Transmission of IPv6 Packets over PLC Networks

draft-ietf-6lo-plc-10

Jianqiang Hou (Huawei)

Bing Liu (Huawei)

Yong-Geun Hong (Daejeon University)

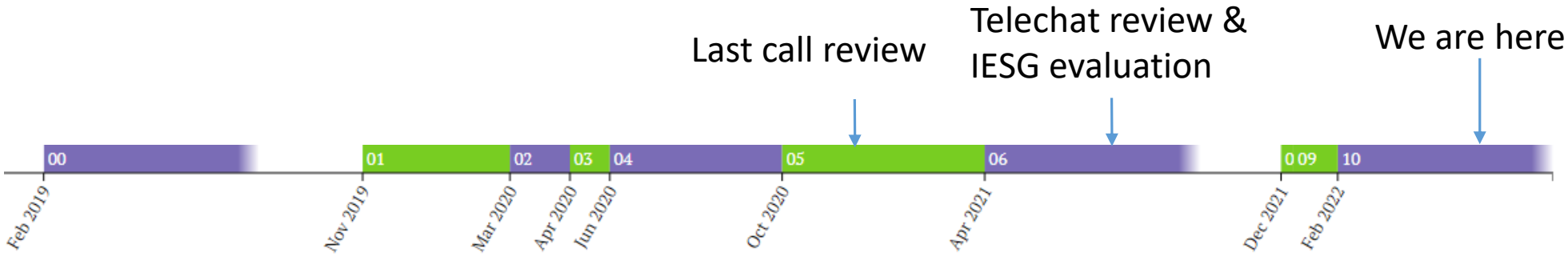
Xiaojun Tang (State Grid EPRI)

Charles Perkins (Lupin Lodge)

Presented by **Paolo Volpato** (Huawei)

IETF 113 – Vienna, March 2022

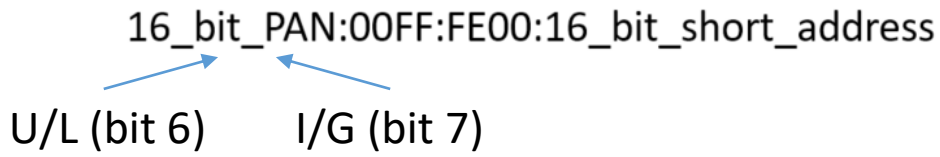
Status of the draft



- Sincere acknowledgements to reviewers of Last Call review, Telechat review and IESG evaluation
- Under IESG evaluation since Aug. 2021, received “Discuss” from
  - Éric Vyncke (changed to “No objection” since version 09)
  - Roman Danyliw (updated the Discuss after reviewing version 09. Revision completed in version 10)
  - Benjamin Kaduk (not updated the Discuss on version 06 yet)

Update 1: U/L & I/G bits semantics

- Benjamin's Discuss
  - Can we briefly discuss the apparent requirement for the PANID/NID to have a couple bits set to zero (the ones that would be U/L and Individual/Group in the resulting IID)? It seems like (but is not entirely clear to me) this is **a new requirement on the layer-2 behavior that is being imposed by the IPv6 adaptation layer**, and in particular that this is setting up a scenario where certain existing layer-2 deployments would be unable to utilize the IPv6 adaptation layer, which would be a very surprising behavior for an IETF Proposed Standard.
- The 64-bit IID generated by L2 short address



- Version 06: Constraints were too strong
  - 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.
- Version 10: Let the network operator decide the semantics
  - As investigated in [**RFC7136**], besides [RFC4291], some other IID generation methods defined in IETF do not imply any semantics for the "Universal/Local" (U/L) bit (bit 6) and the Individual/Group bit (bit 7), so that **these two bits are not reliable indicators for their original meanings**. Thus when using an IID derived by a short address, **the operators of the PLC network can choose to comply with original meaning of these two bits or not**. If so, since the IID derived from the short address is not global, these two bits 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. If not, 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.

Update 2: IID entropy

- Dave ’ s comment in the last call review
  - RFC 8065 section 4 provides a checklist of what adaptation layer documents like this need to address. I'd recommend addressing each point separately in the Security Considerations section, so it's clear that the draft addresses the whole checklist. For example, there's nothing in the document that mentions what **the typical link lifetime** is (years maybe?) As another 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.
- Revision in the draft
  - [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. And an effective way to deal with these threats is to have **enough entropy in the IID comparing to the link lifetime**. Consider **a PLC network with 1024 devices and its 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 suggest in the section 4.1, a **hash function can be used to generate a 64 bits IID**. **When the version number of the PLC network is changed, the IPv6 addresses can be changed as well**.

Update 3: Security considerations

- Roman's Discuss
  - On 2021-08-10: Wouldn't there also be **the possibility of significant integrity risks given that possible actuators or sensors being controlled**?
  - On 2022-02-07: If I understand the architecture right, there is **a communication mesh formed** (looking at Figure 7). It would seem like there could be a possibility of **a compromised PLC device**. If a uncompromised PLC device passes traffic through it, it could be modified without integrity protection. Figures 5 – 7 seems to present architectures which **connects operational technology to the Internet via the PANC. However, this section doesn't acknowledgement of that risk outright or by citation**.

- Revision in the draft
  - **On-path malicious PLC device could eavesdrop or modify packets sent through it** if appropriate confidentiality and integrity mechanisms are not implemented. … **Additional "end-to-end security services" is a complementary to the network side security mechanisms**, e.g., if a devices is compromised and it has joined in the network, and then it claims itself as the PANC and try to make the rest 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.

Next steps

- Feedback from Roman and Benjamin are expected
- One or two revision before entering the publication queue ?