

Transmission of IPv6 Packets over PLC Networks

draft-ietf-6lo-plc-04

Jianqiang Hou (Huawei)

Bing Liu (Huawei)

Yong-Geun Hong (ETRI)

Xiaojun Tang (State Grid EPRI)

Charles Perkins

IETF 108 – July 2020

Comments received during the WGLC

- Many thanks to Yizhou Li and Michael Richardson
- From Yizhou Li
 - Comment: Reference link of [IEEE_1901.1] seems not link to a downloadable file. By a simple search, I found out that standard document is available at <https://ieeexplore.ieee.org/document/8360785>. So authors may want to change it to a more specific link.
 - Modification: Reference Updated

Comments received during the WGLC

- From Michael Richardson
 - 8 editorial comments & 4 technical comments.
 - Technical Comment #1
 - Original text: 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.
 - Comment: Add "Short addresses can be assigned during the onboarding process, such as by using CoJP [I.D-ietf-6tisch-minimal-security]"
 - Modification: Short addresses can be assigned during the onboarding process, by the PANC or the JRC in CoJP [I.D-ietf-6tisch-minimal-security].

Comments received during the WGLC

- From Michael Richardson (cont.)
 - Technical Comment #2
 - Comment: You will get pushback by using RFC4291 on privacy issues. I would change that. Implementations should look at RFC8064 as well.
 - Modification: For privacy reasons, the IID derived by the MAC address SHOULD only be used for link-local address configuration. A PLC host SHOULD use the IID derived by the link-layer short address to configure the IPv6 address used for communication with the public network; otherwise, the host's MAC address is exposed. Implementations should look at [RFC8064] as well, in order to generate a stable IPv6 address using an opaque IID.

Comments received during the WGLC

- From Michael Richardson (cont.)
 - Technical Comment #3
 - Original text: If the PLC network uses route-over mesh, the IPv6 prefix MAY be disseminated by the layer 3 routing protocol, such as RPL which includes the prefix in the DIO message. In this case, the prefix information option (PIO) MUST NOT be included in the Router Advertisement.
 - Comment: That isn't necessarily the case. The rpl-unaware-leaves document says more, and probably should be referenced instead.
 - Modification: As per [I-D.ietf-roll-unaware-leaves], it is possible to have PLC devices configured as RPL-unaware-leaves, which don't not participate to RPL at all, along with RPL-aware PLC devices. In this case, the prefix dissemination SHOULD use the RS/RA messages.

Comments received during the WGLC

- From Michael Richardson (cont.)
 - Technical Comment #4: the onboarding process in security considerations
 - Original text: The security can be enhanced by using DTLS to authenticate a PLC device when it enrolls itself. If the PLC device is not direct neighbor to the PANC, where the authenticate is conducted, another PLC device which has joined the network can act as a proxy to help exchange the authenticate messages. The key used for encryption can also be negotiated via DTLS.
 - Comment: "Just use DTLS" doesn't really work (should give more details on the authentication process)
 - Modification: Mutual authentication of network and 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.

Next Steps

- Pass the WGLC and move forward?