable broadcast that is typical of wireless media, DAD is bound to fail to discover duplications [I-D.yourtchenko-6man-dad-issues]. In other words, because the broadcast service is unreliable, DAD appears to work on wireless media not because address duplication is detected and solved as designed, but because the duplication is a very rare event as a side effect of the sheer amount of entropy in 64-bits Interface IDs.

In the real world, IPv6 multicast messages are effectively broadcast, so they are processed by most if not all wireless nodes over the ESS fabric even when very few if any of the nodes is effectively listening to the multicast address. It results that a simple Neighbor Solicitation (NS) lookup message [RFC4861], that is supposedly targeted to a very small group of nodes, ends up polluting the whole wireless bandwidth across the fabric [I-D.vyncke-6man-mcast-not-efficient]. In other words, the reactive IPv6 ND operation leads to undesirable power consumption in battery-operated devices.

The inefficiencies of using radio broadcasts to support IPv6 NDP lead the community to consider (again) splitting the broadcast domain between the wired and the wireless access links. One classical way to achieve this is to split the subnet in multiple ones, and at the extreme provide a /64 per wireless device. Another is to proxy the Layer-3 protocols that rely on broadcast operation at the boundary of the wired and wireless domains, effectively emulating the Layer-2 association at layer-3. To that effect, the current IEEE std. 802.11 specifications require the capability to perform ARP and ND proxy [RFC4389] functions at the Access Points (APs).

But for the lack a comprehensive specification for the ND proxy and in particular the lack of an equivalent to an association process,

implementations have to rely on snooping for acquiring the related state, which is unsatisfactory in a lossy and mobile conditions. With snooping, a state (e.g. a new IPv6 address) may not be discovered or a change of state (e.g. a movement) may be missed, leading to unreliable connectivity.

In the context of IEEE std. 802.15.4 [IEEEstd802154], the step of considering the radio as a medium that is different from Ethernet was already taken with the publication of Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) [RFC6775]. RFC 6775 is updated as [I-D.ietf-6lo-rfc6775-update]; the update includes changes that are required by this document.

This specification applies that same thinking to other wireless links such as Low-Power IEEE std. 802.11 (Wi-Fi) and IEEE std. 802.15.1 (Bluetooth) [IEEEstd802151], and extends [RFC6775] to enable proxy operation by the 6BBR so as to decouple the broadcast domain in the backbone from the wireless links. The proxy operation can be maintained asynchronous so that low-power nodes or nodes that are deep in a mesh do not need to be bothered synchronously when a lookup is performed for their addresses, effectively implementing the ND contribution to the concept of a Sleep Proxy [I-D.nordmark-6man-dad-approaches].

2. Applicability and Requirements Served

Efficiency aware IPv6 Neighbor Discovery Optimizations [I-D.chakrabarti-nordmark-6man-efficient-nd] suggests that 6LoWPAN ND [RFC6775] can be extended to other types of links beyond IEEE std. 802.15.4 for which it was defined. The registration technique is beneficial when the Link-Layer technique used to carry IPv6 multicast packets is not sufficiently efficient in terms of delivery ratio or energy consumption in the end devices, in particular to enable energy-constrained sleeping nodes. The value of such extension is especially apparent in the case of mobile wireless nodes, to reduce the multicast operations that are related to classical ND ([RFC4861], [RFC4862]) and plague the wireless medium.

This specification updates and generalizes 6LoWPAN ND to a broader range of Low power and Lossy Networks (LLNs) with a solid support for Duplicate Address Detection (DAD) and address lookup that does not require broadcasts over the LLNs. The term LLN is used loosely in this specification to cover multiple types of WLANs and WPANs, including Low-Power Wi-Fi, BLUETOOTH(R) Low Energy, IEEE std. 802.11AH and IEEE std. 802.15.4 wireless meshes, so as to address the requirements listed in Appendix A.3

The scope of this draft is a Backbone Link that federates multiple LLNs as a single IPv6 MultiLink Subnet. Each LLN in the subnet is anchored at an IPv6 Backbone Router (6BBR). The Backbone Routers interconnect the LLNs over the Backbone Link and emulate that the LLN nodes are present on the Backbone using proxy-ND operations. This specification extends IPv6 ND over the backbone to discriminate address movement from duplication and eliminate stale state in the backbone routers and backbone nodes once a LLN node has roamed. This way, mobile nodes may roam rapidly from a 6BBR to the next and requirements in Appendix A.1 are met.

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

The Link Layer Address (LLA) that is returned as Target LLA (TLLA) in Neighbor Advertisements (NA) messages by the 6BBR on behalf of the Registered Node over the backbone may be that of the Registering Node, in which case the 6BBR needs to bridge the unicast packets (Bridging proxy), or that of the 6BBR on the backbone, in which case the 6BBRs needs to route the unicast packets (Routing proxy). In the latter case, the 6BBR may maintain the list of correspondents to which it has advertised its own MAC address on behalf of the LLN node and the IPv6 ND operation is minimized as the number of nodes scale up in the LLN. This enables to meet the requirements in Appendix A.6 as long has the 6BBRs are dimensioned for the number of registration that each needs to support.

In the context of the the TimeSlotted Channel Hopping (TSCH) mode of [IEEEstd802154], the 6TiSCH architecture [I-D.ietf-6tisch-architecture] introduces how a 6LoWPAN ND host could connect to the Internet via a RPL mesh Network, but this requires additions to the 6LOWPAN ND protocol to support mobility and reachability in a secured and manageable environment. This specification details the new operations that are required to implement the 6TiSCH architecture and serves the requirements listed in Appendix A.2.

In the case of Low-Power IEEE std. 802.11, a 6BBR may be collocated with a standalone AP or a CAPWAP [RFC5415] wireless controller, and the wireless client (STA) leverages this specification to register its IPv6 address(es) to the 6BBR over the wireless medium. In the case of a 6TiSCH LLN mesh, the RPL root is collocated with a 6LoWPAN Border Router (6LBR), and either collocated with or connected to the 6BBR over an IPv6 Link. The 6LBR leverages this specification to register the LLN nodes on their behalf to the 6BBR. In the case of

BTLE, the 6BBR is collocated with the router that implements the BTLE central role as discussed in section 2.2 of [RFC7668].

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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

Readers would benefit from reading "Multi-Link Subnet Issues" [RFC4903], ,"Mobility Support in IPv6" [RFC6275], "Neighbor Discovery Proxies (ND Proxy)" [RFC4389] and "Optimistic Duplicate Address Detection" [RFC4429] prior to this specification for a clear understanding of the art in ND-proxying and binding.

Additionally, this document uses terminology from [RFC7102], [I-D.ietf-6lo-rfc6775-update] and [I-D.ietf-6tisch-terminology], and introduces the following terminology:

Sleeping Proxy A 6BBR acts as a Sleeping Proxy if it answers ND Neighbor Solicitation over the backbone on behalf of the Registered Node whenever possible. This is the default mode for this specification but it may be overridden, for instance by configuration, into Unicasting Proxy.

Unicasting Proxy As a Unicasting Proxy, the 6BBR forwards NS messages to the Registering Node, transforming Layer-2 multicast into unicast whenever possible.

Routing proxy A 6BBR acts as a routing proxy if it advertises its own MAC address, as opposed to that of the node that performs the registration, as the TLLA in the proxied NAs over the backbone. In that case, the MAC address of the node is not visible at Layer-2 over the backbone and the bridging fabric is not aware of the addresses of the LLN devices and their mobility. The 6BBR installs a connected host route towards the registered node over the interface to the node, and acts as a Layer-3 router for unicast packets to the node. The 6BBR updates the ND Neighbor Cache Entries (NCE) in correspondent

nodes if the wireless node moves and registers to another 6BBR, either with a single broadcast, or with a series of unicast NA(O) messages, indicating the TLLA of the new router.

Bridging proxy A 6BBR acts as a bridging proxy if it advertises the MAC address of the node that performs the registration as the TLLA in the proxied NAs over the backbone. In that case, the MAC address and the mobility of the node is still visible across the bridged backbone fabric, as is traditionally the case with Layer-2 APs. The 6BBR acts as a Layer-2 bridge for unicast packets to the registered node. The MAC address exposed in the S/TLLA is that of the Registering Node, which is not necessarily the Registered Device. When a device moves within a LLN mesh, it may end up attached to a different 6LBR acting as Registering Node, and the LLA that is exposed over the backbone will change.

Primary BBR The BBR that will defend a Registered Address for the purpose of DAD over the backbone.

Secondary BBR A BBR to which the address is registered. A Secondary Router MAY advertise the address over the backbone and proxy for it.

4. Overview

An LLN node can move freely from an LLN anchored at a Backbone Router to an LLN anchored at another Backbone Router on the same backbone and conserve any of the IPv6 addresses that it has formed, transparently.

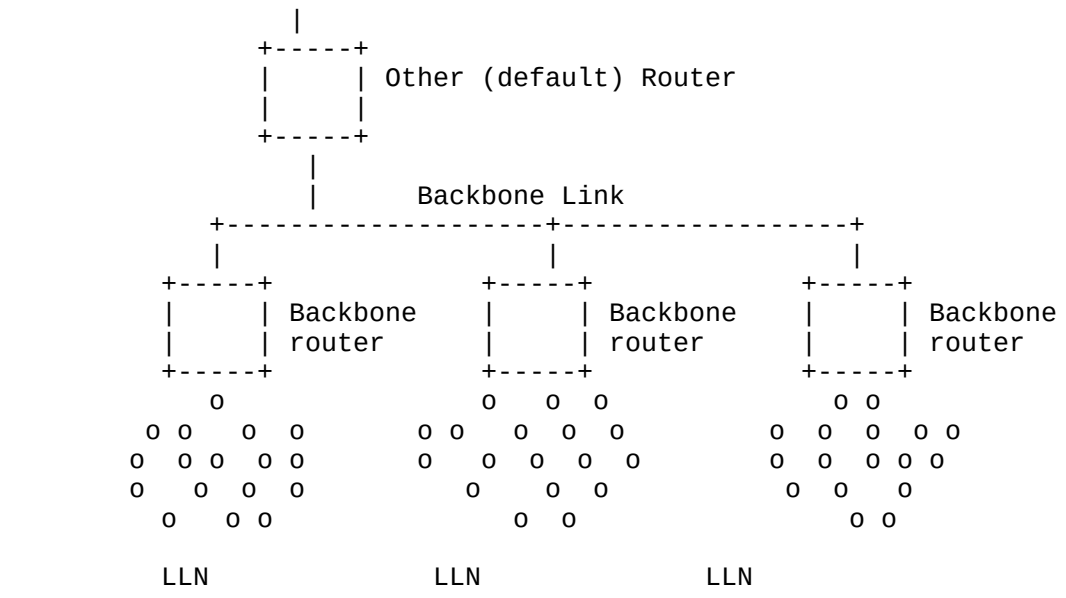

Figure 1: Backbone Link and Backbone Routers

The Backbone Routers maintain an abstract Binding Table of their Registered Nodes. The Binding Table operates as a distributed database of all the wireless Nodes whether they reside on the LLNs or on the backbone, and use an extension to the Neighbor Discovery Protocol to exchange that information across the Backbone in the classical ND reactive fashion.

The Extended Address Registration Option (ARO) defined in [I-D.ietf-6lo-rfc6775-update] is used to enable the registration for routing and proxy Neighbor Discovery operations by the 6BBR, and the Extended ARO (EARO) option is included in the ND exchanges over the backbone between the 6BBRs to sort out duplication from movement.

Address duplication is sorted out with the Owner Unique-ID field in the EARO, which is a generalization of the EUI-64 that allows different types of unique IDs beyond the name space derived from the MAC addresses. First-Come First-Serve rules apply, whether the duplication happens between LLN nodes as represented by their respective 6BBRs, or between an LLN node and a classical node that defends its address over the backbone with classical ND and does not include the EARO option.

In case of conflicting registrations to multiple 6BBRs from a same node, a sequence counter called Transaction ID (TID) is introduced

that enables 6BBRs to sort out the latest anchor for that node. Registrations with a same TID are compatible and maintained, but, in case of different TIDs, only the freshest registration is maintained and the stale state is eliminated.

With this specification, Backbone Routers perform ND proxy over the Backbone Link on behalf of their Registered Nodes. The Backbone Router operation is essentially similar to that of a Mobile IPv6 (MIPv6) [RFC6275] Home Agent. This enables mobility support for LLN nodes that would move outside of the network delimited by the Backbone link attach to a Home Agent from that point on. This also enables collocation of Home Agent functionality within Backbone Router functionality on the same backbone interface of a router. Further specification may extend this be allowing the 6BBR to redistribute host routes in routing protocols that would operate over the backbone, or in MIPv6 or the Locator/ID Separation Protocol (LISP) [RFC6830] to support mobility on behalf of the nodes, etc...

The Optimistic Duplicate Address Detection [RFC4429] (ODAD) specification details how an address can be used before a Duplicate Address Detection (DAD) is complete, and insists that an address that is TENTATIVE should not be associated to a Source Link-Layer Address Option in a Neighbor Solicitation message. This specification leverages ODAD to create a temporary proxy state in the 6BBR till DAD is completed over the backbone. This way, the specification enables to distribute proxy states across multiple 6BBR and co-exist with classical ND over the backbone.

5. Backbone Router Routing Operations

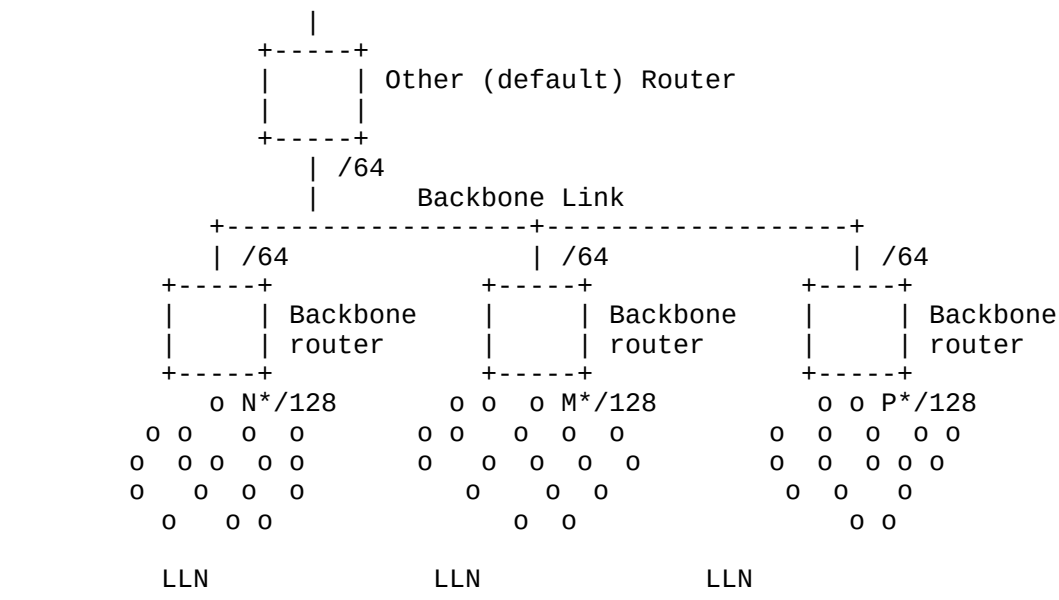

Figure 2: Routing Configuration in the ML Subnet

5.1. Over the Backbone Link

The Backbone Router is a specific kind of Border Router that performs proxy Neighbor Discovery on its backbone interface on behalf of the nodes that it has discovered on its LLN interfaces.

The backbone is expected to be a high speed, reliable Backbone link, with affordable and reliable multicast capabilities, such as a bridged Ethernet Network, and to allow a full support of classical ND as specified in [RFC4861] and subsequent RFCs. In other words, the backbone is not a LLN.

Still, some restrictions of the attached LLNs will apply to the backbone. In particular, it is expected that the MTU is set to the same value on the backbone and all attached LLNs, and the scalability of the whole subnet requires that broadcast operations are avoided as much as possible on the backbone as well. Unless configured otherwise, the Backbone Router MUST echo the MTU that it learns in RAs over the backbone in the RAs that it sends towards the LLN links.

As a router, the Backbone Router behaves like any other IPv6 router on the backbone side. It has a connected route installed towards the backbone for the prefixes that are present on that backbone and that it proxies for on the LLN interfaces.

As a proxy, the 6BBR uses an EARO option in the NS-DAD and the multicast NA messages that it generates on behalf of a Registered Node, and it places an EARO in its unicast NA messages if and only if the NS/NA that stimulates it had an EARO in it.

When possible, the 6BBR SHOULD use unicast or solicited-node multicast address (SNMA) [RFC4291] to defend its Registered Addresses over the backbone. In particular, the 6BBR MUST join the SNMA group that corresponds to a Registered Address as soon as it creates an entry for that address and as long as it maintains that entry, whatever the state of the entry. The expectation is that it is possible to get a message delivered to all the nodes on the backbone that listen to a particular address and support this specification - which includes all the 6BBRs in the MultiLink Subnet - by sending a multicast message to the associated SNMA over the backbone.

The support of Optimistic DAD (ODAD) [RFC4429] is recommended for all nodes in the backbone and followed by the 6BBRs in their proxy activity over the backbone. With ODAD, any optimistic node MUST join the SNMA of a Tentative address, which interacts better with this specification.

This specification allows the 6BBR in Routing Proxy mode to advertise the Registered IPv6 Address with the 6BBR Link Layer Address, and attempts to update Neighbor Cache Entries (NCE) in correspondent nodes over the backbone, using gratuitous NA(Override). This method may fail of the multicast message is not properly received, and correspondent nodes may maintain an incorrect neighbor state, which they will eventually discover through Neighbor Unreachability Detection (NUD). Because mobility may be slow, the NUD procedure defined in [RFC4861] may be too impatient, and the support of [RFC7048] is recommended in all nodes in the network.

Since the MultiLink Subnet may grow very large in terms of individual IPv6 addresses, multicasts should be avoided as much as possible even on the backbone. Though it is possible for plain hosts to participate with legacy IPv6 ND support, the support by all nodes connected to the backbone of [I-D.ietf-6man-rs-refresh] is recommended, and this implies the support of [RFC7559] as well.

5.2. Over the LLN Link

As a router, the Nodes and Backbone Router operation on the LLN follows [RFC6775]. Per that specification, LLN Hosts generally do not depend on multicast RAs to discover routers. It is still generally required for LLN nodes to accept multicast RAs [RFC7772], but those are rare on the LLN link. Nodes are expected to follow the Simple Procedures for Detecting Network Attachment in IPv6 [RFC6059]

(DNA procedures) to assert movements, and to support the Packet-Loss Resiliency for Router Solicitations [RFC7559] to make the unicast RS more reliable.

The Backbone Router acquires its states about the addresses on the LLN side through a registration process from either the nodes themselves, or from a node such as a RPL root / 6LBR (the Registering Node) that performs the registration on behalf of the address owner (the Registered Node).

When operating as a Routing Proxy, the router installs hosts routes (/128) to the Registered Addresses over the LLN links, via the Registering Node as identified by the Source Address and the SLLAO option in the NS(EARO) messages.

In that mode, the 6BBR handles the ND protocol over the backbone on behalf of the Registered Nodes, using its own MAC address in the TLLA and SLLA options in proxyed NS and NA messages. It results that for each Registered Address, a number of peer Nodes on the backbone have resolved the address with the 6BBR MAC address and keep that mapping stored in their Neighbor cache.

The 6BBR SHOULD maintain, per Registered Address, the list of the peers on the backbone to which it answered with it MAC address, and when a binding moves to a different 6BBR, it SHOULD send a unicast gratuitous NA(O) individually to each of them to inform them that the address has moved and pass the MAC address of the new 6BBR in the TLLAO option. If the 6BBR can not maintain that list, then it SHOULD remember whether that list is empty or not and if not, send a multicast NA(O) to all nodes to update the impacted Neighbor Caches with the information from the new 6BBR.

The Bridging Proxy is a variation where the BBR function is implemented in a Layer-3 switch or an wireless Access Point that acts as a Host from the IPv6 standpoint, and, in particular, does not operate the routing of IPv6 packets. In that case, the SLLAO in the proxied NA messages is that of the Registering Node and classical bridging operations take place on data frames.

If a registration moves from one 6BBR to the next, but the Registering Node does not change, as indicated by the S/TLLAO option in the ND exchanges, there is no need to update the Neighbor Caches in the peers Nodes on the backbone. On the other hand, if the LLAO changes, the 6BBR SHOULD inform all the relevant peers as described above, to update the impacted Neighbor Caches. In the same fashion, if the Registering Node changes with a new registration, the 6BBR SHOULD also update the impacted Neighbor Caches over the backbone.

6. BackBone Router Proxy Operations

This specification enables a Backbone Router to proxy Neighbor Discovery operations over the backbone on behalf of the nodes that are registered to it, allowing any node on the backbone to reach a Registered Node as if it was on-link. The backbone and the LLNs are considered different Links in a MultiLink subnet but the prefix that is used may still be advertised as on-link on the backbone to support legacy nodes; multicast ND messages are link-scoped and not forwarded across the backbone routers.

ND Messages on the backbone side that do not match to a registration on the LLN side are not acted upon on the LLN side, which stands protected. On the LLN side, the prefixes associated to the MultiLink Subnet are presented as not on-link, so address resolution for other hosts do not occur.

The default operation in this specification is Sleeping proxy which means:

- creating a new entry in an abstract Binding Table for a new Registered Address and validating that the address is not a duplicate over the backbone
- defending a Registered Address over the backbone using NA messages with the Override bit set on behalf of the sleeping node whenever possible
- advertising a Registered Address over the backbone using NA messages, asynchronously or as a response to a Neighbor Solicitation messages.
- Looking up a destination over the backbone in order to deliver packets arriving from the LLN using Neighbor Solicitation messages.
- Forwarding packets from the LLN over the backbone, and the other way around.
- Eventually triggering a liveliness verification of a stale registration.

A 6BBR may act as a Sleeping Proxy only if the state of the binding entry is REACHABLE, or TENTATIVE in which case the answer is delayed. In any other state, the Sleeping Proxy operates as a Unicasting Proxy.

As a Unicasting Proxy, the 6BBR forwards NS messages to the Registering Node, transforming Layer-2 multicast into unicast whenever possible. This is not possible in UNREACHABLE state, so the NS messages are multicasted, and rate-limited to protect the medium with an exponential back-off. In other states, The messages are forwarded to the Registering Node as unicast Layer-2 messages. In TENTATIVE state, the NS message is either held till DAD completes, or dropped.

The draft introduces the optional concept of primary and secondary BBRs. The primary is the backbone router that has the highest EUI-64 address of all the 6BBRs that share a registration for a same Registered Address, with the same Owner Unique ID and same Transaction ID, the EUI-64 address being considered as an unsigned 64bit integer. The concept is defined with the granularity of an address, that is a given 6BBR can be primary for a given address and secondary or another one, regardless on whether the addresses belong to the same node or not. The primary Backbone Router is in charge of protecting the address for DAD over the Backbone. Any of the Primary and Secondary 6BBR may claim the address over the backbone, since they are all capable to route from the backbone to the LLN node, and the address appears on the backbone as an anycast address.

The Backbone Routers maintain a distributed binding table, using classical ND over the backbone to detect duplication. This specification requires that:

1. All addresses that can be reachable from the backbone, including IPv6 addresses based on burn-in EUI64 addresses MUST be registered to the 6BBR.

2. A Registered Node MUST include the EARO option in an NS message that used to register an addresses to a 6LR; the 6LR MUST propagate that option unchanged to the 6LBR in the DAR/DAC exchange, and the 6LBR MUST propagate that option unchanged in proxy registrations.

3. The 6LR MUST echo the same EARO option in the NA that it uses to respond, but for the status filed which is not used in NS messages, and significant in NA.

A false positive duplicate detection may arise over the backbone, for instance if the Registered Address is registered to more than one LBR, or if the node has moved. Both situations are handled gracefully unbeknownst to the node. In the former case, one LBR becomes primary to defend the address over the backbone while the others become secondary and may still forward packets back and forth.

In the latter case the LBR that receives the newest registration wins and becomes primary.

The expectation in this specification is that there is a single Registering Node at a time per Backbone Router for a given Registered Address, but that a Registered Address may be registered to Multiple 6BBRs for higher availability.

Over the LLN, and for any given Registered Address, it is REQUIRED that:

de-registrations (newer TID, same OUID, null Lifetime) are accepted and responded immediately with a status of 4; the entry is deleted;

newer registrations (newer TID, same OUID, non-null Lifetime) are accepted and responded with a status of 0 (success); the entry is updated with the new TID, the new Registration Lifetime and the new Registering Node, if any has changed; in TENTATIVE state the response is held and may be overwritten; in other states the Registration-Lifetime timer is restarted and the entry is placed in REACHABLE state.

identical registrations (same TID, same OUID) from a same Registering Node are not processed but responded with a status of 0 (success); they are expected to be identical and an error may be logged if not; in TENTATIVE state, the response is held and may be overwritten, but it MUST be eventually produced and it carries the result of the DAD process;

older registrations (not(newer or equal) TID, same OUID) from a same Registering Node are ignored;

identical and older registrations (not-newer TID, same OUID) from a different Registering Node are responded immediately with a status of 3 (moved); this may be rate limited to protect the medium;

and any registration for a different Registered Node (different OUID) are responded immediately with a status of 1 (duplicate).

6.1. Registration and Binding State Creation

Upon a registration for a new address with an NS(EARO), the 6BBR performs a DAD operation over the backbone placing the new address as target in the NS-DAD message. The EARO from the registration MUST be placed unchanged in the NS-DAD message, and an entry is created in TENTATIVE state for a duration of TENTATIVE_DURATION. The NS-DAD

message is sent multicast over the backbone to the SNMA address associated with the registered address. If that operation is known to be costly, and the 6BBR has an indication from another source (such as a NCE) that the Registered Address was present on the backbone, that information may be leveraged to send the NS-DAD message as a Layer-2 unicast to the MAC that was associated with the Registered Address.

In TENTATIVE state:

- the entry is removed if an NA is received over the backbone for the Registered Address with no EARO option, or with an EARO option with a status of 1 (duplicate) that indicates an existing registration for another LLN node. The OUID and TID fields in the EARO option received over the backbone are ignored. A status of 1 is returned in the EARO option of the NA back to the Registering Node;

- the entry is also removed if an NA with an ARO option with a status of 3 (moved), or a NS-DAD with an ARO option that indicates a newer registration for the same Registered Node, is received over the backbone for the Registered Address. A status of 3 is returned in the NA(EARO) back to the Registering Node;

- when a registration is updated but not deleted, e.g. from a newer registration, the DAD process on the backbone continues and the running timers are not restarted;

- Other NS (including DAD with no EARO option) and NA from the backbone are not responded in TENTATIVE state, but the list of their origins may be kept in memory and if so, the 6BBR may send them each a unicast NA with eventually an EARO option when the TENTATIVE_DURATION timer elapses, so as to cover legacy nodes that do not support ODAD.

- When the TENTATIVE_DURATION timer elapses, a status 0 (success) is returned in a NA(EARO) back to the Registering Node(s), and the entry goes to REACHABLE state for the Registration Lifetime; the DAD process is successful and the 6BBR MUST send a multicast NA(EARO) to the SNMA associated to the Registered Address over the backbone with the Override bit set so as to take over the binding from other 6BBRs.

6.2. Defending Addresses

If a 6BBR has an entry in REACHABLE state for a Registered Address:

- If the 6BBR is primary, or does not support the concept, it MUST defend that address over the backbone upon an incoming NS-DAD, either if the NS does not carry an EARO, or if an EARO is present that indicates a different Registering Node (different OUID). The 6BBR sends a NA message with the Override bit set and the NA carries an EARO option if and only if the NS-DAD did so. When present, the EARO in the NA(O) that is sent in response to the NS-DAD(EARO) carries a status of 1 (duplicate), and the OUID and TID fields in the EARO option are obfuscated with null or random values to avoid network scanning and impersonation attacks.

- If the 6BBR receives an NS-DAD(EARO) that reflect a newer registration, the 6BBR updates the entry and the routing state to forward packets to the new 6BBR, but keeps the entry REACHABLE. In that phase, it MAY use REDIRECT messages to reroute traffic for the Registered Address to the new 6BBR.

- If the 6BBR receives an NA(EARO) that reflect a newer registration, the 6BBR removes its entry and sends a NA(AERO) with a status of 3 (moved) to the Registering Node, if the Registering Node is different from the Registered Node. If necessary, the 6BBR cleans up ND cache in peers nodes as discussed in Section 5.1, by sending a series of unicast to the impacted nodes, or one broadcast NA(O) to all-nodes.

- If the 6BBR received a NS(LOOKUP) for a Registered Address, it answers immediately with an NA on behalf of the Registered Node, without polling it. There is no need of an EARO in that exchange.

- When the Registration-Lifetime timer elapses, the entry goes to STALE state for a duration of STABLE_STALE_DURATION in LLNs that keep stable addresses such as LWPANs, and UNSTABLE_STALE_DURATION in LLNs where addresses are renewed rapidly, e.g. for privacy reasons.

The STALE state is a chance to keep track of the backbone peers that may have an ND cache pointing on this 6BBR in case the Registered Address shows back up on this or a different 6BBR at a later time. In STALE state:

- If the Registered Address is claimed by another node on the backbone, with an NS-DAD or an NA, the 6BBR does not defend the address. Upon an NA(O), or the stale time elapses, the 6BBR removes its entry and sends a NA(AERO) with a status of 4 (removed) to the Registering Node.

- If the 6BBR received a NS(LOOKUP) for a Registered Address, the 6BBR MUST send an NS(NUD) following rules in [RFC7048] to the

registering Node targeting the Registered Address prior to answering. If the NUD succeeds, the operation in REACHABLE state applies. If the NUD fails, the 6BBR refrains from answering the lookup. The NUD expected to be mapped by the Registering Node into a liveliness validation of the Registered Node if they are in fact different nodes.

7. Security Considerations

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

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

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

8. Protocol Constants

This Specification uses the following constants:

TENTATIVE_DURATION: 800 milliseconds

STABLE_STALE_DURATION: 24 hours

UNSTABLE_STALE_DURATION: 5 minutes

DEFAULT_NS_POLLING: 3 times

9. IANA Considerations

This document has no request to IANA.

10. Acknowledgments

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

11. References

11.1. Normative References

[I-D.ietf-6lo-rfc6775-update]
Thubert, P., Nordmark, E., and S. Chakrabarti, "An Update to 6LoWPAN ND", draft-ietf-6lo-rfc6775-update-06 (work in progress), June 2017.

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

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <http://www.rfc-editor.org/info/rfc4429>.

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

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC6059] Krishnan, S. and G. Daley, "Simple Procedures for Detecting Network Attachment in IPv6", RFC 6059, DOI 10.17487/RFC6059, November 2010, <http://www.rfc-editor.org/info/rfc6059>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <http://www.rfc-editor.org/info/rfc6550>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <http://www.rfc-editor.org/info/rfc6775>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <http://www.rfc-editor.org/info/rfc8200>.

11.2. Informative References

[I-D.chakrabarti-nordmark-6man-efficient-nd] Chakrabarti, S., Nordmark, E., Thubert, P., and M. Wasserman, "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", draft-chakrabarti-nordmark-6man-efficient-nd-07 (work in progress), February 2015.

[I-D.delcarpio-6lo-wlanah] Vega, L., Robles, I., and R. Morabito, "IPv6 over 802.11ah", draft-delcarpio-6lo-wlanah-01 (work in progress), October 2015.

[I-D.ietf-6lo-ap-nd] Sarikaya, B., Thubert, P., and M. Sethi, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-02 (work in progress), May 2017.

[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-07 (work in progress), June 2017.

[I-D.ietf-6man-rs-refresh] Nordmark, E., Yourtchenko, A., and S. Krishnan, "IPv6 Neighbor Discovery Optional RS/RA Refresh", draft-ietf-6man-rs-refresh-02 (work in progress), October 2016.

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

[I-D.ietf-6tisch-terminology]
Palattella, M., Thubert, P., Watteyne, T., and Q. Wang, "Terminology in IPv6 over the TSCH mode of IEEE 802.15.4e", draft-ietf-6tisch-terminology-09 (work in progress), June 2017.

[I-D.ietf-bier-architecture]
Wijnands, I., Rosen, E., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast using Bit Index Explicit Replication", draft-ietf-bier-architecture-07 (work in progress), June 2017.

[I-D.ietf-ipv6-multilink-subnets]
Thaler, D. and C. Huitema, "Multi-link Subnet Support in IPv6", draft-ietf-ipv6-multilink-subnets-00 (work in progress), July 2002.

[I-D.nordmark-6man-dad-approaches]
Nordmark, E., "Possible approaches to make DAD more robust and/or efficient", draft-nordmark-6man-dad-approaches-02 (work in progress), October 2015.

[I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks]
Popa, D. and J. Hui, "6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks", draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00 (work in progress), March 2014.

[I-D.vyncke-6man-mcast-not-efficient]
Vyncke, E., Thubert, P., Levy-Abegnoli, E., and A. Yourtchenko, "Why Network-Layer Multicast is Not Always Efficient At Datalink Layer", draft-vyncke-6man-mcast-not-efficient-01 (work in progress), February 2014.

[I-D.yourtchenko-6man-dad-issues]
Yourtchenko, A. and E. Nordmark, "A survey of issues related to IPv6 Duplicate Address Detection", draft-yourtchenko-6man-dad-issues-01 (work in progress), March 2015.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <http://www.rfc-editor.org/info/rfc3810>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <http://www.rfc-editor.org/info/rfc3971>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <http://www.rfc-editor.org/info/rfc3972>.

[RFC4389] Thaler, D., Talwar, M., and C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389, DOI 10.17487/RFC4389, April 2006, <http://www.rfc-editor.org/info/rfc4389>.

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

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <http://www.rfc-editor.org/info/rfc4919>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <http://www.rfc-editor.org/info/rfc5415>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <http://www.rfc-editor.org/info/rfc6275>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <http://www.rfc-editor.org/info/rfc6282>.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <http://www.rfc-editor.org/info/rfc6830>.

[RFC7048] Nordmark, E. and I. Gashinsky, "Neighbor Unreachability Detection Is Too Impatient", RFC 7048, DOI 10.17487/RFC7048, January 2014, <http://www.rfc-editor.org/info/rfc7048>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <http://www.rfc-editor.org/info/rfc7102>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <http://www.rfc-editor.org/info/rfc7217>.

[RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015, <http://www.rfc-editor.org/info/rfc7428>.

[RFC7559] Krishnan, S., Anipko, D., and D. Thaler, "Packet-Loss Resiliency for Router Solicitations", RFC 7559, DOI 10.17487/RFC7559, May 2015, <http://www.rfc-editor.org/info/rfc7559>.

[RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <http://www.rfc-editor.org/info/rfc7668>.

[RFC7772] Yourtchenko, A. and L. Colitti, "Reducing Energy Consumption of Router Advertisements", BCP 202, RFC 7772, DOI 10.17487/RFC7772, February 2016, <http://www.rfc-editor.org/info/rfc7772>.

[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, <http://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, <http://www.rfc-editor.org/info/rfc8163>.

11.3. External Informative References

[IEEEstd8021]
IEEE standard for Information Technology, "IEEE Standard for Information technology-- Telecommunications and information exchange between systems Local and metropolitan area networks Part 1: Bridging and Architecture".

[IEEEstd80211]
IEEE standard for Information Technology, "IEEE Standard for Information technology-- Telecommunications and information exchange between systems Local and metropolitan area networks-- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[IEEEstd802151]
IEEE standard for Information Technology, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)".

[IEEEstd802154]
IEEE standard for Information Technology, "IEEE Standard for Local and metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)".

Appendix A. Requirements

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

A.1. Requirements Related to Mobility

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

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

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

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

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

A.2. Requirements Related to Routing Protocols

The point of attachment of a 6LoWPAN Node may be a 6LR in an LLN mesh. IPv6 routing in a LLN can be based on RPL, which is the routing protocol that was defined at the IETF for this particular purpose. Other routing protocols than RPL are also considered by Standard Defining Organizations (SDO) on the basis of the expected network characteristics. It is required that a 6LoWPAN Node attached via ND to a 6LR would need to participate in the selected routing protocol to obtain reachability via the 6LR.

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

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

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

Related requirements are:

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

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

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

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

6LoWPAN ND [RFC6775] was defined with a focus on IEEE std. 802.15.4 and in particular the capability to derive a unique Identifier from a globally unique MAC-64 address. At this point, the 6lo Working Group is extending the 6LoWPAN Header Compression (HC) [RFC6282] technique to other link types ITU-T G.9959 [RFC7428], Master-Slave/Token-Passing [RFC8163], DECT Ultra Low Energy [RFC8105], Near Field Communication [I-D.ietf-6lo-nfc], IEEE std. 802.11ah [I-D.delcarpio-6lo-wlanah], as well as IEEE1901.2 Narrowband Powerline Communication Networks [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks] and BLUETOOTH(R) Low Energy [RFC7668].

Related requirements are:

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

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

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

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

A.4. Requirements Related to Proxy Operations

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

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

Related requirements are:

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

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

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

A.5. Requirements Related to Security

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

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

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

Related requirements are:

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

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

Req5.3: 6LoWPAN ND security mechanisms SHOULD lead to small packet sizes. In particular, the NS, NA, DAR and DAC messages for a re-registration flow SHOULD NOT exceed 80 octets so as to fit in a secured IEEE std. 802.15.4 frame.

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

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

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

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

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

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

A.6. Requirements Related to Scalability

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

Related requirements are:

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

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

Author's Address

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

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

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 2, 2018

Y. Choi, Ed.
Y-G. Hong, Ed.
ETRI
J-S. Youn
Dongeui Univ
D-K. Kim
KNU
J-H. Choi
Samsung Electronics Co.,
October 29, 2017

Transmission of IPv6 Packets over Near Field Communication
draft-ietf-6lo-nfc-08

Abstract

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

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at 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 2, 2018.

Table of Contents

1. Introduction

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

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

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

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

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Overview of Near Field Communication Technology

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

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

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

3.1. Peer-to-peer Mode of NFC

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

3.2. Protocol Stacks of NFC

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

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

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

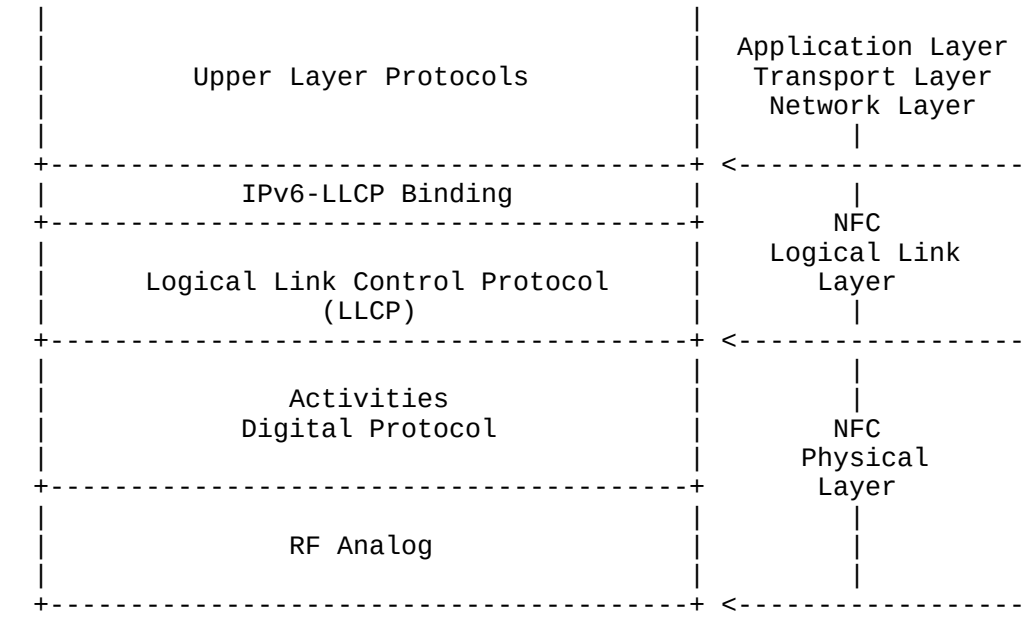

Figure 1: Protocol Stacks of NFC

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

3.3. NFC-enabled Device Addressing

According to NFC Logical Link Control Protocol v1.3 [LLCP-1.3], NFC-enabled devices have two types of 6-bit addresses (i.e., SSAP and DSAP) to identify service access points. The several service access points can be installed on a NFC device. However, the SSAP and DSAP can be used as identifiers for NFC link connections with the IPv6 over NFC adaptation layer. Therefore, the SSAP can be used to generate an IPv6 interface identifier. Address values between 00h and 0Fh of SSAP and DSAP are reserved for identifying the well-known service access points, which are defined in the NFC Forum Assigned Numbers Register. Address values between 10h and 1Fh SHALL be assigned by the local LLC to services registered by local service environment. In addition, address values between 20h and 3Fh SHALL be assigned by the local LLC as a result of an upper layer service request. Therefore, the address values between 20h and 3Fh can be used for generating IPv6 interface identifiers.

3.4. MTU of NFC Link Layer

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

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

$$MIU = 128 + MIUX.$$

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

4. Specification of IPv6 over NFC

NFC technology also has considerations and requirements owing to low power consumption and allowed protocol overhead. 6LoWPAN standards [RFC4944], [RFC6775], and [RFC6282] provide useful functionality for reducing overhead which can be applied to NFC. This functionality consists of link-local IPv6 addresses and stateless IPv6 address auto-configuration (see Section 4.3), Neighbor Discovery (see Section 4.5) and header compression (see Section 4.7).

4.1. Protocol Stacks

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

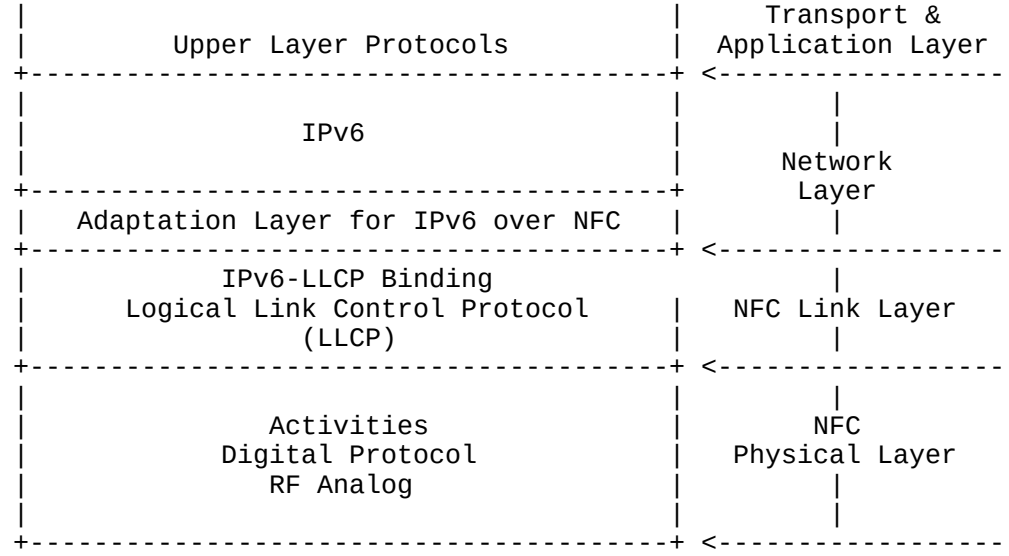

Figure 2: Protocol Stacks for IPv6 over NFC

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

4.2. Link Model

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

contrast, does not support the FAR functionality, so IPv6 over NFC needs to consider the FAR functionality, defined in [RFC4944]. However, the MTU on an NFC link can be configured in a connection procedure and extended enough to fit the MTU of IPv6 packet (see Section 4.8).

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

4.3. Stateless Address Autoconfiguration

An NFC-enabled device (i.e., 6LN) performs stateless address autoconfiguration as per [RFC4862]. A 64-bit Interface identifier (IID) for an NFC interface is formed by utilizing the 6-bit NFC LLCP address (see Section 3.3). In the viewpoint of address configuration, such an IID SHOULD guarantee a stable IPv6 address because each data link connection is uniquely identified by the pair of DSAP and SSAP included in the header of each LLC PDU in NFC.

Following the guidance of [RFC7136], interface identifiers of all unicast addresses for NFC-enabled devices are 64 bits long and constructed by using the generation algorithm of random (but stable) identifier (RID) [RFC7217] (see Figure 3).

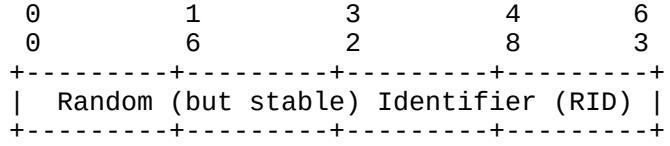

Figure 3: IID from NFC-enabled device

The RID is an output which MAY be created by the algorithm, F() with input parameters. One of the parameters is Net_IFace, and NFC Link Layer address (i.e., SSAP) MAY be a source of the NetIFace parameter. The 6-bit address of SSAP of NFC is easy and short to be targeted by attacks of third party (e.g., address scanning). The F() can provide secured and stable IIDs for NFC-enabled devices.

In addition, the "Universal/Local" bit (i.e., the ’u’ bit) of an NFC-enabled device address MUST be set to 0 [RFC4291].

4.4. IPv6 Link Local Address

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

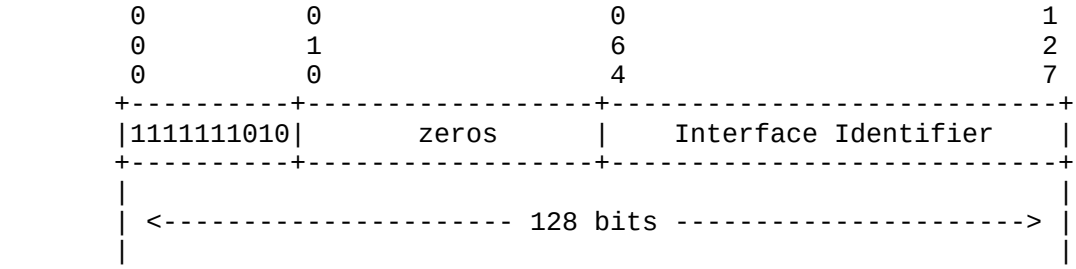

Figure 4: IPv6 link-local address in NFC

The tool for a 6LBR to obtain an IPv6 prefix for numbering the NFC network is can be accomplished via DHCPv6 Prefix Delegation ([RFC3633]).

4.5. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs ([RFC6775]) describes the neighbor discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC does not support a complicated mesh topology but only a simple multi-hop network topology or directly connected peer-to-peer network. Therefore, the following aspects of RFC 6775 are applicable to NFC:

- In a case that an NFC-enabled device (6LN) is directly connected to a 6LBR, an NFC 6LN MUST register its address with the 6LBR by sending a Neighbor Solicitation (NS) message with the Address Registration Option (ARO) and process the Neighbor Advertisement (NA) accordingly. In addition, if DHCPv6 is used to assign an address, Duplicate Address Detection (DAD) MAY not be required.

- In a case that two or more NFC 6LNs meet within a sigle hop range (e.g., isolated network), one of them can become a router for 6LR/6LBR. If they have the same properties, any of them can be a router. Unless they are the same (e.g., different MTU, level of remaining energy, connectivity, etc.), a performance-outstanding device can become a router.

o For sending Router Solicitations and processing Router Advertisements, the NFC 6LNs MUST follow Sections 5.3 and 5.4 of RFC 6775.

4.6. Dispatch Header

All IPv6-over-NFC encapsulated datagrams are prefixed by an encapsulation header stack consisting of a Dispatch value followed by zero or more header fields. The only sequence currently defined for IPv6-over-NFC is the LOWPAN_IPHC header followed by payload, as depicted in Figure 5.

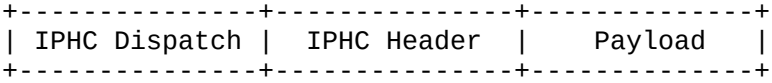

Figure 5: A IPv6-over-NFC Encapsulated 6LOWPAN_IPHC Compressed IPv6 Datagram

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

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

Figure 6: Dispatch Values

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

4.7. Header Compression

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

Therefore, IPv6 header compression in [RFC6282] MUST be implemented. Further, implementations MAY also support Generic Header Compression (GHC) of [RFC7400].

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

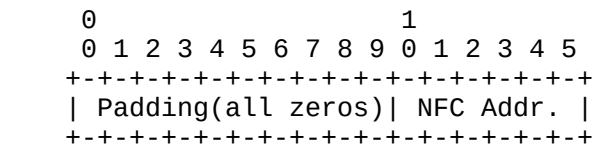

Figure 7: NFC short address format

4.8. Fragmentation and Reassembly

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

4.9. Unicast Address Mapping

The address resolution procedure for mapping IPv6 non-multicast addresses into NFC link-layer addresses follows the general description in Section 7.2 of [RFC4861], unless otherwise specified.

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

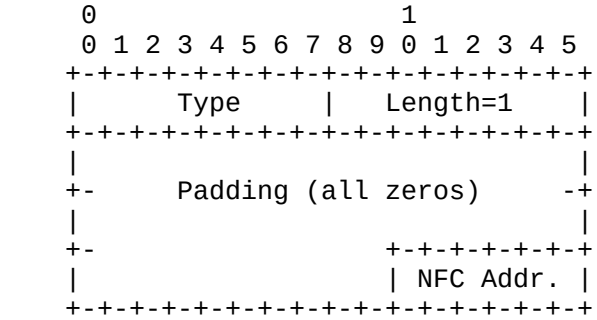

Figure 8: Unicast address mapping

Option fields:

Type:

1: for Source Link-layer address.

2: for Target Link-layer address.

Length:

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

NFC address:

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

4.10. Multicast Address Mapping

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

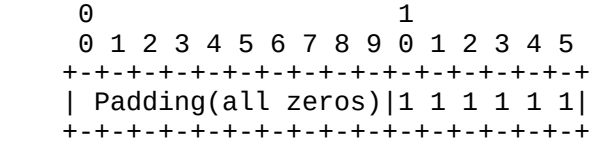

Figure 9: Multicast address mapping

5. Internet Connectivity Scenarios

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

5.1. NFC-enabled Device Connected to the Internet

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

Wi-Fi, NFC, etc.) to send data depending on the characteristics of the data.

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

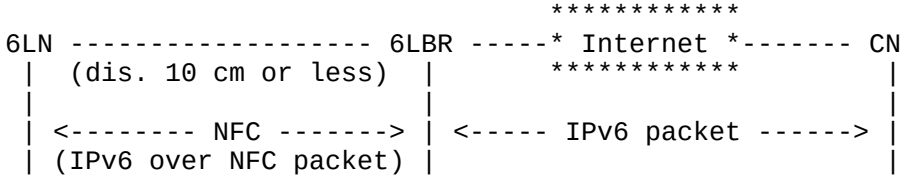

Figure 10: NFC-enabled device network connected to the Internet

5.2. Isolated NFC-enabled Device Network

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

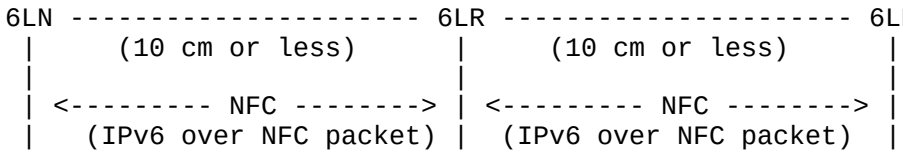

Figure 11: Isolated NFC-enabled device network

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

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

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

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

IPv6-over-NFC uses an IPv6 interface identifier formed from a "Short Address" and a set of well-known constant bits (such as padding with ’0’s) for the modified EUI-64 format. However, the short address of NFC link layer (LLC) is not generated as a physically permanent value but logically generated for each connection. Thus, every single touch connection can use a different short address of NFC link with an extremely short-lived link. This can mitigate address scanning as well as location tracking and device-specific vulnerability exploitation.

8. Acknowledgements

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

Michael Richardson, Suresh Krishnan, Pascal Thubert, Carsten Bormann, Alexandru Petrescu, James Woodyatt, Dave Thaler, Samita Chakrabarti, and Gabriel Montenegro have provided valuable feedback for this draft.

9. References

9.1. Normative References

[LLCP-1.3] "NFC Logical Link Control Protocol version 1.3", NFC Forum Technical Specification , March 2016.

[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>.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, DOI 10.17487/RFC3633, December 2003, <https://www.rfc-editor.org/info/rfc3633>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

9.2. Informative References

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

Authors' Addresses

Younghwan Choi (editor)
Electronics and Telecommunications Research Institute
218 Gajeongno, Yuseung-gu
Daejeon 34129
Korea

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

Yong-Geun Hong (editor)
Electronics and Telecommunications Research Institute
161 Gajeong-Dong Yuseung-gu
Daejeon 305-700
Korea

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

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

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

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

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

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

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

6lo
Internet-Draft
Updates: 6775 (if approved)
Intended status: Standards Track
Expires: April 16, 2018

P. Thubert, Ed.
cisco
E. Nordmark
S. Chakrabarti

C. Perkins
Futurewei

October 13, 2017

An Update to 6LoWPAN ND
draft-ietf-6lo-rfc6775-update-10

Abstract

This specification updates RFC 6775 - 6LoWPAN Neighbor Discovery, to clarify the role of the protocol as a registration technique, simplify the registration operation in 6LoWPAN routers, as well as to provide enhancements to the registration capabilities and mobility detection for different network topologies including the backbone routers performing proxy Neighbor Discovery in a low power network.

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 April 16, 2018.

Copyright Notice

Table of Contents

1. Introduction

The scope of this draft is an IPv6 Low Power Networks including star and mesh topologies. This specification modifies and extends the behavior and protocol elements of "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks" (6LoWPAN ND) [RFC6775] to enable additional capabilities and enhancements such as:

- Support for indicating mobility vs retry (T-bit)
- Reduce requirement of registration for link-local addresses
- Enhancement to Address Registration Option (ARO)
- Permitting registration of a target address
- Clarification of support of privacy and temporary addresses

The applicability of 6LoWPAN ND registration is discussed in Section 2, and new extensions and updates to [RFC6775] are presented in Section 4. Considerations on Backward Compatibility, Security and Privacy are also elaborated upon in Section 7, Section 8 and in Section 9, respectively.

2. Applicability of Address Registration Options

The purpose of the Address Registration Option (ARO) in the legacy 6LoWPAN ND specification is to facilitate duplicate address detection (DAD) for hosts as well as populate Neighbor Cache Entries (NCE) [RFC4861] in the routers. This reduces the reliance on multicast operations, which are often as intrusive as broadcast, in IPv6 ND operations.

With this specification, a failed or useless registration can be detected for reasons other than address duplication. Examples include: the router having run out of space; a registration bearing a stale sequence number perhaps denoting a movement of the host after the registration was placed; a host misbehaving and attempting to register an invalid address such as the unspecified address

[RFC4291]; or a host using an address which is not topologically correct on that link.

In such cases the host will receive an error to help diagnose the issue and may retry, possibly with a different address, and possibly registering to a different router, depending on the returned error. The ability to return errors to address registrations is not intended to be used to restrict the ability of hosts to form and use addresses, as recommended in "Host Address Availability Recommendations" [RFC7934].

In particular, the freedom to form and register addresses is needed for enhanced privacy; each host may register a number of addresses using mechanisms such as "Privacy Extensions for Stateless Address Autoconfiguration (SLAAC) in IPv6" [RFC4941].

In IPv6 ND [RFC4861], a router must have enough storage to hold neighbor cache entries for all the addresses to which it may forward. A router using the Address Registration mechanism also needs enough storage to hold NCEs for all the addresses that may be registered to it, regardless of whether or not they are actively communicating. The number of registrations supported by a 6LoWPAN Router (6LR) or 6LoWPAN Border Router (6LBR) must be clearly documented.

A network administrator should deploy updated 6LR/6LBRs to support the number and type of devices in his network, based on the number of IPv6 addresses that those devices require and their address renewal rate and behaviour.

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Readers are expected to be familiar with all the terms and concepts that are discussed in

- "Neighbor Discovery for IP version 6" [RFC4861],
- "IPv6 Stateless Address Autoconfiguration" [RFC4862],
- "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919],
- "Neighbor Discovery Optimization for Low-power and Lossy Networks" [RFC6775] and

o "Multi-link Subnet Support in IPv6" [I-D.ietf-ipv6-multilink-subnets],

as well as the following terminology:

Backbone Link: An IPv6 transit link that interconnects two or more Backbone Routers. It is expected to be a higher speed device speed compared to the LLN in order to carry the traffic that is required to federate multiple segments of the potentially large LLN into a single IPv6 subnet.

Backbone Router: A logical network function in an IPv6 router that federates a LLN over a Backbone Link. In order to do so, the Backbone Router (6BBR) proxies the 6LoWPAN ND operations detailed in the document onto the matching operations that run over the backbone, typically IPv6 ND. Note that 6BBR is a logical function, just like 6LR and 6LBR, and that a same physical router may operate all three.

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

Registration: The process during which a 6LN registers its address(es) with the Border Router so the 6BBR can serve as proxy for ND operations over the Backbone.

Binding: The association between an IP address with a MAC address, a port and/or other information about the node that owns the IP address.

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

Registering Node: The node that performs the registration to the 6BBR, which may proxy for the registered node.

Registered Address: An address owned by the Registered Node node that was or is being registered.

IPv6 ND: The IPv6 Neighbor Discovery protocol as specified in [RFC4861] and [RFC4862].

legacy: a 6LN, a 6LR or a 6LBR that supports [RFC6775] but not this specification.

updated: a 6LN, a 6LR or a 6LBR that supports this specification.

4. Updating RFC 6775

This specification introduces the Extended Address Registration Option (EARO) based on the ARO as defined in [RFC6775]; in particular a "T" flag is added that MUST be set in NS messages when this specification is used, and echoed in NA messages to confirm that the protocol is supported.

The extensions to the ARO option are used in the Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages, so as to convey the additional information all the way to the 6LBR. In turn the 6LBR may proxy the registration using IPv6 ND over a backbone as illustrated in Figure 1. Note that this specification avoids the extended DAR flow for Link Local Addresses in Route-Over mode.

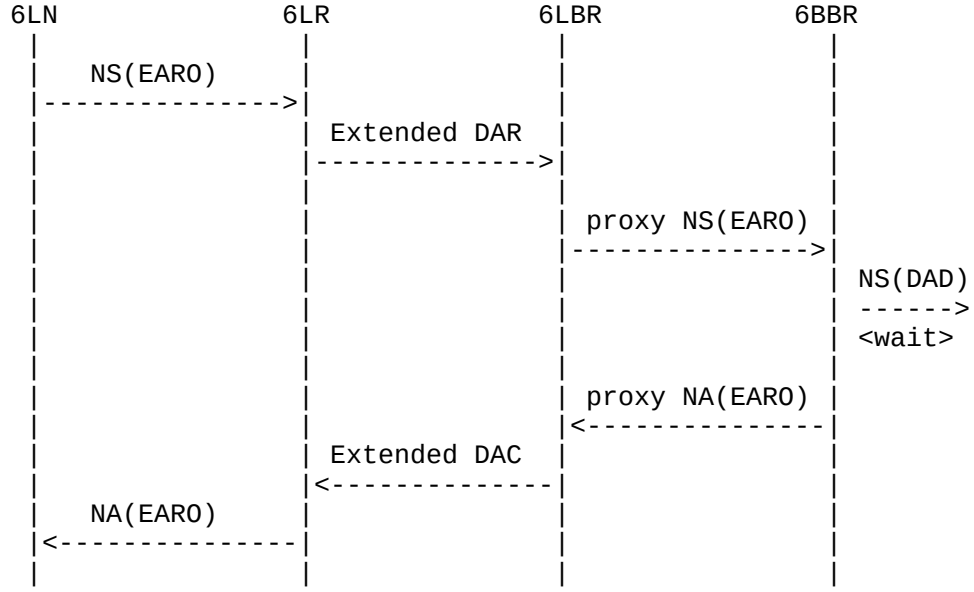

Figure 1: (Re-)Registration Flow

In order to support various types of link layers, it is RECOMMENDED to allow multiple registrations, including for privacy / temporary addresses, and provides new mechanisms to help clean up stale registration states as soon as possible.

A Registering Node SHOULD prefer registering to a 6LR that is found to support this specification, as discussed in Section 7.1, over a legacy one.

4.1. Extended Address Registration Option (EARO)

The Extended ARO (EARO) deprecates the ARO and is backward compatible with it. More details on backward compatibility can be found in Section 7.

The semantics of the ARO are modified as follows:

- The address that is being registered with a Neighbor Solicitation (NS) with an EARO is now the Target Address, as opposed to the Source Address as specified in [RFC6775] (see Section 4.5). This change enables a 6LBR to use one of its addresses as source to the proxy-registration of an address that belongs to a LLN Node to a 6BBR. This also limits the use of an address as source address before it is registered and the associated DAD process is complete.

- The Unique ID in the EARO Option is not required to be a MAC address (see Section 4.3).

- The specification introduces a Transaction ID (TID) field in the EARO (see Section 4.2). The TID MUST be provided by a node that supports this specification and a new "T" flag MUST be set to indicate so.

- Finally, this specification introduces new status codes to help diagnose the cause of a registration failure (see Table 1).

4.2. Transaction ID

The Transaction ID (TID) is a sequence number that is incremented with each re-registration. The TID is used to detect the freshness of the registration request and useful to detect one single registration by multiple 6LOWPAN border routers (e.g., 6LBRs and 6BBRs) supporting the same 6LOWPAN. The TID may also be used by the network to track the sequence of movements of a node in order to route to the current (freshest known) location of a moving node.

When a Registered Node is registered with multiple BBRs in parallel, the same TID SHOULD be used, to enable the 6BBRs to determine that the registrations are the same, and distinguish that situation from a movement.

4.2.1. Comparing TID values

The TID is a sequence counter and its operation is the exact match of the path sequence specified in RPL, the IPv6 Routing Protocol for Low-Power and Lossy Networks [RFC6550] specification.

In order to keep this document self-contained and yet compatible, the text below is an exact copy from section 7.2. "Sequence Counter Operation" of [RFC6550].

A TID is deemed to be fresher than another when its value is greater per the operations detailed in this section.

The TID range is subdivided in a 'lollipop' fashion ([Perlman83]), where the values from 128 and greater are used as a linear sequence to indicate a restart and bootstrap the counter, and the values less than or equal to 127 used as a circular sequence number space of size 128 as in [RFC1982]. Consideration is given to the mode of operation when transitioning from the linear region to the circular region. Finally, when operating in the circular region, if sequence numbers are detected to be too far apart then they are not comparable, as detailed below.

A window of comparison, SEQUENCE_WINDOW = 16, is configured based on a value of 2^N, where N is defined to be 4 in this specification.

For a given sequence counter,

1. The sequence counter SHOULD be initialized to an implementation defined value which is 128 or greater prior to use. A recommended value is 240 (256 - SEQUENCE_WINDOW).

2. When a sequence counter increment would cause the sequence counter to increment beyond its maximum value, the sequence counter MUST wrap back to zero. When incrementing a sequence counter greater than or equal to 128, the maximum value is 255. When incrementing a sequence counter less than 128, the maximum value is 127.

3. When comparing two sequence counters, the following rules MUST be applied:

    1. When a first sequence counter A is in the interval [128..255] and a second sequence counter B is in [0..127]:

        1. If (256 + B - A) is less than or equal to SEQUENCE_WINDOW, then B is greater than A, A is less than B, and the two are not equal.

        2. If (256 + B - A) is greater than SEQUENCE_WINDOW, then A is greater than B, B is less than A, and the two are not equal.

For example, if A is 240, and B is 5, then (256 + 5 - 240) is 21. 21 is greater than SEQUENCE_WINDOW (16), thus 240 is greater than 5. As another example, if A is 250 and B is 5, then (256 + 5 - 250) is 11. 11 is less than SEQUENCE_WINDOW (16), thus 250 is less than 5.

2. In the case where both sequence counters to be compared are less than or equal to 127, and in the case where both sequence counters to be compared are greater than or equal to 128:

    1. If the absolute magnitude of difference between the two sequence counters is less than or equal to SEQUENCE_WINDOW, then a comparison as described in [RFC1982] is used to determine the relationships greater than, less than, and equal.

    2. If the absolute magnitude of difference of the two sequence counters is greater than SEQUENCE_WINDOW, then a desynchronization has occurred and the two sequence numbers are not comparable.

4. If two sequence numbers are determined to be not comparable, i.e. the results of the comparison are not defined, then a node should consider the comparison as if it has evaluated in such a way so as to give precedence to the sequence number that has most recently been observed to increment. Failing this, the node should consider the comparison as if it has evaluated in such a way so as to minimize the resulting changes to its own state.

4.3. Owner Unique ID

The Owner Unique ID (OUID) enables a duplicate address registration to be distinguished from a double registration or a movement. An ND message from the 6BBR over the Backbone that is proxied on behalf of a Registered Node must carry the most recent EARO option seen for that node. A NS/NA with an EARO and a NS/NA without a EARO thus represent different nodes; if they relate to a same target then an address duplication is likely.

The Owner Unique ID in [RFC6775] is a EUI-64 preconfigured address, under the assumption that duplicate EUI-64 addresses are avoided. With this specification, the Owner Unique ID is allowed to be extended to different types of identifier, as long as the type is clearly indicated. For instance, the type can be a cryptographic string and used to prove the ownership of the registration as discussed in "Address Protected Neighbor Discovery for Low-power and Lossy Networks" [I-D.ietf-6lo-ap-nd].

The node SHOULD store the unique ID, or a way to generate that ID, in persistent memory. Otherwise, if a reboot causes a loss of memory, re-registering the same address could be impossible until the 6LBR times out the previous registration.

4.4. Extended Duplicate Address Messages

In order to map the new EARO content in the DAR/DAC messages, a new TID field is added to the Extended DAR (EDAR) and the Extended DAC (EDAC) messages as a replacement to a Reserved field, and an odd value of the ICMP Code indicates support for the TID, to transport the "T" flag.

In order to prepare for future extensions, and though no option has been defined for the Duplicate Address messages, implementations SHOULD expect ND options after the main body, and SHOULD ignore them.

As for the EARO, the Extended Duplicate Address messages are backward compatible with the legacy versions, and remarks concerning backwards compatibility for the protocol between the 6LN and the 6LR apply similarly between a 6LR and a 6LBR.

4.5. Registering the Target Address

The Registering Node is the node that performs the registration to the 6BBR. As in [RFC6775], it may be the Registered Node as well, in which case it registers one of its own addresses, and indicates its own MAC Address as Source Link Layer Address (SLLA) in the NS(EARO).

This specification adds the capability to proxy the registration operation on behalf of a Registered Node that is reachable over a LLN mesh. In that case, if the Registered Node is reachable from the 6BBR over a Mesh-Under mesh, the Registering Node indicates the MAC Address of the Registered Node as SLLA in the NS(EARO). If the Registered Node is reachable over a Route-Over mesh from the Registering Node, the SLLA in the NS(ARO) is that of the Registering Node. This enables the Registering Node to attract the packets from the 6BBR and route them over the LLN to the Registered Node.

In order to enable the latter operation, this specification changes the behavior of the 6LN and the 6LR so that the Registered Address is found in the Target Address field of the NS and NA messages as opposed to the Source Address. With this convention, a TLLA option indicates the link-layer address of the 6LN that owns the address, whereas the SLLA Option in a NS message indicates that of the Registering Node, which can be the owner device, or a proxy.

The Registering Node is reachable from the 6LR, and is also the one expecting packets for the 6LN. Therefore, it MUST place its own Link Layer Address in the SLLA Option that MUST always be placed in a registration NS(EARO) message. This maintains compatibility with legacy 6LoWPAN ND [RFC6775].

4.6. Link-Local Addresses and Registration

Considering that LLN nodes are often not wired and may move, there is no guarantee that a Link-Local address stays unique between a potentially variable and unbounded set of neighboring nodes.

Compared to [RFC6775], this specification only requires that a Link-Local address is unique from the perspective of the two nodes that use it to communicate (e.g. the 6LN and the 6LR in an NS/NA exchange). This simplifies the DAD process in Route-Over Mode for Link-Local addresses, and there is no exchange of Duplicate Address messages between the 6LR and a 6LBR for Link-Local addresses.

In more details:

An exchange between two nodes using Link-Local addresses implies that they are reachable over one hop and that at least one of the 2 nodes acts as a 6LR. A node MUST register a Link-Local address to a 6LR in order to obtain reachability from that 6LR beyond the current exchange, and in particular to use the Link-Local address as source address to register other addresses, e.g. global addresses.

If there is no collision with an address previously registered to this 6LR by another 6LN, then the Link-Local address is unique from the standpoint of this 6LR and the registration is acceptable. Alternatively, two different 6LRs might expose the same Link-Local address but different link-layer addresses. In that case, a 6LN MUST only interact with one of the 6LRs.

The DAD process between the 6LR and a 6LBR, which is based on an exchange of Duplicate Address messages, does not need to take place for Link-Local addresses.

It is preferable for a 6LR to avoid modifying its state associated to the Source Address of an NS(EARO) message. For that reason, when possible, an address that is already registered with a 6LR SHOULD be used by a 6LN.

When registering to a 6LR that conforms this specification, a node MUST use a Link-Local address as the source address of the registration, whatever the type of IPv6 address that is being

registered. That Link-Local Address MUST be either already registered, or the address that is being registered.

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

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

A node needs to register its IPv6 Global Unicast IPv6 Addresses (GUAs) to a 6LR in order to establish global reachability for these addresses via that 6LR. When registering with an updated 6LR, a Registering Node does not use its GUA as Source Address, in contrast to a node that complies to [RFC6775]. For non-Link-Local addresses, the Duplicate Address exchange MUST conform to [RFC6775], but the extended formats described in this specification for the DAR and the DAC are used to relay the extended information in the case of an EARO.

4.7. Maintaining the Registration States

This section discusses protocol actions that involve the Registering Node, the 6LR and the 6LBR. It must be noted that the portion that deals with a 6LBR only applies to those addresses that are registered to it; as discussed in Section 4.6, this is not the case for Link-Local addresses. The registration state includes all data that is stored in the router relative to that registration, in particular, but not limited to, an NCE in a 6LR. 6LBRs and 6BBRs may store additional registration information in more complex data structures and use protocols that are out of scope of this document to keep them synchonized when they are distributed.

When its Neighbor Cache is full, a 6LR cannot accept a new registration. In that situation, the EARO is returned in a NA message with a Status of 2, and the Registering Node may attempt to register to another 6LR.

If the registry in the 6LBR is be saturated, in which case the LBR cannot guarantee that a new address is effectively not a duplicate. In that case, the 6LBR replies to a EDAR message with a EDAC message

that carries a Status code 9 indicating "6LBR Registry saturated", and the address stays in TENTATIVE state. Note: this code is used by 6LBRs instead of Status 2 when responding to a Duplicate Address message exchange and passed on to the Registering Node by the 6LR. There is no point for the node to retry this registration immediately via another 6LR, since the problem is global to the network. The node may either abandon that address, deregister other addresses first to make room, or keep the address in TENTATIVE state and retry later.

A node renews an existing registration by sending a new NS(EARO) message for the Registered Address. In order to refresh the registration state in the 6LBR, the registration MUST be reported to the 6LBR.

A node that ceases to use an address SHOULD attempt to deregister that address from all the 6LRs to which it has registered the address, which is achieved using an NS(EARO) message with a Registration Lifetime of 0.

A node that moves away from a particular 6LR SHOULD attempt to deregister all of its addresses registered to that 6LR and register to a new 6LR with an incremented TID. When/if the node shows up elsewhere, an asynchronous NA(EARO) or EDAC message with a status of 3 "Moved" SHOULD be used to clean up the state in the previous location. For instance, the "Moved" status can be used by a 6BBR in a NA(EARO) message to indicate that the ownership of the proxy state on the Backbone was transferred to another 6BBR, as the consequence of a movement of the device. The receiver of the message SHOULD propagate the status down the chain towards the Registered node and clean up its state.

Upon receiving a NS(EARO) message with a Registration Lifetime of 0 and determining that this EARO is the freshest for a given NCE (see Section 4.2), a 6LR cleans up its NCE. If the address was registered to the 6LBR, then the 6LR MUST report to the 6LBR, through a Duplicate Address exchange with the 6LBR, or an alternate protocol, indicating the null Registration Lifetime and the latest TID that this 6LR is aware of.

Upon receiving the Extended DAR message, the 6LBR evaluates if this is the most recent TID it has received for that particular registry entry. If so, then the entry is scheduled to be removed, and the EDAR is answered with a EDAC message bearing a Status of 0 ("Success"). Otherwise, a Status 3 ("Moved") is returned instead, and the existing entry is maintained.

When an address is scheduled to be removed, the 6LBR SHOULD keep its entry in a DELAY state for a configurable period of time, so as to protect a mobile node that deregistered from one 6LR and did not register yet to a new one, or the new registration did not reach yet the 6LBR due to propagation delays in the network. Once the DELAY time is passed, the 6LBR removes silently its entry.

5. Detecting Enhanced ARO Capability Support

The "Generic Header Compression for IPv6 over 6LoWPANs" [RFC7400] introduces the 6LoWPAN Capability Indication Option (6CIO) to indicate a node's capabilities to its peers. This specification extends the format defined in [RFC7400] to signal support for EARO, as well as the node's capability to act as a 6LR, 6LBR and 6BBR.

The 6CIO is typically sent in a Router Solicitation (RS) message. When used to signal capabilities per this specification, the 6CIO is typically present in Router Advertisement (RA) messages but can also be present in RS, Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

6. Extended ND Options And Messages

This specification does not introduce new options, but it modifies existing ones and updates the associated behaviors as specified in the following subsections.

6.1. Enhanced Address Registration Option (EARO)

The Address Registration Option (ARO) is defined in section 4.1. of [RFC6775].

The Enhanced Address Registration Option (EARO) updates the ARO option within Neighbor Discovery NS and NA messages between a 6LN and its 6LR. On the other hand, the Extended Duplicate Address messages, EDAR and EDAC, replace the DAR and DAC messages so as to transport the new information between 6LRs and 6LBRs across LLNs meshes such as 6TiSCH networks.

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

When using the EARO option, the address being registered is found in the Target Address field of the NS and NA messages.

The EARO extends the ARO and is indicated by the "T" flag set. The format of the EARO option is as follows:

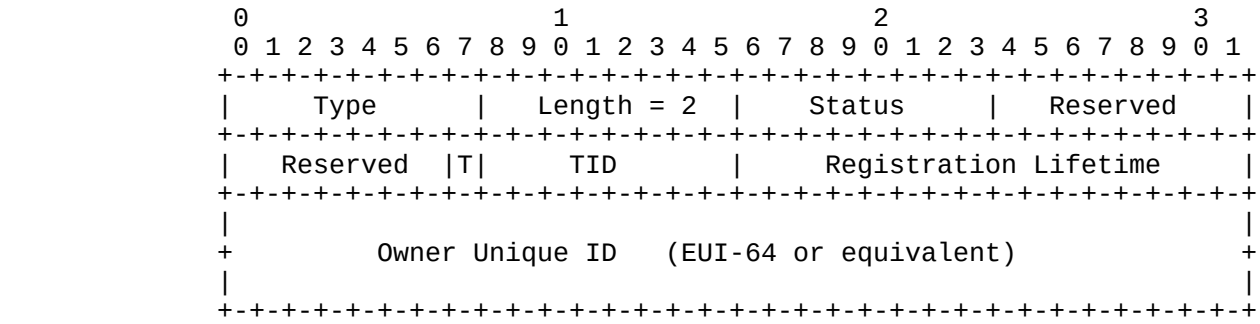

Figure 2: EARO

Option Fields

Type: 33

Length: 8-bit unsigned integer. The length of the option in units of 8 bytes. Always 2.

Status: 8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. See Table 1 below.

Value	Description
0..2	See [RFC6775]. Note: a Status of 1 "Duplicate Address" applies to the Registered Address. If the Source Address conflicts with an existing registration, "Duplicate Source Address" should be used.
3	Moved: The registration fails because it is not the freshest. This Status indicates that the registration is rejected because another more recent registration was done, as indicated by a same OUI and a more recent TID. One possible cause is a stale registration that has progressed slowly in the network and was passed by a more recent one. It could also indicate a OUI collision.
4	Removed: The binding state was removed. This may be placed in an asynchronous NS(ARO) message, or as the rejection of a proxy registration to a Backbone Router

5	Validation Requested: The Registering Node is challenged for owning the Registered Address or for being an acceptable proxy for the registration. This Status is expected in asynchronous messages from a registrar (6LR, 6LBR, 6BBR) to indicate that the registration state is removed, for instance due to a movement of the device.
6	Duplicate Source Address: The address used as source of the NS(ARO) conflicts with an existing registration.
7	Invalid Source Address: The address used as source of the NS(ARO) is not a Link-Local address as prescribed by this document.
8	Registered Address topologically incorrect: The address being registered is not usable on this link, e.g. it is not topologically correct
9	6LBR Registry saturated: A new registration cannot be accepted because the 6LBR Registry is saturated. Note: this code is used by 6LBRs instead of Status 2 when responding to a Duplicate Address message exchange and passed on to the Registering Node by the 6LR.
10	Validation Failed: The proof of ownership of the registered address is not correct.

Table 1: EARO Status

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

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

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

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

Owner Unique Identifier (OUI): A globally unique identifier for the node associated. This can be the EUI-64 derived IID

of an interface, or some provable ID obtained cryptographically.

6.2. Extended Duplicate Address Message Formats

The Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC) messages are defined in section 4.4 of [RFC6775]. Those messages follow a common base format, which enables information from the ARO to be transported over multiple hops.

The Duplicate Address Messages are extended to adapt to the Extended ARO format, as follows:

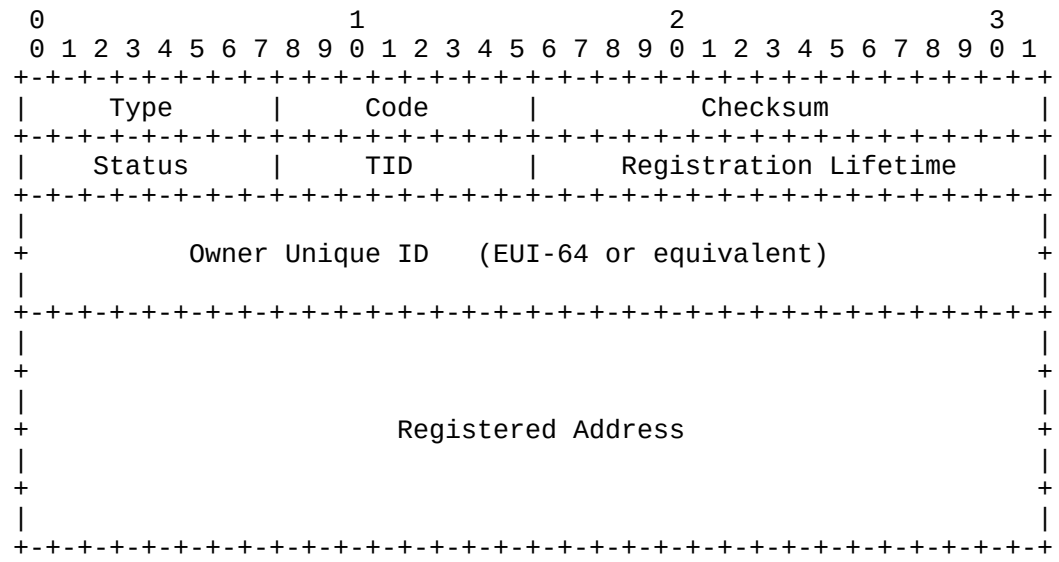

Figure 3: Duplicate Address Messages Format

Modified Message Fields

Code: The ICMP Code as defined in [RFC4443]. The ICMP Code MUST be set to 1 with this specification. An odd value of the ICMP Code indicates that the TID field is present and obeys this specification.

TID: 1-byte integer; same definition and processing as the TID in the EARO option as defined in Section 6.1.

Owner Unique Identifier (OUI): 8 bytes; same definition and processing as the OUI in the EARO option as defined in Section 6.1.

6.3. New 6LoWPAN Capability Bits in the Capability Indication Option

This specification defines new capability bits for use in the 6CIO, which was introduced by [RFC7400] for use in IPv6 ND RA messages.

Routers that support this specification SHOULD set the "E" flag and 6LN SHOULD favor 6LR routers that support this specification over those that do not. Routers that are capable of acting as 6LR, 6LBR and 6BBR SHOULD set the "L", "B" and "P" flags, respectively. In particular, the function 6LR is often collocated with that of 6LBR.

Those flags are not mutually exclusive and if a router is capable of performing multiple functions, it SHOULD set all the related flags.

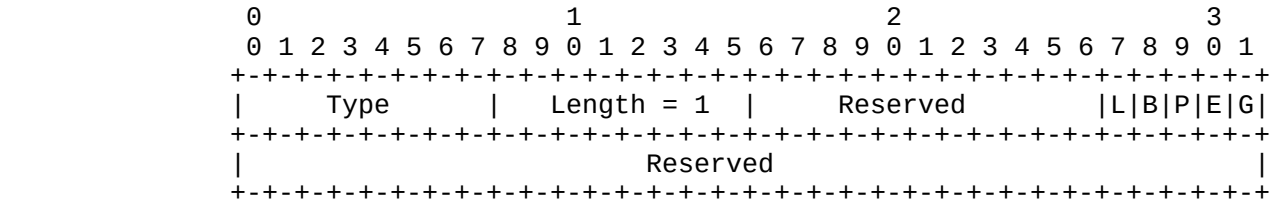

Figure 4: New capability Bits L, B, P, E in the 6CIO

Option Fields

Type: 36

L: Node is a 6LR, it can take registrations.

B: Node is a 6LBR.

P: Node is a 6BBR, proxying for nodes on this link.

E: This specification is supported and applied.

7. Backward Compatibility

7.1. Discovering the capabilities of an ND peer

7.1.1. Using the "E" Flag in the 6CIO

If the 6CIO is used in an ND message and the sending node supports this specification, then the "E" Flag MUST be set.

A router that supports this specification SHOULD indicate that with a 6CIO.

If the Registering Node (RN) receives a 6CIO in a Router Advertisement message, then the setting of the "E" Flag indicates whether or not this specification is supported.

7.1.2. Using the "T" Flag in the EARO

One alternate way for a 6LN to discover the router’s capabilities to first register a Link Local address, placing the same address in the Source and Target Address fields of the NS message, and setting the "T" Flag. The node may for instance register an address that is based on EUI-64. For such address, DAD is not required and using the SLLAO option in the NS is actually more consistent with existing ND specifications such as the "Optimistic Duplicate Address Detection (DAD) for IPv6" [RFC4429].

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

A node that supports this specification MUST always use an EARO as a replacement to an ARO in its registration to a router. This is harmless since the "T" flag and TID field are reserved in [RFC6775], and are ignored by a legacy router. A router that supports this specification answers an ARO with an ARO and answers an EARO with an EARO.

This specification changes the behavior of the peers in a registration flows. To enable backward compatibility, a 6LB that registers to a 6LR that is not known to support this specification MUST behave in a manner that is compatible with [RFC6775]. A 6LN can achieve that by sending a NS(EARO) message with a Link-Local Address used as both Source and Target Address, as described in Section 4.6. Once the 6LR is known to support this specification, the 6LN MUST obey this specification.

7.2. Legacy 6LoWPAN Node

A legacy 6LN will use the Registered Address as source and will not use an EARO option. An updated 6LR MUST accept that registration if it is valid per [RFC6775], and it MUST manage the binding cache accordingly. The updated 6LR MUST then use the legacy Duplicate Address messages as specified in [RFC6775] to indicate to the 6LBR that the TID is not present in the messages.

The main difference with [RFC6775] is that Duplicate Address exchange for DAD is avoided for Link-Local addresses. In any case, the 6LR SHOULD use an EARO in the reply, and may use any of the Status codes defined in this specification.

7.3. Legacy 6LoWPAN Router

The first registration by an updated 6LN MUST be for a Link-Local address, using that Link-Local address as source. A legacy 6LR will not make a difference and treat that registration as if the 6LN was a legacy node.

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

After detecting a legacy 6LR, an updated 6LN may attempt to find an alternate 6LR that is updated.

An updated 6LN SHOULD use an EARO in the request regardless of the type of 6LR, legacy or updated, which implies that the "T" flag is set.

If an updated 6LN moves from an updated 6LR to a legacy 6LR, the legacy 6LR will send a legacy DAR message, which can not be compared with an updated one for freshness.

Allowing legacy DAR messages to replace a state established by the updated protocol in the 6LBR would be an attack vector and that cannot be the default behavior.

But if legacy and updated 6LRs coexist temporarily in a network, then it makes sense for an administrator to install a policy that allows so, and the capability to install such a policy should be configurable in a 6LBR though it is out of scope for this document.

7.4. Legacy 6LoWPAN Border Router

With this specification, the Duplicate Address messages are extended to transport the EARO information. Similarly to the NS/NA exchange, updated 6LBR devices always use the Extended Duplicate Address messages and all the associated behavior so they can amlways be differentiated from legacy ones.

Note that a legacy 6LBR will accept and process an EDAR message as if it was a legacy DAR, so legacy support of DAD is preserved.

8. Security Considerations

This specification extends [RFC6775], and the security section of that draft also applies to this as well. In particular, it is expected that the link layer is sufficiently protected to prevent a rogue access, either by means of physical or IP security on the Backbone Link and link layer cryptography on the LLN.

This specification also expects that the LLN MAC provides secure unicast to/from the Backbone Router and secure Broadcast from the Backbone Router in a way that prevents tempering with or replaying the RA messages.

This specification recommends to using privacy techniques (see Section 9, and protection against address theft such as provided by "Address Protected Neighbor Discovery for Low-power and Lossy Networks" [I-D.ietf-6lo-ap-nd], which guarantees the ownership of the Registered Address using a cryptographic OUID.

The registration mechanism may be used by a rogue node to attack the 6LR or the 6LBR with a Denial-of-Service attack against the registry. It may also happen that the registry of a 6LR or a 6LBR is saturated and cannot take any more registration, which effectively denies the requesting a node the capability to use a new address. In order to alleviate those concerns, Section 4.7 provides a number of recommendations that ensure that a stale registration is removed as soon as possible from the 6LR and 6LBR. In particular, this specification recommends that:

- A node that ceases to use an address SHOULD attempt to deregister that address from all the 6LRs to which it is registered. See Section 4.2 for the mechanism to avoid replay attacks and avoiding the use of stale registration information.

- The Registration lifetimes SHOULD be individually configurable for each address or group of addresses. The nodes SHOULD be configured with a Registration Lifetime that reflects their

expectation of how long they will use the address with the 6LR to which it is registered. In particular, use cases that involve mobility or rapid address changes SHOULD use lifetimes that are larger yet of a same order as the duration of the expectation of presence.

- o The router (6LR or 6LBR) SHOULD be configurable so as to limit the number of addresses that can be registered by a single node, as identified at least by MAC address and preferably by security credentials. When that maximum is reached, the router should use a Least-Recently-Used (LRU) algorithm to clean up the addresses, keeping at least one Link-Local address. The router SHOULD attempt to keep one or more stable addresses if stability can be determined, e.g. from the way the IID is formed or because they are used over a much longer time span than other (privacy, shorter-lived) addresses. Address lifetimes SHOULD be individually configurable.

- o In order to avoid denial of registration for the lack of resources, administrators should take great care to deploy adequate numbers of 6LRs to cover the needs of the nodes in their range, so as to avoid a situation of starving nodes. It is expected that the 6LBR that serves a LLN is a more capable node then the average 6LR, but in a network condition where it may become saturated, a particular deployment should distribute the 6LBR functionality, for instance by leveraging a high speed Backbone and Backbone Routers to aggregate multiple LLNs into a larger subnet.

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

9. Privacy Considerations

As indicated in section Section 2, this protocol does not aim at limiting the number of IPv6 addresses that a device can form. A host should be able to form and register any address that is topologically correct in the subnet(s) advertised by the 6LR/6LBR.

This specification does not mandate any particular way for forming IPv6 addresses, but it discourages using EUI-64 for forming the Interface ID in the Link-Local address because this method prevents the usage of "SEcure Neighbor Discovery (SEND)" [RFC3971] and "Cryptographically Generated Addresses (CGA)" [RFC3972], and that of address privacy techniques.

"Privacy Considerations for IPv6 Adaptation-Layer Mechanisms" [RFC8065] explains why privacy is important and how to form such addresses. All implementations and deployment must consider the option of privacy addresses in their own environment. Also future specifications involving 6LOWPAN Neighbor Discovery should consult "Recommendation on Stable IPv6 Interface Identifiers" [RFC8064] for default interface identifaction.

10. IANA Considerations

IANA is requested to make a number of changes under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry, as follows.

10.1. ARO Flags

IANA is requested to create a new subregistry for "ARO Flags". This specification defines 8 positions, bit 0 to bit 7, and assigns bit 7 for the "T" flag in Section 6.1. The policy is "IETF Review" or "IESG Approval" [RFC8126]. The initial content of the registry is as shown in Table 2.

New subregistry for ARO Flags under the "Internet Control Message Protocol version 6 (ICMPv6) [RFC4443] Parameters"

ARO Status	Description	Document
0..6	Unassigned	
7	"T" Flag	This RFC

Table 2: new ARO Flags

10.2. ICMP Codes

IANA is requested to create a new entry in the ICMPv6 "Code" Fields subregistry of the Internet Control Message Protocol version 6 (ICMPv6) Parameters for the ICMP codes related to the ICMP type 157 and 158 Duplicate Address Request (shown in Table 3) and Confirmation (shown in Table 4), respectively, as follows:

New entries for ICMP types 157 DAR message

Code	Name	Reference
0	Original DAR message	RFC 6775
1	Extended DAR message	This RFC

Table 3: new ICMPv6 Code Fields

New entries for ICMP types 158 DAC message

Code	Name	Reference
0	Original DAC message	RFC 6775
1	Extended DAC message	This RFC

Table 4: new ICMPv6 Code Fields

10.3. New ARO Status values

IANA is requested to make additions to the Address Registration Option Status Values Registry as follows:

Address Registration Option Status Values Registry

ARO Status	Description	Document
3	Moved	This RFC
4	Removed	This RFC
5	Validation Requested	This RFC
6	Duplicate Source Address	This RFC
7	Invalid Source Address	This RFC
8	Registered Address topologically incorrect	This RFC
9	6LBR registry saturated	This RFC
10	Validation Failed	This RFC

Table 5: New ARO Status values

10.4. New 6LoWPAN capability Bits

IANA is requested to make additions to the Subregistry for "6LoWPAN capability Bits" as follows:

Subregistry for "6LoWPAN capability Bits" under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters"

Capability Bit	Description	Document
11	6LR capable (L bit)	This RFC
12	6LBR capable (B bit)	This RFC
13	6BBR capable (P bit)	This RFC
14	EARO support (E bit)	This RFC

Table 6: New 6LoWPAN capability Bits

11. Acknowledgments

Kudos to Eric Levy-Abegnoli who designed the First Hop Security infrastructure upon which the first backbone router was implemented. Many thanks to Sedat Gormus, Rahul Jadhav and Lorenzo Colitti for their various contributions and reviews. Also many thanks to Thomas Watteyne for his early implementation of a 6LN that was instrumental to the early tests of the 6LR, 6LBR and Backbone Router.

12. References

12.1. 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>.

[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>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[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>.

[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>.

[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>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

12.2. Informative References

[I-D.chakrabarti-nordmark-6man-efficient-nd] Chakrabarti, S., Nordmark, E., Thubert, P., and M. Wasserman, "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", draft-chakrabarti-nordmark-6man-efficient-nd-07 (work in progress), February 2015.

[I-D.delcarpio-6lo-wlanah] Vega, L., Robles, I., and R. Morabito, "IPv6 over 802.11ah", draft-delcarpio-6lo-wlanah-01 (work in progress), October 2015.

[I-D.ietf-6lo-ap-nd]
Sarikaya, B., Thubert, P., and M. Sethi, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-03 (work in progress), September 2017.

[I-D.ietf-6lo-backbone-router]
Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-04 (work in progress), July 2017.

[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-07 (work in progress), June 2017.

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-12 (work in progress), August 2017.

[I-D.ietf-bier-architecture]
Wijnands, I., Rosen, E., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast using Bit Index Explicit Replication", draft-ietf-bier-architecture-08 (work in progress), September 2017.

[I-D.ietf-ipv6-multilink-subnets]
Thaler, D. and C. Huitema, "Multi-link Subnet Support in IPv6", draft-ietf-ipv6-multilink-subnets-00 (work in progress), July 2002.

[I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks]
Popa, D. and J. Hui, "6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks", draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00 (work in progress), March 2014.

[RFC1982] Elz, R. and R. Bush, "Serial Number Arithmetic", RFC 1982, DOI 10.17487/RFC1982, August 1996, <https://www.rfc-editor.org/info/rfc1982>.

[RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, DOI 10.17487/RFC3610, September 2003, <https://www.rfc-editor.org/info/rfc3610>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/info/rfc3972>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <https://www.rfc-editor.org/info/rfc4429>.

[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>.

[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>.

[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>.

[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>.

[RFC7934] Colitti, L., Cerf, V., Cheshire, S., and D. Schinazi, "Host Address Availability Recommendations", BCP 204, RFC 7934, DOI 10.17487/RFC7934, July 2016, <https://www.rfc-editor.org/info/rfc7934>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[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>.

[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>.

12.3. External Informative References

[IEEEstd802154] IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE Standard 802.15.4, DOI 10.1109/IEEE P802.15.4-REVd/D01, June 2017, <http://ieeexplore.ieee.org/document/7460875/>.

[Perlman83] Perlman, R., "Fault-Tolerant Broadcast of Routing Information", North-Holland Computer Networks 7: 395-405, 1983, <http://www.cs.illinois.edu/~pbg/courses/cs598fa09/readings/p83.pdf>.

Appendix A. Applicability and Requirements Served

This specification extends 6LoWPAN ND to sequence the registration and serves the requirements expressed Appendix B.1 by enabling the mobility of devices from one LLN to the next based on the complementary work in the "IPv6 Backbone Router" [I-D.ietf-6lo-backbone-router] specification.

In the context of the the TimeSlotted Channel Hopping (TSCH) mode of IEEE Std. 802.15.4 [IEEEstd802154], the "6TiSCH architecture" [I-D.ietf-6tisch-architecture] introduces how a 6LoWPAN ND host could connect to the Internet via a RPL mesh Network, but this requires additions to the 6LOWPAN ND protocol to support mobility and reachability in a secured and manageable environment. This specification details the new operations that are required to implement the 6TiSCH architecture and serves the requirements listed in Appendix B.2.

The term LLN is used loosely in this specification to cover multiple types of WLANs and WPANs, including Low-Power Wi-Fi, BLUETOOTH(R) Low Energy, IEEE Std.802.11AH and IEEE Std.802.15.4 wireless meshes, so as to address the requirements discussed in Appendix B.3.

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

"Efficiency aware IPv6 Neighbor Discovery Optimizations" [I-D.chakrabarti-nordmark-6man-efficient-nd] suggests that 6LoWPAN ND [RFC6775] can be extended to other types of links beyond IEEE Std. 802.15.4 for which it was defined. The registration technique is beneficial when the Link-Layer technique used to carry IPv6 multicast packets is not sufficiently efficient in terms of delivery ratio or energy consumption in the end devices, in particular to enable energy-constrained sleeping nodes. The value of such extension is especially apparent in the case of mobile wireless nodes, to reduce the multicast operations that are related to IPv6 ND ([RFC4861], [RFC4862]) and plague the wireless medium. This serves scalability requirements listed in Appendix B.6.

Appendix B. Requirements

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

B.1. Requirements Related to Mobility

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

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

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

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

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

B.2. Requirements Related to Routing Protocols

The point of attachment of a 6LN may be a 6LR in an LLN mesh. IPv6 routing in a LLN can be based on RPL, which is the routing protocol that was defined at the IETF for this particular purpose. Other routing protocols than RPL are also considered by Standard Defining Organizations (SDO) on the basis of the expected network characteristics. It is required that a 6LoWPAN Node attached via ND to a 6LR would need to participate in the selected routing protocol to obtain reachability via the 6LR.

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

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

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

Related requirements are:

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

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

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

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

6LoWPAN ND [RFC6775] was defined with a focus on IEEE Std.802.15.4 and in particular the capability to derive a unique Identifier from a globally unique MAC-64 address. At this point, the 6lo Working Group is extending the 6LoWPAN Header Compression (HC) [RFC6282] technique to other link types ITU-T G.9959 [RFC7428], Master-Slave/Token-Passing [RFC8163], DECT Ultra Low Energy [RFC8105], Near Field Communication [I-D.ietf-6lo-nfc], IEEE Std. 802.11ah [I-D.delcarpio-6lo-wlanah], as well as IEEE1901.2 Narrowband Powerline Communication Networks [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks] and BLUETOOTH(R) Low Energy [RFC7668].

Related requirements are:

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

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

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

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

B.4. Requirements Related to Proxy Operations

Duty-cycled devices may not be able to answer themselves to a lookup from a node that uses IPv6 ND on a Backbone and may need a proxy. Additionally, the duty-cycled device may need to rely on the 6LBR to perform registration to the 6BBR.

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

Related requirements are:

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

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

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

B.5. Requirements Related to Security

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

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

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

Related requirements are:

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

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

Req5.3: 6LoWPAN ND security mechanisms SHOULD lead to small packet sizes. In particular, the NS, NA, DAR and DAC messages for a re-registration flow SHOULD NOT exceed 80 octets so as to fit in a secured IEEE Std.802.15.4 [IEEEstd802154] frame.

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

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

Req5.6: The 6LoWPAN ND security mechanisms SHOULD enable the variation of CCM [RFC3610] called CCM* for use at both Layer 2 and Layer 3, and SHOULD enable the reuse of security code that has to be present on the device for upper layer security such as TLS.

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

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

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

B.6. Requirements Related to Scalability

Use cases from Automatic Meter Reading (AMR, collection tree operations) and Advanced Metering Infrastructure (AMI, bi-directional communication to the meters) indicate the needs for a large number of

LLN nodes pertaining to a single RPL DODAG (e.g. 5000) and connected to the 6LBR over a large number of LLN hops (e.g. 15).

Related requirements are:

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

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

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Sophia Antipolis
FRANCE

Email: pthubert@cisco.com

Erik Nordmark
Santa Clara, CA
USA

Email: nordmark@sonic.net

Samita Chakrabarti
San Jose, CA
USA

Email: samitac.ietf@gmail.com

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

Email: charliep@computer.org

6Lo Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

Y-G. Hong
ETRI
C. Gomez
UPC/i2cat
Y-H. Choi
ETRI
D-Y. Ko
SKtelecom
AR. Sangi
Huaiyin Institute of Technology
T. Aanstoot
Modio AB
S. Chakrabarti
October 30, 2017

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

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, PLC (IEEE 1901.2), and IEEE 802.15.4e (6tisch) are used as examples. The document targets an audience who like to understand and evaluate running end-to-end IPv6 over the constrained link layer networks connecting devices to each other or to each cloud.

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 3, 2018.

Table of Contents

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 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], 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), Power Line Communication (PLC), and IEEE 802.15.4e (TSCH), have been defined at [IETF_6lo] working group. 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 is new to IPv6-over-lowpower networks concept and wants to assess if variance of 6LoWPAN stack [6lo] can be applied to the constrained 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. And it described 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 and possible candidates

3.1. ITU-T G.9959 (specified)

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

3.2. Bluetooth LE (specified)

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

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

on the Internet [RFC7668]. A typical usage of Bluetooth LE is smartphone-based interaction with constrained devices.

3.3. DECT-ULE (specified)

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 (specified)

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

An MS/TP device is typically based on a low-cost microcontroller with limited processing power and memory. Together with low data rates and a small address space, these constraints are similar to those faced in 6LoWPAN networks and suggest some elements of that solution might be leveraged. MS/TP differs significantly from 6LoWPAN in at least three aspects: a) MS/TP devices typically have a continuous source of power, b) all MS/TP devices on a segment can communicate directly so there are no hidden node or mesh routing issues, and c)

recent changes to MS/TP provide support for large payloads, eliminating the need for link-layer fragmentation and reassembly.

MS/TP is designed to enable multidrop networks over shielded twisted pair wiring, although not according to standards, in lower speeds, normally 9600 bit/s, re-purposed telecom wiring is widely in use, keeping deployment cost down. It can support a data rate of 115,200 baud on segments up to 1000 meters in length, or segments up to 1200 meters in length at lower baud rates. An MS/TP link requires only a UART, an RS-485 transceiver with a driver that can be disabled, and a 5ms resolution timer. These features make MS/TP a cost-effective and very reliable field bus for the most numerous and least expensive devices in a building automation network [RFC8163]. MS/TP can be used for the management of district heating.

3.5. NFC (specified)

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 (specified)

Unlike other dedicated communication infrastructure, the required medium (power conductor) is 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.

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 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 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. IEEE 802.15.4e (specified)

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

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

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

The main benefits of IEEE 802.15.4 TSCH are:

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

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

- 6TiSCH at IETF defines communications of TSCH network and it uses 6LoWPAN stack [RFC7554].

IEEE 802.15.4e can be used for industrial automation.

3.8. LTE MTC (example of a potential candidate)

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

LTE MTC offer advantages in comparison to above category 2 and is appropriate to be used for low rate IoT services such as low power and low cost. LTE MTC can be used for a gateway of a wireless bachhaul network.

3.9. 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 paramters of each use case corresponding to the 6lo link layer technology.

	Z-Wave	BLE	DECT-ULE	MS/TP	NFC	PLC	TSCH
Usage	Home Auto-mation	Interact w/ Smart Phone	Meter Reading	District Heating	Health-care Service	Smart Grid	Industr-ial Aut-mation
Topology & Subnet	L2-mesh or L3-mesh	Star No mesh	Star No mesh	Bus MS/TP	P2P L2-mesh	Star Tree Mesh	Mesh
Mobility Reqmt	No	Low	No	No	Moderate	No	No
Security Reqmt	High + Privacy required	Parti-ally	High + Privacy required	High + Authen. required	High	High + Encrypt. required	High + Privacy required
Buffering Reqmpt	Low	Low	Low	Low	Low	Low	Low
Latency, QoS Reqmt	High	Low	Low	High	High	Low	High
Data Rate	Infrequ-ent	Infrequ-ent	Infrequ-ent	Frequent	Small	Infrequ-ent	Infrequ-ent
RFC # or Draft	RFC7428	RFC7668	RFC8105	RFC8163	draft-ietf-6lo-nfc	draft-hou-6lo-plc	RFC7554

Table 2: Comparison between 6lo Link layer technologies

4. 6lo Deployment Scenarios

4.1. jupitermesh in Smart Grid using 6lo in network layer

jupiterMesh is a multi-hop wireless mesh network specification designed mainly for deployment in large geographical areas. Each subnet in jupiterMesh is able to cover an entire neighborhood with thousands of nodes consisting of IPv6-enabled routers and end-points

(e.g., hosts). Automated network joining and load balancing allows a seamless deployment of a large number of subnets.

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

- Automated meter reading
- Distribution Automation (DA)
- Demand-side management (DSM)
- Demand-side response (DSR)
- Power outage reporting
- Street light monitoring and control
- Transformer load management
- EV charging coordination
- Energy theft
- Parking space locator

jupiterMesh specification is based on the following technologies:

- The PHY layer is based on IEEE 802.15.4 SUN specification [IEEE 802.15.4-2015], supporting multiple operating modes for deployment in different regulatory domains and deployment scenarios in terms of density and bandwidth requirements. jupiterMesh supports bit rates from 50 kbps to 800 kbps, frame size up to 2048 bytes, up to 11 different RF bands and 3 modulation types (i.e., FSK, OQPSK and OFDM).
- The MAC layer is based on IEEE 802.15.4 TSCH specification [IEEE 802.15.4-2015]. With frequency hopping capability, TSCH MAC supports scheduling of dedicated timeslot enabling bandwidth management and QoS.
- The security layer consists of a certificate-based (i.e. X.509) network access authentication using EAP-TLS, with IEEE 802.15.9-based KMP (Key Management Protocol) transport, and PANA and link layer encryption using AES-128 CCM as specified in IEEE 802.15.4-2015 [IEEE 802.15.4-2015].

- Address assignment and network configuration are specified using DHCPv6 [RFC3315]. Neighbor Discovery (ND) [RFC6775] and stateless address auto-configuration (SLAAC) are not supported.

- The network layer consists of IPv6, ICMPv6 and 6lo/6LoPWAN header compression [RFC6282]. Multicast is supported using MPL. Two domains are supported, a delay sensitive MPL domain for low latency applications (e.g. DSM, DSR) and a delay insensitive one for less stringent applications (e.g. OTA file transfers).

- The routing layer uses RPL [RFC6550] in non-storing mode with the MRHOF objective function based on the ETX metric.

4.2. Wi-SUN usage of 6lo stacks

Wireless Smart Ubiquitous Network (Wi-SUN) is a technology based on the IEEE 802.15.4g standard. Wi-SUN networks support star and mesh topologies, as well as hybrid star/mesh deployments, but 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.

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:

- Advanced Metering Infrastructure (AMI)

- Distribution Automation

- Home Energy Management

- Infrastructure Management

- Intelligent Transportation Systems

- Smart Street Lighting

- Agriculture

- Structural health (bridges, buildings etc)

- Monitoring and Asset Management

- Smart Thermostats, Air Conditioning and Heat Controls

- 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. Examples include from meter to outdoor access point/router for AMI and DR, or between switches for DA. However, nothing in the profile restricts it to outdoor use. It has the following features;

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

In the Wi-SUN FAN specification, adaptation layer based on 6lo and IPv6 network layer are described. So, IPv6 protocol suite including TCP/UDP, 6lo Adaptation, Header Compression, DHCPv6 for IP address management, Routing using RPL, ICMPv6, and Unicast/Multicast forwarding is utilized.

5. Design Space and Guidelines for 6lo Deployment

5.1. 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], 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:

- Deployment/Bootstrapping: 6lo nodes can be connected randomly, or in an organized manner. The bootstrapping has different characteristics for each link layer technology.

- 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.

- 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.

- Multi-link subnet, single subnet: The selection of multi-link subnet and single subnet depends on connectivity and the number of 6lo nodes.

- Data rate: Originally, the link layer technologies of 6lo have low rate of data transmission. But, by adjusting the MTU, it can deliver higher data rate.

- 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.

- 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.

- Mobility across 6lo networks and subnets: The movement of 6lo nodes is dependent on the 6lo use case. If the 6lo nodes can move or moved around, it requires a mobility management mechanism.

- 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.

- Reliability and QoS: Some 6lo use case requires high reliability, for example real-time service or health-related services.

- 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.

- Security Bootstrapping: Without the external operations, 6lo nodes must have the security bootstrapping mechanism.

- Power use strategy: to enable certain use cases, there may be requirements on the class of energy availability and the strategy followed for using power for communication [RFC7228]. Each link layer technology defines a particular power use strategy which may be tuned [I-D.ietf-lwig-energy-efficient]. Readers are expected to be familiar with [RFC7228] terminology.

- 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 bandwith is low and the number of identical devices is high.

- 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 and some 6lo use cases may require continuous source of power.

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

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

- 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 lowpower 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.

- MTU Considerations: The deployment SHOULD consider their need for maximum transmission unit of a packet (MTU) 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.

- Mesh or L3-Routing: 6LoWPAN specifications do provide mechanisms to support for mesh routing at L2. [RFC6550] defines 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.

- Address Assignment: 6LoWPAN requires that IPv6 Neighbor Discovery for low power networks [RFC6775] be used for autoconfiguration of stateless IPv6 address assignment. Considering the energy sensitive networks [RFC6775] makes optimization from classical IPv6 ND [RFC4861] protocol. 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.

- 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].

- Security and Encryption: Though 6LoWPAN basic specifications do not address security at network layer, the assumption is that L2 security must be present. In addition, application level security is highly desirable. The working groups [ace] and [core] should be consulted for application and transport level security. 6lo working group is working on address authentication [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 quite 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, one 6lo use case example of Bluetooth LE (Smartphone-Based Interaction with Constrained Devices) is described. Other 6lo use case examples are described in Appendix.

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.

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

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.

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>.

[RFC7554] Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC 7554, DOI 10.17487/RFC7554, May 2015, <https://www.rfc-editor.org/info/rfc7554>.

[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>.

10.2. Informative References

[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>.

[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>.

[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-07 (work in progress), June 2017.

[I-D.ietf-lwig-energy-efficient] Gomez, C., Kovatsch, M., Tian, H., and Z. Cao, "Energy-Efficient Features of Internet of Things Protocols", draft-ietf-lwig-energy-efficient-08 (work in progress), October 2017.

[I-D.ietf-roll-aodv-rpl] Anamalamudi, S., Zhang, M., Sangi, A., Perkins, C., and S. Anand, "Asymmetric AODV-P2P-RPL in Low-Power and Lossy Networks (LLNs)", draft-ietf-roll-aodv-rpl-02 (work in progress), September 2017.

[I-D.ietf-6tisch-6top-sf0] Dujovne, D., Grieco, L., Palattella, M., and N. Accettura, "6TiSCH 6top Scheduling Function Zero (SF0)", draft-ietf-6tisch-6top-sf0-05 (work in progress), July 2017.

[I-D.satish-6tisch-6top-sf1] Anamalamudi, S., Zhang, M., Sangi, A., Perkins, C., and S. Anand, "Scheduling Function One (SF1) for hop-by-hop Scheduling in 6tisch Networks", draft-satish-6tisch-6top-sf1-03 (work in progress), February 2017.

[I-D.hou-6lo-plc] Hou, J., Hong, Y., and X. Tang, "Transmission of IPv6 Packets over PLC Networks", draft-hou-6lo-plc-01 (work in progress), June 2017.

[IETF_6lo] "IETF IPv6 over Networks of Resource-constrained Nodes (6lo) working group", <https://datatracker.ietf.org/wg/6lo/charter/>.

[G.9959] "International Telecommunication Union, "Short range narrow-band digital radiocommunication transceivers - PHY and MAC layer specifications", ITU-T Recommendation", January 2015.

[LTE_MTC] "3GPP TS 36.306 V13.0.0, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities (Release 13)", December 2015.

[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 (work-in-progress), IEEE-SA Standards Board", <http://sites.ieee.org/sagroups-1901-1/>.

[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>.

Appendix A. Other 6lo Use Case Examples

A.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].

A.2. 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.

A.3. Use case of MS/TP: Management of District Heating

The key feature of MS/TP is it’s ability to run on the same cabling as BACnet and some use of ModBus, the defacto standard for low bandwith industry communication. Specially Modbus has been around since the 1980 and is still the standard for talking to fans, heat pumps, water purifying equipment and everything else delivering electricity, clean water and ventilation.

Example: Use of MS/TP for management of district heating

The mechanical room in the cellar of an apartment building gets district heating and electricity from the utility providers. The room has a Supervisory Control And Data Acquisition (SCADA) computer talking to a centralized server and command center somewhere else over IP, on the other hand it is controlling the heating, fans and distribution panel over a 2-wire RS-485 based protocol to make sure the logic controller for district heating keeps a constant temperature at the tapwater, the logic controller for heat produktion keeps the right radiator temperature depending on the weather and the fans have a correct speed and are switched off in case district heating fails to prevent cooling out the building and give certain commands in case smoke is detected. Speed is not important, in this usecase, 19,200 bit/s capable equipment is sold as high speed communication capable. Reliability is important, this not working will easily give millions of dollars of damage. Normally the setup is that the SCADA device asks a question to a specific controlling device, gets an answer from the controlling device, asks a new question to some other device.

A.4. 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.

A.5. 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.

A.6. Use case of IEEE 802.15.4e: Industrial Automation

Typical scenario of Industrial Automation where sensor and actuators are connected through the time-slotted radio access (IEEE 802.15.4e). For that, there will be a point-to-point control signal exchange in between sensors and actuators to trigger the critical control information. In such scenarios, point-to-point traffic flows are significant to exchange the controlled information in between sensors and actuators within the constrained networks.

Example: Use of IEEE 802.15.4e for P2P communication in closed-loop application

AODV-RPL [I-D.ietf-roll-aodv-rpl] is proposed as a standard P2P routing protocol to provide the hop-by-hop data transmission in closed-loop constrained networks. Scheduling Functions i.e. SF0 [I-D.ietf-6tisch-6top-sf0] and SF1 [I-D.satish-6tisch-6top-sf1] is proposed to provide distributed neighbor-to-neighbor and end-to-end resource reservations, respectively for traffic flows in deterministic networks (6TiSCH).

The potential scenarios that can make use of the end-to-end resource reservations can be in health-care and industrial applications. AODV-RPL and SF0/SF1 are the significant routing and resource reservation protocols for closed-loop applications in constrained networks.

Authors' Addresses

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

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

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

Email: carlesgo@entel.upc.edu

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

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

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

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

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

6Lo Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

MS. Akbar
Bournemouth University
AR. Sangi
Huaiyin Institute of Technology
M. Zhang
J. Hou
Huawei Technologies
C. Perkins
Futurewei
A. Petrescu
CEA, LIST
R.N.B.Rais
Ajman University

October 30, 2017

Transmission of IPv6 Packets over Wireless Body Area Networks (WBANs) draft-sajjad-6lo-wban-01

Abstract

Wireless Body Area Networks (WBANs) intend to facilitate use cases related to medical field. IEEE 802.15.6 defines PHY and MAC layer and is designed to deal with better penetration through the human tissue without creating any damage to human tissues with the approved MICS (Medical Implant Communication Service) band by USA Federal Communications Commission (FCC). Devices of WBANs conform to this IEEE standard.

This specification defines details to enable transmission of IPv6 packets, method of forming link-local and statelessly autoconfigured IPv6 addresses on WBANs.

This Internet-Draft will expire on May 3, 2018.

Table of Contents

1. Introduction

Wireless Body Area Networks (WBANs) are comprised of devices that conform to the [IEEE802.15.6], standard by the IEEE. IEEE 802.15.6 provides specification for the MAC layer to access the channel. The coordinator divides the channel into superframe time structures to

allocate resources [SURVEY-WBAN] [MAC-WBAN]. Superframes are bounded by equal length beacons through the coordinator. Usually beacons are sent at beacon periods except inactive superframes or limited by regulation.

Task group for 802.15.6 was established by IEEE in November 2007 for standardisation of WBANs and it was approved in 2012. This standard works in and around human body and focus on operating at lower frequencies and short range. The focus of this document is to design a communication standard for MAC and physical layer to support different applications, namely, medical and no-medical applications. Medical applications refer to collection of vital information in real time (monitoring) for diagnoses and treatment of various diseases with help of different sensors (accelerometer, temperature, BP and EMG etc.). It defines a MAC layer that can operate with three different PHY layers i.e. human body communication (HBC), ultra-wideband (UWB) and Narrowband (NB). IEEE 802.15.6 provides specification for MAC layer to access the channel. The coordinator divides the channel into superframe time structures to allocate resources. Superframes are bounded by equal length beacons through coordinator. The purpose of the draft is to highlight the need of IEEE 802.15.6 for WBASNs and its integration issues while connecting it with IPv6 network. The use cases are provided to elaborate the scenarios with implantable and wearable biomedical sensors. 6lowpan provides IPv6 connectivity for IEEE 802.15.4; however, it does not work with IEEE 802.15.6 due to the difference in frame format in terms of size and composition.

1.1. Frame Format and Addressing Modes

Figure 1 shows the general MAC frame format consisting of a 56-bit header, variable length frame body, and 18-bit FrameCheck Sequence (FCS). The maximum length of the frame body is 255 octets. The MAC header further consists of 32-bit frame control, 8-bit recipient Identification (ID), 8-bit sender ID, and 8-bit WBAN ID fields. The frame control field carries control information including the type of frame, that is, beacon, acknowledgement, or other control frames. The recipient and sender ID fields contain the address information of the recipient and the sender of the data frame, respectively. The WBAN ID contains information on the WBAN in which the transmission is active. The first 8-bit field in the MAC frame body carries message freshness information required for nonce construction and replay detection. The frame payload field carries data frames, and the last 32-bit Message Integrity Code (MIC) carries information about the authenticity and integrity of the frame. The IEEE 802.15.6 standard supports two kinds of addresses:

1. 8-bit short address, which is the sender ID. This address is located in the MAC header used for communication.

2. 48-bit EUI-48 address, which is used for the association process. For some certain frame types, e.g. Security Association frames, this MAC address exists inside the MAC payload, for the node joining process.

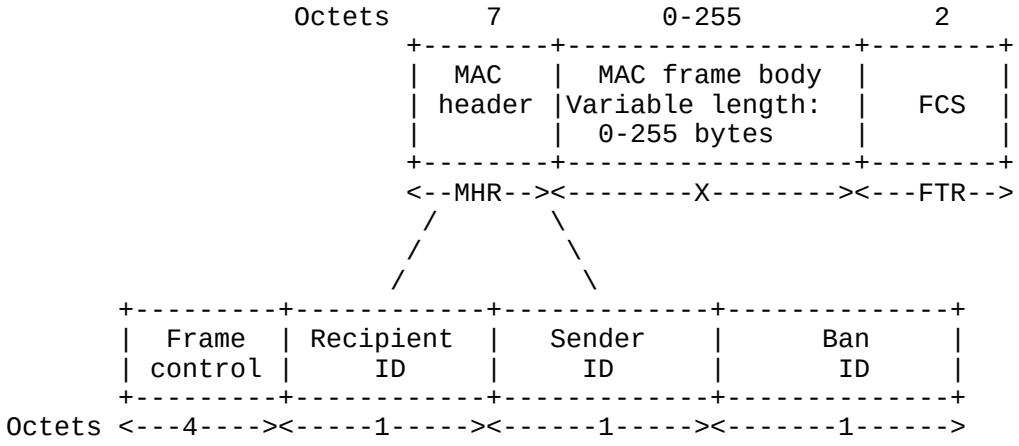

Figure 1: The general MAC frame format of IEEE 802.15.6

1.2. Why 6lo is required for IEEE 802.15.6

Based on the characteristics defined in the overview section, the following sections elaborate on the main problems with IP for WBANs.

The requirement for IPv6 connectivity within WBANs is driven by the following:

- The number of devices in WBANs makes network auto configuration and statelessness highly desirable. And for this, IPv6 has (default auto-configuration as a) ready solutions.

- The large number of devices poses the need for a large address space, moreover a WBAN may consist of 256 nodes maximum and IPv6 is helpful to solve this address space limitation.

- Given the limited packet size of WBANs, the IPv6 address format allows subsuming of IEEE 802.15.6 addresses if so desired. Applications within WBANs are expected to originate small packets. Adding all layers for IP connectivity should still allow transmission in one frame, without incurring excessive fragmentation and reassembly. Furthermore, protocols must be

designed or chosen so that the individual "control/protocol packets" fit within a single 802.15.6 frame. Along these lines, IPv6's requirement of sub-IP reassembly may pose challenges for low-end WBANs healthcare devices that do not have enough RAM or storage for a 1280-octet packet [RFC2460].

- o Simple interconnectivity to other IP networks including the Internet.
- o However, given the limited packet size, headers for IPv6 and layers above must be compressed whenever possible.

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. Topology and Scope of Communication

This is a standard for short-range, wireless communication in the vicinity of, or inside, a human body (but not limited to humans). It uses existing industrial scientific medical (ISM) bands as well as frequency bands approved by national medical and/or regulatory authorities. Support for quality of service (QoS), extremely low power, and data rates from 10Kbps to 10 Mbps is required while simultaneously complying with strict non-interference guidelines where needed. The Table 1 shows a comparison of WBAN and other available technologies in terms of data rate and power consumption.

Standard	Provided data rate	Power requirement	Battery lifetime
802.11 ac (WiFi)	700 Mbps	100 mW - 1000 mW	Hours - days
Bluetooth	1Mbps - 10 Mbps	4 mW - 100 mW	Days - weeks
Wibree	600 Kbps maximum	2 mW - 10 mW	Weeks - months
ZigBee	250 Kbps	3 mW - 10 mW	Weeks - months
802.15.4	250 Kbps maximum	3 mW - 10 mW	Weeks - months
802.15.6	1Kbps - 10 Mbps	0.1 mW - 2 mW	Months - years

Table 1: Comparison of WBAN

Data rates, typically up to 10Mbps, can be offered to satisfy an evolutionary set of entertainment and healthcare services. Current personal area networks (PANs) do not meet the medical (proximity to human tissue) and relevant communication regulations for some application environments. They also do not support the combination of reliability, QoS, low power, data rate, and non-interference required to broadly address the breadth of body area network (BAN) applications.

The IEEE 802.15.6 working group has considered WBANs to operate in either a one-hop or two-hop star topology with the node in the centre of the star being placed on a location like the waist. Two feasible types of data transmission exist in the one-hop star topology: transmission from the device to the coordinator and transmission from the coordinator to the device. The communication methods that exist in the star topology are beacon mode and non-beacon mode. In a two-hop start WBAN, a relay-capable node may be used to exchange data frames between a node and the hub.

4. Protocol Stack

The IPv6 over IEEE 802.15.6 protocol stack is presented in Figure 2. It contains six elements from bottom to top including IEEE 802.15.6 PHY layer, IEEE 802.15.6 MAC layer, Adaptation layer for IPv6 over

IEEE 802.15.6, IPv6 layer, TCP/UDP layer and Application layer.The adaptation layer supports the mechanisms like stateless address auto-configuration, header compression and fragmentation and reassembly.

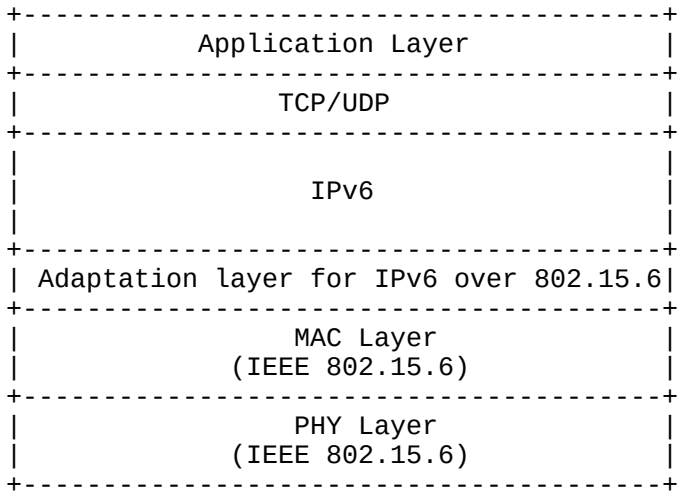

Figure 2: Protocol stack for IPv6 over IEEE 802.15.4

5. Maximum Transmission Unit (MTU)

The IPv6 packets have the MTU of 1280 octects and its expects from every link layer to send data by following this MTU or greater. Thus maximum Transmission Unit (MTU) of MAC layer describes the implementation of fragmentation and reassembly mechanism for the adaption IPv6 layer over IEEE 802.15.6.

The IEEE 802.15.6 has the MTU of 256 octects, if we consider link layer security overhead (16 octects for AES-128) leaves 240 octects which is not sufficient to complete a IPv6 packet.Therefore, an adaption layer below IP layer is required to manage fragmentation and reassembly issues.

6. Specification of IPv6 over WBAN

Due to stringent QoS requirements in WBAN, a 6lo adaption layer is needed to support the transmission of IPv6 packets.6 LoWPAN standards [RFC4944], [RFC6775] and [RFC6282] provides useful information including link-local IPv6 address,stateless address auto-configuration, unicast and multicast address mapping,header compression and fragmentation and reassembly. These standards are reffered in the specifications of 6lo adaptation layer which is illustrated in the following following subsections:

6.1. Stateless Address Autoconfiguration

An IEEE 802.15.6 device performs stateless address autoconfiguration to obtain an IPv6 Iterface Identifier(IID). The IPv6 EUI-64 format address is obtained through the EUI-48 bit MAC address of IEEE 802.15.6 node.The 64-bit IID SHALL be derived by utilizing 8-bit node address and 8-bit BAN ID (part of MAC header) as follows:

ID: 0xYY00:00FF:FE00:00XX

Where YY is the BAN ID, XX is the node address. As this generated IID is not golbally unique, the "Universal/Local" (U/L) bit (7th bit) SHALL be set to zero.

6.2. IPv6 Link-Local Address

The IPv6 link-local address [RFC4291] for an IEEE 802.15.6 interface is generated by appending the interface identifier to the prefix FE80::/64.

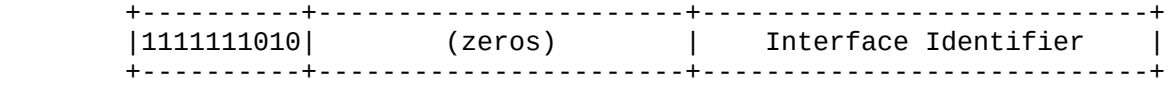

Figure 3: IPv6 Link Local Address in IEEE 802.15.6

6.3. Unicast and Multicast Address Mapping

The address resolution procedure for mapping IPv6 unicast addresses into IEEE 802.15.6 link-layer addresses follows the general description in section 7.2 of [RFC4861], unless otherwise specified. Multicast address mapping is not supported in IEEE 802.15.6.

6.4. Header Compression

The IEEE 802.15.6 PHY layer supports a maximum PSDU (PHY Service Data Unit) of 256 octets. Because of the limited PHY payload, header compression at 6lo adaptation layer is of great importance and MUST be applied. The compression of IPv6 datagrams within IEEE 802.15.6 frames refers to [RFC6282], which updates [RFC4944].Multiple header compression stacks are defined in RFC6282 which specifies the fragmentation methods for IPv6 datagrams on top of IEEE 802.15.4;however, for IEEE 802.15.6, a LoWPAN encapsulated LoWPAN_HC1 compressed IPv6 datagram can be used as IEEE 802.15.6 does not require mesh header due to IEEE 802.15.6 communication scope.Moreover, static header compression techniques of [RFC7400] can also be used as header compression.

6.5. Fragmentation and Reassembly

IEEE 802.15.6 provides Fragmentation and reassembly (FAR) for payload of 256 bytes. FAR as defined in [RFC4944], which specifies the fragmentation methods for IPv6 datagrams on top of IEEE 802.15.4 MUST be adapted to work with IEEE 802.15.6. All headers MUST be compressed according to [RFC4944] encoding formats, but the default MTU of IEEE 802.15.6 is 256 bytes which MUST be considered.

7. IANA Considerations

[TBD]

8. Security and Privacy Considerations

IPv6 over WBAN's applications often require confidentiality and integrity protection. This can be provided at the application, transport, network, and/or at the link.IEEE 802.15.6 considers the security as a key requirement for healthcare applications and defines a complete framework. This framework defines three levels of security which can be used according to requirements.Overall, it covers privacy, confidentiality, encryption and authentication.AES-64 is preffered for encryption due to its efficiency.

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>.

[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>.

[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>.

[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>.

[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>.

[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>.

9.2. Informative References

[IEEE802.15.6]
"IEEE Standard, 802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks", 2012, <https://standards.ieee.org/findstds/standard/802.15.6-2012.html>.

[SURVEY-WBAN]
Diffie, W., Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour, "Wireless body area networks: A survey", Communications Surveys and Tutorials, IEEE , vol. 16, no. 3, pp. 1658-1686, 2014.

[MAC-WBAN]
Minglei Shu, Dongfeng Yuan, Chongqing Zhang, Yinglong Wang, and Changfang Chen, "A MAC Protocol for Medical Monitoring Applications of Wireless Body Area Networks.", Sensors , vol. 15, no. 6, 2015.

Appendix A. Patient monitoring use case - Spoke Hub

Refer following diagram:

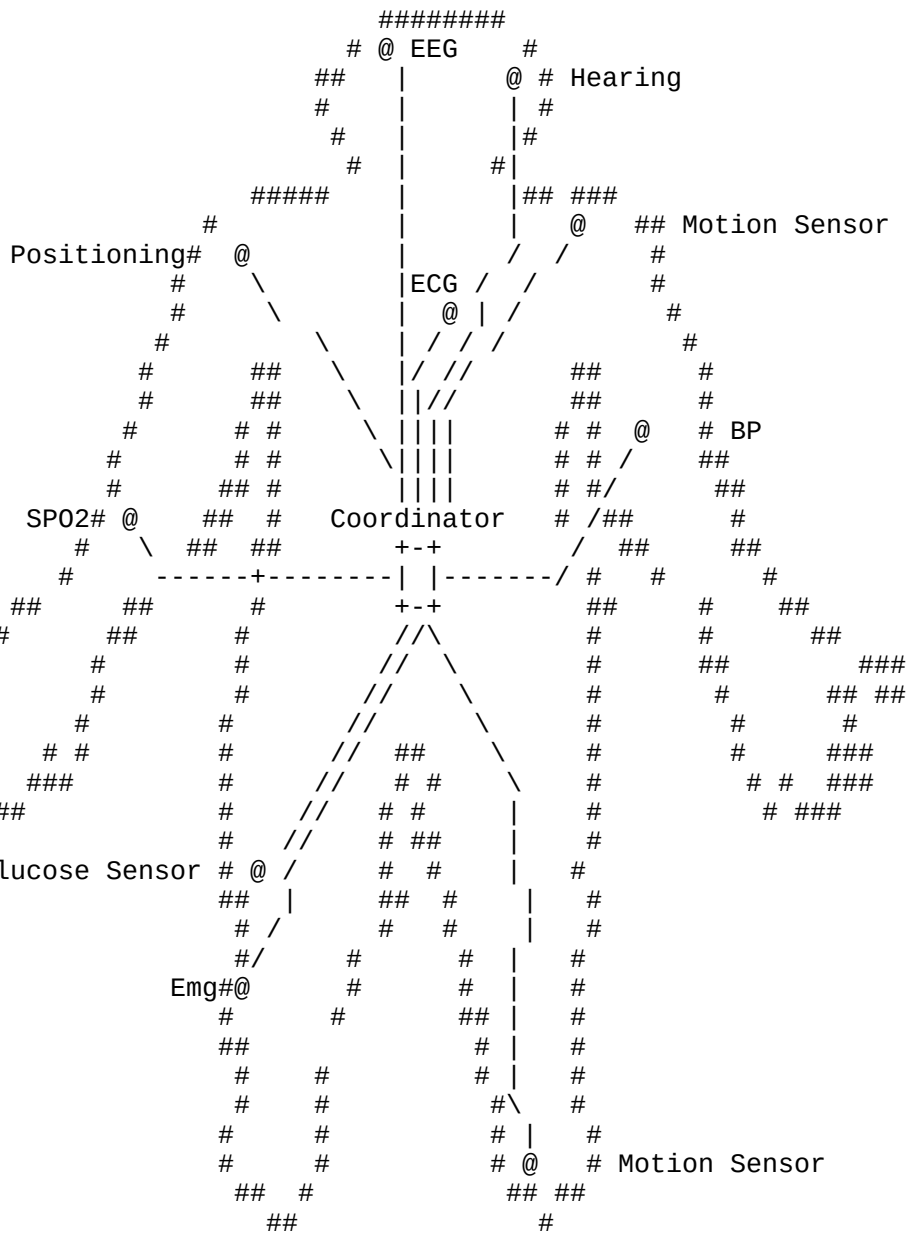

Figure 4: Patient monitoring use case - Spoke Hub

Appendix B. Patient monitoring use case - Connected

Refer following diagram:

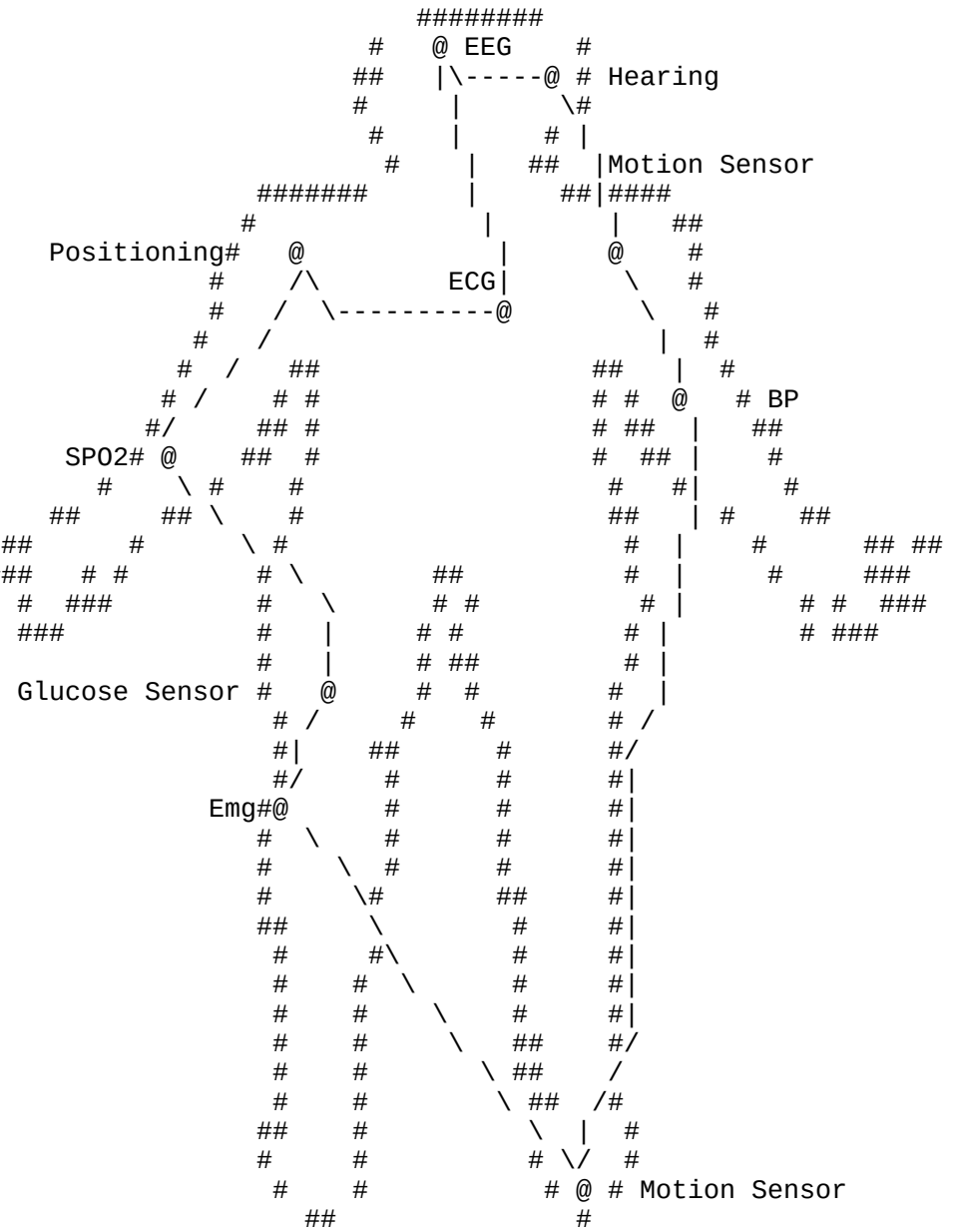

Figure 5: Patient monitoring use case - Connected

Appendix C. Changes

Compared with version-00, this updated draft is no longer all informative. Two main changes have been made as below:

1. Introduction part of 802.15.6 is simplified and more focused on the features that relates to the 6lo-WBAN adaptation layer, e.g. MAC frame format including MAC address and MTU, topology and scope of communication, and why the 6lo-WBAN adaptation layer is needed.

2. The 6lo-WBAN adaptation layer is specified in this draft titled as "Specification of IPv6 over WBAN" that lists the main features needs to be added in the 6lo adaptation layer including the formation of IID, IPv6 link-local address, unicast address mapping, header compression, and fragmentation and reassembly. These parts have never been mentioned in other documents related to WBAN, and in this version, we provide a guidance for such IPv6 enabled WBAN implementations.

Authors' Addresses

Muhammad Sajjad Akbar
Bournemouth University
Fern Barrow, Dorset
Poole BH12 5BB
United Kingdom

Email: makbar@bournemouth.ac.uk

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

Email: sangi_bahrian@yahoo.com

Mingui Zhang
Huawei Technologies
No. 156 Beiqing Rd. Haidian District
Beijing 100095
China

Email: zhangmingui@huawei.com

Jianqiang Hou
Huawei Technologies
101 Software Avenue
Nanjing 210012
China

Phone: +86 15852944235
Email: houjianqiang@huawei.com

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

Email: charliep@computer.org

Alexandre Petrescu
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
France

Phone: +33169089223
Email: alexandre.petrescu@cea.fr

Naveed Bin Rais
Ajman University
University Street,Al jerf 1
Ajman 346
United Arab Emirates

Email: naveedbinrais@gmail.com