Stream: Internet Engineering Task Force (IETF)
RFC: 9354
Category: Standards Track
Published: January 2023
ISSN: 2070-1721
Authors: J. Hou, *Huawei Technologies*; B. Liu, *Huawei Technologies*; Y-G. Hong, *Daejeon University*; X. Tang, *SGEPRI*; C. Perkins, *Lupin Lodge*

RFC 9354
Transmission of IPv6 Packets over Power Line Communication (PLC) Networks

Abstract

Power Line Communication (PLC), namely using electric power lines for indoor and outdoor communications, has been widely applied to support Advanced Metering Infrastructure (AMI), especially smart meters for electricity. The existing electricity infrastructure facilitates the expansion of PLC deployments due to its potential advantages in terms of cost and convenience. 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 those described in ITU-T G.9903, IEEE 1901.1, and IEEE 1901.2.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9354.

Copyright Notice

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. Using the existing power grid to transmit messages, 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 grids, and in Advanced Metering Infrastructure (AMI) [SCENA]. The data-acquisition devices in these scenarios share common features such as fixed position, large quantity of nodes, 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 scenarios related to the Internet of Things (IoT) lie in the low voltage PLC networks with most applications in the area of 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 autoconfiguration.

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 those described in [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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the following acronyms and terminologies:

6BBR: 6LoWPAN Backbone Router

6LBR: 6LoWPAN Border Router

6lo: IPv6 over Networks of Resource-constrained Nodes

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

6LR: 6LoWPAN Router

AMI: Advanced Metering Infrastructure

BBPLC: Broadband Power Line Communication

Coordinator: A device capable of relaying messages

DAD: Duplicate Address Detection

EUI: Extended Unique Identifier

IID: Interface Identifier

LLN: Low-Power and Lossy Network

MTU: Maximum Transmission Unit

NBPLC: Narrowband Power Line Communication

PAN: Personal Area Network

PANC: PAN Coordinator, a coordinator that 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 document

RA: Router Advertisement

RPL: Routing Protocol for Low-Power and Lossy Networks

Below is a mapping table of the terminology between [IEEE_1901.2], [IEEE_1901.1], [ITU-T_G.9903], and this document.

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 electrically connected devices such as electricity meters and street lights. PLC can also be used in smart home scenarios, such as the control of indoor lights and switches. 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 Media Access Control (MAC) and Physical (PHY) layers. For example, standards for BBPLC (1.8-250 MHz) include IEEE 1901 and ITU-T G.hn, and standards for NBPLC (3-500 kHz) include ITU-T G.9902 (G.hnem), ITU-T G.9903 (G3-PLC) [ITU-T_G.9903], ITU-T G.9904 (PRIME), IEEE 1901.2 (a combination of G3-PLC and PRIME PLC) [IEEE_1901.2], and IEEE 1901.2a (an amendment to IEEE 1901.2) [IEEE_1901.2a].

IEEE 1901.1 [IEEE_1901.1], a PLC standard that is aimed at the medium frequency band of less than 12 MHz, was 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 and PLC PHY layers correspond to the layers described in 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 Sections 3.4 and 4.4.

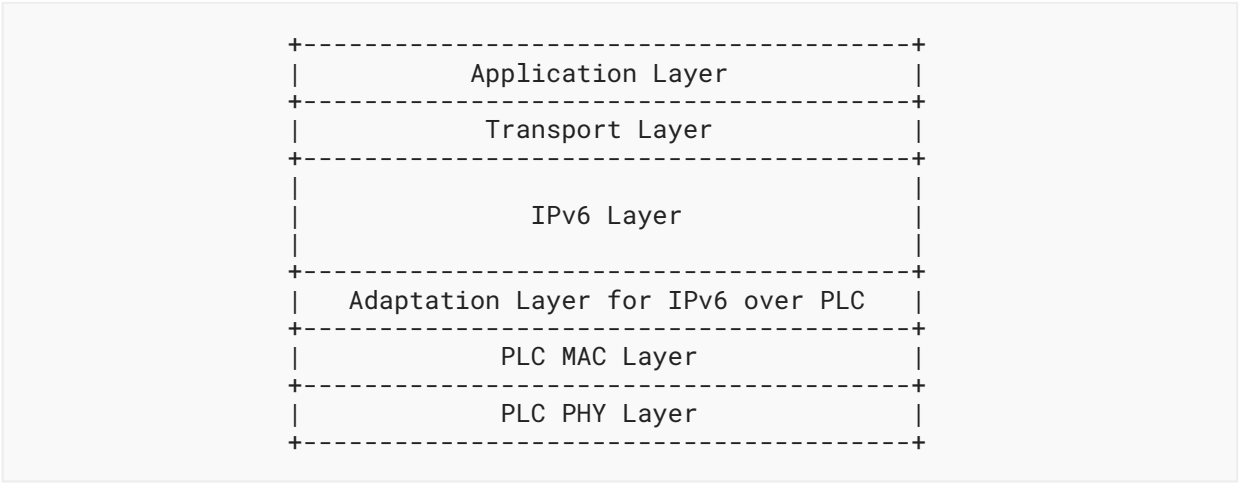

Figure 1: PLC Protocol Stack

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 bits [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) [RFC9031].

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 an 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 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 originally without fragmentation and reassembly, it is possible to configure a smaller MTU in a 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, which is insufficient for supporting IPv6's MTU. For this reason, fragmentation and reassembly are required for G.9903-based networks to carry 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 [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 a Layer 3 routing protocol for parent selection.
- IEEE 1901.1 supports the mesh-under routing scheme. Each PLC node maintains a 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 (Lightweight On-demand Ad hoc Distance vector routing protocol, Next Generation) 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

A PLC node distinguishes between an IPv6 PDU and a non-IPv6 PDU based on the equivalent of an Ethertype in a Layer 2 PLC PDU. [RFC7973] defines an Ethertype of "A0ED" for LoWPAN encapsulation, and this information can be carried in the IE field in the MAC header of [IEEE_1901.2] or [ITU-T_G.9903]. And regarding [IEEE_1901.1], the IP packet type has been

defined with the corresponding MAC Service Data Unit (MSDU) type value 49. And the 4-bit Internet Protocol version number in the IP header helps to distinguish between an IPv4 PDU and an IPv6 PDU.

6LoWPAN and 6lo standards, as described in [RFC4944], [RFC6282], [RFC6775], and [RFC8505], provide useful functionality, including link-local IPv6 addresses, stateless address autoconfiguration, 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 IID by inserting 0xFFFE at the fourth and fifth octets as specified in [RFC2464]. The IPv6 IID is derived from the 64-bit IID by inverting the U/L (Universal/Local) 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 as follows:

16_bit_PAN:0000:16_bit_short_address

Then, the 64-bit IID **MUST** be derived by inserting the 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 a 24-bit NID (Network Identifier, YYYYYY), 12 zero bits, and a 12-bit TEI (Terminal Equipment Identifier, XXX) as follows:

YYYY:YY00:0XXX

The 64-bit IID **MUST** be derived by inserting the 16-bit 0xFFFE into this 48-bit pseudo-address as follows:

YYYY:YYFF:FE00:0XXX

As investigated in [RFC7136], aside from the method discussed in [RFC4291], other IID-generation methods defined by the IETF do not imply any additional semantics for the Universal/Local (U/L) bit (bit 6) and the Individual/Group bit (bit 7). Therefore, these two bits are not reliable indicators. Thus, when using an IID derived by a short address, the operators of the PLC network can choose whether or not to comply with the original meaning of these two bits. If they choose to comply with the original meaning, these two bits **MUST** both be set to zero, since the IID derived from the short address is not global. In order to avoid any ambiguity in the derived IID,

these two bits **MUST NOT** be a valid part of the PAN ID (for IEEE 1901.2 and ITU-T G.9903) or NID (for IEEE 1901.1). For example, the PAN ID or NID must always be chosen so that the two bits are zeros or the high six bits in PAN ID or NID are left shifted by two bits. If they choose not to comply with the original meaning, the operator must be aware that these two bits are not reliable indicators, and the IID cannot be transformed back into a short link-layer address via a reverse operation of the mechanism presented above. However, the short address can still be obtained via the Unicast Address Mapping mechanism described in Section 4.3.

For privacy reasons, the IID derived from the MAC address (with padding and bit clamping) **SHOULD** only be used for link-local address configuration. A PLC host **SHOULD** use the IID derived from the short link-layer address to configure IPv6 addresses 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. By default, the hash algorithm **SHOULD** be SHA256, using the version number, the PAN ID or NID, and the short address as the input arguments, and the 256-bit hash output is truncated into the IID by taking the high 64 bits.

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).

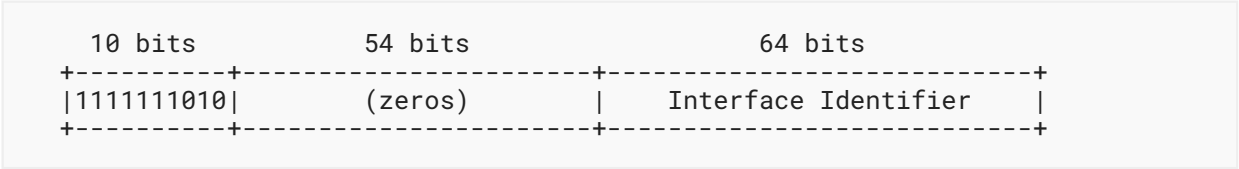

Figure 2: IPv6 Link-Local Address for a PLC Interface

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 (Neighbor Solicitation). The resolution is realized by the NCEs (neighbor cache entries) 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 Link-Layer Address and Target Link-Layer Address options for IEEE_1901.1 used in the NS and Neighbor Advertisement (NA) have the following form.

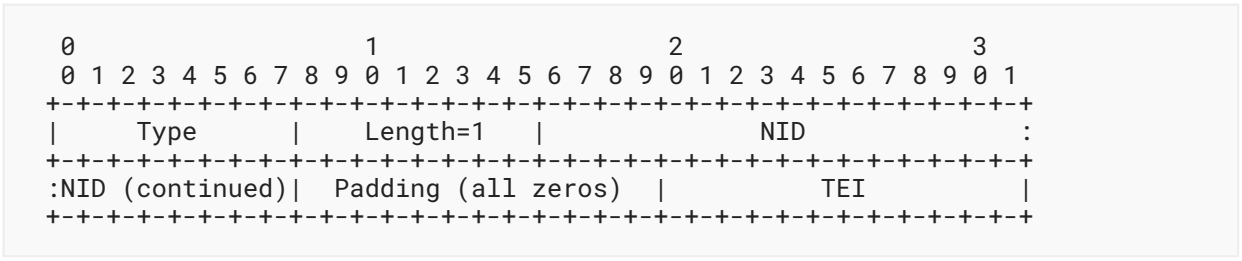

Figure 3: Unicast Address Mapping for IEEE 1901.1

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

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

The Source Link-Layer Address and Target Link-Layer Address options for IEEE_1901.2 and ITU-T G.9903 used in the NS and NA have the following form.

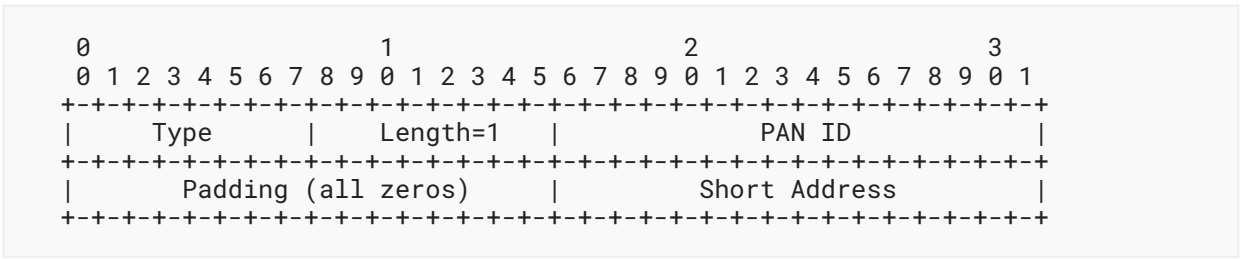

Figure 4: Unicast Address Mapping for IEEE 1901.2

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

4.4. Neighbor Discovery

Neighbor discovery procedures for 6LoWPAN networks are described in [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 prefix dissemination, Router Solicitations (RSs) and Router Advertisements (RAs) **MAY** be used as per [RFC6775]. If the PLC network uses route-over mode, the IPv6 prefix **MAY** be disseminated by the Layer 3 routing protocol, such as RPL, which may include the prefix in the DIO (DODAG Information Object) message. As per [RFC9010], it is possible to have PLC devices configured as RPL-unaware leaves, which do not participate in RPL at all, along with RPL-aware PLC devices. In this case, the prefix dissemination **SHOULD** use the RS/RA messages.

For dissemination of context information, RAs **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 NS to the 6LR. If the registered address is link local, the 6LR **SHOULD NOT** further register it to the registrar (6LBR or 6BBR). Otherwise, the address **MUST** be registered via an ARO (Address Registration Option) or EARO (Extended Address Registration Option) included in the DAR (Duplicate Address Request) [RFC6775] or EDAR (Extended Duplicate Address Request) [RFC8505] messages. For PLC devices compliant with [RFC8505], the 'R' flag in the EARO **MUST** be set when sending NSs in order to extract the status information in the replied NAs from the 6LR. If DHCPv6 is used to assign addresses or the IPv6 address is derived from the unique long or short link-layer address, Duplicate Address Detection (DAD) **SHOULD NOT** be utilized. Otherwise, DAD **MUST** be performed at the 6LBR (as per [RFC6775]) or proxied by the routing registrar (as per [RFC8505]). The registration status is fed back via the DAC (Duplicate Address Confirmation) or EDAC (Extended Duplicate Address Confirmation) message from the 6LBR and the NA from the 6LR. Section 6 of [RFC8505] shows how devices that only behave as specified in [RFC6775] can work with devices that have been updated per [RFC8505].

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 fed back via the NA message from the 6LBR.

4.5. Header Compression

IPv6 header compression in PLC is based on [RFC6282] (which updates [RFC4944]). [RFC6282] specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4; therefore, this format is used for compression of IPv6 datagrams within PLC MAC frames. For situations when the PLC MAC MTU cannot support the 1280-octet IPv6 packet, the headers **MUST** be compressed according to the encoding formats specified in [RFC6282], including the Dispatch Header, the LOWPAN_IPHC, and the compression residue carried inline.

For IEEE 1901.2 and ITU-T 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" and the "Destination Address Mode" when set as "10" in Section 3.1 of [RFC6282], which is illustrated as follows.

SAM: Source Address Mode:

If SAC=0: Stateless compression

10: 16 bits. The first 112 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 0XXX are the 16 bits carried inline, in which the first 4 bits are zero.

If SAC=1: Stateful context-based compression

10: 16 bits. The address is derived using context information and the 16 bits carried inline. 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 mapping between the 16-bit short address and the IID as provided by 0000:00ff:fe00:0XXX, where 0XXX are the 16 bits carried inline, in which the first 4 bits are zero. Any remaining bits are zero.

DAM: Destination Address Mode:

If M=0 and DAC=0: Stateless compression

10: 16 bits. The first 112 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 0XXX are the 16 bits carried inline, in which the first 4 bits are zero.

If M=0 and DAC=1: Stateful context-based compression

10: 16 bits. The address is derived using context information and the 16 bits carried inline. 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 mapping between the 16-bit short address and the IID as provided by 0000:00ff:fe00:0XXX, where 0XXX are the 16 bits carried inline, in which the first 4 bits are zero. Any remaining bits are zero.

4.6. Fragmentation and Reassembly

The constrained PLC MAC layer provides the functions of fragmentation and reassembly. However, fragmentation and reassembly are 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, smaller packets have a higher transmission success rate, and the operator can choose to configure smaller MTU at the MAC layer. If the configured MTU is smaller than 1280 octets, 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 constrained PLC, the data rate is much lower than the situation mentioned in [RFC4963]; thus, the 16-bit tag is sufficient to assemble the fragments correctly.

5. Internet Connectivity Scenarios and Topologies

The PLC network model can be simplified to two kinds of network devices: PAN Coordinator (PANC) and PLC device. The PANC is the primary coordinator of the PLC subnet and can be seen as a primary node; PLC devices are typically PLC meters and sensors. The address registration and DAD features can also be deployed on the PANC, for example, the 6LBR [RFC6775] or the routing registrar [RFC8505]. IPv6 over PLC networks are built as tree, mesh, or star topologies 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 PLC device and a PANC. The PANC typically collects data (e.g., a meter reading) from the PLC devices and then concentrates and uploads the data through Ethernet or cellular networks (see Figure 5). The collected data is transmitted by the smart meters through PLC, aggregated by a concentrator, and sent to the utility and then to a Meter Data Management System for data storage, analysis, and billing. This topology has been widely applied in the deployment of smart meters, especially in apartment buildings.

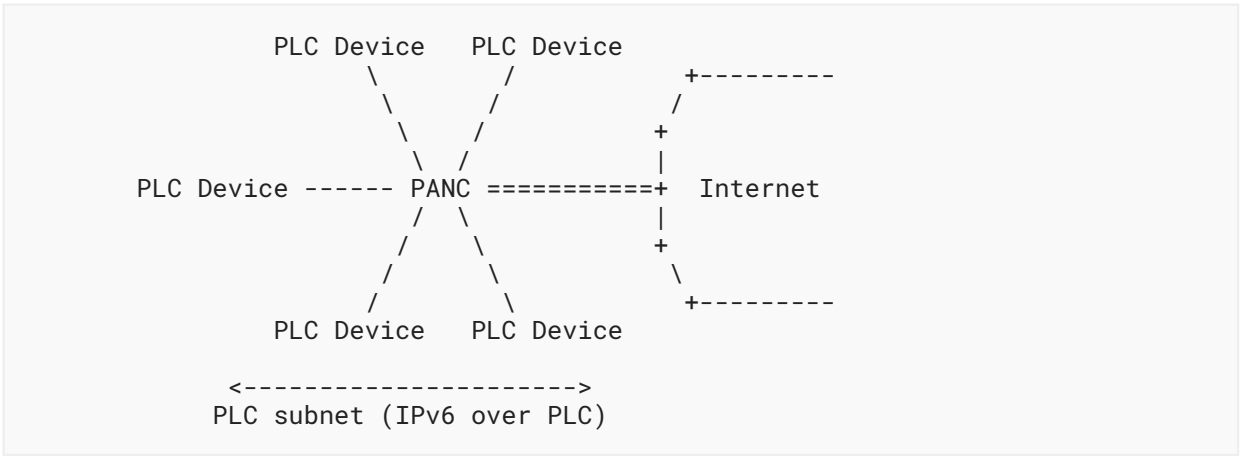

Figure 5: PLC Star Network Connected to the Internet

A tree topology is useful when the distance between a device A and 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 as both a 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 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 data-transmission distance in the street lighting scenario is normally above several kilometers; thus, a PLC tree network is required. A more sophisticated AMI network may also be constructed into the tree topology that is depicted in [RFC8036]. A tree topology is suitable for AMI scenarios that require large coverage but low density, e.g., the deployment of smart meters in rural areas. RPL is suitable for maintenance of a tree topology in which there is no need for communication directly between PAN devices.

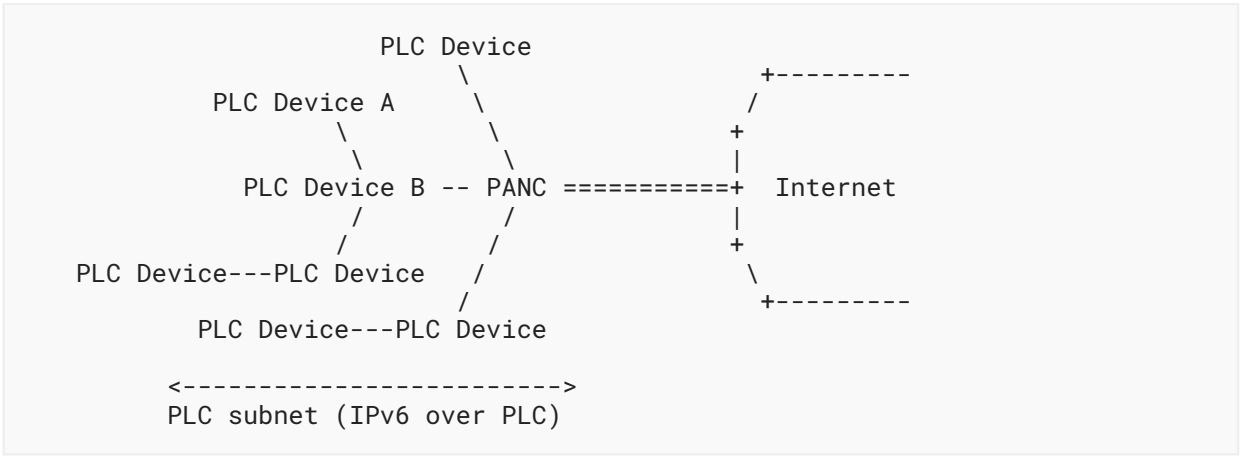

Figure 6: PLC Tree Network Connected to the Internet

Mesh networking in PLC has many 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 [AODV-RPL] enables direct communication between PLC devices, without being obliged to transmit frames through the PANC, which is a requirement often cited for the AMI infrastructure.

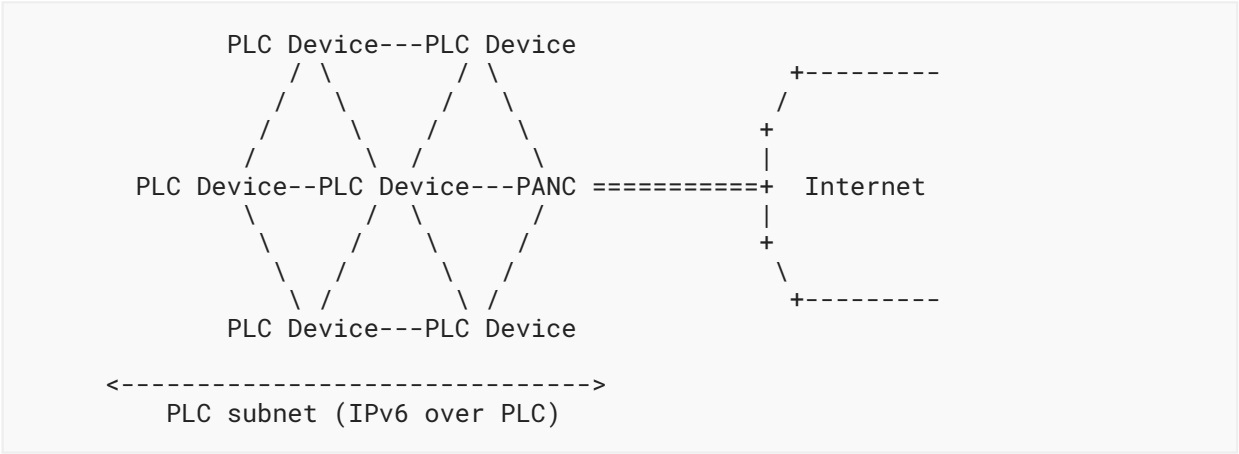

Figure 7: PLC Mesh Network Connected to the Internet

6. Operations and Manageability Considerations

Constrained PLC networks are not managed in the same way as enterprise networks or carrier networks. Constrained PLC networks, like the other IoT networks, are designed to be self-organized and self-managed. The software or firmware is flashed 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 PANC. The recently formed IOTOPS WG in the IETF aims to identify the requirements in IoT network management, and operational practices will be published. Developers and operators of PLC networks should be able to learn operational experiences from this WG.

7. IANA Considerations

This document has no IANA actions.

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. Link-layer security mechanisms, such as payload encryption and device authentication, are designed in the PLC technologies mentioned in this document. Additionally, an on-path malicious PLC device could eavesdrop or modify packets sent through it if appropriate confidentiality and integrity mechanisms are not implemented.

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 inadvertently join a wrong or even malicious network, exposing its data to malicious users. When communicating with a device outside the PLC network, the traffic has to go through the PANC. Thus, the PANC must be a trusted entity. Moreover, the PLC network must prevent malicious devices from joining the network. Thus, mutual authentication of a PLC network and a new device is important, and it can be conducted during the onboarding process of the new device. Methods include protocols such as the TLS/DTLS Profile [RFC7925] (exchanging pre-installed certificates over DTLS), the Constrained Join Protocol (CoJP) [RFC9031] (which uses pre-shared keys), and Zero-Touch Secure Join [ZEROTOUCH] (an IoT version of the Bootstrapping Remote Secure Key Infrastructure (BRSKI), which uses an Initial Device Identifier (IDevID) and a Manufacturer Authorized Signing Authority (MASA) service to facilitate authentication). It is also possible to use Extensible Authentication Protocol (EAP) methods such as the one defined in [RFC9140] via transports like Protocol for Carrying Authentication for Network Access (PANA) [RFC5191]. No specific mechanism is specified by this document, as an appropriate mechanism will depend upon deployment circumstances. In some cases, the PLC devices can be deployed in uncontrolled places, where the devices may be accessed physically and be compromised via key extraction. The compromised device may be still able to join in the network since its credentials are still valid. When group-shared symmetric keys are used in the network, the consequence is even more severe, i.e., the whole network or a large part of the network is at risk. Thus, in scenarios where physical attacks are considered to be relatively highly possible, per-device credentials **SHOULD** be used. Moreover, additional end-to-end security services are complementary to the network-side security mechanisms, e.g., if a device is compromised and has joined in the network, and then it claims itself as the PANC and tries to make the rest of the devices join its network. In this situation, the real PANC can send an alarm to the operator to acknowledge the risk. Other behavior-analysis mechanisms can be deployed to recognize the malicious PLC devices by inspecting the packets and the data.

IP addresses may be used to track devices on the Internet; such devices can often 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 an IID is generated without sufficient entropy, including correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning. And an

effective way to deal with these threats is to have enough entropy in the IID compared to the link lifetime. Consider a PLC network with 1024 devices and a link lifetime is 8 years, according to the formula in [RFC8065], an entropy of 40 bits is sufficient. Padding the short address (12 or 16 bits) to generate the IID of a routable IPv6 address in the public network may be vulnerable to deal with address scans. Thus, as suggested in Section 4.1, a hash function can be used to generate a 64-bit IID. When the version number of the PLC network is changed, the IPv6 addresses can be changed as well. Other schemes such as limited lease period in DHCPv6 [RFC8415], Cryptographically Generated Addresses (CGAs) [RFC3972], Temporary Address Extensions [RFC8981], Hash-Based Addresses (HBAs) [RFC5535], or semantically opaque addresses [RFC7217] **SHOULD** be used to enhance the IID privacy.

9. References

9.1. Normative References

[IEEE_1901.1] IEEE, "IEEE Standard for Medium Frequency (less than 12 MHz) Power Line Communications for Smart Grid Applications", DOI 10.1109/IEEESTD.2018.8360785, IEEE Std 1901.1, May 2018, <https://ieeexplore.ieee.org/document/8360785>.

[IEEE_1901.2] IEEE, "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications", DOI 10.1109/IEEESTD.2013.6679210, IEEE Std 1901.2, December 2013, <https://ieeexplore.ieee.org/document/6679210>.

[ITU-T_G.9903] ITU-T, "Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks", ITU-T Recommendation G.9903, August 2017, <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>.

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

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

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

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

[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>.

[RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <https://www.rfc-editor.org/info/rfc7136>.

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

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

9.2. Informative References

[AODV-RPL] Perkins, C. E., Anand, S.V.R., Anamalamudi, S., and B. Liu, "Supporting Asymmetric Links in Low Power Networks: AODV-RPL", Work in Progress, Internet-Draft, draft-ietf-roll-aodv-rpl-15, 30 September 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-roll-aodv-rpl-15>.

[EUI-64] IEEE Standards Association, "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)", August 2017, <https://standards.ieee.org/wp-content/uploads/import/documents/tutorials/eui.pdf>.

[IEEE_1901.2a] IEEE, "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications - Amendment 1", DOI 10.1109/IEEESTD.2013.6679210, IEEE Std 1901.2a, October 2015, <https://ieeexplore.ieee.org/document/7286946>.

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

[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>.

[RFC7973] Droms, R. and P. Duffy, "Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation", RFC 7973, DOI 10.17487/RFC7973, November 2016, <https://www.rfc-editor.org/info/rfc7973>.

[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>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RFC9010] Thubert, P., Ed. and M. Richardson, "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves", RFC 9010, DOI 10.17487/RFC9010, April 2021, <https://www.rfc-editor.org/info/rfc9010>.

[RFC9031] Vučinić, M., Ed., Simon, J., Pister, K., and M. Richardson, "Constrained Join Protocol (CoJP) for 6TiSCH", RFC 9031, DOI 10.17487/RFC9031, May 2021, <https://www.rfc-editor.org/info/rfc9031>.

[RFC9140] Aura, T., Sethi, M., and A. Peltonen, "Nimble Out-of-Band Authentication for EAP (EAP-NOOB)", RFC 9140, DOI 10.17487/RFC9140, December 2021, <https://www.rfc-editor.org/info/rfc9140>.

[SCENA] Cano, C., Pittolo, A., Malone, D., Lampe, L., Tonello, A., and A. Dabak, "State of the Art in Power Line Communications: From the Applications to the Medium", IEEE Journal on Selected Areas in Communications, Volume 34, Issue 7, DOI 10.1109/JSAC.2016.2566018, July 2016, <https://ieeexplore.ieee.org/document/7467440>.

[ZEROTOUCH] Richardson, M., "6tisch Zero-Touch Secure Join protocol", Work in Progress, Internet-Draft, draft-ietf-6tisch-dtsecurity-zerotouch-join-04, 8 July 2019, <https://datatracker.ietf.org/doc/html/draft-ietf-6tisch-dtsecurity-zerotouch-join-04>.

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 authors thank Scott Mansfield, Ralph Droms, and Pat Kinney for their guidance in the liaison process. The authors wish to thank Stefano Galli, Thierry Lys, Yizhou Li, Yuefeng Wu, and Michael Richardson for their valuable comments and contributions. The authors wish to thank Carles Gomez for shepherding this document. The authors also thank Paolo Volpato for delivering the presentation at IETF 113. Sincere acknowledgements to the valuable comments from the following reviewers: Dave Thaler, Dan Romascanu, Murray Kucherawy, Benjamin Kaduk, Alvaro Retana, Éric Vyncke, Meral Shirazipour, Roman Danyliw, and Lars Eggert.

Authors' Addresses

Jianqiang Hou
Huawei Technologies
101 Software Avenue,
Nanjing
210012
China
Email: houjianqiang@huawei.com

Bing Liu
Huawei Technologies
Haidian District
No. 156 Beiqing Rd.
Beijing
100095
China
Email: remy.liubing@huawei.com

Yong-Geun Hong
Daejeon University
Dong-gu
62 Daehak-ro
Daejeon
34520
Republic of Korea
Email: yonggeun.hong@gmail.com

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