Transmission of IPv6 Packets over PLC Networks

draft-ietf-6lo-plc-05

Jianqiang Hou (Huawei)
Bing Liu (Huawei)
Yong-Geun Hong (ETRI)
Xiaojun Tang (State Grid EPRI)
Charles Perkins (Lupin Lodge)

IETF 110, March 2021

secdir last call review by Robert Sparks (1)

1. The document has content that is not needed for its purpose. Section 5 in particular might be useful in an informational RFC, but is has no impact on someone implementing what this document is trying to standardize.

[Remy] Yes, this section is more like informational. We'll ask the WG if we should remove it or not.

2. The security considerations section speaks primarily to generic considerations for 6lo-like networks. There is no specific discussion of the impact of the **identifier mappings** with the underlying protocols, in particular the constraints that don't allow using the full number of bits of entropy in the identifiers in those underlying protocols. There is only a passing mention of RFC8065.

[Remy] We would like to extend the description as follows: 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. 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.

[Robert] It's better, yes, but I hope people with more expertise and experience with the recommendations than me look closely at it.

secdir last call review by Robert Sparks (2)

3. Implementors are advised to "look at" RFC8064 when considering **building stable addresses**, but this document specifies doing things that RFC8604 recommends against (see the use of RFC2464, for example). More discussion seems warranted.

[Remy] In the same paragraph we reference RFC8604, we limit the usage of MAC generated IID as per RFC2464 in link-local address configuration.

[Robert]I think RFC8064 recommends NOT to do the things in 2464 that you are saying to do. I could be wrong. But having clearer text noting how what you are requiring avoids the issues 8064 brings up would help. Again, I hope people with more expertise than me look closely here.

[Remy] The problem has been solved in RFC8065 (designed in 6lo), when short addresses (the 16 or 12 bits link layer address) 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. We will update the draft to change the reference to RFC8064 into the reference to RFC8065, and specify the solution in section 4.1 instead of the security considerations.

4. There is a short mention of the possibility of acquiring a network encryption key during onboarding but there's no discussion about what that means for these specific layer-2 protocols.

[Remy] The acquirement of layer-2 encryption key is specified in the IEEE and ITU-T standards and not related to the authentication process in the same paragraph. Thus this phrase is redundant, and we prefer to remove this phrase.

tsv-art last call review by Joseph Touch

1. Secs 3.3 and 4.6 refers to underlying frag/reassembly per RFC4944. First, these sections seem redundant; normative requirements should appear in only one section if both are retained.

[Remy]Thanks for indicating this redundancy. We will remove the reference of RFC4944 in the section 3.3.

2. More notably, the use of a **16-bit tag** in that spec is already known to be problematic for IPv4 fragmentation and could cause problems here as well, e.g., per **RFC4963**. This issue should be addressed, notably if there is a reason why a 16-bit tag is considered sufficient for this use it should be stated or some other shim layer should be proposed with a more robust tag (e.g., 32 bits).

[Remy] I think this question has already been discussed when RFC4944 was defined. The situation shown in RFC 4963 "a host sending 1500-byte packets with a 30-second maximum packet lifetime could send at only about 26 Mbps before exceeding 65535 packets per packet lifetime" cannot be reached by the constrained PLC networks discussed in this draft. Because the constrained PLC networks are used for metering and other IOT use cases, in which the packet is not that big, and the data rate is much lower, when compared to the "high data rates networks" discussed in RFC4963.

[Joseph] Regarding fragmentation, the explanation below is fine, but IMO should appear in the doc. It would be important to note that this *could* be a limitation for future PLC, even if it isn’t now (e.g., if data rate capabilities increase).

opsdir last call review by Dan Romascanu

[Dan] I have however one concern that I would suggest the OPS AD to clarify before approving this document. There is no mention in the document of the **operational and manageability aspects**. How will these networks be managed, monitored, troubleshooted? Which existing OAM protocols and procedures apply and will extensions be needed? Are there / will there be any new new interface types ("ifType" values) required as per RFC 8892? Maybe other documents exist in the IEEE or ITU-T that document these aspects - if so it would be useful to reference them. If other documents are in planning in the IETF on this respect - please clarify.

[Remy]That's a very good question. The constrained PLC networks are not managed in the same way as the enterprise network or carrier network. The constrained PLC networks as the other IoT networks, are designed to be **self-organized and self-managed**. The software or firmware is flushed into the devices before deployment by the vendor or operator. And during the deployment process, no extra configuration is needed to get the device connected to each other. Once a device becomes offline, it will go back to the bootstrapping stage and tries to rejoin the network. The onboard 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.

[Dan] This makes sense to me. It would be good to catch this in a short section or subsection of the document ('Operations and Manageability Considerations' is a possible title).