6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 22, 2021

J. Hou
B. Liu
Huawei Technologies
Y-G. Hong
ETRI
X. Tang
SGEPRI
C. Perkins
Lupin Lodge
April 20, 2021

Transmission of IPv6 Packets over PLC Networks
draft-ietf-6lo-plc-06

Abstract

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

Status of This Memo

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

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

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

This Internet-Draft will expire on October 22, 2021.

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 an existing power grid, Power Line Communication (PLC) is a good candidate for supporting various service scenarios such as in houses and offices, in trains and vehicles, in smart grid and advanced metering infrastructure (AMI) [SCENA]. The data acquisition devices in these scenarios share common features such as fixed position, large quantity, low data rate and low power consumption.

Although PLC technology has evolved over several decades, it has not been fully adapted for IPv6 based constrained networks. The resource-constrained IoT related scenarios lie in the low voltage PLC networks with most applications in the area of Advanced Metering Infrastructure (AMI), Vehicle-to-Grid communications, in-home energy Management, and smart street lighting. IPv6 is important for PLC networks, due to its large address space and efficient address auto-configuration.

Commented [DT1]: typo

This document provides a brief overview of PLC technologies. Some of them have LLN (low power and lossy network) characteristics, i.e., limited power consumption, memory, and processing resources. This document specifies the transmission of IPv6 packets over those "constrained" PLC networks. The general approach is to adapt elements of the 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) and 6lo (IPv6 over Networks of Resource-constrained Nodes) specifications, such as [RFC4944], [RFC6282], [RFC6775] and [RFC8505] to constrained 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 BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the following acronyms and terminologies:

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

6lo: IPv6 over Networks of Resource-constrained Nodes

AMI: Advanced Metering Infrastructure

BBPLC: Broadband Power Line Communication

CID: Context ID

Coordinator: A device capable of relaying messages.

DAD: Duplicate Address Detection

EV: Electric Vehicle

IID: IPv6 Interface Identifier

IPHC: IP Header Compression

LAN: Local Area Network

LLN: Low power and Lossy Network

MSDU: MAC Service Data Unit

MTU: Maximum Transmission Unit

NBPLC: Narrowband Power Line Communication

OFDM: Orthogonal Frequency Division Multiplexing

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

PLC: Power Line Communication

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

PSDU: PHY Service Data Unit

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

RA: Router Advertisement

WAN: Wide Area Network

Commented [DT2]: nit: may be ok, but it seems odd to me that some definitions end in periods and some don't.

Commented [DT3]: Undefined acronym (and it does not have a * at https://www.rfc-editor.org/materials/abbrev.expansion.txt so does need to be expanded). Either add PAN as a separate term or change this to 6LoWPAN

The terminology used in this draft is aligned with IEEE 1901.2.

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

Table 1: Terminology Mapping between PLC standards

3. Overview of PLC

PLC technology enables convenient two-way communications for home users and utility companies to monitor and control electric plugged devices such as electricity meters and street lights. Due to the large range of communication frequencies, PLC is generally classified into two categories: Narrowband PLC (NBPLC) for automation of sensors (which have a low frequency band and low power cost), and Broadband PLC (BBPLC) for home and industry networking applications.

Various standards have been addressed on the MAC and PHY layers for this communication technology, e.g., BBPLC (1.8-250 MHz) including IEEE 1901 and ITU-T G.hn, and NBPLC (3-500 kHz) including ITU-T G.9902 (G.hnem), ITU-T G.9903 (G3-PLC) [ITU-T_G.9903], ITU-T G.9904 (PRIME), IEEE 1901.2 [IEEE_1901.2] (a combination of G3-PLC and PRIME PLC) and IEEE 1901.2a [IEEE_1901.2a] (an amendment to IEEE 1901.2).

A new PLC standard IEEE 1901.1 [IEEE_1901.1], which is aimeds at the medium frequency band of less than 12 MHz, has been published by the IEEE standard for Smart Grid Powerline Communication Working Group (SGPLC WG). IEEE 1901.1 balances the needs for bandwidth versus communication range, and is thus a promising option for 6lo applications.

This specification is focused on IEEE 1901.1, IEEE 1901.2, and ITU-T G.9903.

3.1. Protocol Stack

The protocol stack for IPv6 over PLC is illustrated in Figure 1. The PLC MAC/PHY layer corresponds to IEEE 1901.1, IEEE 1901.2 or ITU-T G.9903. The 6lo adaptation layer for PLC is illustrated in

Section 4. For multihop tree and mesh topologies, a routing protocol is likely to be necessary. The routes can be built in mesh-under mode at layer 2 or in route-over mode at layer 3, as explained in Section 3.4.

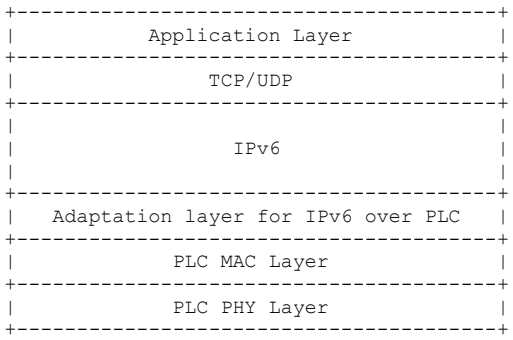

Figure 1: PLC Protocol Stack

3.2. Addressing Modes

Each PLC device has a globally unique long address of 48-bits ([IEEE_1901.1]) or 64-bits ([IEEE_1901.2], [ITU-T_G.9903]) and a short address of 12-bits ([IEEE_1901.1]) or 16-bit ([IEEE_1901.2], [ITU-T_G.9903]). The long address is set by the manufacturer according to the IEEE EUI-48 MAC address or the IEEE EUI-64 address. Each PLC device joins the network by using the long address and communicates with other devices by using the short address after joining the network. Short addresses can be assigned during the onboarding process, by the PANC or the JRC (join registrar/ coordinator) in CoJP (Constrained Join Protocol) [I-D.ietf-6tisch-minimal-security].

3.3. Maximum Transmission Unit

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

The IEEE 1901.1 MAC supports upper layer packets up to 2031 octets. The IEEE 1901.2 MAC layer supports ~~the~~ an MTU of 1576 octets (the original value of 1280 bytes was updated in 2015 [IEEE_1901.2a]).

Though these two technologies can support IPv6 natively without fragmentation and reassembly, it is possible to configure a smaller MTU in high-noise communication environment. Thus the 6lo functions, including header compression, fragmentation and reassembly, are still applicable and useful.

The MTU for ITU-T G.9903 is 400 octets, insufficient for supporting IPv6's MTU. For this reason, fragmentation and reassembly is required for G.9903-based networks to adapt IPv6.

3.4. Routing Protocol

Routing protocols suitable for use in PLC networks include:

- RPL (Routing Protocol for Low-Power and Lossy Networks) [RFC6550] is a layer 3 routing protocol. AODV-RPL [I-D.ietf-roll-aodv-rpl] updates RPL to include reactive, point-to-point, and asymmetric routing. IEEE 1901.2 specifies Information Elements (IEs) with MAC layer metrics, which can be provided to L3 routing protocol for parent selection.

- IEEE 1901.1 supports L2 routing. Each PLC node maintains an L2 routing table, in which each route entry comprises the short addresses of the destination and the related next hop. The route entries are built during the network establishment via a pair of association request/confirmation messages. The route entries can be changed via a pair of proxy change request/confirmation messages. These association and proxy change messages must be approved by the central coordinator (PANC in this document).

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

4. IPv6 over PLC

6LoWPAN and 6lo standards [RFC4944], [RFC6282], [RFC6775], and [RFC8505] provides useful functionality including link-local IPv6 addresses, stateless address auto-configuration, neighbor discovery, header compression, fragmentation, and reassembly. However, due to the different characteristics of the PLC media, the 6LoWPAN adaptation layer, as it is, cannot perfectly fulfill the requirements of PLC environments. These considerations suggest the need for a dedicated adaptation layer for PLC, which is detailed in the following subsections.

4.1. Stateless Address Autoconfiguration

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

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

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

    16_bit_PAN:00FF:FE00:16_bit_short_address

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

    YYYY:YYFF:FE00:0XXX

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

For privacy reasons, the IID derived from the MAC address SHOULD only be used for link-local address configuration. A PLC host SHOULD use the IID derived from the link-layer short address to configure the IPv6 address used for communication with the public network; otherwise, the host's MAC address is exposed. As per [RFC8065], when short addresses are used on PLC links, a shared secret key or version number from the Authoritative Border Router Option [RFC6775] can be used to improve the entropy of the hash input, thus the generated IID can be spread out to the full range of the IID address space while stateless address compression is still allowed.

Commented [DT4]: "the" implies there can only be one. Does this mean it won't work if you have two prefixes, such as from a router homed to 2 ISPs, or from 2 routers on the link? If so, state this limitation explicitly as this is not typical in IPv6.

Or should this say "... to configure IPv6 addresses ..."?

Commented [DT5]: Do you specify which mechanism to use? I don't think you can get both compression and interoperability without specifying the details for such a hash, and I was expecting this document to specify the hash algorithm.

Especially in the scenario discussed in the paragraph above Figure 7, I don't think you can simply assume all devices are from the same vendor, at least not without stating it as an assumption that you don't care about interoperability (in which case why would you need this to be an IETF standard...)

4.2. IPv6 Link Local Address

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

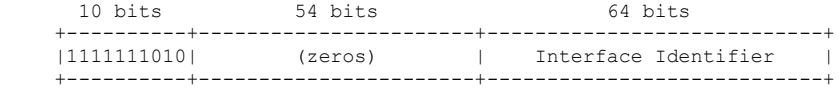

Figure 2: IPv6 Link Local Address for a PLC interface

4.3. Unicast Address Mapping

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

4.3.1. Unicast Address Mapping for IEEE 1901.1

The Source/Target Link-layer Address options for IEEE_1901.1 used in the Neighbor Solicitation and Neighbor Advertisement have the following form.

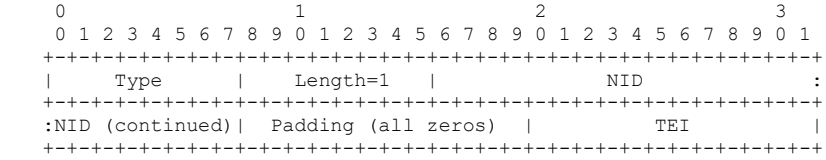

Figure 3: Unicast Address Mapping for IEEE 1901.1

Option fields:

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

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

NID: 24-bit Network IDentifier

Padding: 12 zero bits

TEI: 12-bit Terminal Equipment Identifier

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

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

The Source/Target Link-layer Address options for IEEE_1901.2 and ITU-T G.9903 used in the Neighbor Solicitation and Neighbor Advertisement have the following form.

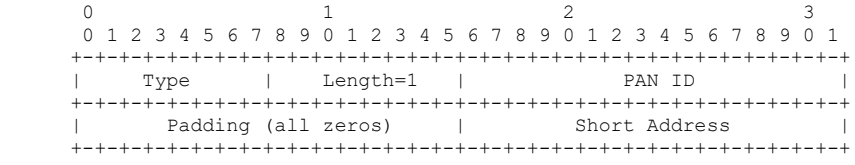

Figure 4: Unicast Address Mapping for IEEE 1901.2

Option fields:

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

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

PAN ID: 16-bit PAN IDentifier

Padding: 16 zero bits

Short Address: 16-bit short address

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

4.4. Neighbor Discovery

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

For IPv6 address prefix dissemination, Router Solicitations (RS) and Router Advertisements (RA) MAY be used as per [RFC6775]. If the PLC network uses route-over, the IPv6 prefix MAY be disseminated by the layer 3 routing protocol, such as RPL, which may include~~s~~ the prefix in the DIO message. As per [I-D.ietf-roll-unaware-leaves], it is possible to have PLC devices configured as RPL-unaware-leaves, which do not participate to RPL at all, along with RPL-aware PLC devices. In this case, the prefix dissemination SHOULD use the RS/RA messages.

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

For address registration in route-over mode, a PLC device MUST register its addresses by sending a unicast link-local Neighbor Solicitation to the 6LR. If the registered address is link-local, the 6LR SHOULD NOT further register it to the registrar (6LBR, 6BBR). Otherwise, the address MUST be registered via an ARO or EARO included in the DAR ([RFC6775]) or EDAR ([RFC8505]) messages. For RFC8505 compliant PLC devices, the 'R' flag in the EARO MUST be set when sending Neighbor Solicita~~i~~tions in order to extract the status information in the replied Neighbor Advertisements from the 6LR. If DHCPv6 is used to assign addresses or the IPv6 address is derived from unique long or short link layer address, Duplicate Address Detection (DAD) MUST NOT be utilized. Otherwise, the DAD MUST be performed at the 6LBR (as per [RFC6775]) or proxied by the routing registrar (as per [RFC8505]). The registration status is fe~~e~~d_back~~ed~~ via the DAC or EDAC message from the 6LBR and the Neighbor Advertisement (NA) from the 6LR.

Commented [DT6]: typo

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

4.5. Header Compression

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

For IEEE 1901.2 and G.9903, the IP header compression follows the instruction in [RFC6282]. However, additional adaptation MUST be considered for IEEE 1901.1 since it has a short address of 12 bits instead of 16 bits. The only modification is the semantics of the "Source Address Mode" when set as "10" in the section 3.1 of [RFC6282], which is illustrated as following.

SAM: Source Address Mode:

If SAC=0: Stateless compression

10: 12 bits. The first 116 bits of the address are elided. The value of the first 64 bits is the link-local prefix padded with zeros. The following 64 bits are 0000:00ff:fe00:0XXX, where XXX are the 12 bits carried in-line.

If SAC=1: stateful context-based compression

10: 12 bits. The address is derived using context information and the 12 bits carried in-line. Bits covered by context information are always used. Any IID bits not covered by context information are taken directly from their corresponding bits in the 12-bit to IID mapping given by 0000:00ff:fe00:0XXX, where XXX are the 12 bits carried inline. Any remaining bits are zero.

4.6. Fragmentation and Reassembly

The Constrained PLC MAC layer provides the function of fragmentation and Reassembly. ~~,~~ ~~H~~however, fragmentation and reassembly is still required at the adaptation layer~~,~~ if the MAC layer cannot support the minimum MTU demanded by IPv6, which is 1280 octets.

In IEEE 1901.1 and IEEE 1901.2, the MAC layer supports payloads as big as 2031 octets and 1576 octets respectively. However when the channel condition is noisy, it is possible to configure smaller MTU at the MAC layer. If the configured MTU is smaller than 1280

octeets, the fragmentation and reassembly defined in [RFC4944] MUST be used.

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 the 6lo adaptation layer MUST be provided as specified in [RFC4944].

[RFC4944] uses a 16-bit datagram tag to identify the fragments of the same IP packet. [RFC4963] specifies that at high data rates, the 16-bit IP identification field is not large enough to prevent frequent incorrectly assembled IP fragments. For constrainied PLC, the data rate is much lower than the situation mentioned in RFC4963, thus the 16-bit tag is sufficient to assemble the fragements correctly.

5. Internet Connectivity Scenarios and Topologies

The PLC network model can be simplified to two kinds of network devices: PAN Coordinator (PANC) and PAN PLC Device. The PANC is the primary coordinator of the PLC subnet and can be seen as a master node; PAN Devices are typically PLC meters and sensors. The PANC also serves as the Routing Registrar for proxy registration and DAD procedures, making use of the updated registration procedures in [RFC8505]. IPv6 over PLC networks are built as trees, meshes, or stars according to the use cases. Generally, each PLC network has one PANC. In some cases, the PLC network can have alternate coordinators to replace the PANC when the PANC leaves the network for some reason. Note that the PLC topologies in this section are based on logical connectivity, not physical links. The term "PLC subnet" refers to a multilink subnet, in which the PLC devices share the same address prefix.

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

Commented [DT7]: typo

Commented [DT8]: typo

Commented [DT9]: typo

Commented [DT10]: Table 1 said the term "PAN Device" is only for ITU-T G.9903, but this section implies it's generic. Shouldn't this instead be "PLC Device"?

Commented [DT11]: grammar: Because "networks" is plural as the subject, these should be too. Or change the subject to "An IPv6 over PLC network is..."

Commented [DT12]: Can one device (not PANC) easily enumerate the link-layer addresses of all other devices on the PLC network? If not, then privacy of IPv6 link local addresses becomes interesting as noted in RFC 8065, and my reading of this doc is that it does not try to provide any entropy for link-local addresses. So this should at least be discussed in the security considerations section.

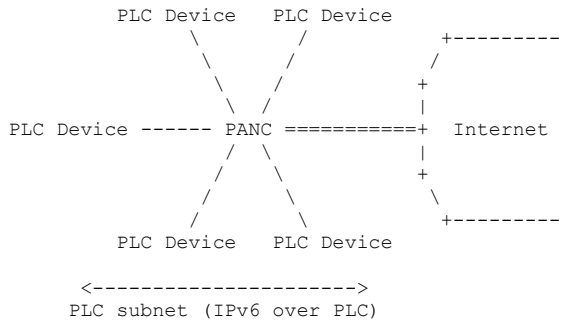

Figure 5: PLC Star Network connected to the Internet

A tree topology is useful when the distance between a device A and the PANC is beyond the PLC allowed limit and there is another device B in between able to communicate with both sides. Device B in this case acts both as a ~~PAN~~ PLC Device and a Coordinator. For this scenario, the link layer communications take place between device A and device B, and between device B and PANC. An example of a PLC tree network is depicted in Figure 6. This topology can be applied in ~~the~~ smart street lighting, where the lights adjust the brightness to reduce energy consumption while sensors are deployed on the street~~—~~lights to provide information such as light intensity, temperature, and humidity. The d~~D~~ata transmission distance in the street lighting scenario is normally above several kilometers, thus ~~the~~ a PLC tree network is required. A more sophisticated AMI network may also be constructed into the tree topology which is depicted in [RFC8036]. A tree topology is suitable for AMI scenarios that require large coverage but low density, e.g., the deployment of smart meters in rural areas. RPL is suitable for maintenance of a tree topology in which there is no need for communication directly between PAN devices.

Commented [DT13]: Wrong term per Table 1

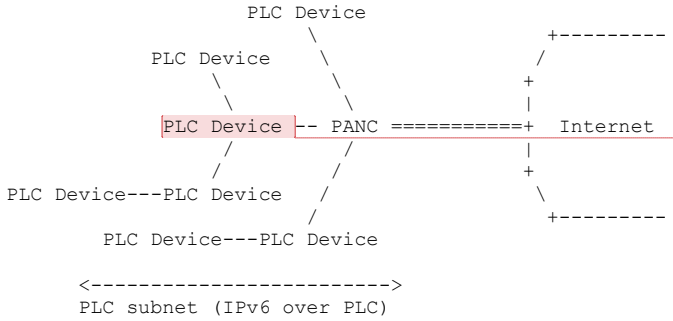

Figure 6: PLC Tree Network connected to the Internet

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

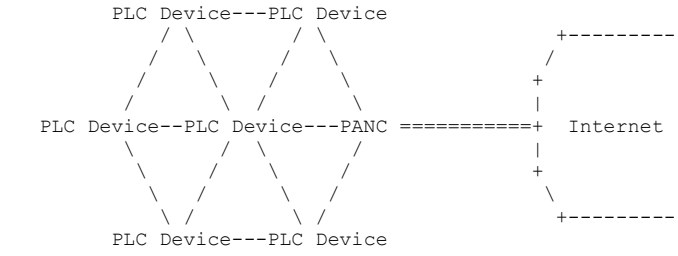

Figure 7: PLC Mesh Network connected to the Internet

Commented [DT14]: Per Table 1 and the paragraphs above, shouldn't this be called "PLC Device + Coordinator"? Same for the other two intermediate devices in this diagram?

Commented [DT15]: Fix terms

6. Operations and Manageability Considerations

The constrained PLC networks are not managed in the same way as ~~the~~an enterprise network or carrier network. ~~The~~ eConstrained PLC networks~~ as the~~ like other IoT networks, are designed to be self-organized and self-managed. The software or firmware is flau~~s~~shed into the devices before deployment by the vendor or operator. And during the deployment process, the devices are bootstrapped, and no extra configuration is needed to get the devices connected to each other. Once a device becomes offline, it goes back to the bootstrapping stage and tries to rejoin the network. The onboarding status of the devices and the topology of the PLC network can be visualized via the gateway. The recently-formed iotops WG in IETF is aiming to design more features for the management of IOT networks.

Commented [DT16]: I'm guessing this was a typo

Commented [DT17]: typo

7. IANA Considerations

There are no IANA considerations related to this document.

8. Security Considerations

Due to the high accessibility of power grids, 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. Thus link layer security mechanisms are designed in the PLC technologies mentioned in this document.

Malicious PLC devices could paralyze the whole network via DOS attacks, e.g., keep joining and leaving the network frequently, or sending multicast routing messages containing fake metrics. A device may also join a wrong or even malicious network, exposing its data to ~~illegal~~ malicious users. Mutual authentication of a network and a new device can be conducted during the onboarding process of the new device. Methods include protocols such as [RFC7925] (exchanging pre-installed certificates over DTLS)~~—~~, [I-D.ietf-6tisch-minimal-security] (which uses pre-shared keys), and [I-D.ietf-6tisch-dtsecurity-zerotouch-join] (which uses IDevID and MASA service). It is also possible to use EAP methods such as [I-D.ietf-emu-eap-noob] via transports like PANA [RFC5191]. No specific mechanism is specified by this document as an appropriate mechanism will depend upon deployment circumstances.

IP addresses may be used to track devices on the Internet; such devices can in turn be linked to individuals and their activities. Depending on the application and the actual use pattern, this may be undesirable. To impede tracking, globally unique and non-changing characteristics of IP addresses should be avoided, e.g., by

frequently changing the global prefix and avoiding unique link-layer derived IIDs in addresses. [RFC8065] discusses the privacy threats when interface identifiers (IID) are generated without sufficient entropy, including correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning. Schemes such as limited lease period in DHCPv6 [RFC3315], Cryptographically Generated Addresses (CGAs) [RFC3972], privacy extensions [RFC4941], Hash-Based Addresses (HBAs) [RFC5535], or semantically opaque addresses [RFC7217] SHOULD be considered to enhance the IID privacy.

Commented [DT18]: I don't think this is sufficient for a security considerations section. RFC 8065 section 4 provides a checklist. I'd recommend addressing each point separately so it's clear that you covered the whole checklist.

For example, it's really hard to tell from reading the last paragraph of section 4.5 of this draft how it addresses RFC 8065's statement that "any specification using Short Addresses should carefully construct an IID generation mechanism so as to provide sufficient entropy compared to the link lifetime" so elaboration here is warranted here in my opinion.

9. Acknowledgements

We gratefully acknowledge suggestions from the members of the IETF 6lo working group. Great thanks to Samita Chakrabarti and Gabriel Montenegro for their feedback and support in connecting the IEEE and ITU-T sides. The aAuthors thank Scott Mansfield, Ralph Droms, and Pat Kinney for their guidance in the liaison process. The aAuthors wish to thank Stefano Galli, Thierry Lys, Yizhou Li, Yuefeng Wu, and Michael Richardson for their valuable comments and contributions.

10. References

10.1. Normative References

[IEEE_1901.1]
IEEE-SA Standards Board, "Standard for Medium Frequency (less than 15 MHz) Power Line Communications for Smart Grid Applications", IEEE 1901.1, May 2018, <https://ieeexplore.ieee.org/document/8360785>.

[IEEE_1901.2]
IEEE-SA Standards Board, "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications", IEEE 1901.2, October 2013, <https://standards.ieee.org/findstds/standard/1901.2-2013.html>.

[ITU-T_G.9903]
International Telecommunication Union, "Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks", ITU-T G.9903, February 2014, <https://www.itu.int/rec/T-REC-G.9903>.

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

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <https://www.rfc-editor.org/info/rfc2464>.

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

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

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

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

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

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

10.2. Informative References

[EUI-64] IEEE-SA Standards Board, "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", IEEE EUI-64, March 1997, <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf>.

[I-D.ietf-6tisch-dtsecurity-zerotouch-join] Richardson, M., "6tisch Zero-Touch Secure Join protocol", draft-ietf-6tisch-dtsecurity-zerotouch-join-04 (work in progress), July 2019.

[I-D.ietf-6tisch-minimal-security] Vucinic, M., Simon, J., Pister, K., and M. Richardson, "Constrained Join Protocol (CoJP) for 6TiSCH", draft-ietf-6tisch-minimal-security-15 (work in progress), December 2019.

[I-D.ietf-emu-eap-noob] Aura, T., Sethi, M., and A. Peltonen, "Nimble out-of-band authentication for EAP (EAP-NOOB)", draft-ietf-emu-eap-noob-03 (work in progress), December 2020.

[I-D.ietf-roll-aodv-rpl] Anamalamudi, S., Zhang, M., Perkins, C., Anand, S., and B. Liu, "AODV based RPL Extensions for Supporting Asymmetric P2P Links in Low-Power and Lossy Networks", draft-ietf-roll-aodv-rpl-08 (work in progress), May 2020.

[I-D.ietf-roll-unaware-leaves] Thubert, P. and M. Richardson, "Routing for RPL Leaves", draft-ietf-roll-unaware-leaves-30 (work in progress), January 2021.

[IEEE_1901.2a] IEEE-SA Standards Board, "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications - Amendment 1", IEEE 1901.2a, September 2015, <https://standards.ieee.org/findstds/standard/1901.2a-2015.html>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

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

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

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <https://www.rfc-editor.org/info/rfc4941>.

[RFC4963] Heffner, J., Mathis, M., and B. Chandler, "IPv4 Reassembly Errors at High Data Rates", RFC 4963, DOI 10.17487/RFC4963, July 2007, <https://www.rfc-editor.org/info/rfc4963>.

[RFC5191] Forsberg, D., Ohba, Y., Ed., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, DOI 10.17487/RFC5191, May 2008, <https://www.rfc-editor.org/info/rfc5191>.

[RFC5535] Bagnulo, M., "Hash-Based Addresses (HBA)", RFC 5535, DOI 10.17487/RFC5535, June 2009, <https://www.rfc-editor.org/info/rfc5535>.

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

[RFC7925] Tschofenig, H., Ed. and T. Fossati, "Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things", RFC 7925, DOI 10.17487/RFC7925, July 2016, <https://www.rfc-editor.org/info/rfc7925>.

[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>.

[SCENA] Cano, C., Pittolo, A., Malone, D., and L. Lampe, "State of the Art in Power Line Communications: From the Applications to the Medium", July 2016, <https://ieeexplore.ieee.org/document/7467440>.

Authors' Addresses

Jianqiang Hou
Huawei Technologies
101 Software Avenue,
Nanjing 210012
China

Email: houjianqiang@huawei.com

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

Email: remy.liubing@huawei.com

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

Email: yghong@etri.re.kr

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

Email: itc@sgepri.sgcc.com.cn

Charles E. Perkins
Lupin Lodge

Email: charliep@computer.org