Abstract

This document defines an extension to 6LoWPAN Neighbor Discovery (ND) [RFC6775] [I-D.ietf-6lo-rfc6775-update] called Address Protected ND (AP-ND); AP-ND protects the owner of an address against address theft and impersonation inside a low-power and lossy network (LLN). Nodes supporting this extension compute a cryptographic Owner Unique Interface ID and associate it with one or more of their Registered Addresses. The Cryptographic ID identifies the owner of the Registered Address and can be used for proof-of-ownership. It is used in 6LoWPAN ND in place of the EUI-64-based unique ID that is associated with the registration. Once an address is registered with a Cryptographic ID, only the owner of that ID can modify the registration information of the Registered Address, and Source Address Validation can be enforced.

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 March 7, 2019.
Table of Contents

1. Introduction ............................................. 3
2. Terminology ............................................. 4
   2.1. BCP 14 ............................................ 4
   2.2. References ........................................ 4
   2.3. 6LoWPAN sub-glossary ............................... 5
   2.4. Crypto-ID .......................................... 6
3. Updating RFC 6775 ....................................... 6
4. New Fields and Options .................................... 6
   4.1. Encoding the Public Key ............................ 7
   4.2. New Crypto-ID ..................................... 7
   4.3. Updated EARO ...................................... 7
   4.4. Crypto-ID Parameters Option ....................... 9
   4.5. Nonce Option ...................................... 10
   4.6. NDP Signature Option .............................. 10
5. Protocol Scope .......................................... 10
6. Protocol Flows .......................................... 11
   6.1. First Exchange with a 6LR ......................... 12
   6.2. Multihop Operation ................................ 13
7. Security Considerations ................................... 15
   7.1. Inheriting from RFC 3971 ........................... 15
   7.2. Related to 6LoWPAN ND ............................. 16
   7.3. ROVR Collisions .................................. 16
8. IANA considerations ...................................... 17
   8.1. CGA Message Type .................................. 17
   8.2. Crypto-Type Subregistry ........................... 17
9. Acknowledgments .......................................... 17
10. References ............................................. 18
   10.1. Normative References ............................. 18
   10.2. Informative references ........................... 19
Appendix A. Requirements Addressed in this Document ........... 21
Authors’ Addresses .......................................... 21
1. Introduction

"Neighbor Discovery Optimizations for 6LoWPAN networks" [RFC6775] (6LoWPAN ND) adapts the IPv6 ND (NDv6) protocol [RFC4861][RFC4862] (IPv6 ND) for operations over a constrained low-power and lossy network (LLN). In particular, 6LoWPAN ND introduces a unicast host address registration mechanism that reduces the use of multicast messages that are present in the NDv6 protocol. 6LoWPAN ND defines a new Address Registration Option (ARO) that is carried in the unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages exchanged between a 6LoWPAN Node (6LN) and a 6LoWPAN Router (6LR). It also defines the Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages between the 6LR and the 6LoWPAN Border Router (6LBR). In LLN networks, the 6LBR is the central repository of all the registered addresses in its domain.

The registration mechanism in 6LoWPAN ND [RFC6775] prevents the use of an address if that address is already registered in the subnet (first come first serve). In order to validate address ownership, the registration mechanism enables the 6LR and 6LBR to validate the association between a registered address and a Registration Ownership Verifier (ROVR). 6LoWPAN ND specifies that the ROVR is derived from the MAC address of the device (using the 64-bit Extended Unique Identifier EUI-64 address format specified by IEEE), which can be spoofed. Therefore, any node connected to the subnet and aware of a registered-address-to-ROVR mapping could effectively fake the ROVR, steal the address and redirect traffic for that address towards a different 6LN. The "Registration Extensions for 6LoWPAN Neighbor Discovery" [I-D.ietf-6lo-rfc6775-update] defines an Extended ARO (EARO) option that allows to transport alternate forms of ROVRs, and is a prerequisite for this specification.

According to this specification, a 6LN generates a cryptographic ID (Crypto-ID) and places it in the ROVR field in the registration of one (or more) of its addresses with the 6LR(s) that the 6LN uses as default router(s). Proof of ownership of the cryptographic ID (Crypto-ID) is passed with the first registration exchange to a new 6LR, and enforced at the 6LR. The 6LR validates ownership of the cryptographic ID before it can create a registration, or a change the information, that is the Link-Layer Address and associated parameters, in an existing registration state.

The protected address registration protocol proposed in this document enables Source Address Validation (SAVI) [RFC7039], which ensures that only the owner uses a registered address in the source address field in IPv6 packets. Consequently, a 6LN that sources a packet has to use a 6LR to which the source address of the packet is registered to forward the packet. The 6LR maintains state information for the
registered addressed, including the MAC address, and a link-layer cryptographic key associated with the 6LN. In SAVI-enforcement mode, the 6LR allows only packets from a connected Host if the connected Host owns the registration of the source address of the packet.

The 6lo adaptation layer framework ([RFC4944], [RFC6282]) specifies that a device forms its IPv6 addresses based on Layer-2 address, so as to enable a better compression. This is incompatible with "Secure Neighbor Discovery (SeND)" [RFC3971] and "Cryptographically Generated Addresses (CGAs)" [RFC3972], which derive the Interface ID (IID) in the IPv6 addresses from key material. "Privacy Considerations for IPv6 Address Generation Mechanisms" [RFC7721] places additional recommendations on the way addresses should be formed and renewed.

This document specifies that a device may form and register addresses at will, without a constraint on the way the address is formed or the number of addresses that are registered in parallel. Multiple addresses with a single ROVR, which only needs to be sent once to a given 6LR for multiple addresses and registration updates.

2. Terminology

2.1. BCP 14

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.

2.2. References

In this document, readers will encounter terms and concepts that are discussed in the following documents:

- "SEcure Neighbor Discovery (SEND)" [RFC3971],
- "Cryptographically Generated Addresses (CGA)" [RFC3972],
- "Neighbor Discovery for IP version 6" [RFC4861],
- "IPv6 Stateless Address Autoconfiguration" [RFC4862],
- "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing" [RFC6606],
- "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919],

Thubert, et al. Expires March 7, 2019
2.3. 6LoWPAN sub-glossary

This document often uses the following acronyms:

6BBR: 6LoWPAN Backbone Router (proxy for the registration)
[ draft-ietf-6lo-backbone-router ]

6LBR: 6LoWPAN Border Router

6LN: 6LoWPAN Node

6LR: 6LoWPAN Router (relay to the registration process)

CIPO: Crypto-ID Parameters Option

(E)ARO: (Extended) Address Registration Option

DAD: Duplicate Address Detection

LLN: Low-Power and Lossy Network (a typical IoT network)

NA: Neighbor Advertisement

ND: Neighbor Discovery

NDP: Neighbor Discovery Protocol

NDPSO: NDP Signature Option

NS: Neighbor Solicitation

ROVR: Registration Ownership Verifier (pronounced rover)

RA: Router Advertisement

RS: Router Solicitation
2.4. Crypto-ID

This document defines a new Crypto-ID as an identifier of variable size which is 64 to 256 bits long. It is generated using cryptographic means explained later in this document Section 4.2. "Elliptic Curves for Security" [RFC7748] and "Edwards-Curve Digital Signature Algorithm (EdDSA)" [RFC8032] provides information on Elliptic Curve Cryptography (ECC) and a (twisted) Edwards curve, Ed25519, which can be used with this specification. "Alternative Elliptic Curve Representations" [I-D.struik-lwig-curve-representations] provides additional information on how to represent Montgomery curves and (twisted) Edwards curves as curves in short-Weierstrass form and illustrates how this can be used to implement elliptic curve computations using existing implementations that already implement, e.g., ECDSA and ECDH using NIST [FIPS-186-4] prime curves.

3. Updating RFC 6775

This specification defines a cryptographic identifier (Crypto-ID) that can be used as a replacement to the MAC address in the ROVR field of the EARO option; the computation of the Crypto-ID is detailed in Section 4.2. A node in possession of the necessary cryptographic material SHOULD use Crypto-ID by default as ROVR in its registration. Whether a ROVR is a Crypto-ID is indicated by a new "C" flag in the NS(EARO) message.

In order to prove its ownership of a Crypto-ID, the registering node needs to supply certain parameters including a nonce and a signature that will prove that the node has the private key corresponding to the public key used to build the Crypto-ID. This specification adds the capability to carry new options in the NS(EARO) and the NA(EARO). The NS(EARO) carries a variation of the CGA Option (Section 4.4), a Nonce option and a variation of the RSA Signature option (Section 4.6) in the NS(EARO). The NA(EARO) carries a Nonce option.

4. New Fields and Options

In order to avoid the need for new ND option types, this specification reuses / extends options defined in SEND [RFC3971] and 6LoWPAN ND [RFC6775] [I-D.ietf-6lo-rfc6775-update]. This applies in particular to the CGA option and the RSA Signature Option. This specification provides aliases for the specific variations of those options as used in AP-ND. The presence of the EARO option in the NS/
NA messages indicates that the crypto options are to be processed as specified in this document, not as a SEND message.

4.1. Encoding the Public Key

A 6LN provides its public key in an NS message. The public key could be in uncompressed form or in compressed form where the first octet of the OCTET STRING is 0x04 and 0x02 or 0x03, respectively. Point compression can further reduce the key size by about 32 octets.

4.2. New Crypto-ID

Each 6LN using a Crypto-ID for registration MUST have a public/private key pair.

The Crypto-ID is computed as follows:

1. An 8-bit modifier is selected, enabling a device to form multiple Crypto-IDs with a single key pair. This is useful for privacy reasons in order to avoid the correlation of addresses based on their Crypto-ID;

2. the modifier value and the DER-encoded public key (Section 4.1) are concatenated from left to right;

3. The digital signature is constructed by using the 6LN’s private key over its EUI-64 (MAC) address. The signature value is computed using the ECDSA signature algorithm and the hash function used is SHA-256 [RFC6234].

4. the leftmost bits of the resulting hash are used as the Crypto-ID, up to the size of the ROVR field.

4.3. Updated EARO

This specification updates the EARO option as follows:
Figure 1: Enhanced Address Registration Option

Type: 33
Length: 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 bytes.
Status: 8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages.
Opaque: Defined in [I-D.ietf-6lo-rfc6775-update].
Rsvd (Reserved): This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
C: This "C" flag is set to indicate that the Owner Unique ID field contains a Crypto-ID and that the 6LN MAY be challenged for ownership as specified in this document.
I: Defined in [I-D.ietf-6lo-rfc6775-update].
R: Defined in [I-D.ietf-6lo-rfc6775-update].
T and TID: Defined in [I-D.ietf-6lo-rfc6775-update].
Registration Ownership Verifier (ROVR): When the "C" flag is set, this field contains a Crypto-ID.

This specification uses Status values "Validation Requested" and "Validation Failed", which are defined in 6LoWPAN ND [I-D.ietf-6lo-rfc6775-update]. No other new Status values is defined.
4.4. Crypto-ID Parameters Option

This specification defines the Crypto-ID Parameters Option (CIPO), as a variation of the CGA Option that carries the parameters used to form a Crypto-ID. In order to provide cryptographic agility [RFC7696], AP-ND supports two possible signature algorithms, indicated by a Crypto-Type field. Elliptic Curve Cryptography (ECC) is used to calculate the Crypto-ID. NIST P-256 [FIPS186-4] MUST be supported by all implementations. The Edwards-Curve Digital Signature Algorithm (EdDSA) curve Ed25519ph (pre-hashing) [RFC8032] MAY be supported as an alternate.

```
+-----------------+-----------------+-----------------+-----------------+
<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Pad Length</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto-Type</td>
<td>Modifier</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>. Public Key (variable length) .</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------+-----------------+-----------------+-----------------+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pad Length</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------+-----------------+-----------------+-----------------+</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 2: Crypto-ID Parameters Option

**Type:** 11. This is the same value as the CGA Option, CIPO is a particular case of the CGA option.

**Length:** 8-bit unsigned integer. The length of the option in units of 8 octets.

**Modifier:** 8-bit unsigned integer.

**Pad Length:** 8-bit unsigned integer. The length of the Padding field.
Crypto-Type: The type of cryptographic algorithm used in calculation Crypto-ID. A value of 0 indicates NIST P-256, with SHA-256 as the hash algorithm. A value of 1 is assigned for Ed25519ph, with SHA-256 as the hash algorithm.

Public Key: DER-Encoded Public Key.

Padding: A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

4.5. Nonce Option

This document reuses the Nonce Option defined in section 5.3.2. of SEND [RFC3971] without a change.

4.6. NDP Signature Option

This document reuses the RSA Signature Option (RSAO) defined in section 5.2. of SEND [RFC3971]. Admittedly, the name is ill-chosen since the option is extended for non-RSA Signatures and this specification defines an alias to avoid the confusion.

The description of the operation on the option detailed in section 5.2. of SEND [RFC3971] apply, but for the following changes:

- The 128-bit CGA Message Type tag [RFC3972] for AP-ND is 0x8701 55c8 0cca dd32 6ab7 e415 f148 84d0. (The tag value has been generated by the editor of this specification on random.org).

- The signature is computed using the hash algorithm and the digital signature indicated in the Crypto-Type field of the CIPO option using the private key associated with the public key in the CIPO.

- The alias NDP Signature Option (NDPSO) can be used to refer to the RSAO when used as described in this specification.

5. Protocol Scope

The scope of the present work is a 6LoWPAN Low Power Lossy Network (LLN), typically a stub network connected to a larger IP network via a Border Router called a 6LBR per [RFC6775]. A 6LBR has sufficient capability to satisfy the needs of DAD.

The 6LBR maintains registration state for all devices in its attached LLN. Together with the first-hop router (the 6LR), the 6LBR assures uniqueness and grants ownership of an IPv6 address before it can be

used in the LLN. This is in contrast to a traditional network that relies on IPv6 address auto-configuration [RFC4862], where there is no guarantee of ownership from the network, and each IPv6 Neighbor Discovery packet must be individually secured [RFC3971].

![Diagram of Basic Configuration]

Figure 3: Basic Configuration

In a mesh network, the 6LR is directly connected to the host device. This specification mandates that the peer-wise layer-2 security is deployed so that all the packets from a particular host are securely identifiable by the 6LR. The 6LR may be multiple hops away from the 6LBR. Packets are routed between the 6LR and the 6LBR via other 6LRs. This specification mandates that a chain of trust is established so that a packet that was validated by the first 6LR can be safely routed by the next 6LRs to the 6LBR.

6. Protocol Flows

The 6LR/6LBR ensures first-come/first-serve by storing the EARO information including the Crypto-ID associated to the node being registered. The node can claim any address as long as it is the first to make such a claim. After a successful registration, the node becomes the owner of the registered address and the address is bound to the Crypto-ID in the 6LR/6LBR registry.

This specification enables the 6LR to verify the ownership of the binding at any time assuming that the "C" flag is set. The verification prevents other nodes from stealing the address and trying to attract traffic for that address or use it as their source address.

A node may use multiple IPv6 addresses at the same time. The node may use a same Crypto-ID, or multiple crypto-IDs derived from a same key pair, to protect multiple IPv6 addresses. The separation of the address and the cryptographic material avoids the constrained device
to compute multiple keys for multiple addresses. The registration process allows the node to use the same Crypto-ID for all of its addresses.

6.1. First Exchange with a 6LR

A 6LN registers to a 6LR that is one hop away from it with the "C" flag set in the EARO, indicating that the ROVR field contains a Crypto-ID. The on-link (local) protocol interactions are shown in Figure 4. If the 6LR does not have a state with the 6LN that is consistent with the NS(EARO), then it replies with a challenge NA (EARO, status=Validation Requested) that contains a Nonce Option. The Nonce option MUST contain a Nonce value that was never used with this device.

The 6LN replies to the challenge with an NS(EARO) that includes the echoed Nonce option, the CIPO Section 4.4, and the NDPSO with the signature. The information associated to a crypto-ID stored by the 6LR on the first NS exchange where it appears. The 6LR SHOULD store the CIPO parameters associated with the crypto-ID so it can be used for more than one address.

```
6LN                                                     6LR
<------------------------- RA ------------------------->
|                                                       | ^
|<-------------------------- NS with EARO (Crypto-ID) ------>|
|                                                       | v
|<- NA with EARO (status=Validation Requested), Nonce ---|
|---------------- NS with EARO, CIPO, Nonce and NDPSO ----->|
|<--------------------- NA with EARO ----------------------|
|                                                       |
|...                                                       |
|-------- NS with EARO (Crypto-ID) -------->
|<--------------------- NA with EARO ----------------------|
|                                                       |
|...                                                       |
|-------- NS with EARO (Crypto-ID) -------->
|<--------------------- NA with EARO ----------------------|

Figure 4: On-link Protocol Operation
```
The steps for the registration to the 6LR are as follows:

- Upon the first exchange with a 6LR, a 6LN may be challenged to prove ownership of the Crypto-ID. The proof is not needed again in later registrations for that address, or when registering other addresses with the same ROVR. When a 6LR receives a NS(EARO) registration with a new Crypto-ID as a ROVR, it SHOULD challenge by responding with a NA(EARO) with a status of "Validation Requested". This process of validation MAY be skipped in networks where there is no mobility.

- The challenge is triggered when the registration for a Source Link-Layer Address is not verifiable either at the 6LR or the 6LBR. In the latter case, the 6LBR returns a status of "Validation Requested" in the DAR/DAC exchange, which is echoed by the 6LR in the NA (EARO) back to the registering node. The challenge MUST NOT alter a valid registration in the 6LR or the 6LBR.

- Upon receiving a NA(EARO) with a status of "Validation Requested", the registering node SHOULD retry its registration with a Crypto-ID Parameters Option (CIPO) (Section 4.4) that contains all the necessary material for building the Crypto-ID, the Nonce and the NDP signature (Section 4.6) options that prove its ownership of the Crypto-ID.

- In order to validate the ownership, the 6LR performs the same steps as the 6LN and rebuilds the Crypto-ID based on the parameters in the CIPO. If the result is different then the validation fails. Else, the 6LR checks the signature in the NDPSO using the public key in the CIPO. If it is correct then the validation passes, else it fails.

- If the 6LR fails to validate the signed NS(EARO), it responds with a status of "Validation Failed". After receiving a NA(EARO) with a status of "Validation Failed", the registering node SHOULD try an alternate Crypto-ID. The registering node MUST NOT use the same Crypto-ID for subsequent registration attempts.

6.2. Multihop Operation

In a multihop 6LoWPAN, the registration with Crypto-ID is propagated to 6LBR as described in this section. If the 6LR and the 6LBR maintain a security association, then there is no need to propagate the proof of ownership to the 6LBR.

A new device that joins the network auto-configures an address and performs an initial registration to a neighboring 6LR with an NS
message that carries an Address Registration Option (EARO) [RFC6775].
The 6LR validates the address with an 6LBR using a DAR/DAC exchange,
and the 6LR confirms (or denies) the address ownership with an NA
message that also carries an Address Registration Option.

Figure 5 illustrates a registration flow all the way to a 6LowPAN
Backbone Router (6BBR).

In a multihop 6LoWPAN, a 6LBR sends RAs with prefixes downstream and
the 6LR receives and relays them to the nodes. 6LR and 6LBR
communicate using ICMPv6 Duplicate Address Request (DAR) and
Duplicate Address Confirmation (DAC) messages. The DAR and DAC use
the same message format as NS and NA, but have different ICMPv6 type
values.

In AP-ND we extend DAR/DAC messages to carry cryptographically
generated ROVR. In a multihop 6LoWPAN, the node exchanges the
messages shown in Figure 5. The 6LBR must identify who owns an
address (EUI-64) to defend it, if there is an attacker on another
6LR.
7. Security Considerations

7.1. Inheriting from RFC 3971

Observations regarding the following threats to the local network in
[RFC3971] also apply to this specification.

Neighbor Solicitation/Advertisement Spoofing

Threats in section 9.2.1 of RFC3971 apply. AP-ND counters the
threats on NS(EARO) messages by requiring that the NDP Signature
and CIPO options be present in these solicitations.

Neighbor Unreachability Detection Failure

With RFC6775, a NUD can still be used by the endpoint to assess
the liveness of a device. The NUD request may be protected by
SEND in which case the provision in section 9.2 of RFC 3972
applies. The response to the NUD may be proxied by a backbone
router only if it has a fresh registration state for it. For a
registration being protected by this specification, the proxied
NUD response provides truthful information on the original owner
of the address but it cannot be proven using SEND. If the NUD
response is not proxied, the 6LR will pass the lookup to the end
device which will respond with a traditional NA. If the 6LR does
not have a registration associated for the device, it can issue a
NA with EARO (status=Validation Requested) upon the NA from the
device, which will trigger a NS that will recreate and revalidate
the ND registration.

Duplicate Address Detection DoS Attack

Inside the LLN, Duplicate Addresses are sorted out using the ROVR,
which differentiates it from a movement. DAD coming from the
backbone are not forwarded over the LLN, which provides some
protection against DoS attacks inside the resource-constrained
part of the network. Over the backbone, the EARO option is
present in NS/NA messages. This protects against misinterpreting
a movement for a duplication, and enables the backbone routers to
determine which one has the freshest registration and is thus the
best candidate to validate the registration for the device
attached to it. But this specification does not guarantee that
the backbone router claiming an address over the backbone is not
an attacker.

Router Solicitation and Advertisement Attacks
This specification does not change the protection of RS and RA which can still be protected by SEND.

Replay Attacks

A Nonce given by the 6LR in the NA with EARO (status=Validation Requested) and echoed in the signed NS guarantees against replay attacks of the NS(EARO). The NA(EARO) is not protected and can be forged by a rogue node that is not the 6LR in order to force the 6LN to rebuild a NS(EARO) with the proof of ownership, but that rogue node must have access to the L2 radio network next to the 6LN to perform the attack.

Neighbor Discovery DoS Attack

A rogue node that managed to access the L2 network may form many addresses and register them using AP-ND. The perimeter of the attack is all the 6LRs in range of the attacker. The 6LR must protect itself against overflows and reject excessive registration with a status 2 "Neighbor Cache Full". This effectively blocks another (honest) 6LN from registering to the same 6LR, but the 6LN may register to other 6LRs that are in its range but not in that of the rogue.

7.2. Related to 6LoWPAN ND

The threats discussed in 6LoWPAN ND [RFC6775] and its update [I-D.ietf-6lo-rfc6775-update] also apply here. Compared with SeND, this specification saves about 1Kbyte in every NS/NA message. Also, this specification separates the cryptographic identifier from the registered IPv6 address so that a node can have more than one IPv6 address protected by the same cryptographic identifier. SeND forces the IPv6 address to be cryptographic since it integrates the CGA as the IID in the IPv6 address. This specification frees the device to form its addresses in any fashion, thereby enabling not only 6LoWPAN compression which derives IPv6 addresses from Layer-2 addresses but also privacy addresses.

7.3. ROVR Collisions

A collision of Registration Ownership Verifiers (ROVR) (i.e., the Crypto-ID in this specification) is possible, but it is a rare event. The formula for calculating the probability of a collision is \(1 - e^{-k^2/(2n)}\) where \(n\) is the maximum population size (\(2^{64}\) here, 1.84E19) and \(K\) is the actual population (number of nodes). If the Crypto-ID is 64-bits, the chance of a collision is 0.01% when the network contains 66 million nodes. Moreover, the collision is only relevant when this happens within one stub network (6LBR).
case of such a collision, an attacker may be able to claim the registered address of another legitimate node. However for this to happen, the attacker would also need to know the address which was registered by the legitimate node. This registered address is never broadcasted on the network and therefore providing an additional 64-bits that an attacker must correctly guess. To prevent address disclosure, it is RECOMMENDED that nodes derive the address being registered independently of the ROVR.

8. IANA considerations

8.1. CGA Message Type

This document defines a new 128-bit value under the CGA Message Type [RFC3972] namespace, 0x8701 55c8 0cca dd32 6ab7 e415 f148 84d0.

8.2. Crypto-Type Subregistry

IANA is requested to create a new subregistry "Crypto-Type Subregistry" in the "Internet Control Message Protocol version 6 (ICMPv6) Parameters". The registry is indexed by an integer 0..255 and contains a Signature Algorithm and a Hash Function as shown in Table 1. The following Crypto-Type values are defined in this document:

<table>
<thead>
<tr>
<th>Crypto-Type value</th>
<th>Signature Algorithm</th>
<th>Hash Function</th>
<th>Defining Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NIST P-256 [FIPS186-4]</td>
<td>SHA-256 [RFC6234]</td>
<td>RFC THIS</td>
</tr>
<tr>
<td>1</td>
<td>Ed25519ph [RFC8032]</td>
<td>SHA-256 [RFC6234]</td>
<td>RFC THIS</td>
</tr>
</tbody>
</table>

Table 1: Crypto-TYPES

Assignment of new values for new Crypto-Type MUST be done through IANA with "Specification Required" and "IESG Approval" as defined in [RFC8126].

9. Acknowledgments

Many thanks to Charlie Perkins for his in-depth review and constructive suggestions. We are also especially grateful to Rene Struijk and Robert Moskowitz for their comments that lead to many improvements to this document, in particular WRT ECC computation and references.
10. References

10.1. Normative References


Internet-Draft        Address Protection ND for LLN       September 2018


10.2. Informative references


Internet-Draft Address Protection ND for LLN September 2018


Appendix A. Requirements Addressed in this Document

In this section we state requirements of a secure neighbor discovery protocol for low-power and lossy networks.

- The protocol MUST be based on the Neighbor Discovery Optimization for Low-power and Lossy Networks protocol defined in [RFC6775]. RFC6775 utilizes optimizations such as host-initiated interactions for sleeping resource-constrained hosts and elimination of multicast address resolution.

- New options to be added to Neighbor Solicitation messages MUST lead to small packet sizes, especially compared with existing protocols such as SEcure Neighbor Discovery (SEND). Smaller packet sizes facilitate low-power transmission by resource-constrained nodes on lossy links.

- The support for this registration mechanism SHOULD be extensible to more LLN links than IEEE 802.15.4 only. Support for at least the LLN links for which a 6lo "IPv6 over foo" specification exists, as well as Low-Power Wi-Fi SHOULD be possible.

- As part of this extension, a mechanism to compute a unique Identifier should be provided with the capability to form a Link Local Address that SHOULD be unique at least within the LLN connected to a 6LBR.

- The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of Unique Interface IDentifier.

- The Neighbour Discovery should specify the formation of a site-local address that follows the security recommendations from [RFC7217].

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis  06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com
Behcet Sarikaya  
Plano, TX  
USA  

Email: sarikaya@ieee.org

Mohit Sethi  
Ericsson  
Hirsalantie  
Jorvas  02420  

Email: mohit@piuha.net
IPv6 Backbone Router
draft-ietf-6lo-backbone-router-07

Abstract

Backbone Routers placed at the wireless edge of a backbone link interconnect multiple wireless links at Layer-3 to form a large MultiLink Subnet, so that the broadcast domain of the backbone does not extend to the wireless links. Wireless nodes register or are proxy-registered to a Backbone Router to establish IPv6 Neighbor Discovery proxy services, and the Backbone Router takes care of the ND operation on behalf of registered nodes and ensures and routes towards the registered addresses over the wireless interface.

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 March 7, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect
1. Introduction

One of the key services provided by IEEE STD. 802.1 [IEEEstd8021] Ethernet Bridging is an efficient and reliable broadcast service, and multiple applications and protocols have been built that heavily depend on that feature for their core operation. Unfortunately, a wide range of wireless networks do not provide economical broadcast capabilities of Ethernet Bridging; protocols designed for bridged networks that rely on broadcast often exhibit disappointing behaviours when applied unmodified to a wireless medium.

Wi-Fi [IEEEstd80211] Access Points (APs) deployed in an Extended Service Set (ESS) act as bridges. However, in order to ensure a solid connectivity to the devices and protect the medium against harmful broadcasts, they refrain from relying on broadcast-intensive protocols such as Transparent Bridging on the wireless side. Instead, an association process is used to register proactively the MAC addresses of the wireless device (STA) to the AP. Then, the APs proxy the bridging operation and cancel the broadcasts.
The IPv6 [RFC8200] Neighbor Discovery [RFC4861] [RFC4862] Protocol (NDP) operations are reactive and rely heavily on multicast transmissions to locate an on-link correspondent and ensure address uniqueness. When the Duplicate Address Detection [RFC4862] (DAD) mechanism was designed, it was a natural match with the efficient broadcast operation of Ethernet Bridging. However, since broadcast can be unreliable over wireless media, DAD often fails to discover duplications [I-D.yourtchenko-6man-dad-issues]. DAD usually appears to work on wireless media, not because address duplication is detected and solved as designed, but because the use of 64-bit Interface IDs makes duplication into a very rare event.

IPv6 multicast messages are usually broadcast over the wireless medium. They are processed by most if not all wireless nodes over the ESS fabric even when very few if any of the nodes are subscribed to the multicast address. Consequently a simple Neighbor Solicitation (NS) lookup message [RFC4861], that is supposedly targeted to a very small group of nodes, can consume the whole wireless bandwidth across the fabric [I-D.vyncke-6man-mcast-not-efficient]. The reactive IPv6 ND operation leads to undesirable power consumption in battery-operated devices.

The inefficiencies of using radio broadcasts to support IPv6 NDP suggest restricting broadcast transmissions over the wireless access links. This can be done by splitting the subnet in multiple ones, and in extreme cases providing a /64 per wireless device. Another way is to take over (proxy) the Layer-3 protocols that rely on broadcast operation at the boundary of the wired and wireless domains, emulating the Layer-2 association at Layer-3. Indeed, the IEEE STD. 802.11 [IEEEstd80211] specifications require ARP and ND proxy [RFC4389] functions at the Access Points (APs) but the specification for the ND proxy operations is still missing.

Current devices rely on snooping for detecting association state, which is unsatisfactory in a lossy and mobile conditions. With snooping, a state (e.g. a new IPv6 address) may not be discovered or a change of state (e.g. a movement) may be missed, leading to unreliable connectivity.

WPAN devices (i.e., those implementing IEEE STD. 802.15.4 [IEEEstd802154]) can make use of Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) [RFC6775] which treats the wireless medium as different from Ethernet. RFC 6775 is updated as [I-D.ietf-6lo-rfc6775-update]; the update includes changes that are required by this document.
This specification applies to other wireless links such as Low-Power IEEE STD. 802.11 (Wi-Fi) and IEEE STD. 802.15.1 (Bluetooth) [IEEEstd802151], and extends [RFC6775] to enable proxy operation by the 6BBR. The proxy operation on the BBR eliminates the need for low-power nodes or nodes that are deep in a mesh to respond synchronously when a lookup is performed for their addresses. This provides the function of a Sleep Proxy for ND [I-D.nordmark-6man-dad-approaches].

2. Applicability and Requirements Served

Efficiency aware IPv6 Neighbor Discovery Optimizations [I-D.chakrabarti-nordmark-6man-efficient-nd] suggests that 6LoWPAN ND [RFC6775] can be extended to other types of links beyond IEEE STD. 802.15.4 for which it was defined. The registration technique is beneficial when the Link-Layer technique used to carry IPv6 multicast packets has poor delivery ratio or requires high energy consumption in the end devices, all the more in use cases that involve mobility.

This specification updates and generalizes 6LoWPAN ND to a broader range of Low power and Lossy Networks (LLNs) with support for Duplicate Address Detection (DAD) and address lookup that does not require broadcasts over the LLNs. The term LLN is used loosely in this specification to cover multiple types of WLANs and WPANs, including Low-Power Wi-Fi, BLUETOOTH(R) Low Energy, IEEE STD. 802.11AH and IEEE STD. 802.15.4 wireless meshes, so as to address the requirements listed in Appendix B.3 of [I-D.ietf-6lo-rfc6775-update] "Requirements Related to the Variety of Low-Power Link types".

The scope of this draft is a Backbone that enable the federation of multiple LLNs into a IPv6 MultiLink Subnet. Each LLN in the subnet is anchored at an IPv6 Backbone Router (6BBR). The Backbone Routers interconnect the LLNs and advertise the addresses of the LLN nodes using proxy-ND operations. This specification extends IPv6 ND over the backbone to distinguish address movement from duplication and eliminate stale state in the backbone routers and backbone nodes once a LLN node has roamed. In this way, mobile nodes may roam rapidly from one 6BBR to the next and requirements in Appendix B.1 of [I-D.ietf-6lo-rfc6775-update]"Requirements Related to Mobility" are met.

This specification can be used by any wireless node to associate at Layer-3 with a 6BBR and register its IPv6 addresses to obtain routing services including proxy-ND operations over the backbone, providing a solution to the requirements expressed in Appendix B.4 of [I-D.ietf-6lo-rfc6775-update] "Requirements Related to Proxy Operations".
The Link Layer Address (LLA) that is returned as Target LLA (TLLA) in Neighbor Advertisements (NA) messages by the 6BBR on behalf of the Registered Node over the backbone may be that of the Registering Node. In that case, the 6BBR needs to bridge the unicast packets (Bridging proxy), or that of the 6BBR on the backbone, in which case the 6BBRs needs to route the unicast packets (Routing proxy). In the latter case, the 6BBR maintains the list of correspondents to which it has advertised its own MAC address on behalf of the LLN node. The IPv6 ND operation is minimized as the number of nodes scale up in the LLN. This meets the requirements in Appendix B.6 of [I-D.ietf-6lo-rfc6775-update] "Requirements Related to Scalability", as long as the 6BBRs are dimensioned for the number of registrations that each needs to support.

For the TimeSlotted Channel Hopping (TSCH) mode of [IEEEstd802154], the 6TiSCH architecture [I-D.ietf-6tisch-architecture] describes how a 6LoWPAN ND host could connect to the Internet via a RPL mesh network, but doing so requires additions to the 6LOWPAN ND protocol to support mobility and reachability in a secure and manageable environment. This document details such additions for the 6TiSCH architecture, and serves the requirements listed in Appendix B.2 of [I-D.ietf-6lo-rfc6775-update] "Requirements Related to Routing Protocols".

In the case of Low-Power IEEE STD. 802.11, a 6BBR may be collocated with a standalone AP or a CAPWAP [RFC5415] wireless controller. Then the wireless client (STA) makes use of this specification to register its IPv6 address(es) to the 6BBR over the wireless medium. In the case of a 6TiSCH LLN mesh, the RPL root is collocated with a 6LoWPAN Border Router (6LBR), and either collocated with or connected to the 6BBR over an IPv6 Link. The 6LBR makes use of this specification to register the LLN nodes on their behalf to the 6BBR. In the case of BTLE, the 6BBR is collocated with the router that implements the BTLE central role as discussed in section 2.2 of [RFC7668].

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Readers are expected to be familiar with all the terms and concepts that are discussed in "Neighbor Discovery for IP version 6" [RFC4861], "IPv6 Stateless Address Autoconfiguration" [RFC4862], "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919], Neighbor Discovery Optimization for Low-power and Lossy Networks...
[RFC6775] and "Multi-link Subnet Support in IPv6"
[I-D.ietf-ipv6-multilink-subnets].

Readers would benefit from reading "Multi-Link Subnet Issues"
[RFC4903], "Mobility Support in IPv6" [RFC6275], "Neighbor Discovery
Proxies (ND Proxy)" [RFC4389] and "Optimistic Duplicate Address
Detection" [RFC4429] prior to this specification for a clear
understanding of the art in ND-proxying and binding.

Additionally, this document uses terminology from [RFC7102],
[I-D.ietf-6lo-rfc6775-update] and [I-D.ietf-6tisch-terminology], and
introduces the following terminology:

Sleeping Proxy

A 6BBR acts as a Sleeping Proxy if it answers ND Neighbor
Solicitation over the backbone on behalf of the Registered
Node.

Unicasting Proxy

A Unicasting Proxy forwards NS messages to the Registering
Node, transforming Layer-2 multicast into unicast.

Routing proxy

A routing proxy advertises its own MAC address, as opposed to
that of the node that performs the registration, as the TLLA in
the proxied NAs over the backbone.

Bridging proxy

A Bridging proxy advertises the MAC address of the node that
performs the registration as the TLLA in the proxied NAs over
the backbone. In that case, the MAC address and the mobility
of the node is still visible across the bridged backbone
fabric.

Primary BBR

The BBR that will defend a Registered Address for the purpose
of DAD over the backbone.

Secondary BBR

A BBR other than the Primary BBR to which an address is
registered. A Secondary Router MAY advertise the address over
the backbone and proxy for it.
4. Overview

An LLN node can move freely from an LLN anchored at a Backbone Router to an LLN anchored at another Backbone Router on the same backbone and keep any or all of the IPv6 addresses that it has formed.

```
+-----+     +-----+     +-----+
|     | Gateway (default) Router |
+-----+     +-----+     +-----+
|     |
+-----+     +-----+     +-----+
|     | Backbone Link          |
+-----+     +-----+     +-----+
|     | Backbone router        |
+-----+     +-----+     +-----+
| o o o o o o o o o o o o o o |
| o o o o o o o o o o o o o o |
| o o o o o o o o o o o o o o |
| o o o o o o o o o o o o o o |
| o o o o o o o o o o o o o o |
| o o o o o o o o o o o o o o |
| LLN | LLN | LLN |

Figure 1: Backbone Link and Backbone Routers
```

Each Backbone Router (6BBR) maintains a Binding Table of its Registered Nodes. The Binding Table operates as a distributed database of wireless Nodes whether they reside on the LLNs or on the backbone, and use an extension to the Neighbor Discovery Protocol to exchange that information across the Backbone as with IPv6 ND.

The Extended Address Registration Option (EARO) defined in [I-D.ietf-6lo-rfc6775-update] is used to enable the registration for routing and proxy options in the ND exchanges over the backbone between the 6BBRs to disambiguate duplication from movement.

Address duplication is detected using the ROVR field in the EARO, which is a generalization of the EUI-64 that allows different types of unique IDs beyond the name space derived from the MAC addresses. First-Come First-Serve rules apply, whether the duplication happens between LLN nodes as represented by their respective 6BBRs, or between an LLN node and a node that defends its address over the backbone with IPv6 ND and does not include the EARO.
In case of conflicting registrations to multiple 6BBRs from a same node, a sequence counter called Transaction ID (TID) in the EARO enables 6BBRs to determine the latest registration for that node. Registrations with a same TID are compatible and maintained, but, in case of different TIDs, only the freshest registration is maintained and the stale state is eliminated. The EARO also transports a ‘R’ flag to be used by a 6LN when registering, to indicate that this 6LN is not a router and that it will not handle its own reachability.

With this specification, Backbone Routers perform a ND proxy operation over the Backbone Link on behalf of their Registered Nodes. The registration to the proxy service is done with a NS/NA(EARO) exchange. The EARO with a ‘R’ flag is used in this specification to request the 6BBR to perform this proxy operation. The Backbone Router operation is essentially similar to that of a Mobile IPv6 (MIPv6) [RFC6275] Home Agent. This enables mobility support for LLN nodes that would move outside of the network delimited by the Backbone link attach to a Home Agent from that point on. This also enables collocation of Home Agent functionality within Backbone Router functionality on the same backbone interface of a router. Further specification may extend this be allowing the 6BBR to redistribute host routes in routing protocols that would operate over the backbone, or in MIPv6 or the Locator/ID Separation Protocol (LISP) [RFC6830] to support mobility on behalf of the nodes, etc...

The Optimistic Duplicate Address Detection [RFC4429] (ODAD) specification details how an address can be used before a Duplicate Address Detection (DAD) is complete, and insists that an address that is TENTATIVE should not be associated to a Source Link-Layer Address Option in a Neighbor Solicitation message. This specification makes use of ODAD to create a temporary proxy state in the 6BBR till DAD is completed over the backbone. This way, the specification enables to distribute proxy states across multiple 6BBR and co-exist with IPv6 ND over the backbone.

5. Backbone Router Routing Operations
5.1. Over the Backbone Link

A 6BBR is a specific kind of Border Router that performs proxy Neighbor Discovery on its backbone interface on behalf of the nodes that it has discovered on its LLN interfaces.

Some restrictions of the attached LLNs will apply to the backbone. In particular, the MTU MUST be set to the same value on the backbone and all attached LLNs. The scalability of the whole subnet requires that broadcast operations are avoided as much as possible on the backbone as well. Unless configured otherwise, in the RAs that it sends towards the LLN links, the Backbone Router MUST use the same MTU that it learns from RAs over the backbone.

On the backbone side, the 6BBR behaves like any other IPv6 router. It advertises on the backbone the prefixes of the LLNs for which it serves as a proxy.

The 6BBR uses an EARO in the NS-DAD and the multicast NA messages that it generates over the Backbone Link on behalf of a Registered Node, and it places an EARO in its unicast NA messages, if and only if the NS/NA that stimulates it had an EARO in it and the ‘R’ bit set.

The 6BBR SHOULD use unicast or solicited-node multicast address (SNMA) [RFC4291] to defend its Registered Addresses over the
backbone. In particular, the 6BBR MUST join the SNMA group that corresponds to a Registered Address as soon as it creates an entry for that address, and as long as it maintains that entry.

Optimistic DAD (ODAD) [RFC4429] SHOULD be supported by the 6BBRs in their proxy activity over the backbone. A node supporting ODAD MUST join the SNMA of a Tentative address.

A 6BBR in Routing Proxy mode advertises the Registered IPv6 Address with the 6BBR Link Layer Address, and updates Neighbor Cache Entries (NCE) in correspondent nodes over the backbone, using gratuitous NA(Override). This method may fail if the multicast message is not properly received, and correspondent nodes may maintain an incorrect neighbor state, which they will eventually discover through Neighbor Unreachability Detection (NUD). For slow movements, the NUD procedure defined in [RFC4861] may time out too quickly, and the support of [RFC7048] is recommended in all nodes in the network.

Since the MultiLink Subnet may grow to contain many nodes, multicast should be avoided as much as possible even on the backbone. Though hosts can participate using legacy IPv6 ND, all nodes connected to the backbone SHOULD support [I-D.ietf-6man-rs-refresh], which also requires the support of [RFC7559].

5.2. Over the LLN Link

BBRs and LLN hosts on the LLN follow [RFC6775] and do not depend on multicast RAs to discover routers. LLN nodes SHOULD accept multicast RAs [RFC7772], but those are rare on the LLN link. Nodes SHOULD follow the Simple Procedures for Detecting Network Attachment in IPv6 [RFC6059] (DNA procedures) to assert movements, and to support the Packet-Loss Resiliency for Router Solicitations [RFC7559] to make the unicast RS more reliable.

LLN node signals that it requires IPv6 ND proxy services from a 6BBR by registering the corresponding IPv6 Address with an NS(EARO) message with the ‘R’ flag set. The LLN node that performs the registration (the Registering Node) may be the owner of the IPv6 Address (the Registered Node) or a 6LBR that performs the registration on its behalf.

When operating as a Routing Proxy, the BBR installs host routes (/128) to the Registered Addresses over the LLN links, via the Registering Node as identified by the Source Address and the SLLA option in the NS(EARO) messages. In that case, the MAC address of the node is not visible at Layer-2 over the backbone and the bridging fabric is not aware of the addresses of the LLN devices and their mobility. The 6BBR installs a connected host route towards the
registered node over the interface to the node, and acts as a Layer-3 router for unicast packets to the node.

In that mode, the 6BBR handles the ND protocol over the backbone on behalf of the Registered Nodes, using its own MAC address in the TLLA and SLLA options in proxied NS and NA messages. For each Registered Address, multiple peer Nodes on the backbone may have resolved the address with the 6BBR MAC address and store that mapping in their Neighbor cache.

For each Registered Address, the 6BBR SHOULD maintain a list of the peers on the backbone which have associated its MAC address with the Registered Address. If that Registered Address moves to a different 6BBR, the first 6BBR SHOULD unicast a gratuitous NA(Override) to each such peer, to supply the MAC address of the new 6BBR in the TLLA option for the Address.

A Bridging Proxy can be implemented in a Layer-3 switch, or in a wireless Access Point that acts as an IPv6 Host. In the latter case, the SLLA option in the proxied NA messages is that of the Registering Node, and the 6BBR acts as a Layer-2 bridge for unicast packets to the Registered Address. The MAC address in the S/TLLA is that of the Registering Node, which is not necessarily the Registered Node. When a device moves within a LLN mesh, it may attach to a different 6LBR acting as Registering Node, and the MAC address advertised over the backbone will change.

If a registration moves from one 6BBR to the next, but the Registering Node does not change, as indicated by the S/TLLA option in the ND exchanges, there is no need to update the Neighbor Caches in the peers Nodes on the backbone. On the other hand, if the LLA changes, the 6BBR SHOULD inform all the relevant peers as described above, to update the impacted Neighbor Caches. In the same fashion, if the Registering Node changes with a new registration, the 6BBR SHOULD also update the impacted Neighbor Caches over the backbone.

6. Backbone Router Proxy Operations

This specification enables a Backbone Router to proxy Neighbor Discovery operations over the backbone on behalf of the nodes that are registered to it, allowing any node on the backbone to reach a Registered Node as if it was on-link. The backbone and the LLNs are considered different Links in a MultiLink subnet but the prefix that is used may still be advertised as on-link on the backbone to support legacy nodes; multicast ND messages are link-scoped and not forwarded across the backbone routers.

By default, a 6BBR operates as a Sleeping Proxy, as follows:
- Create a new entry in a Binding Table for a new Registered Address and ensure that the address is not a duplicate over the backbone.

- Defend a Registered Address over the backbone using NA messages with the Override bit set on behalf of the sleeping node.

- Advertise a Registered Address over the backbone using NA messages, asynchronously or as a response to a Neighbor Solicitation messages.

- To deliver packets arriving from the LLN, use Neighbor Solicitation messages to look up the destination over the backbone.

- Forward packets between the LLN and the backbone.

- Verify liveliness when needed for a stale registration.

A 6BBR may act as a Sleeping Proxy only for a Registered Address that is REACHABLE, or TENTATIVE in which case the answer is delayed. In any other state, the Sleeping Proxy operates as a Unicasting Proxy.

The 6BBR does not act on ND Messages over the backbone unless they are relevant to a Registered Node on the LLN side, saving wireless interference. On the LLN side, the prefixes associated to the MultiLink Subnet are presented as not on-link, so address resolution for other hosts do not occur.

As a Unicasting Proxy, the 6BBR forwards NS lookup messages to the Registering Node, transforming Layer-2 multicast into unicast. This is not possible in UNREACHABLE state, so the NS messages are multicasted, and rate-limited with an exponential back-off to protect the medium. In other states, the messages are forwarded to the Registering Node as unicast Layer-2 messages. In TENTATIVE state, the NS message is either held till DAD completes, or dropped.

The draft introduces the optional concept of primary and secondary BBRs. The primary is the backbone router that has the highest EUI-64 address of all the 6BBRs that share a registration for a same Registered Address, with the same ROVR and same Transaction ID, the EUI-64 address being considered as an unsigned 64bit integer. A given 6BBR can be primary for a given address and secondary for another address, regardless on whether or not the addresses belong to the same node. The primary Backbone Router is in charge of protecting the address for DAD over the Backbone. Any of the Primary and Secondary 6BBR may claim the address over the backbone, since they are all capable to route from the backbone to the LLN node; the address appears on the backbone as an anycast address.
The Backbone Routers maintain a distributed binding table, using IPv6 ND over the backbone to detect duplication. This specification requires that:

1. Addresses in a LLN that can be reachable from the backbone by way of a 6BBR MUST be registered to that 6BBR.

2. A Registered Node MUST include the EARO in the NS message when registering its addresses to a 6LR. The 6LR MUST forward the EARO unchanged to the 6LBR in the DAR/DAC exchange. The 6LBR MUST propagate the EARO unchanged to 6BBR.

3. The 6LR MUST respond with the same EARO in the NA, except for the status field.

A false positive duplicate detection may arise over the backbone, for instance if the Registered Address is registered to more than one LBR, or if the node has moved. Both situations are handled by the 6BBR transparently to the node. In the former case, one LBR becomes primary to defend the address over the backbone while the others become secondary and may still forward packets. In the latter case the LBR that receives the newest registration becomes primary.

Only one node may register a given Address at a particular 6BBR. However, that Registered Address may be registered to Multiple 6BBRs for higher availability.

Over the LLN, Binding Table management is as follows:

De-registrations (newer TID, same ROVR, null Lifetime) are accepted and acknowledged with a status of 4; the entry is deleted;

Newer registrations (newer TID, same ROVR, non-null Lifetime) are acknowledged with a status of 0 (success); the binding is updated with the new TID, the Registration Lifetime and the Registering Node; in TENTATIVE state the acknowledgement is held and may be overwritten; in other states the Registration-Lifetime timer is restarted and the entry is placed in REACHABLE state.

Identical registrations (same TID, same ROVR) from a same Registering Node are acknowledged with a status of 0 (success). If they are not identical, an error SHOULD be logged. In TENTATIVE state, the response is held and may be overwritten, but it MUST be eventually produced and it carries the result of the DAD process;
Older registrations (older TID, same ROVR) from a Registering Node are ignored;

Identical and older registrations (not-newer TID, same ROVR) from a different Registering Node are acknowledged with a status of 3 (moved); this may be rate limited to protect the medium;

Any registration for a different Registered Node (different ROVR) are acknowledged with a status of 1 (duplicate).

6.1. Registration and Binding State Creation

Upon receiving a registration for a new address with an NS(EARO) with the ‘R’ bit set, the 6BBR performs DAD over the backbone, placing the new address as target in the NS-DAD message. The EARO from the registration MUST be placed unchanged in the NS-DAD message, and a Neighbor Cache entry created in TENTATIVE state for a duration of TENTATIVE_DURATION. The NS-DAD message is sent multicast over the backbone to the SNMA associated with the registered address, unless that operation is known to be costly, and the 6BBR has an indication from another source (such as a Neighbor Cache entry) that the Registered Address was known on the backbone; in the latter case, an NS-DAD message may be sent as a Layer-2 unicast to the MAC Address that was associated with the Registered Address.

In TENTATIVE state after EARO with ‘R’ bit set:

1. The entry is removed if an NA is received over the backbone for the Registered Address with no EARO, or with an EARO with a status of 1 (duplicate) that indicates an existing registration for another LLN node. The ROVR and TID fields in the EARO received over the backbone are ignored. A status of 1 is returned in the EARO of the NA back to the Registering Node;

2. The entry is also removed if an NA with an ARO option with a status of 3 (moved), or a NS-DAD with an ARO option that indicates a newer registration for the same Registered Node, is received over the backbone for the Registered Address. A status of 3 is returned in the NA(EARO) back to the Registering Node;

3. When a registration is updated but not deleted, e.g. from a newer registration, the DAD process on the backbone continues and the running timers are not restarted;

4. Other NS (including DAD with no EARO) and NA from the backbone are not acknowledged in TENTATIVE state. To cover legacy nodes that do not support ODAD, the list of their origins MAY be stored
and then, if the TENTATIVE_DURATION timer elapses, the 6BBR MAY send each such legacy node a unicast NA.

5. When the TENTATIVE_DURATION timer elapses, a status 0 (success) is returned in a NA(EARO) back to the Registering Node(s), and the entry goes to REACHABLE state for the Registration Lifetime. The 6BBR MUST send a multicast NA(EARO) to the SNMA associated to the Registered Address over the backbone with the Override bit set so as to take over the binding from other 6BBRs.

6.2. Defending Addresses

If a 6BBR has an entry in REACHABLE state for a Registered Address:

  o If the 6BBR is primary, or does not support the function of primary, it MUST defend that address over the backbone upon receiving NS-DAD, either if the NS does not carry an EARO, or if an EARO is present that indicates a different Registering Node (different ROVR). The 6BBR sends a NA message with the Override bit set and the NA carries an EARO if and only if the NS-DAD did so. When present, the EARO in the NA(Override) that is sent in response to the NS-DAD(EARO) carries a status of 1 (duplicate), and the ROVR and TID fields in the EARO are obfuscated with null or random values to avoid network scanning and impersonation attacks.

  o If the 6BBR receives an NS-DAD(EARO) for a newer registration, the 6BBR updates the entry and the routing state to forward packets to the new 6BBR, but keeps the entry REACHABLE. Afterwards, the 6BBR MAY use REDIRECT messages to reroute traffic for the Registered Address to the new 6BBR.

  o If the 6BBR receives an NA(EARO) for a newer registration, the 6BBR removes its entry and sends a NA(EARO) with a status of 3 (MOVED) to the Registering Node, if the Registering Node is different from the Registered Node. The 6BBR cleans up existing Neighbor Cache Entries in peer nodes as discussed in Section 5.1, by unicasting to each such peer, or one broadcast NA(Override).

  o If the 6BBR receives a NS(LOOKUP) for a Registered Address, it answers immediately with an NA on behalf of the Registered Node, without polling it. There is no need of an EARO in that exchange.

  o When the Registration-Lifetime timer elapses, the entry goes to STALE state for a duration of STABLE_STALE_DURATION in LLNs that keep stable addresses such as LWPANs, and UNSTABLE_STALE_DURATION in LLNs where addresses are renewed rapidly, e.g. for privacy reasons.
The STALE state enables tracking of the backbone peers that have a Neighbor Cache entry pointing to this 6BBR in case the Registered Address shows up later. If the Registered Address is claimed by another node on the backbone, with an NS-DAD or an NA, the 6BBR does not defend the address. In STALE state:

- If STALE_DURATION elapses, the 6BBR removes the entry.
- Upon receiving an NA(Override) the 6BBR removes its entry and sends a NA(EARO) with a status of 4 (removed) to the Registering Node.
- If the 6BBR receives a NS(LOOKUP) for a Registered Address, the 6BBR MUST send an NS(NUD) following rules in [RFC7048] to the Registering Node targeting the Registered Address prior to answering. If the NUD succeeds, the operation in REACHABLE state applies. If the NUD fails, the 6BBR refrains from answering the lookup. The NUD SHOULD be used by the Registering Node to indicate liveness of the Registered Node, if they are different nodes.

7. Security Considerations

This specification applies to LLNS in which the link layer is protected, either by means of physical or IP security for the Backbone Link or MAC sublayer cryptography. In particular, the LLN MAC is required to provide secure unicast to/from the Backbone Router and secure Broadcast from the Backbone Router in a way that prevents tempering with or replaying the RA messages.

The use of EUI-64 for forming the Interface ID in the link local address prevents the usage of Secure ND ([RFC3971] and [RFC3972]) and address privacy techniques. This specification RECOMMENDS the use of additional protection against address theft such as provided by [I-D.ietf-6lo-ap-nd], which guarantees the ownership of the ROVR.

When the ownership of the ROVR cannot be assessed, this specification limits the cases where the ROVR and the TID are multicasted, and obfuscates them in responses to attempts to take over an address.

8. Protocol Constants

This Specification uses the following constants:

- TENTATIVE_DURATION: 800 milliseconds
- STABLE_STALE_DURATION: 24 hours
9. IANA Considerations

This document has no request to IANA.

10. Acknowledgments

Kudos to Eric Levy-Abegnoli who designed the First Hop Security infrastructure at Cisco.

11. References

11.1. Normative References

[I-D.ietf-6lo-rfc6775-update]


Thubert & Perkins Expires March 7, 2019 [Page 17]
11.2. Informative References

[I-D.chakrabarti-nordmark-6man-efficient-nd]

[I-D.delcarpio-6lo-wlanah]

[I-D.ietf-6lo-ap-nd]

[I-D.ietf-6lo-nfc]
[I-D.ietf-6man-rs-refresh]

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-14 (work in progress), April 2018.

[I-D.ietf-6tisch-terminology]
Palattella, M., Thubert, P., Watteyne, T., and Q. Wang, "Terms Used in IPv6 over the TSCH mode of IEEE 802.15.4e", draft-ietf-6tisch-terminology-10 (work in progress), March 2018.

[I-D.ietf-bier-architecture]

[I-D.ietf-ipv6-multilink-subnets]

[I-D.nordmark-6man-dad-approaches]
Nordmark, E., "Possible approaches to make DAD more robust and/or efficient", draft-nordmark-6man-dad-approaches-02 (work in progress), October 2015.

[I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks]

[I-D.vyncke-6man-mcast-not-efficient]


11.3. External Informative References

[IEEEstd8021]
IEEE standard for Information Technology, "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks Part 1: Bridging and Architecture".

[IEEEstd80211]
IEEE standard for Information Technology, "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks-- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[IEEEstd802151]
IEEE standard for Information Technology, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)".

[IEEEstd802154]
IEEE standard for Information Technology, "IEEE Standard for Local and metropolitan area networks -- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)".

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis  06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com
Charles E. Perkins
Futurewei
2330 Central Expressway
Santa Clara  95050
United States of America

Email: charliep@computer.org
Abstract

This specification updates RFC 6775 - 6LoWPAN Neighbor Discovery, to clarify the role of the protocol as a registration technique, simplify the registration operation in 6LoWPAN routers, as well as to provide enhancements to the registration capabilities and mobility detection for different network topologies including the backbone routers performing proxy Neighbor Discovery in a low power network.

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 http://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 December 23, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Applicability of Address Registration Options ................. 3
3. Terminology ..................................................... 4
4. Updating RFC 6775 .............................................. 5
   4.1. Extended Address Registration Option .................... 6
   4.2. Transaction ID ............................................. 6
   4.3. Owner Unique ID ........................................... 7
   4.4. Registering the Target Address .......................... 7
   4.5. Link-Local Addresses and Registration .................. 8
   4.6. Maintaining the Registration States ..................... 9
5. Detecting Enhanced ARO Capability Support ..................... 10
6. Updated ND Options ............................................. 11
   6.1. The Enhanced Address Registration Option (EARO) ......... 11
   6.2. New 6LoWPAN capability Bits in the Capability Indication Option ............................................. 14
7. Backward Compatibility ......................................... 14
   7.1. Discovering the capabilities of an ND peer ............... 14
   7.1.1. Using the E Flag in the CIO ......................... 14
   7.1.2. Using the T Flag in the EARO ......................... 15
   7.2. Legacy 6LoWPAN Node ....................................... 15
   7.3. Legacy 6LoWPAN Router ..................................... 16
   7.4. Legacy 6LoWPAN Border Router ............................. 16
8. Security Considerations ....................................... 16
9. Privacy Considerations ......................................... 18
10. IANA Considerations .......................................... 18
11. Acknowledgments .............................................. 20
12. References .................................................... 20
   12.1. Normative References .................................... 20
   12.2. Informative References .................................. 21
   12.3. External Informative References ........................ 23
Appendix A. Applicability and Requirements Served .............. 24
Appendix B. Requirements .......................................... 24
   B.1. Requirements Related to Mobility ......................... 25
   B.2. Requirements Related to Routing Protocols .............. 25
   B.3. Requirements Related to the Variety of Low-Power Link types ............................................. 26
   B.4. Requirements Related to Proxy Operations ............... 27
   B.5. Requirements Related to Security ........................ 27
   B.6. Requirements Related to Scalability ...................... 28
Authors’ Addresses .............................................. 29
1. Introduction

The scope of this draft is an IPv6 Low Power Networks including star and mesh topologies. This specification modifies and extends the behavior and protocol elements of RFC 6775 "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC6775] to enable additional capabilities such as:

* Support the indication of mobility vs retry (T-bit)
* Ease up requirement of registration for link-local addresses
* Introducing Enhancement to Address Registration Option (ARO)
* Permitting registration of target address
* Clarification of support of privacy and temporary addresses

The following sections will discuss applicability of 6LoWPAN ND registration, new extensions and updates to RFC 6775. Finally, we will discuss how the extensions of registration framework can be useful for a scenario such as Backbone router (6BBR) proxy ND operations.

2. Applicability of Address Registration Options

The purpose of the Address Registration Option (ARO) [RFC6775] and of the Extended ARO (EARO) that is introduced in this document is to facilitate duplicate address detection (DAD) for hosts and pre-populate Neighbor Cache Entries (NCE) [RFC4861] in the routers to reduce the need for sending ‘multicast neighbor solicitations’ which may be harmful in low power constrained nodes networks where multicast is most often treated as broadcasts.

In some cases the address registration can fail or becomes useless for reasons other than a duplicate address. Examples are the router having run out of space, a registration bearing a stale sequence number (e.g. denoting a movement of the host after this registration was placed), a host misbehaving and attempting to register an invalid address such as the unspecified address [RFC4291], or the host using an address which is not topologically correct on that link. In such cases the host will receive an error to help diagnose the issue and may retry, possibly with a different address, and possibly registering to a different 6LR, depending on the returned error.

However, the ability to return errors to address registrations MUST NOT be used to restrict the ability of hosts to form and use addresses as recommended in "Host Address Availability"
Recommendations" [RFC7934]. In particular, this is needed for enhanced privacy, which implies that each host will register a multiplicity of address as part mechanisms like "Privacy Extensions for Stateless Address Autoconfiguration (SLAAC) in IPv6" [RFC4941]. This implies that the capabilities of 6LR and 6LBRs in terms of number of registrations must be clearly announced in the router documentation, and that a network administrator should deploy adapted 6LR/6LBRs to support the number and type of devices in his network, based on the number of IPv6 addresses that those devices require.

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Readers are expected to be familiar with all the terms and concepts that are discussed in

"Neighbor Discovery for IP version 6" [RFC4861],
"IPv6 Stateless Address Autoconfiguration" [RFC4862],
"IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919],
"Neighbor Discovery Optimization for Low-power and Lossy Networks" [RFC6775] and
"Multi-link Subnet Support in IPv6" [I-D.ietf-ipv6-multilink-subnets].

as well as this additional terminology:

Backbone  This is an IPv6 transit link that interconnects 2 or more Backbone Routers. It is expected to be deployed as a high speed Backbone in order to federate a potentially large set of LLNS. Also referred to as a LLN Backbone or Backbone network.

Backbone Router  An IPv6 router that federates the LLN using a Backbone link as a Backbone. A 6BBR acts as a 6LoWPAN Border Routers (6LBR) and an Energy Aware Default Router (NEAR).

Extended LLN  This is the aggregation of multiple LLNs as defined in RFC 4919 [RFC4919], interconnected by a Backbone Link via Backbone Routers, and forming a single IPv6 MultiLink Subnet.
Registration  The process during which a wireless Node registers its address(es) with the Border Router so the 6BBR can proxy ND for it over the Backbone.

Binding  The state in the 6BBR that associates an IP address with a MAC address, a port and some other information about the node that owns the IP address.

Registered Node  The node for which the registration is performed, which owns the fields in the EARO option.

Registering Node  The node that performs the registration to the 6BBR, either for one of its own addresses, in which case it is Registered Node and indicates its own MAC Address as Source Link Layer Address (SLLA) in the NS(EARO), or on behalf of a Registered Node that is reachable over a LLN mesh. In the latter case, if the Registered Node is reachable from the 6BBR over a Mesh-Under mesh, the Registering Node indicates the MAC Address of the Registered Node as SLLA in the NS(EARO). Otherwise, it is expected that the Registered Device is reachable over a Route-Over mesh from the Registering Node, in which case the SLLA in the NS(ARO) is that of the Registering Node, which causes it to attract the packets from the 6BBR to the Registered Node and route them over the LLN.

Registered Address  The address owned by the Registered Node that is being registered.

4. Updating RFC 6775

This specification extends the Address Registration Option (ARO) defined in RFC 6775 [RFC6775]; in particular a "T" flag is added that must be set in NS messages when this specification is used, and echo’ed in NA messages to confirm that the protocol effectively supported. Support for this specification can thus be inferred from the presence of the Extended ARO ("T" flag set) in ND messages.

In order to support various types of link layers, this specification also adds recommendation to allow multiple registrations, including for privacy / temporary addresses, and provides new mechanisms to help clean up stale registration states as soon as possible.

A Registering Node that supports this specification will favor registering to a 6LR that indicates support for this specification over that of RFC 6775 [RFC6775].
4.1. Extended Address Registration Option

This specification extends the ARO option that is used for the process of address registration. The new ARO is referred to as Extended ARO (EARO), and its semantics are modified as follows:

The address that is being registered with a Neighbor Solicitation (NS) with an EARO is now the Target Address, as opposed to the Source Address as specified in RFC 6775 [RFC6775] (see Section 4.4 for more). This change enables a 6LBR to use an address of his as source to the proxy-registration of an address that belongs to a LLN Node to a 6BBR. This also limits the use of an address as source address before it is registered and the associated Duplicate Address Detection (DAD) is complete.

The Unique ID in the EARO option does no more have to be a MAC address (see Section 4.3 for more). This enables in particular the use of a Provable Temporary UID (PT-UID) as opposed to burn-in MAC address, the PT-UID providing a trusted anchor by the 6LR and 6LBR to protect the state associated to the node.

The specification introduces a Transaction ID (TID) field in the EARO (see Section 4.2 for more on TID). The TID MUST be provided by a node that supports this specification and a new T flag MUST be set to indicate so. The T bit can be used to determine whether the peer supports this specification.

Finally, this specification introduces a number of new Status codes to help diagnose the cause of a registration failure (more in Table 1).

4.2. Transaction ID

The specification expects that the Registered Node can provide a sequence number called Transaction ID (TID) that is incremented with each re-registration. The TID is used to detect the freshness of the registration request and useful to detect one single registration by multiple 6LOWPAN border routers supporting the same large 6LOWPAN, as is the case for backbone routers (BBR).

For example, when a Registered Node is registered with multiple BBRs in parallel, it is expected that the same TID is used, to enable the 6BBRs to correlate the registrations as being a single one, and differentiate that situation from a movement.

Thus TID could be tracked to follow the sequence of mobility of a node. The details protocols of mobility verification by the border routers is not part of this specification.
4.3. Owner Unique ID

The Owner Unique ID (OUID) enables to differentiate a real duplicate address registration from a double registration or a movement. An ND message from the 6BBR over the Backbone that is proxied on behalf of a Registered Node must carry the most recent EARO option seen for that node. A NS/NA with an EARO and a NS/NA without a EARO thus represent different nodes and if they relate to a same target then they reflect an address duplication. The Owner Unique ID can be as simple as a EUI-64 burn-in address, if duplicate EUI-64 addresses are avoided.

Alternatively, the unique ID can be a cryptographic string that can be used to prove the ownership of the registration as discussed in "Address Protected Neighbor Discovery for Low-power and Lossy Networks" [I-D.ietf-6lo-ap-nd].

In any fashion, it is recommended that the node stores the unique Id or the keys used to generate that ID in persistent memory. Otherwise, it will be prevented to re-register after a reboot that would cause a loss of memory until the Backbone Router times out the registration.

4.4. Registering the Target Address

This specification changes the behavior of the 6LN and the 6LR so that the Registered Address is found in the Target Address field of the NS and NA messages as opposed to the Source Address.

The reason for this change is to enable proxy-registrations on behalf of other nodes in Route-Over meshes, for instance to enable that a RPL root registers addresses on behalf LLN nodes that are deeper in a 6TiSCH mesh, as discussed in Appendix B.4. In that case, the Registering Node MUST indicate its own address as source of the ND message and its MAC address in the Source Link-Layer Address Option (SLLAO), since it still expects to get the packets and route them down the mesh. But the Registered Address belongs to another node, the Registered Node, and that address is indicated in the Target Address field of the NS message.

With this convention, a TLLA option indicates the link-layer address of the 6LN that owns the address, whereas the SLLA Option in a NS message indicates that of the Registering Node, which can be the owner device, or a proxy.

Since the Registering Node is the one that has reachability with the 6LR, and is the one expecting packets for the 6LN, it makes sense to maintain compatibility with RFC 6775 [RFC6775], and it is REQUIRED...
that an SLLA Option is always placed in a registration NS(EARO)
message.

4.5.  Link-Local Addresses and Registration

Considering that LLN nodes are often not wired and may move, there is
no guarantee that a Link-Local address stays unique between a
potentially variable and unbounded set of neighboring nodes.
Compared to RFC 6775 [RFC6775], this specification only requires that
a Link-Local address is unique from the perspective of the peering
nodes. This simplifies the Duplicate Address Detection (DAD) for
Link-Local addresses, and there is no Duplicate Address Request (DAR)
/Duplicate Address Confirmation (DAC) exchange between the 6LR and a
6LBR for Link-Local addresses.

Additionally, RFC 6775 [RFC6775] requires that a 6LoWPAN Node (6LN)
uses an address being registered as the source of the registration
message. This generates complexities in the 6LR to be able to cope
with a potential duplication, in particular for global addresses. To
simplify this, a 6LN and a 6LR that conform this specification always
use Link-Local addresses as source and destination addresses for the
registration NS/NA exchange. As a result, the registration is
globally faster, and some of the complexity is removed.

In more details:

An exchange between two nodes using Link-Local addresses implies that
they are reachable over one hop and that at least one of the 2 nodes
acts as a 6LR. A node MUST register a Link-Local address to a 6LR in
order to obtain reachability from that 6LR beyond the current
exchange, and in particular to use the Link-Local address as source
address to register other addresses, e.g. global addresses.

If there is no collision with an address previously registered to
this 6LR by another 6LN, then, from the standpoint of this 6LR, this
Link-Local address is unique and the registration is acceptable.
Conversely, it may possibly happen that two different 6LRs expose a
same Link-Local address but different link-layer addresses. In that
case, a 6LN may only interact with one of the 6LR so as to avoid
confusion in the 6LN neighbor cache.

The DAD process between the 6LR and a 6LoWPAN Border Router (6LBR),
which is based on a Duplicate Address Request (DAR) / Duplicate
Address Confirmation (DAC) exchange as described in RFC 6775
[RFC6775], does not need to take place for Link-Local addresses.

It is desired that a 6LR does not need to modify its state associated
to the Source Address of an NS(EARO) message. For that reason, when
possible, it is RECOMMENDED to use an address that is already
registered with a 6LR

When registering to a 6LR that conforms this specification, a node
MUST use a Link-Local address as the source address of the
registration, whatever the type of IPv6 address that is being
registered. That Link-Local Address MUST be either already
registered, or the address that is being registered.

When a Registering Node does not have an already-Registered Address,
it MUST register a Link-Local address, using it as both the Source
and the Target Address of an NS(EARO) message. In that case, it is
RECOMMENDED to use a Link-Local address that is (expected to be)
globally unique, e.g. derived from a burn-in MAC address. An EARO
option in the response NA indicates that the 6LR supports this
specification.

Since there is no DAR/DAC exchange for Link-Local addresses, the 6LR
may answer immediately to the registration of a Link-Local address,
based solely on its existing state and the Source Link-Layer Option
that MUST be placed in the NS(EARO) message as required in RFC 6775
[RFC6775].

A node needs to register its IPv6 Global Unicast IPv6 Addresses (GUA)
to a 6LR in order to obtain a global reachability for these addresses
via that 6LR. As opposed to a node that complies to RFC 6775
[RFC6775], a Registering Node registering a GUA does not use that GUA
as Source Address for the registration to a 6LR that conforms this
specification. The DAR/DAC exchange MUST take place for non-Link-
Local addresses as prescribed by RFC 6775 [RFC6775].

4.6. Maintaining the Registration States

This section discusses protocol actions that involve the Registering
Node, the 6LR and the 6LBR. It must be noted that the portion that
deals with a 6LBR only applies to those addresses that are registered
to it, which, as discussed in Section 4.5, is not the case for Link-
Local addresses. The registration state includes all data that is
stored in the router relative to that registration, in particular,
but not limited to, an NCE in a 6LR. 6LBRs and 6BBRs may store
additional registration information in more complex data structures
and use protocols that are out of scope of this document to keep them
synchronized when they are distributed.

When its Neighbor Cache is full, a 6LR cannot accept a new
registration. In that situation, the EARO is returned in a NA
message with a Status of 2, and the Registering Node may attempt to
register to another 6LR. Conversely the registry in the 6LBR may be
saturated, in which case the 6LBR cannot guarantee that a new address is effectively not a duplicate. In that case, the 6LBR replies to a DAR message with a DAC message that carries a Status code 9 indicating "6LBR Registry saturated", and the address stays in TENTATIVE state.

A node renews an existing registration by repeatedly sending NS(EARO) messages for the Registered Address. In order to refresh the registration state in the 6LBR, these registrations MUST be reported to the 6LBR.

A node that ceases to use an address SHOULD attempt to deregister that address from all the 6LRs to which it has registered the address, which is achieved using an NS(EARO) message with a Registration Lifetime of 0.

A node that moves away from a particular 6LR SHOULD attempt to deregister all of its addresses registered to that 6LR.

Upon receiving a NS(EARO) message with a Registration Lifetime of 0 and determining that this EARO is the freshest for a given NCE (see Section 4.2), a 6LR cleans up its NCE. If the address was registered to the 6LBR, then the 6LR MUST report to the 6LBR, through a DAR/DAC exchange with the 6LBR, or an alternate protocol, indicating the null Registration Lifetime and the latest TID that this 6LR is aware of.

Upon the DAR message, the 6LBR evaluates if this is the freshest EARO it has received for that particular registry entry. If it is, then the entry is scheduled to be removed, and the DAR is answered with a DAC message bearing a Status of 0 "Success". If it is not the freshest, then a Status 2 "Moved" is returned instead, and the existing entry is conserved. The 6LBR SHOULD conserve the address in a DELAY state for a configurable period of time, so as to protect a mobile node that deregistered from one 6LR and did not register yet to a new one.

5. Detecting Enhanced ARO Capability Support

The nodes and routers in a network may be mixed and if a node wants to use EARO feature for address registration, it has to find a router which supports it. Thus all implementations with EARO option MUST provide the capability detection method using 6CIO option to support both types of registrations (ARO and EARO) as described in later sections. Moreover, any new implementation of 6LoWPAN is also RECOMMENDED to support 6LoWPAN Capability Indication option(6CIO) in general.
RFC 7400 [RFC7400] introduces the 6LoWPAN Capability Indication Option (6CIO) to indicate a node's capabilities to its peers. This specification extends the format defined in RFC 7400 to signal the support for EARO, as well as the capability to act as a 6LR, 6LBR and 6BBR.

With RFC 7400 [RFC7400], the 6CIO is typically sent Router Solicitation (RS) messages. When used to signal the capabilities above per this specification, the 6CIO is typically present Router Advertisement (RA) messages but can also be present in RS, Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

6. Updated ND Options

This specification does not introduce new options, but it modifies existing ones and updates the associated behaviors as follow:

6.1. The Enhanced Address Registration Option (EARO)

The Enhanced Address Registration Option (EARO) is intended to be used as a replacement to the ARO option within Neighbor Discovery NS and NA messages between a LLN node and its 6LoWPAN Router (6LR), as well as in Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC) messages between 6LRs and 6LBRs in LLNs meshes such as 6TiSCH networks.

An NS message with an EARO option is a registration if and only if it also carries an SLLAO option. The AERO option also used in NS and NA messages between Backbone Routers over the Backbone link to sort out the distributed registration state, and in that case, it does not carry the SLLAO option and is not confused with a registration.

The EARO extends the ARO and is recognized by the "T" flag set.

When using the EARO option, the address being registered is found in the Target Address field of the NS and NA messages. This differs from 6LoWPAN ND RFC 6775 [RFC6775] which specifies that the address being registered is the source of the NS.

The format of the EARO option is as follows:
Option Fields

Type: 33

Length: 8-bit unsigned integer.

Status: 8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. See Table 1 below.

Reserved: This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

T: One bit flag. Set if the next octet is used as a TID.

TID: 1-byte integer; a transaction ID that is maintained by the node and incremented with each transaction. It is recommended that the node maintains the TID in a persistent storage.

Registration Lifetime: 16-bit integer; expressed in minutes. 0 means that the registration has ended and the associated state should be removed.

Owner Unique Identifier (OUI): A globally unique identifier for the node associated. This can be the EUI-64 derived IID of an interface, or some provable ID obtained cryptographically.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0..2</td>
<td>See RFC 6775 [RFC6775]. Note that a Status of 1 &quot;Duplicate Address&quot; applies to the Registered Address. If the Source Address conflicts with an existing registration, &quot;Duplicate Source Address&quot; should be used.</td>
</tr>
</tbody>
</table>
Moved: The registration fails because it is not the freshest. This Status indicates that the registration is rejected because another more recent registration was done, as indicated by a same OUI and a more recent TID. One possible cause is a stale registration that has progressed slowly in the network and was passed by a more recent one. It could also indicate a OUI collision.

Removed: The binding state was removed. This may be placed in an asynchronous NS(ARO) message, or as the rejection of a proxy registration to a Backbone Router

Proof requested: The Registering Node is challenged for owning the Registered Address or for being an acceptable proxy for the registration. This Status is expected in asynchronous messages from a registrar (6LR, 6LBR, 6BBR) to indicate that the registration state is removed, for instance due to time out of a lifetime, or a movement. The receiver of the NA is the device that has performed a registration that is now stale and it should clean up its state.

Duplicate Source Address: The address used as source of the NS(ARO) conflicts with an existing registration.

Invalid Source Address: The address used as source of the NS(ARO) is not a Link-Local address as prescribed by this document.

Registered Address topologically incorrect: The address being registered is not usable on this link, e.g. it is not topologically correct

6LBR Registry saturated: A new registration cannot be accepted because the 6LBR Registry is saturated.

Incorrect proof: The proof of ownership of the registered address is not correct.

Table 1: EARO Status

Note: the code "6LBR Registry saturated" is used by 6LBRs instead of Status 2 when responding to a DAR/DAC exchange and passed on to the Registering Node by the 6LR. There is no point for the node to retry this registration immediately via another 6LR, since the problem is global to the network. The node may either abandon that address,
deregister other addresses first to make room, or keep the address in TENTATIVE state and retry later.

6.2. New 6LoWPAN capability Bits in the Capability Indication Option

This specification defines a number of capability bits in the CIO that was introduced by RFC 7400 [RFC7400].

Support for this specification is indicated by setting the "E" flag in a CIO option. Routers that are capable of acting as 6LR, 6LBR and 6BBR SHOULD set the L, B and P flags, respectively.

Those flags are not mutually exclusive and if a router is capable of multiple roles, it SHOULD set all the related flags.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------+
|     Type      |   Length = 1  |_____________________|L|B|P|E|G|
+---------------------------------------------+
|___________________________________________________|
+---------------------------------------------+
|____________________________|L|B|P|E|G|
+---------------------------------------------+
+---------------------------------------------+
```

Figure 2: New capability Bits L, B, P, E in the CIO Option Fields

Type: 36

L: Node is a 6LR, it can take registrations.

B: Node is a 6LBR.

P: Node is a 6BBR, proxying for nodes on this link.

E: This specification is supported and applied.

7. Backward Compatibility

7.1. Discovering the capabilities of an ND peer

7.1.1. Using the E Flag in the CIO

If the CIO is used in an ND message, then the "E" Flag MUST be set by the sending node if supports this specification.
It is RECOMMENDED that a router that supports this specification indicates so with a CIO option, but this might not be practical if the link-layer MTU is too small.

If the Registering Node receives a CIO in a RA, then the setting of the E" Flag indicates whether or not this specification is supported.

A node which does not implement this draft or parse 6CIO option, MUST ignore the packet and the sender of option SHOULD use legacy registration method according to RFC 6775 [RFC6775] after a timeout period.

7.1.2. Using the T Flag in the EARO

One alternate way for a 6LN to discover the router’s capabilities to first register a Link Local address, placing the same address in the Source and Target Address fields of the NS message, and setting the "T" Flag. The node may for instance register an address that is based on EU1-64. For such address, DAD is not required and using the SLLAO option in the NS is actually more amenable with existing ND specifications such as the "Optimistic Duplicate Address Detection (DAD) for IPv6" [RFC4429]. Once that first registration is complete, the node knows from the setting of the "T" Flag in the response whether the router supports this specification. If this is verified, the node may register other addresses that it owns, or proxy-register addresses on behalf some another node, indicating those addresses being registered in the Target Address field of the NS messages, while using one of its own, already registered, addresses as source.

A node that supports this specification MUST always use an EARO as a replacement to an ARO in its registration to a router. This is harmless since the "T" flag and TID field are reserved in RFC 6775 [RFC6775] are ignored by a legacy router. A router that supports this specification answers to an ARO with an ARO and to an EARO with an EARO.

This specification changes the behavior of the peers in a registration flows. To enable backward compatibility, a node that registers to a router that is not known to support this specification MUST behave as prescribed by RFC 6775. Once the router is known to support this specification, the node MUST obey this specification.

7.2. Legacy 6LoWPAN Node

A legacy 6LN will use the Registered Address as source and will not use an EARO option. In order to be backward compatible, an updated 6LR needs to accept that registration if it is valid per the RFC 6775 [RFC6775] specification, and manage the binding cache accordingly.
The main difference with RFC 6775 is that DAR/DAC exchange for DAD may be avoided for Link-Local addresses. Additionally, the 6LR SHOULD use an EARO in the reply, and may use any of the Status codes defined in this specification.

7.3. Legacy 6LoWPAN Router

The first registration by a an updated 6LN is for a Link-Local address, using that Link-Local address as source. A legacy 6LN will not makes a difference and accept -or reject- that registration as if the 6LN was a legacy node.

An updated 6LN will always use an EARO option in the registration NS message, whereas a legacy 6LN will always areply with an ARO option in the NA message. So from that first registration, the updated 6LN can figure whether the 6LR supports this specification or not.

When facing a legacy 6LR, an updated 6LN may attempt to find an alternate 6LR that is updated. In order to be backward compatible, based on the discovery that a 6LR is legacy, the 6LN needs to fallback to legacy behavior and source the packet with the Registered Address.

The main difference is that the updated 6LN SHOULD use an EARO in the request regardless of the type of 6LN, legacy or updated

7.4. Legacy 6LoWPAN Border Router

With this specification, the DAR/DAC transports an EARO option as opposed to an ARO option. As described for the NS/NA exchange, devices that support this specification always use an EARO option and all the associated behavior.

8. Security Considerations

This specification extends RFC 6775 [RFC6775], and the security section of that draft also applies to this as well. In particular, it is expected that the link layer is sufficiently protected to prevent a rogue access, either by means of physical or IP security on the Backbone Link and link layer cryptography on the LLN. This specification also expects that the LLN MAC provides secure unicast to/from the Backbone Router and secure Broadcast from the Backbone Router in a way that prevents tempering with or replaying the RA messages.

This specification recommends to using privacy techniques (more in section Section 9, and protection against address theft such as provided by "Address Protected Neighbor Discovery for Low-power and
Lossy Networks" [I-D.ietf-6lo-ap-nd], which guarantees the ownership of the Registered Address using a cryptographic OUID.

The registration mechanism may be used by a rogue node to attack the 6LR or the 6LBR with a Denial-of-Service attack against the registry. It may also happen that the registry of a 6LR or a 6LBR is saturated and cannot take any more registration, which effectively denies the requesting a node the capability to use a new address. In order to alleviate those concerns, Section 4.6 provides a number of recommendations that ensure that a stale registration is removed as soon as possible from the 6LR and 6LBR. In particular, this specification recommends that:

- A node that ceases to use an address should attempt to deregister that address from all the 6LRs to which it is registered. The flow is propagated to the 6LBR when needed, and a sequence number is used to make sure that only the freshest command is acted upon.

- The nodes should be configured with a Registration Lifetime that reflects their expectation of how long they will use the address with the 6LR to which it is registered. In particular, use cases that involve mobility or rapid address changes should use lifetimes that are homogeneous with the expectation of presence.

- The router (6LR or 6LBR) should be configurable so as to limit the number of addresses that can be registered by a single node, as identified at least by MAC address and preferably by security credentials. When that maximum is reached, the router should use a Least-Recently-Used (LRU) logic so as to clean up the addresses that were not used for the longest time, keeping at least one Link-Local address, and attempting to keep one or more stable addresses if such can be recognized, e.g. from the way the IID is formed or because they are used over a much longer time span than other (privacy, shorter-lived) addresses.

- Administrators should take great care to deploy adequate numbers of 6LR to cover the needs of the nodes in their range, so as to avoid a situation of starving nodes. It is expected that the 6LBR that serves a LLN is a more capable node then the average 6LR, but in a network condition where it may become saturated, a particular deployment should distribute the 6LBR functionality, for instance by leveraging a high speed Backbone and Backbone Routers to aggregate multiple LLNs into a larger subnet.

When the ownership of the OUID cannot be assessed, this specification limits the cases where the OUID and the TID are multicasted, and obfuscates them in responses to attempts to take over an address.
The LLN nodes depend on the 6LBR and the 6BBR for their operation. A trust model must be put in place to ensure that the right devices are acting in these roles, so as to avoid threats such as black-holing, or bombing attack whereby an impersonated 6LBR would destroy state in the network by using the "Removed" Status code.

9. Privacy Considerations

As indicated in Section 2, this protocol does not aim at limiting the number of IPv6 addresses that a device can form. A host should be able to form and register any address that is topologically correct in the subnet(s) advertised by the 6LR/6LBR.

This specification does not mandate any particular way for forming IPv6 addresses, but it recognizes that use of EUI-64 for forming the Interface ID in the Link-Local address prevents the usage of "SEcure Neighbor Discovery (SEND)" [RFC3971] and "Cryptographically Generated Addresses (CGA)" [RFC3972], and that of address privacy techniques.

"Privacy Considerations for IPv6 Adaptation-Layer Mechanisms" [RFC8065] addresses why privacy is important and how to form such addresses. All implementations and deployment must consider the option of privacy addresses in their own environment. Also future specifications involving 6LOWPAN Neighbor Discovery should consult "Recommendation on Stable IPv6 Interface Identifiers" [RFC8064] for default interface identification.

10. IANA Considerations

IANA is requested to create a new subregistry for "ARO Flags" under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters". This specification defines 8 positions, bit 0 to bit 7, and assigns bit 7 for the "T" flag in Section 6.1. The policy is "IETF Review" or "IESG Approval" [RFC5226]. The initial content of the registry is as shown in Table 2.

```
+----------------+-----------+-----------+
| ARO Status | Description | Document |
+----------------+-----------+-----------+
|    0..6    | Unassigned |           |
|            |            |           |
|     7      | "T" Flag   | RFC This  |
+----------------+-----------+-----------+
```

Table 2: new ARO Flags
IANA is requested to make additions to existing registries as follows:

<table>
<thead>
<tr>
<th>ARO Status</th>
<th>Description</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Moved</td>
<td>RFC This</td>
</tr>
<tr>
<td>4</td>
<td>Removed</td>
<td>RFC This</td>
</tr>
<tr>
<td>5</td>
<td>Proof requested</td>
<td>RFC This</td>
</tr>
<tr>
<td>6</td>
<td>Duplicate Source Address</td>
<td>RFC This</td>
</tr>
<tr>
<td>7</td>
<td>Invalid Source Address</td>
<td>RFC This</td>
</tr>
<tr>
<td>8</td>
<td>Registered Address topologically incorrect</td>
<td>RFC This</td>
</tr>
<tr>
<td>9</td>
<td>6LBR registry saturated</td>
<td>RFC This</td>
</tr>
<tr>
<td>10</td>
<td>Incorrect proof</td>
<td>RFC This</td>
</tr>
</tbody>
</table>

Table 3: New ARO Status values

Subregistry for "6LoWPAN capability Bits" under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters"

<table>
<thead>
<tr>
<th>capability Bit</th>
<th>Description</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>6LR capable (L bit)</td>
<td>RFC This</td>
</tr>
<tr>
<td>12</td>
<td>6LBR capable (B bit)</td>
<td>RFC This</td>
</tr>
<tr>
<td>13</td>
<td>6BBR capable (P bit)</td>
<td>RFC This</td>
</tr>
<tr>
<td>14</td>
<td>EARO support (E bit)</td>
<td>RFC This</td>
</tr>
</tbody>
</table>

Table 4: New 6LoWPAN capability Bits
11. Acknowledgments

Kudos to Eric Levy-Abegnoli who designed the First Hop Security infrastructure at Cisco.

12. References

12.1. Normative References


12.2. Informative References

[I-D.chakrabarti-nordmark-6man-efficient-nd]

[I-D.delcarpio-6lo-wlanah]

[I-D.ietf-6lo-ap-nd]

[I-D.ietf-6lo-backbone-router]

[I-D.ietf-6lo-nfc]

[I-D.ietf-6tisch-architecture]

[I-D.ietf-bier-architecture]

[I-D.ietf-ipv6-multilink-subnets]


12.3. External Informative References

[IEEEstd802154]

Appendix A. Applicability and Requirements Served

This specification extends 6LoWPAN ND to sequence the registration and serves the requirements expressed Appendix B.1 by enabling the mobility of devices from one LLN to the next based on the complementary work in the "IPv6 Backbone Router" [I-D.ietf-6lo-backbone-router] specification.

In the context of the the TimeSlotted Channel Hopping (TSCH) mode of IEEE Std. 802.15.4 [IEEEstd802154], the "6TiSCH architecture" [I-D.ietf-6tisch-architecture] introduces how a 6LoWPAN ND host could connect to the Internet via a RPL mesh Network, but this requires additions to the 6LoWPAN ND protocol to support mobility and reachability in a secured and manageable environment. This specification details the new operations that are required to implement the 6TiSCH architecture and serves the requirements listed in Appendix B.2.

The term LLN is used loosely in this specification to cover multiple types of WLANs and WPANs, including Low-Power Wi-Fi, BLUETOOTH(R) Low Energy, IEEE Std.802.11AH and IEEE Std.802.15.4 wireless meshes, so as to address the requirements discussed in Appendix B.3.

This specification can be used by any wireless node to associate at Layer-3 with a 6BBR and register its IPv6 addresses to obtain routing services including proxy-ND operations over the Backbone, effectively providing a solution to the requirements expressed in Appendix B.4.

"Efficiency aware IPv6 Neighbor Discovery Optimizations" [I-D.chakrabarti-nordmark-6man-efficient-nd] suggests that 6LoWPAN ND [RFC6775] can be extended to other types of links beyond IEEE Std. 802.15.4 for which it was defined. The registration technique is beneficial when the Link-Layer technique used to carry IPv6 multicast packets is not sufficiently efficient in terms of delivery ratio or energy consumption in the end devices, in particular to enable energy-constrained sleeping nodes. The value of such extension is especially apparent in the case of mobile wireless nodes, to reduce the multicast operations that are related to classical ND ([RFC4861], [RFC4862]) and plague the wireless medium. This serves scalability requirements listed in Appendix B.6.

Appendix B. Requirements

This section lists requirements that were discussed at 6lo for an update to 6LoWPAN ND. This specification meets most of them, but those listed in Appendix B.5 which are deferred to a different specification such as [I-D.ietf-6lo-ap-nd], and those related to multicast.
B.1. Requirements Related to Mobility

Due to the unstable nature of LLN links, even in a LLN of immobile nodes a 6LN may change its point of attachment to a 6LR, say 6LR-a, and may not be able to notify 6LR-a. Consequently, 6LR-a may still attract traffic that it cannot deliver any more. When links to a 6LR change state, there is thus a need to identify stale states in a 6LR and restore reachability in a timely fashion.

Req1.1: Upon a change of point of attachment, connectivity via a new 6LR MUST be restored timely without the need to de-register from the previous 6LR.

Req1.2: For that purpose, the protocol MUST enable to differentiate between multiple registrations from one 6LoWPAN Node and registrations from different 6LoWPAN Nodes claiming the same address.

Req1.3: Stale states MUST be cleaned up in 6LRs.

Req1.4: A 6LoWPAN Node SHOULD also be capable to register its Address to multiple 6LRs, and this, concurrently.

B.2. Requirements Related to Routing Protocols

The point of attachment of a 6LN may be a 6LR in an LLN mesh. IPv6 routing in an LLN can be based on RPL, which is the routing protocol that was defined at the IETF for this particular purpose. Other routing protocols than RPL are also considered by Standard Defining Organizations (SDO) on the basis of the expected network characteristics. It is required that a 6LoWPAN Node attached via ND to a 6LR would need to participate in the selected routing protocol to obtain reachability via the 6LR.

Next to the 6LBR unicast address registered by ND, other addresses including multicast addresses are needed as well. For example a routing protocol often uses a multicast address to register changes to established paths. ND needs to register such a multicast address to enable routing concurrently with discovery.

Multicast is needed for groups. Groups MAY be formed by device type (e.g. routers, street lamps), location (Geography, RPL sub-tree), or both.

The Bit Index Explicit Replication (BIER) Architecture [I-D.ietf-bier-architecture] proposes an optimized technique to enable multicast in a LLN with a very limited requirement for routing state in the nodes.
Related requirements are:

Req2.1: The ND registration method SHOULD be extended in such a fashion that the 6LR MAY advertise the Address of a 6LoWPAN Node over the selected routing protocol and obtain reachability to that Address using the selected routing protocol.

Req2.2: Considering RPL, the Address Registration Option that is used in the ND registration SHOULD be extended to carry enough information to generate a DAO message as specified in [RFC6550] section 6.4, in particular the capability to compute a Path Sequence and, as an option, a RPLInstanceID.

Req2.3: Multicast operations SHOULD be supported and optimized, for instance using BIER or MPL. Whether ND is appropriate for the registration to the 6BBR is to be defined, considering the additional burden of supporting the Multicast Listener Discovery Version 2 [RFC3810] (MLDv2) for IPv6.

B.3. Requirements Related to the Variety of Low-Power Link types

6LoWPAN ND [RFC6775] was defined with a focus on IEEE Std.802.15.4 and in particular the capability to derive a unique Identifier from a globally unique MAC-64 address. At this point, the 6lo Working Group is extending the 6LoWPAN Header Compression (HC) [RFC6282] technique to other link types ITU-T G.9959 [RFC7428], Master-Slave/Token-Passing [RFC8163], DECT Ultra Low Energy [RFC8105], Near Field Communication [I-D.ietf-6lo-nfc], IEEE Std. 802.11ah [I-D.delcarpio-6lo-wlanah], as well as IEEE1901.2 Narrowband Powerline Communication Networks [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks] and BLUETOOTH(R) Low Energy [RFC7668].

Related requirements are:

Req3.1: The support of the registration mechanism SHOULD be extended to more LLN links than IEEE Std.802.15.4, matching at least the LLN links for which an "IPv6 over foo" specification exists, as well as Low-Power Wi-Fi.

Req3.2: As part of this extension, a mechanism to compute a unique Identifier should be provided, with the capability to form a Link-Local Address that SHOULD be unique at least within the LLN connected to a 6LBR discovered by ND in each node within the LLN.

Req3.3: The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of unique Identifier.
Req3.4: The Neighbour Discovery should specify the formation of a site-local address that follows the security recommendations from [RFC7217].

B.4. Requirements Related to Proxy Operations

Duty-cycled devices may not be able to answer themselves to a lookup from a node that uses classical ND on a Backbone and may need a proxy. Additionally, the duty-cycled device may need to rely on the 6LBR to perform registration to the 6BBR.

The ND registration method SHOULD defend the addresses of duty-cycled devices that are sleeping most of the time and not capable to defend their own Addresses.

Related requirements are:

Req4.1: The registration mechanism SHOULD enable a third party to proxy register an Address on behalf of a 6LoWPAN node that may be sleeping or located deeper in an LLN mesh.

Req4.2: The registration mechanism SHOULD be applicable to a duty-cycled device regardless of the link type, and enable a 6BBR to operate as a proxy to defend the Registered Addresses on its behalf.

Req4.3: The registration mechanism SHOULD enable long sleep durations, in the order of multiple days to a month.

B.5. Requirements Related to Security

In order to guarantee the operations of the 6LoWPAN ND flows, the spoofing of the 6LR, 6LBR and 6BBRs roles should be avoided. Once a node successfully registers an address, 6LoWPAN ND should provide energy-efficient means for the 6LBR to protect that ownership even when the node that registered the address is sleeping.

In particular, the 6LR and the 6LBR then should be able to verify whether a subsequent registration for a given Address comes from the original node.

In a LLN it makes sense to base security on layer-2 security. During bootstrap of the LLN, nodes join the network after authorization by a Joining Assistant (JA) or a Commissioning Tool (CT). After joining nodes communicate with each other via secured links. The keys for the layer-2 security are distributed by the JA/CT. The JA/CT can be part of the LLN or be outside the LLN. In both cases it is needed that packets are routed between JA/CT and the joining node.
Related requirements are:

Req5.1: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR, 6LBR and 6BBR to authenticate and authorize one another for their respective roles, as well as with the 6LoWPAN Node for the role of 6LR.

Req5.2: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR and the 6LBR to validate new registration of authorized nodes. Joining of unauthorized nodes MUST be impossible.

Req5.3: 6LoWPAN ND security mechanisms SHOULD lead to small packet sizes. In particular, the NS, NA, DAR and DAC messages for a re-registration flow SHOULD NOT exceed 80 octets so as to fit in a secured IEEE Std.802.15.4 [IEEEstd802154] frame.

Req5.4: Recurrent 6LoWPAN ND security operations MUST NOT be computationally intensive on the LoWPAN Node CPU. When a Key hash calculation is employed, a mechanism lighter than SHA-1 SHOULD be preferred.

Req5.5: The number of Keys that the 6LoWPAN Node needs to manipulate SHOULD be minimized.

Req5.6: The 6LoWPAN ND security mechanisms SHOULD enable the variation of CCM [RFC3610] called CCM* for use at both Layer 2 and Layer 3, and SHOULD enable the reuse of security code that has to be present on the device for upper layer security such as TLS.

Req5.7: Public key and signature sizes SHOULD be minimized while maintaining adequate confidentiality and data origin authentication for multiple types of applications with various degrees of criticality.

Req5.8: Routing of packets should continue when links pass from the unsecured to the secured state.

Req5.9: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR and the 6LBR to validate whether a new registration for a given address corresponds to the same 6LoWPAN Node that registered it initially, and, if not, determine the rightful owner, and deny or clean-up the registration that is duplicate.

B.6. Requirements Related to Scalability

Use cases from Automatic Meter Reading (AMR, collection tree operations) and Advanced Metering Infrastructure (AMI, bi-directional communication to the meters) indicate the needs for a large number of
LLN nodes pertaining to a single RPL DODAG (e.g. 5000) and connected to the 6LBR over a large number of LLN hops (e.g. 15).

Related requirements are:

Req6.1: The registration mechanism SHOULD enable a single 6LBR to register multiple thousands of devices.

Req6.2: The timing of the registration operation should allow for a large latency such as found in LLNs with ten and more hops.

Authors’ Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Sophia Antipolis
FRANCE

Email: pthubert@cisco.com

Erik Nordmark
Santa Clara, CA
USA

Email: nordmark@sonic.net

Samita Chakrabarti
San Jose, CA
USA

Email: samitac.ietf@gmail.com
IPv6 over Constrained Node Networks (6lo) Applicability & Use cases
draft-ietf-6lo-use-cases-02

Abstract

This document describes the applicability of IPv6 over constrained node networks (6lo) and provides practical deployment examples. In addition to IEEE 802.15.4, various link layer technologies such as ITU-T G.9959 (Z-Wave), BLE, DECT-ULE, MS/TP, NFC, PLC (IEEE 1901), and IEEE 802.15.4e (6tisch) are used as examples. The document targets an audience who like to understand and evaluate running end-to-end IPv6 over the constrained link layer networks connecting devices to each other or to each cloud.

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 http://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 January 4, 2018.
1. Introduction ............................. 3
2. Conventions and Terminology .................. 4
3. 6lo Link layer technologies and possible candidates ... 4
   3.1. ITU-T G.9959 (specified) ................. 4
   3.2. Bluetooth LE (specified) ................ 4
   3.3. DECT-ULE (specified) .................... 5
   3.4. MS/TP (specified) ....................... 5
   3.5. NFC (specified) ......................... 6
   3.6. PLC (specified) .......................... 6
   3.7. IEEE 802.15.4e (specified) ............... 7
   3.8. LTE MTC (example of a potential candidate) 8
   3.9. Comparison between 6lo Link layer technologies ... 8
4. 6lo Deployment Scenarios ..................... 9
   4.1. jupitermesh in Smart Grid using 6lo in network layer .. 9
   4.2. Wi-SUN usage of 6lo stacks ................ 11
5. Design Space and Guidelines for 6lo Deployment .......... 12
   5.1. Design Space Dimensions for 6lo Deployment .......... 12
   5.2. Guidelines for adopting IPv6 stack (6lo/6LoWPAN) ........ 14
6. 6lo Use Case Examples ........................ 16
7. IANA Considerations .......................... 16
8. Security Considerations ....................... 17
9. Acknowledgements ............................ 17
10. References ................................... 17
   10.1. Normative References .................... 17
   10.2. Informative References .................. 19
Appendix A. Other 6lo Use Case Examples ............... 21
   A.1. Use case of ITU-T G.9959: Smart Home ........... 21
   A.2. Use case of DECT-ULE: Smart Home ............. 22
   A.3. Use case of MS/TP: Management of District Heating .... 22
   A.4. Use case of NFC: Alternative Secure Transfer .... 23
   A.5. Use case of PLC: Smart Grid ................ 23
1. Introduction

Running IPv6 on constrained node networks has different features from general node networks due to the characteristics of constrained node networks such as small packet size, short link-layer address, low bandwidth, network topology, low power, low cost, and large number of devices [RFC4919][RFC7228]. For example, some IEEE 802.15.4 link layers have a frame size of 127 octets and IPv6 requires the layer below to support an MTU of 1280 bytes, therefore an appropriate fragmentation and reassembly adaptation layer must be provided at the layer below IPv6. Also, the limited size of IEEE 802.15.4 frame and low energy consumption requirements make the need for header compression. The IETF 6LoWPAN (IPv6 over Low power WPAN) working group published an adaptation layer for sending IPv6 packets over IEEE 802.15.4 [RFC4944], a compression format for IPv6 datagrams over IEEE 802.15.4-based networks [RFC6282], and Neighbor Discovery Optimization for 6LoWPAN [RFC6775].

As IoT (Internet of Things) services become more popular, IPv6 over various link layer technologies such as Bluetooth Low Energy (Bluetooth LE), ITU-T G.9959 (Z-Wave), Digital Enhanced Cordless Telecommunications - Ultra Low Energy (DECT-ULE), Master-Slave/Token Passing (MS/TP), Near Field Communication (NFC), Power Line Communication (PLC), and IEEE 802.15.4e (TSCH), have been defined at [IETF_6lo] working group. IPv6 stacks for constrained node networks use a variation of the 6LoWPAN stack applied to each particular link layer technology.

In the 6LoWPAN working group, the [RFC6568], "Design and Application Spaces for 6LoWPANs" was published and it describes potential application scenarios and use cases for low-power wireless personal area networks. Hence, this 6lo applicability document aims to provide guidance to an audience who is new to IPv6-over-lowpower networks concept and wants to assess if variance of 6LoWPAN stack [6lo] can be applied to the constrained L2 network of their interest. This 6lo applicability document puts together various design space dimensions such as deployment, network size, power source, connectivity, multi-hop communication, traffic pattern, security level, mobility, and QoS requirements etc. And it described a few set of 6LoWPAN application scenarios and practical deployment as examples.

This document provides the applicability and use cases of 6lo, considering the following aspects:
o 6lo applicability and use cases MAY be uniquely different from those of 6LoWPAN defined for IEEE 802.15.4.

o It SHOULD cover various IoT related wire/wireless link layer technologies providing practical information of such technologies.

o A general guideline on how the 6LoWPAN stack can be modified for a given L2 technology.

o Example use cases and practical deployment examples.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. 6lo Link layer technologies and possible candidates

3.1. ITU-T G.9959 (specified)

The ITU-T G.9959 recommendation [G.9959] targets low-power Personal Area Networks (PANs). G.9959 defines how a unique 32-bit HomeID network identifier is assigned by a network controller and how an 8-bit NodeID host identifier is allocated to each node. NodeIDs are unique within the network identified by the HomeID. The G.9959 HomeID represents an IPv6 subnet that is identified by one or more IPv6 prefixes [RFC7428]. The ITU-T G.9959 can be used for smart home applications.

3.2. Bluetooth LE (specified)

Bluetooth LE was introduced in Bluetooth 4.0, enhanced in Bluetooth 4.1, and developed even further in successive versions. Bluetooth SIG has also published Internet Protocol Support Profile (IPSP). The IPSP enables discovery of IP-enabled devices and establishment of link-layer connection for transporting IPv6 packets. IPv6 over Bluetooth LE is dependent on both Bluetooth 4.1 and IPSP 1.0 or newer.

Devices such as mobile phones, notebooks, tablets and other handheld computing devices which will include Bluetooth 4.1 chipsets will probably also have the low-energy variant of Bluetooth. Bluetooth LE will also be included in many different types of accessories that collaborate with mobile devices such as phones, tablets and notebook computers. An example of a use case for a Bluetooth LE accessory is a heart rate monitor that sends data via the mobile phone to a server.
A typical usage of Bluetooth LE is smartphone-based interaction with constrained devices.

3.3. DECT-ULE (specified)

DECT ULE is a low power air interface technology that is designed to support both circuit switched services, such as voice communication, and packet mode data services at modest data rate.

The DECT ULE protocol stack consists of the PHY layer operating at frequencies in the 1880 - 1920 MHz frequency band depending on the region and uses a symbol rate of 1.152 Mbps. Radio bearers are allocated by use of FDMA/TDMA/TDD techniques.

In its generic network topology, DECT is defined as a cellular network technology. However, the most common configuration is a star network with a single Fixed Part (FP) defining the network with a number of Portable Parts (PP) attached. The MAC layer supports traditional DECT as this is used for services like discovery, pairing, security features etc. All these features have been reused from DECT.

The DECT ULE device can switch to the ULE mode of operation, utilizing the new ULE MAC layer features. The DECT ULE Data Link Control (DLC) provides multiplexing as well as segmentation and re-assembly for larger packets from layers above. The DECT ULE layer also implements per-message authentication and encryption. The DLC layer ensures packet integrity and preserves packet order, but delivery is based on best effort.

The current DECT ULE MAC layer standard supports low bandwidth data broadcast. However the usage of this broadcast service has not yet been standardized for higher layers [RFC8105]. DECT-ULE can be used for smart metering in a home.

3.4. MS/TP (specified)

MS/TP is a contention-free access method for the RS-485 physical layer, which is used extensively in building automation networks.

An MS/TP device is typically based on a low-cost microcontroller with limited processing power and memory. Together with low data rates and a small address space, these constraints are similar to those faced in 6lowpan networks and suggest some elements of that solution might be leveraged. MS/TP differs significantly from 6lowpan in at least three aspects: a) MS/TP devices typically have a continuous source of power, b) all MS/TP devices on a segment can communicate directly so there are no hidden node or mesh routing issues, and c)
recent changes to MS/TP provide support for large payloads, eliminating the need for link-layer fragmentation and reassembly.

MS/TP is designed to enable multidrop networks over shielded twisted pair wiring, although not according to standards, in lower speeds, normally 9600 bit/s, re-purposed telecom wiring is widely in use, keeping deployment cost down. It can support a data rate of 115,200 baud on segments up to 1000 meters in length, or segments up to 1200 meters in length at lower baud rates. An MS/TP link requires only a UART, an RS-485 transceiver with a driver that can be disabled, and a 5ms resolution timer. These features make MS/TP a cost-effective and very reliable field bus for the most numerous and least expensive devices in a building automation network [RFC8163]. MS/TP can be used for the management of district heating.

3.5. NFC (specified)

NFC technology enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and it enables a consumer to utilize one device across different systems.

Extending the capability of contactless card technology, NFC also enables devices to share information at a distance that is less than 10 cm with a maximum communication speed of 424 kbps. Users can share business cards, make transactions, access information from a smart poster or provide credentials for access control systems with a simple touch.

NFC’s bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch. In addition to the easy connection and quick transactions, simple data sharing is also available [I-D.ietf-6lo-nfc]. NFC can be used for secure transfer in healthcare services.

3.6. PLC (specified)

Unlike other dedicated communication infrastructure, the required medium (power conductor) is widely available indoors and outdoors. Moreover, wired technologies are more susceptible to cause interference but are more reliable than their wireless counterparts. PLC is a data transmission technique that utilizes power conductors as medium.
The below table shows some available open standards defining PLC.

<table>
<thead>
<tr>
<th>PLC Systems</th>
<th>Frequency Range</th>
<th>Type</th>
<th>Data Rate</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE1901</td>
<td>&lt;100MHz</td>
<td>Broadband</td>
<td>200Mbps</td>
<td>1000m</td>
</tr>
<tr>
<td>IEEE1901.1</td>
<td>&lt;15MHz</td>
<td>PLC-IoT</td>
<td>10Mbps</td>
<td>2000m</td>
</tr>
<tr>
<td>IEEE1901.2</td>
<td>&lt;500kHz</td>
<td>Narrowband</td>
<td>200Kbps</td>
<td>3000m</td>
</tr>
</tbody>
</table>

Table 1: Some Available Open Standards in PLC

[IEEE1901] defines broadband variant of PLC but is effective within short range. This standard addresses the requirements of applications with high data rate such as: Internet, HDTV, Audio, Gaming etc. Broadband operates on OFDM (Orthogonal Frequency Division Multiplexing) modulation.

[IEEE1901.2] defines narrowband variant of PLC with less data rate but significantly higher transmission range that could be used in an indoor or even an outdoor environment. It is applicable to typical IoT applications such as: Building Automation, Renewable Energy, Advanced Metering, Street Lighting, Electric Vehicle, Smart Grid etc. Moreover, IEEE 1901.2 standard is based on the 802.15.4 MAC sub-layer and fully endorses the security scheme defined in 802.15.4. [RFC8036]. A typical use case of PLC is smart grid.

3.7.  IEEE 802.15.4e (specified)

The Time Slotted Channel Hopping (TSCH) mode was introduced in the IEEE 802.15.4-2015 standard. In a TSCH network, all nodes are synchronized. Time is sliced up into timeslots. The duration of a timeslot, typically 10ms, is large enough for a node to send a full-sized frame to its neighbor, and for that neighbor to send back an acknowledgment to indicate successful reception. Timeslots are grouped into one of more slotframes, which repeat over time.

All the communication in the network is orchestrated by a communication schedule which indicates to each node what to do in each of the timeslots of a slotframe: transmit, listen or sleep. The communication schedule can be built so that the right amount of link-layer resources (the cells in the schedule) are scheduled to satisfy the communication needs of the applications running on the network, while keeping the energy consumption of the nodes very low. Cells can be scheduled in a collision-free way, introducing a high level of determinism to the network.
A TSCH network exploits channel hopping: subsequent packet exchanges between neighbor nodes are done on a different frequency. This means that, if a frame isn’t received, the transmitter node will retransmit the frame on a different frequency. The resulting "channel hopping" efficiently combats external interference and multi-path fading.

The main benefits of IEEE 802.15.4 TSCH are:

- ultra high reliability. Off-the-shelf commercial products offer over 99.999% end-to-end reliability.
- ultra low-power consumption. Off-the-shelf commercial products offer over a decade of battery lifetime.
- 6TiSCH at IETF defines communications of TSCH network and it uses 6LoWPAN stack [RFC7554].

IEEE 802.15.4e can be used for industrial automation.

3.8. LTE MTC (example of a potential candidate)

LTE category defines the overall performance and capabilities of the UE (User Equipment). For example, the maximum down rate of category 1 UE and category 2 UE are 10.3 Mbit/s and 51.0 Mbit/s respectively. There are many categories in LTE standard. 3GPP standards defined the category 0 to be used for low rate IoT service in release 12. Since category 1 and category 0 could be used for low rate IoT service, these categories are called LTE MTC (Machine Type Communication) [LTE_MTC].

LTE MTC offer advantages in comparison to above category 2 and is appropriate to be used for low rate IoT services such as low power and low cost. LTE MTC can be used for a gateway of a wireless backhaul network.

3.9. Comparison between 6lo Link layer technologies

In above clauses, various 6lo Link layer technologies and a possible candidate are described. The following table shows that dominant parameters of each use case corresponding to the 6lo link layer technology.
### Table 2: Comparison between 6lo Link layer technologies

<table>
<thead>
<tr>
<th>Usage</th>
<th>Z-Wave</th>
<th>BLE</th>
<th>DECT-ULE</th>
<th>MS/TP</th>
<th>NFC</th>
<th>PLC</th>
<th>TSCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Automation</td>
<td>Home</td>
<td>Interact</td>
<td>Meter Reading</td>
<td>District Heating</td>
<td>Health-care Service</td>
<td>Smart Grid</td>
<td>Industrial Automation</td>
</tr>
<tr>
<td>w/ Smart Phone</td>
<td>Automation</td>
<td>w/ Smart Phone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meter Reading</td>
<td>L2-mesh</td>
<td>Star</td>
<td>L3-mesh</td>
<td>No mesh</td>
<td>No mesh</td>
<td>MS/TP</td>
<td>L2-mesh</td>
</tr>
<tr>
<td>District Heating</td>
<td>Bus</td>
<td>P2P</td>
<td>Tree</td>
<td>Mesh</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health-care Service</td>
<td>High + Privacy required</td>
<td>High + Privacy required</td>
<td>High + Authen. required</td>
<td>High + Encrypt. required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Grid</td>
<td>Moderate</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industrial Automation</td>
<td>High + Privacy required</td>
<td>High + Privacy required</td>
<td>High + Privacy required</td>
<td>High + Privacy required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobility Reqmt</td>
<td>No</td>
<td>Low</td>
<td>No</td>
<td>No</td>
<td>Moderate</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Security Reqmt</td>
<td>High + Privacy required</td>
<td>Partially</td>
<td>High + Privacy required</td>
<td>High + Authen. required</td>
<td>High + Encrypt. required</td>
<td>High + Privacy required</td>
<td></td>
</tr>
<tr>
<td>Buffering Reqmt</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Latency, QoS Reqmt</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Data Rate</td>
<td>Infrequent</td>
<td>Infrequent</td>
<td>Infrequent</td>
<td>Frequent</td>
<td>Small</td>
<td>Infrequent</td>
<td>Infrequent</td>
</tr>
<tr>
<td>RFC # or Draft</td>
<td>RFC7428</td>
<td>RFC7668</td>
<td>RFC8105</td>
<td>RFC8163</td>
<td>6lo-nfc</td>
<td>hou-6lo-plc</td>
<td>RFC7554</td>
</tr>
</tbody>
</table>

4. 6lo Deployment Scenarios

4.1. jupiterMesh in Smart Grid using 6lo in network layer

jupiterMesh is a multi-hop wireless mesh network specification designed mainly for deployment in large geographical areas. Each subnet in jupiterMesh is able to cover an entire neighborhood with thousands of nodes consisting of IPv6-enabled routers and end-points.
(e.g., hosts). Automated network joining and load balancing allows a seamless deployment of a large number of subnets.

The main application domains targeted by jupiterMesh are smart grid and smart cities. This includes, but is not limited to the following applications:

- Automated meter reading
- Distribution Automation (DA)
- Demand-side management (DSM)
- Demand-side response (DSR)
- Power outage reporting
- Street light monitoring and control
- Transformer load management
- EV charging coordination
- Energy theft
- Parking space locator

jupiterMesh specification is based on the following technologies:

- The PHY layer is based on IEEE 802.15.4 SUN specification [IEEE 802.15.4-2015], supporting multiple operating modes for deployment in different regulatory domains and deployment scenarios in terms of density and bandwidth requirements. jupiterMesh supports bit rates from 50 kbps to 800 kbps, frame size up to 2048 bytes, up to 11 different RF bands and 3 modulation types (i.e., FSK, OQPSK and OFDM).

- The MAC layer is based on IEEE 802.15.4 TSCH specification [IEEE 802.15.4-2015]. With frequency hopping capability, TSCH MAC supports scheduling of dedicated timeslot enabling bandwidth management and QoS.

- The security layer consists of a certificate-based (i.e. X.509) network access authentication using EAP-TLS, with IEEE 802.15.9-based KMP (Key Management Protocol) transport, and PANA and link layer encryption using AES-128 CCM as specified in IEEE 802.15.4-2015 [IEEE 802.15.4-2015].
Address assignment and network configuration are specified using DHCPv6 [RFC3315]. Neighbor Discovery (ND) [RFC6775] and stateless address auto-configuration (SLAAC) are not supported.

- The network layer consists of IPv6, ICPMv6 and 6lo/6LoPWAN header compression [RFC6282]. Multicast is supported using MPL. Two domains are supported, a delay sensitive MPL domain for low latency applications (e.g. DSM, DSR) and a delay insensitive one for less stringent applications (e.g. OTA file transfers).

- The routing layer uses RPL [RFC6550] in non-storing mode with the MRHOF objective function based on the ETX metric.

### 4.2. Wi-SUN usage of 6lo stacks

Wireless Smart Ubiquitous Network (Wi-SUN) is a technology based on the IEEE 802.15.4g standard. Wi-SUN networks support star and mesh topologies, as well as hybrid star/mesh deployments, but are typically laid out in a mesh topology where each node relays data for the network to provide network connectivity. Wi-SUN networks are deployed on both powered and battery-operated devices.

The main application domains targeted by Wi-SUN are smart utility and smart city networks. This includes, but is not limited to the following applications:

- Advanced Metering
- Infrastructure (AMI)
- Distribution Automation
- Home Energy Management
- Infrastructure Management
- Intelligent Transportation Systems
- Smart Street Lighting
- Agriculture
- Structural health (bridges, buildings etc)
- Monitoring and Asset Management
- Smart Thermostats, Air Conditioning and Heat Controls
Energy Usage Information Displays

The Wi-SUN Alliance Field Area Network (FAN) covers primarily outdoor networks, and its specification is oriented towards meeting the more rigorous challenges of these environments. Examples include from meter to outdoor access point/router for AMI and DR, or between switches for DA. However, nothing in the profile restricts it to outdoor use. It has the following features:

- Open standards based on IEEE802, IETF, TIA, ETSI
- Architecture is an IPv6 frequency hopping wireless mesh network with enterprise level security
- Simple infrastructure which is low cost, low complexity
- Enhanced network robustness, reliability, and resilience to interference, due to high redundancy and frequency hopping
- Enhanced scalability, long range, and energy friendliness
- Supports multiple global license-exempt sub GHz bands
- Multi-vendor interoperability
- Very low power modes in development permitting long term battery operation of network nodes

In the Wi-SUN FAN specification, adaptation layer based on 6lo and IPv6 network layer are described. So, IPv6 protocol suite including TCP/UDP, 6lo Adaptation, Header Compression, DHCPv6 for IP address management, Routing using RPL, ICMPv6, and Unicast/Multicast forwarding is utilized.

5. Design Space and Guidelines for 6lo Deployment

5.1. Design Space Dimensions for 6lo Deployment

The [RFC6568] lists the dimensions used to describe the design space of wireless sensor networks in the context of the 6LoWPAN working group. The design space is already limited by the unique characteristics of a LoWPAN (e.g., low power, short range, low bit rate). In [RFC6568], the following design space dimensions are described; Deployment, Network size, Power source, Connectivity, Multi-hop communication, Traffic pattern, Mobility, Quality of Service (QoS). However, in this document, the following design space dimensions are considered:
Deployment/Bootstrapping: 6lo nodes can be connected randomly, or in an organized manner. The bootstrapping has different characteristics for each link layer technology.

Topology: Topology of 6lo networks may inherently follow the characteristics of each link layer technology. Point-to-point, star, tree or mesh topologies can be configured, depending on the link layer technology considered.

L2-Mesh or L3-Mesh: L2-mesh and L3-mesh may inherently follow the characteristics of each link layer technology. Some link layer technologies may support L2-mesh and some may not support.

Multi-link subnet, single subnet: The selection of multi-link subnet and single subnet depends on connectivity and the number of 6lo nodes.

Data rate: Originally, the link layer technologies of 6lo have low rate of data transmission. But, by adjusting the MTU, it can deliver higher data rate.

Buffering requirements: Some 6lo use case may require more data rate than the link layer technology support. In this case, a buffering mechanism to manage the data is required.

Security and Privacy Requirements: Some 6lo use case can involve transferring some important and personal data between 6lo nodes. In this case, high-level security support is required.

Mobility across 6lo networks and subnets: The movement of 6lo nodes is dependent on the 6lo use case. If the 6lo nodes can move or moved around, it requires a mobility management mechanism.

Time synchronization requirements: The requirement of time synchronization of the upper layer service is dependent on the 6lo use case. For some 6lo use case related to health service, the measured data must be recorded with exact time and must be transferred with time synchronization.

Reliability and QoS: Some 6lo use case requires high reliability, for example real-time service or health-related services.

Traffic patterns: 6lo use cases may involve various traffic patterns. For example, some 6lo use case may require short data length and random transmission. Some 6lo use case may require continuous data and periodic data transmission.
Security Bootstrapping: Without the external operations, 6lo nodes must have the security bootstrapping mechanism.

Power use strategy: to enable certain use cases, there may be requirements on the class of energy availability and the strategy followed for using power for communication [RFC7228]. Each link layer technology defines a particular power use strategy which may be tuned [I-D.ietf-lwig-energy-efficient]. Readers are expected to be familiar with [RFC7228] terminology.

Update firmware requirements: Most 6lo use cases will need a mechanism for updating firmware. In these cases support for over the air updates are required, probably in a broadcast mode when bandwidth is low and the number of identical devices is high.

5.2. Guidelines for adopting IPv6 stack (6lo/6LoWPAN)

The following guideline targets candidates for new constrained L2 technologies that consider running modified 6LoWPAN stack. The modification of 6LoWPAN stack should be based on the following:

Addressing Model: Addressing model determines whether the device is capable of forming IPv6 Link-local and global addresses and what is the best way to derive the IPv6 addresses for the constrained L2 devices. Whether the device is capable of forming IPv6 Link-local and global addresses, L2-address-derived IPv6 addresses are specified in [RFC4944], but there exist implications for privacy. For global usage, a unique IPv6 address must be derived using an assigned prefix and a unique interface ID. [RFC8065] provides such guidelines. For MAC derived IPv6 address, please refer to [RFC8163] for IPv6 address mapping examples. Broadcast and multicast support are dependent on the L2 networks. Most lowpower L2 implementations map multicast to broadcast networks. So care must be taken in the design when to use broadcast and try to stick to unicast messaging whenever possible.

MTU Considerations: The deployment SHOULD consider their need for maximum transmission unit of a packet (MTU) over the link layer and should consider if fragmentation and reassembly of packets are needed at the 6LoWPAN layer. For example, if the link-layer supports fragmentation and reassembly of packets, then 6LoWPAN layer may skip supporting fragmentation/reassembly. In fact, for most efficiency, choosing a low-power link-layer that can carry unfragmented application packets would be optimum for packet transmission if the deployment can afford it. Please refer to 6lo RFCs [RFC7668], [RFC8163], [RFC8105] for example guidance.
Mesh or L3-Routing: 6LoWPAN specifications do provide mechanisms to support for mesh routing at L2. [RFC6550] defines L3 routing for low power lossy networks using directed graphs. 6LoWPAN is routing protocol agnostic and other L2 or L3 routing protocols can be run using a 6LoWPAN stack.

Address Assignment: 6LoWPAN requires that IPv6 Neighbor Discovery for low power networks [RFC6775] be used for autoconfiguration of stateless IPv6 address assignment. Considering the energy sensitive networks [RFC6775] makes optimization from classical IPv6 ND [RFC4861] protocol. It is the responsibility of the deployment to ensure unique global IPv6 addresses for the Internet connectivity. For local-only connectivity IPv6 ULA may be used. [RFC6775] specifies the 6LoWPAN border router (6LBR) which is responsible for prefix assignment to the 6lo/6LoWPAN network. 6LBR can be connected to the Internet or Enterprise network via its one of the interfaces. Please refer to [RFC7668] and [RFC8105] for examples of address assignment considerations. In addition, privacy considerations [RFC8065] must be consulted for applicability. In certain scenarios, the deployment may not support autoconfiguration of IPv6 addressing due to regulatory and business reasons and may choose to offer a separate address assignment service.

Header Compression: IPv6 header compression [RFC6282] is a vital part of IPv6 over low power communication. Examples of header compression for different link-layers specifications are found in [RFC7668], [RFC8163], [RFC8105]. A generic header compression technique is specified in [RFC7400].

Security and Encryption: Though 6LoWPAN basic specifications do not address security at network layer, the assumption is that L2 security must be present. In addition, application level security is highly desirable. The working groups [ace] and [core] should be consulted for application and transport level security. 6lo working group is working on address authentication [6lo-ap-nd] and secure bootstrapping is also being discussed at IETF. However, there may be different levels of security available in a deployment through other standards such as hardware level security or certificates for initial booting process. Encryption is quite important if the implementation can afford it.

Additional processing: [RFC8066] defines guidelines for ESC dispatch octets use in the 6LoWPAN header. An implementation may take advantage of ESC header to offer a deployment specific processing of 6LoWPAN packets.
6. 6lo Use Case Examples

As IPv6 stacks for constrained node networks use a variation of the 6LoWPAN stack applied to each particular link layer technology, various 6lo use cases can be provided. In this clause, one 6lo use case example of Bluetooth LE (Smartphone-Based Interaction with Constrained Devices) is described. Other 6lo use case examples are described in Appendix.

The key feature behind the current high Bluetooth LE momentum is its support in a large majority of smartphones in the market. Bluetooth LE can be used to allow the interaction between the smartphone and surrounding sensors or actuators. Furthermore, Bluetooth LE is also the main radio interface currently available in wearables. Since a smartphone typically has several radio interfaces that provide Internet access, such as Wi-Fi or 4G, the smartphone can act as a gateway for nearby devices such as sensors, actuators or wearables. Bluetooth LE may be used in several domains, including healthcare, sports/wellness and home automation.

Example: Use of Bluetooth LE-based Body Area Network for fitness

A person wears a smartwatch for fitness purposes. The smartwatch has several sensors (e.g. heart rate, accelerometer, gyrometer, GPS, temperature, etc.), a display, and a Bluetooth LE radio interface. The smartwatch can show fitness-related statistics on its display. However, when a paired smartphone is in the range of the smartwatch, the latter can report almost real-time measurements of its sensors to the smartphone, which can forward the data to a cloud service on the Internet. In addition, the smartwatch can receive notifications (e.g. alarm signals) from the cloud service via the smartphone. On the other hand, the smartphone may locally generate messages for the smartwatch, such as e-mail reception or calendar notifications.

The functionality supported by the smartwatch may be complemented by other devices such as other on-body sensors, wireless headsets or head-mounted displays. All such devices may connect to the smartphone creating a star topology network whereby the smartphone is the central component.

7. IANA Considerations

There are no IANA considerations related to this document.
8. Security Considerations

Security considerations are not directly applicable to this document. The use cases will use the security requirements described in the protocol specifications.

9. Acknowledgements

Carles Gomez has been funded in part by the Spanish Government (Ministerio de Educacion, Cultura y Deporte) through the Jose Castillejo grant CAS15/00336. His contribution to this work has been carried out in part during his stay as a visiting scholar at the Computer Laboratory of the University of Cambridge.

Thomas Watteyne, Pascal Thubert, Xavier Vilajosana, Daniel Migault, and Jianqiang HOU have provided valuable feedback for this draft.

Das Subir and Michel Veillette have provided valuable information of jupiterMesh and Paul Duffy has provided valuable information of Wi-SUN for this draft.

10. References

10.1. Normative References


10.2. Informative References


[I-D.ietf-6tisch-6top-sf0] Dujovne, D., Grieco, L., Palattella, M., and N. Accettura, "6TiSCH 6top Scheduling Function Zero (SF0)", draft-ietf-6tisch-6top-sf0-04 (work in progress), April 2017.


A.1. Use case of ITU-T G.9959: Smart Home

Z-Wave is one of the main technologies that may be used to enable smart home applications. Born as a proprietary technology, Z-Wave was specifically designed for this particular use case. Recently, the Z-Wave radio interface (physical and MAC layers) has been standardized as the ITU-T G.9959 specification.

Example: Use of ITU-T G.9959 for Home Automation

Variety of home devices (e.g. light dimmers/switches, plugs, thermostats, blinds/curtains and remote controls) are augmented with ITU-T G.9959 interfaces. A user may turn on/off or may control home appliances by pressing a wall switch or by pressing a button in a remote control. Scenes may be programmed, so that after a given event, the home devices adopt a specific configuration. Sensors may also periodically send measurements of several parameters (e.g. gas presence, light, temperature, humidity, etc.) which are collected at a sink device, or may generate commands for actuators (e.g. a smoke sensor may send an alarm message to a safety system).

The devices involved in the described scenario are nodes of a network that follows the mesh topology, which is suitable for path diversity to face indoor multipath propagation issues. The multihop paradigm allows end-to-end connectivity when direct range communication is not possible. Security support is required, specially for safety-related communication. When a user interaction (e.g. a button press) triggers a message that encapsulates a command, if the message is
lost, the user may have to perform further interactions to achieve the desired effect (e.g. a light is turned off). A reaction to a user interaction will be perceived by the user as immediate as long as the reaction takes place within 0.5 seconds [RFC5826].

A.2. Use case of DECT-ULE: Smart Home

DECT is a technology widely used for wireless telephone communications in residential scenarios. Since DECT-ULE is a low-power variant of DECT, DECT-ULE can be used to connect constrained devices such as sensors and actuators to a Fixed Part, a device that typically acts as a base station for wireless telephones. Therefore, DECT-ULE is specially suitable for the connected home space in application areas such as home automation, smart metering, safety, healthcare, etc.

Example: Use of DECT-ULE for Smart Metering

The smart electricity meter of a home is equipped with a DECT-ULE transceiver. This device is in the coverage range of the Fixed Part of the home. The Fixed Part can act as a router connected to the Internet. This way, the smart meter can transmit electricity consumption readings through the DECT-ULE link with the Fixed Part, and the latter can forward such readings to the utility company using Wide Area Network (WAN) links. The meter can also receive queries from the utility company or from an advanced energy control system controlled by the user, which may also be connected to the Fixed Part via DECT-ULE.

A.3. Use case of MS/TP: Management of District Heating

The key feature of MS/TP is its ability to run on the same cabling as BACnet and some use of ModBus, the de facto standard for low bandwidth industry communication. Specially Modbus has been around since the 1980 and is still the standard for talking to fans, heat pumps, water purifying equipment and everything else delivering electricity, clean water and ventilation.

Example: Use of MS/TP for management of district heating

The mechanical room in the cellar of an apartment building gets district heating and electricity from the utility providers. The room has a Supervisory Control And Data Acquisition (SCADA) computer talking to a centralized server and command center somewhere else over IP, on the other hand it is controlling the heating, fans and distribution panel over a 2-wire RS-485 based protocol to make sure the logic controller for district heating keeps a constant temperature at the tapwater, the logic controller for heat produktion
keeps the right radiator temperature depending on the weather and the fans have a correct speed and are switched off in case district heating fails to prevent cooling out the building and give certain commands in case smoke is detected. Speed is not important, in this use case, 19,200 bit/s capable equipment is sold as high speed communication capable. Reliability is important, this not working will easily give millions of dollars of damage. Normally the setup is that the SCADA device asks a question to a specific controlling device, gets an answer from the controlling device, asks a new question to some other device.

A.4. Use case of NFC: Alternative Secure Transfer

According to applications, various secured data can be handled and transferred. Depending on security level of the data, methods for transfer can be alternatively selected.

Example: Use of NFC for Secure Transfer in Healthcare Services with Tele-Assistance

A senior citizen who lives alone wears one to several wearable 6lo devices to measure heartbeat, pulse rate, etc. The 6lo devices are densely installed at home for movement detection. An LoWPAN Border Router (LBR) at home will send the sensed information to a connected healthcare center. Portable base stations with LCDs may be used to check the data at home, as well. Data is gathered in both periodic and event-driven fashion. In this application, event-driven data can be very time-critical. In addition, privacy also becomes a serious issue in this case, as the sensed data is very personal.

While the senior citizen is provided audio and video healthcare services by a tele-assistance based on LTE connections, the senior citizen can alternatively use NFC connections to transfer the personal sensed data to the tele-assistance. At this moment, hidden hackers can overhear the data based on the LTE connection, but they cannot gather the personal data over the NFC connection.

A.5. Use case of PLC: Smart Grid

Smart grid concept is based on numerous operational and energy measuring sub-systems of an electric grid. It comprises of multiple administrative levels/segments to provide connectivity among these numerous components. Last mile connectivity is established over LV segment, whereas connectivity over electricity distribution takes place in HV segment.

Although other wired and wireless technologies are also used in Smart Grid (Advance Metering Infrastructure – AMI, Demand Response – DR,
Home Energy Management System - HEMS, Wide Area Situational Awareness - WASA etc), PLC enjoys the advantage of existing (power conductor) medium and better reliable data communication. PLC is a promising wired communication technology in that the electrical power lines are already there and the deployment cost can be comparable to wireless technologies. The 6lo related scenarios lie in the low voltage PLC networks with most applications in the area of Advanced Metering Infrastructure, Vehicle-to-Grid communications, in-home energy management and smart street lighting.

Example: Use of PLC for Advanced Metering Infrastructure

Household electricity meters transmit time-based data of electric power consumption through PLC. Data concentrators receive all the meter data in their corresponding living districts and send them to the Meter Data Management System (MDMS) through WAN network (e.g. Medium-Voltage PLC, Ethernet or GPRS) for storage and analysis. Two-way communications are enabled which means smart meters can do actions like notification of electricity charges according to the commands from the utility company.

With the existing power line infrastructure as communication medium, cost on building up the PLC network is naturally saved, and more importantly, labor operational costs can be minimized from a long-term perspective. Furthermore, this AMI application speeds up electricity charge, reduces losses by restraining power theft and helps to manage the health of the grid based on line loss analysis.

Example: Use of PLC (IEEE1901.1) for WASA in Smart Grid

Many sub-systems of Smart Grid require low data rate and narrowband variant (IEEE1901.2) of PLC fulfils such requirements. Recently, more complex scenarios are emerging that require higher data rates.

WASA sub-system is an appropriate example that collects large amount of information about the current state of the grid over wide area from electric substations as well as power transmission lines. The collected feedback is used for monitoring, controlling and protecting all the sub-systems.

A.6. Use case of IEEE 802.15.4e: Industrial Automation

Typical scenario of Industrial Automation where sensor and actuators are connected through the time-slotted radio access (IEEE 802.15.4e). For that, there will be a point-to-point control signal exchange in between sensors and actuators to trigger the critical control information. In such scenarios, point-to-point traffic flows are
significant to exchange the controlled information in between sensors and actuators within the constrained networks.

Example: Use of IEEE 802.15.4e for P2P communication in closed-loop application

AODV-RPL [I-D.ietf-roll-aodv-rpl] is proposed as a standard P2P routing protocol to provide the hop-by-hop data transmission in closed-loop constrained networks. Scheduling Functions i.e. SF0 [I-D.ietf-6tisch-6top-sf0] and SF1 [I-D.satish-6tisch-6top-sf1] is proposed to provide distributed neighbor-to-neighbor and end-to-end resource reservations, respectively for traffic flows in deterministic networks (6TiSCH).

The potential scenarios that can make use of the end-to-end resource reservations can be in health-care and industrial applications. AODV-RPL and SF0/SF1 are the significant routing and resource reservation protocols for closed-loop applications in constrained networks.

Authors’ Addresses

Yong-Geun Hong
ETRI
161 Gajeong-Dong Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 6557
Email: yghong@etri.re.kr

Carles Gomez
Universitat Politecnica de Catalunya/Fundacio i2cat
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: carlesgo@entel.upc.edu
Transmission of IPv6 Packets over Wireless Body Area Networks (WBANs)  
draft-sajjad-6lo-wban-00

Abstract

Wireless Body Area Networks (WBANs) intend to facilitate use cases related to medical field. IEEE 802.15.6 defines PHY and MAC layer and is designed to deal with better penetration through the human tissue without creating any damage to human tissues with the approved MICS (Medical Implant Communication Service) band by USA Federal Communications Commission (FCC). Devices in WBANs conform to this IEEE standard.

This specification defines details to enable transmission of IPv6 packets, method of forming link-local and statelessly autoconfigured IPv6 addresses on WBANs.

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 http://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 December 15, 2017.
1. Introduction

Wireless Body Area Networks (WBANs) are comprised of devices that conform to the [IEEE802.15.6], standard by the IEEE. IEEE 802.15.6 provides specification for the MAC layer to access the channel. The
coordinator divides the channel into superframe time structures to allocate resources [SURVEY-WBAN] [MAC-WBAN]. Superframes are bounded by equal length beacons through the coordinator. Usually beacons are sent at beacon periods except inactive superframes or limited by regulation. This standard works under following three channel access modes.

Task group for 802.15.6 was established by IEEE in November 2007 for standardisation of WBANs and it was approved in 2012. This standard works in and around human body and focus on operating at lower frequencies and short range. The focus of this standard is to design a communication standard for MAC and physical layer to support different applications, namely, medical and no-medical applications. Medical applications refer to collection of vital information in real time (monitoring) for diagnoses and treatment of various diseases with help of different sensors (accelerometer, temperature, BP and EMG etc.). It defines a MAC layer that can operate with three different PHY layers i.e. human body communication (HBC), ultra-wideband (UWB) and Narrowband (NB). IEEE 802.15.6 provides specification for MAC layer to access the channel. The coordinator divides the channel into superframe time structures to allocate resources. Superframes are bounded by equal length beacons through coordinator. The purpose of the draft is to highlight the need of IEEE 802.15.6 for WBANs and its integration issues while connecting it with IPv6 network. The use cases are provided to elaborate the scenarios with implantable and wearable biomedical sensors. 6lowpan provides IPv6 connectivity for IEEE 802.15.4; however, it will not work with IEEE 802.15.6 due to the difference in frame format in terms of size and composition.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Use cases for IEEE 802.15.6

3.1. Hospital Patient Monitoring

In the hospital environment, several levels of patient monitoring services are required as different patients need different monitoring services e.g., a patient in Intensive Care Unit (ICU) requires high prioritized periodic data services with limited delay and high throughput than the patient in a normal ward. Usually, a patient is equipped with multiple sensors that measure vital signals like heart activity, muscle movements, blood pressure, body oxygen level and brain stimulation via integrated sensors i.e.,
(Electrocardiography), BP (Blood Pressure) monitor, EMG (Electromyography), pulse oximeter and EEG (Electroencephalography) etc. These sensors are categorized as wearable and implantable sensors, hence we are assuming that equipped sensors are mixture of wearable and implantable sensors which creates restriction to use IEEE 802.15.6 as it is designed to deal with better penetration through the human tissue without creating any damage to human tissues with the approved MICS band by USA Federal Communications Commission (FCC). In a hospital use case scenario, the initial data generated by numerous biomedical sensor nodes is collected by a central coordinator.

In this case, Table 3 presents the summary of traffic patterns for different biomedical sensor nodes attached to human body with data generation rate, required data rate from channel and QoS requirements.

<table>
<thead>
<tr>
<th>Sensor Nodes</th>
<th>Data Generation Interval</th>
<th>Required Data Rate (Kbps)</th>
<th>Delay Requirement</th>
<th>Power Consumption</th>
<th>Reliability Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECG</td>
<td>4 ms</td>
<td>34</td>
<td>&lt;125ms</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>EMG</td>
<td>6 ms</td>
<td>19.6</td>
<td>&lt;125ms</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>EEG</td>
<td>4 ms</td>
<td>19.6</td>
<td>&lt;125ms</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>SpO2 (Pulse Oximeter)</td>
<td>10 ms</td>
<td>13.2</td>
<td>&lt;250ms</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>BP</td>
<td>10 ms</td>
<td>13.2</td>
<td>&lt;250ms</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Respiration</td>
<td>40 ms</td>
<td>3.2</td>
<td>&lt;250ms</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Skin temperature</td>
<td>60 s</td>
<td>2.27</td>
<td>&lt;250ms</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Glucose sensor</td>
<td>250 s</td>
<td>0.528</td>
<td>&lt;250ms</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Table 1: Traffic patterns and requirements of sensor nodes
3.2. Patient monitoring for Chronic Diseases

For a chronic disease patient, the formal procedure of routine visits is required to monitor the progress, development of complications or relapse of the disease. The questions like what, how and when to monitor are really crucial for disease treatment. In this context, various biosensors can be used for monitoring the patient’s physiological conditions which brings relevant information on a regular basis. Appendix A and B shows patient monitoring use case scenario for WBAN.

3.3. Elderly Patient Monitoring

The fast growth in the elderly population will produce a considerable shortage of healthcare experts in the near future. WBAN delivers a highly cost effective solution to monitor the physiological parameters of the elderly persons by seamless integration of their daily routine activities. Moreover, the physician can monitor the health conditions of an elderly person remotely by the courtesy of WBANs.

4. Why 6lo is required for IEEE 802.15.6

Based on the characteristics defined in the overview section, the following sections elaborate on the main problems with IP for WBANs.

4.1. IPv6 Connectivity requirements

The requirement for IPv6 connectivity within WBANs is driven by the following:

- The number of devices in WBANs makes network auto configuration and statelessness highly desirable. And for this, IPv6 has (default auto-configuration as a) ready solutions.
- The large number of devices poses the need for a large address space, moreover a WBAN may consist of 256 nodes maximum and IPv6 is helpful to solve addressing issues.
- Given the limited packet size of WBANs, the IPv6 address format allows subsuming of IEEE 802.15.6 addresses if so desired.
- Simple interconnectivity to other IP networks including the Internet.
- However, given the limited packet size, headers for IPv6 and layers above must be compressed whenever possible.
However, given the limited packet size, headers for IPv6 and layers above must be compressed whenever possible.

4.2. Limited Packet Size

Applications within WBANs are expected to originate small packets. Adding all layers for IP connectivity should still allow transmission in one frame, without incurring excessive fragmentation and reassembly. Furthermore, protocols must be designed or chosen so that the individual "control/protocol packets" fit within a single 802.15.6 frame. Along these lines, IPv6's requirement of sub-IP reassembly may pose challenges for low-end WBANs healthcare devices that do not have enough RAM or storage for a 1280-octet packet [RFC2460].

4.3. Topology requirements

The IEEE 802.15.6 working group has considered WBANs to operate in either a one-hop or two-hop star topology with the node in the centre of the star being placed on a location like the waist. Two feasible types of data transmission exist in the one-hop star topology: transmission from the device to the coordinator and transmission from the coordinator to the device. The communication methods that exist in the star topology are beacon mode and non-beacon mode. In a two-hop start WBAN, a relay-capable node may be used to exchange data frames between a node and the hub.

5. Scope/Purpose

This is a standard for short-range, wireless communication in the vicinity of, or inside, a human body (but not limited to humans). It uses existing industrial scientific medical (ISM) bands as well as frequency bands approved by national medical and/or regulatory authorities. Support for quality of service (QoS), extremely low power, and data rates from 10Kbps to 10 Mbps is required while simultaneously complying with strict non-interference guidelines where needed. The Table 1 shows a comparison of WBAN and other available technologies in terms of data rate and power consumption.
The purpose of this document is to provide an international standard for a short-range (i.e., about human body range), low power, and highly reliable wireless communication for use in close proximity to, or inside, a human body. Data rates, typically up to 10Mbps, can be offered to satisfy an evolutionary set of entertainment and healthcare services. Current personal area networks (PANs) do not meet the medical (proximity to human tissue) and relevant communication regulations for some application environments. They also do not support the combination of reliability, QoS, low power, data rate, and non-interference required to broadly address the breadth of body area network (BAN) applications.

6. Layer 2 Overview

All nodes and hubs (coordinator in 802.15.4) are to be organized into logical sets, referred to as body area networks (BANs) in this specification, and coordinated by their respective hubs for medium access and power management as illustrated in Table 1. There is to be one and only one hub in a BAN, whereas the number of nodes in a BAN is to range from zero to mMaxBANSize. In a one-hop star BAN [SURVEY-WBAN][RFC7326], frame exchanges are to occur directly between nodes and the hub of the BAN. In a two-hop extended star BAN, the hub and a node are to exchange frames optionally via a relay-capable node. Some of the characteristics of WBANs are as follows:

Table 2: Comparison of WBAN

<table>
<thead>
<tr>
<th>Standard</th>
<th>Provided data rate</th>
<th>Power requirement</th>
<th>Battery lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 ac (WiFi)</td>
<td>700 Mbps</td>
<td>100 mW - 1000 mW</td>
<td>Hours - days</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>1Mbps - 10 Mbps</td>
<td>4 mW - 100 mW</td>
<td>Days - weeks</td>
</tr>
<tr>
<td>Wibree</td>
<td>600 Kbps maximum</td>
<td>2 mW - 10 mW</td>
<td>Weeks - months</td>
</tr>
<tr>
<td>ZigBee</td>
<td>250 Kbps maximum</td>
<td>3 mW - 10 mW</td>
<td>Weeks - months</td>
</tr>
<tr>
<td>802.15.4</td>
<td>250 Kbps maximum</td>
<td>3 mW - 10 mW</td>
<td>Weeks - months</td>
</tr>
<tr>
<td>802.15.6</td>
<td>1Kbps - 10 Mbps</td>
<td>0.1 mW - 2 mW</td>
<td>Months - years</td>
</tr>
</tbody>
</table>

Table 2: Comparison of WBAN
6.1. Frame format

Figure 1 shows the general MAC frame format consisting of a 56-bit header, variable length frame body, and 18-bit FrameCheck Sequence (FCS). The maximum length of the frame body is 255 octets. The MAC header further consists of 32-bit frame control, 8-bit recipient Identification (ID), 8-bit sender ID, and 8-bit WBAN ID fields. The frame control field carries control information including the type of frame, that is, beacon, acknowledgement, or other control frames. The recipient and sender ID fields contain the address information of the recipient and the sender of the data frame, respectively. The WBAN ID contains information on the WBAN in which the transmission is active. The first 8-bit field in the MAC frame body carries message freshness information required for nonce construction and replay detection. The frame payload field carries data frames, and the last 32-bit Message Integrity Code (MIC) carries information about the authenticity and integrity of the frame.

![MAC frame format diagram]

6.2. Frequency bands

The USA Federal Communications Commission (FCC) and communication authorities of other countries have allocated the MICS band at 402-405 MHz with 300 KHz channels to enable wireless communication with implanted medical devices. This leads to better penetration through the human tissue compared to higher frequencies, high level of mobility, comfort and better patient care in implant to implant (S1), implant to body surface (S2) and implant to external (S3) scenarios. Additionally, the 402-405 MHz frequencies offers conducive propagation characteristics for the transmission of radio signals in the human body and do not cause
severe interference for other radio operations in the same band. In fact, the MICS band is an unlicensed, ultra-low power, mobile radio service for transmitting data to support therapeutic or diagnostic operation related to implant medical devices and is internationally available. It is specifically chosen to provide low-power, small size, fast data transfer as well as a long communication range. The frequency range of the MICS band allows high-level integration with the radio frequency IC (RFIC) technology, which leads to miniaturization and low power consumption. The PHY layer of IEEE 802.15.6 is responsible for the following tasks: activation and deactivation of the radio transceiver, Clear channel assessment (CCA) within the current channel and data transmission and reception. The choice of the physical layer depends on the target application: medical/non-medical, in, on and off-body. The PHY layer provides a procedure for transforming a physical layer service data unit (PSDU) into a physical layer protocol data unit (PPDU). IEEE 802.15.6 has specified three different physical layers: Human Body Communication (HBC), Narrow Band (NB) and Ultra-Wide Band (UWB). Various frequency bands are supported and shown in Table 2.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Frequency</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBC</td>
<td>16 MHz</td>
<td>4 MHz</td>
</tr>
<tr>
<td>HBC</td>
<td>27 MHz</td>
<td>4 MHz</td>
</tr>
<tr>
<td>NB</td>
<td>402-405 MHz</td>
<td>300 KHz</td>
</tr>
<tr>
<td>NB</td>
<td>420-450 MHz</td>
<td>300 KHz</td>
</tr>
<tr>
<td>NB</td>
<td>863-870 MHz</td>
<td>400 KHz</td>
</tr>
<tr>
<td>NB</td>
<td>902-928 MHz</td>
<td>500 KHz</td>
</tr>
<tr>
<td>NB</td>
<td>956-956 MHz</td>
<td>400 KHz</td>
</tr>
<tr>
<td>NB</td>
<td>2360-2400 MHz</td>
<td>1 MHz</td>
</tr>
<tr>
<td>NB</td>
<td>2400-2438.5 MHz</td>
<td>1 MHz</td>
</tr>
<tr>
<td>UWB</td>
<td>13.2-4.7 GHz</td>
<td>499 MHz</td>
</tr>
<tr>
<td>UWB</td>
<td>6.2-10.3 GHz</td>
<td>499 MHz</td>
</tr>
</tbody>
</table>

Table 3: Frequency bands and Channel bandwidth of IEEE 802.15.6
6.3. Channel modes of IEEE 802.15.6

- Beacon Mode with Beacon Period Superframe Boundaries:

Beacons are sent at beacon periods by the coordinator and the superframe structure is managed by the coordinator by using beacon frames. The Physical Protocol Data Unit (PPDU) frame of Narrowband (NB) consists of a PHY Service Data Unit (PSDU) and Physical Layer Convergence Procedure (PLCP). PLCP preamble supports the receiver for synchronization process and considers as first module being send at given symbol rate. PLCP header sends decoding information for the receiver and it is transmitted after PLCP preamble. PSDU is last module of PPDU and consists of MAC header, Frame Check Sequence (FCS) and MAC frame body. PSDU is transmitted after PLCP with help of available frequency band with specific data rates. Different modulations schemes can be used with NB, namely, Differential Binary Phase-shift Keying (DBPSK), Differential Quadrature Phase-shift Keying (DQPSK) and Differential 8-Phase-shift Keying (D8PSK). NB uses seven frequency bands and operates under different data rates and modulation schemes. Medical Implant Communication Service (MICS) is the first licensed band of NB and used for implant communication with range of 402-405 MHz in most countries. Lower frequencies possess less attenuation and shadowing effect from body. Wireless Telemetry Medical Services (WMTS) is another license band and used for telemetry services. Although, Industrial, Scientific and Medical (ISM) band is free worldwide but it generates high probability of interference for IEEE 802.15.4 and IEEE 802.15.6 devices and considered as 7th license-free band. The 6th band (2360-2400 MHz) is used for medical devices instead of ISM band and offers less interference.

The superframe structure consists of several phases: exclusive access phase 1 (EAP 1), random access phase 1 (RAP1), type I/II phase, an EAP 2, RAP 2 and contention access phase (CAP). CSMA/CA or slotted Aloha is used by EAPs, RAPs and CAPs. For emergency services and high priority data, the EAP 1 and EAP 2 are used, whereas, CAP, RAP 1 and RAP 2 are used for regular data traffic. Type I/II are used for bi-link allocation intervals, up-link and down-link allocation intervals and delay bi-link intervals. For resource allocation, the type I/II polling is used.

A node's backoff counter value is set to a random integer number in the range \([1, CW (Contention Window)]\), where CW (default value is CWmin) belongs to CWmin and CWmax which is dependent on user priority. When the algorithm starts, node begins counter decrement by one for every idle CSMA/CA slot duration (slot duration is equal to Pcsma/CA slot length). A node considers a CSMA/CA slot idle if the channel has been idle between start of slot and pCCATime. When
the backoff counter reaches zero, the node transmits the data frame. In case the channel is busy because of some other frame transmission, then node locks its backoff counter until the channel gets idle. The value of CW get double in case of even number of failures until it reaches $CW_{max}$ [CHALLENGES-WBAN] [RFC7548].

- Beacon Mode with Superframe Boundaries:

For this mode, the coordinator provides an unscheduled polled allocation and each node establishes its own schedule. Different access mechanisms are used in superframe phases: schedule access (connection oriented and contention-free access), improvised and unscheduled access (connectionless and contention free access) and random access (CSMA/CA or slotted Aloha based).

- Beacon Mode without Superframe Boundaries:

In this channel access mode, beacons are not transmitted and channel is assigned by using polling mechanism.

7. --IETF to standardize--

This draft intend to standardize IEEE 802.15.6 for WBANs, specifically for implantable and wearable sensors. By standardizing means that integration of frame format need to be done i.e., how the IEEE 802.15.6 frame format will communicate with IPv6? How 6LoWPAN can accommodate this different frame format? The purpose of the mentioned use cases is to highlight the importance of the standard.

The 6LoWPAN is used to provide integration between IEEE 802.15.4 and IPv6. The details are mentioned in [RFC7548]. The 6LoWPAN concept originated with the purpose of connectivity of internet protocol with low-power smaller devices so they could claim to be part of Internet of Things (IoT) Networks.

The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow ipv6 packets to be sent and received over IEEE 802.15.4 based networks, similarly the draft intent to define these mechanisms for IEEE 802.15.6. The 6LoWPAN can not be used with IEEE 802.15.6 due to frame size differences of IEEE 802.15.4 and IEEE 802.15.6.

8. IANA Considerations

[TBD]
9. Security Considerations

IPv6 over WBAN’s applications often require confidentiality and integrity protection. This can be provided at the application, transport, network, and/or at the link.

10. Acknowledgements

[TBD]

11. References

11.1. Normative References


11.2. Informative References

[I-D.ietf-6tisch-6top-sf0] Dujovne, D., Grieco, L., Palattella, M., and N. Accettura, "6TiSCH 6top Scheduling Function Zero (SF0)", draft-ietf-6tisch-6top-sf0-02 (work in progress), October 2016.
Appendix A. Patient monitoring use case - Spoke Hub

Refer following diagram:
Figure 2: Patient monitoring use case - Spoke Hub
Appendix B. Patient monitoring use case - Connected

Refer following diagram:

---

Figure 3: Patient monitoring use case - Connected

---
Authors’ Addresses

Muhammad Sajjad Akbar
Bournemouth University
Fern Barrow, Dorset
Poole BH12 5BB
United Kingdom
Email: makbar@bournemouth.ac.uk

Naveed Bin Rais
Ajman University
University Street, Al jerf 1
Ajman 346
United Arab Emirates
Email: naveedbinrais@gmail.com

Abdur Rashid Sangi
Individual Contributor
Email: sangi_bahrian@yahoo.com

Mingui Zhang
Huawei Technologies
No. 156 BeiQing Rd. Haidian District
Beijing 100095
China
Email: zhangmingui@huawei.com

Charles E. Perkins
Futurewei
2330 Central Expressway
Santa Clara 95050
United States
Email: charliep@computer.org
Abstract

Considering that an LLN link-layer frame can have a payload below 100 bytes, an IPv6 packet might be fragmented more than 10 fragments at the 6LoWPAN layer. In a 6LoWPAN mesh-under mesh network, the fragments can be forwarded individually across the mesh, whereas a route-over mesh network, a fragmented 6LoWPAN packet must be reassembled at every hop, which causes latency and congestion. This draft introduces a simple protocol to forward individual fragments across a route-over mesh network, and, regardless of the type of mesh, recover the loss of individual fragments across the mesh and protect the network against bloat with a minimal flow control.

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 http://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 8, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of
1. Introduction

In most Low Power and Lossy Network (LLN) applications, the bulk of the traffic consists of small chunks of data (in the order few bytes to a few tens of bytes) at a time. Given that an IEEE Std. 802.15.4 [IEEE.802.15.4] frame can carry 74 bytes or more in all cases, fragmentation is usually not required. However, and though this happens only occasionally, a number of mission critical applications do require the capability to transfer larger chunks of data, for instance to support a firmware upgrades of the LLN nodes or an extraction of logs from LLN nodes. In the former case, the large chunk of data is transferred to the LLN node, whereas in the latter, the large chunk flows away from the LLN node. In both cases, the size can be on the order of 10K bytes or more and an end-to-end reliable transport is required.
"Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [RFC4944] defines the original 6LoWPAN datagram fragmentation mechanism for LLNs. One critical issue with this original design is that routing an IPv6 packet across a route-over mesh requires to reassemble the full packet at each hop, which may cause latency along a path and an overall buffer bloat in the network. Those undesirable effects can be alleviated by a hop-by-hop fragment forwarding technique such as the one proposed in this specification, and arguably this could be achieved without the need to define a new protocol. However, adding that capability alone to the local implementation of the original 6LoWPAN fragmentation would not address the bulk of the issues raised against it, and may create new issues like uncontrolled state in the network.

Another issue against RFC 4944 [RFC4944] is that it does not define a mechanism to first discover the loss of a fragment along a multi-hop path (e.g. having exhausted the link-layer retries at some hop on the way), and then to recover that loss. With RFC 4944, the forwarding of a whole datagram fails when one fragment is not delivered properly to the destination 6LoWPAN endpoint. End-to-end transport or application-level mechanisms may require a full retransmission of the datagram, wasting resources in an already constrained network.

In that situation, the source 6LoWPAN endpoint will not be aware that a loss occurred and will continue sending all fragments for a datagram that is already doomed. The original support is missing signaling to abort a multi-fragment transmission at any time and from either end, and, if the capability to forward fragments is implemented, clean up the related state in the network. It is also lacking flow control capabilities to avoid participating to a congestion that may in turn cause the loss of a fragment and trigger the retransmission of the full datagram.

This specification proposes a method to forward fragments across a multi-hop route over mesh, and to recover individual fragments between LLN endpoints. The method is designed to limit congestion loss in the network and addresses the requirements that are detailed in Appendix B.

2. Updating RFC 4944

This specification deprecates the fragmentation mechanism that is specified in RFC 4944 [RFC4944] and replaces it with a model where fragments can be forwarded end-to-end across a 6LoWPAN mesh network of any type, and where fragments that are lost on the way can be recovered individually. New dispatch types are defined in Section 4.
3. Terminology and Referenced Work

Past experience with fragmentation has shown that miss-associated or lost fragments can lead to poor network behavior and, occasionally, trouble at application layer. The reader is encouraged to read RFC 4963 [RFC4963] and follow the references for more information.

That experience led to the definition of "Path MTU discovery" [RFC1191] (PMTUD) protocol that limits fragmentation over the Internet.

Specifically in the case of UDP, valuable additional information can be found in "UDP Usage Guidelines for Application Designers" [RFC5405].

Readers are expected to be familiar with all the terms and concepts that are discussed in "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919] and "Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [RFC4944].

"The Benefits of Using Explicit Congestion Notification (ECN)" [RFC8087] provides useful information on the potential benefits and pitfalls of using ECN.

Quoting the "Multiprotocol Label Switching (MPLS) Architecture" [RFC8087]: with MPLS, "packets are "labeled" before they are forwarded. At subsequent hops, there is no further analysis of the packet's network layer header. Rather, the label is used as an index into a table which specifies the next hop, and a new label". That technique is leveraged in this specification to forward fragments that actually do not have a network layer header, since the fragmentation occurs below IP.

This specification uses the following terms:

6LoWPAN endpoints

The LLN nodes in charge of generating or expanding a 6LoWPAN header from/to a full IPv6 packet. The 6LoWPAN endpoints are the points where fragmentation and reassembly take place.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
4. New Dispatch types and headers

This specification aims at enabling to provide an MTU that is equivalent to 2048 bytes to the upper layer, which can be the 6LoWPAN Header Compression that is defined in the "Compression Format for IPv6 Datagrams" [RFC6282] specification. In order to achieve this, this specification enables the fragmentation and the reliable transmission of fragments over a multihop 6LoWPAN mesh network.

This specification provides a technique that is derived from MPLS and allows to forward fragments across a 6LoWPAN route-over mesh, but is not needed in the mesh-under case. The datagram_tag is used as the label and is locally unique to the node that is the MAC-layer source of the fragment. There is thus no need for a global registry of datagram_tags and a node may build the datagram_tag in its own locally-significant way, as long as the resulting tag stays unique to the particular datagram for the lifetime of that datagram.

This specification extends RFC 4944 [RFC4944] with 4 new Dispatch types, for Recoverable Fragments (RFRAG) headers with or without Acknowledgment Request (RFRAG vs. RFRAG-ARQ), and for the RFRAG Acknowledgment back, with or without ECN Echo (RFRAG-ACK vs. RFRAG-ECN).

(to be confirmed by IANA) The new 6LoWPAN Dispatch types use the Value Bit Pattern of 11 1010xx, as follows:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Header Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 101000</td>
<td>RFRAG - Recoverable Fragment</td>
</tr>
<tr>
<td>11 101001</td>
<td>RFRAG-ARQ - RFRAG with Ack Request</td>
</tr>
<tr>
<td>11 101010</td>
<td>RFRAG-ACK - RFRAG Acknowledgment</td>
</tr>
<tr>
<td>11 101011</td>
<td>RFRAG-ECN - RFRAG Ack with ECN Echo</td>
</tr>
</tbody>
</table>

Figure 1: Additional Dispatch Value Bit Patterns

4.1. Recoverable Fragment Dispatch type and Header

In this specification, the size and offset of the fragments are expressed on the compressed packet per as opposed to the uncompressed - native packet - form.

The first fragment is recognized by a sequence of 0; it carries its fragment_size and the datagram_size of the compressed packet, whereas the other fragments carry their fragment_size and fragment_offset.

The last fragment for a datagram is recognized when its fragment_offset and its fragment_size add up to the datagram_size.
Recoverable Fragments are sequenced and a bitmap is used in the RFRAG Acknowledgment to indicate the received fragments by setting the individual bits that correspond to their sequence.

```
+----------------+-------------------+
<p>| 1 1 1 0 1 0 X  |</p>
<table>
<thead>
<tr>
<th>R</th>
<th>fragment_size</th>
</tr>
</thead>
</table>
+----------------+-------------------+
| sequence       |
| fragment_offset|
+----------------+-------------------+
```

X set == Ack Requested

Figure 2: RFRAG Dispatch type and Header

X: 1 bit; Ack Requested: when set, the sender requires an RFRAG Acknowledgment from the receiver.

R: 1 bit; Reserved, MUST be set to 0 by the source and ignored by all nodes.

Fragment_size: 7 bits unsigned integer. The size of this fragment in units that depend on the MAC layer technology. For IEEE Std. 802.15.4, the unit is octet.

Sequence: 5 bits unsigned integer; the sequence number of the fragment. Fragments are sequence numbered [0..N] where N is in [0..31].

Fragment_offset: 10 bits unsigned integer; when set to 0, this field indicates an abort condition; else, its value depends on the value of the Sequence. When the sequence is not 0, this field indicates the offset of the fragment in the compressed form. When the sequence is 0, denoting the first fragment of a datagram, this field is overloaded to indicate the total_size of the compressed packet, to help the receiver allocate an adapted buffer for the reception and reassembly operations.

4.2. RFRAG Acknowledgment Dispatch type and Header

The specification also defines a 4-octet RFRAG Acknowledgment bitmap that is used to confirm selectively the reception of individual fragments. A given offset in the bitmap maps one to one with a given sequence number.

The offset of the bit in the bitmap indicates which fragment is acknowledged as follows:
Figure 3: RFRAG Acknowledgment bitmap encoding

Figure 4 shows an example Acknowledgment bitmap which indicates that all fragments from sequence 0 to 20 were received, except for fragments 1, 2 and 16 that were either lost or are still in the network over a slower path.

Figure 4: Expanding 3 octets encoding

The RFRAG Acknowledgment Bitmap is included in a RFRAG Acknowledgment header, as follows:

Figure 5: RFRAG Acknowledgment Dispatch type and Header

Y: 1 bit; Explicit Congestion Notification

When set, the sender indicates that at least one of the acknowledged fragments was received with an Explicit Congestion Notification, indicating that the path followed by the fragments is subject to congestion.

RFRAG Acknowledgment Bitmap

Thubert & Hui Expires October 8, 2017 [Page 7]
An RFRAG Acknowledgment Bitmap, whereby but at offset \( x \) indicates that fragment \( x \) was received.

5. Fragments Recovery

The Recoverable Fragment headers RFRAG and RFRAG-ARQ are used to transport a fragment and optionally request an RFRAG Acknowledgment that will confirm the good reception of a one or more fragments. An RFRAG Acknowledgment can optionally carry an ECN indication; it is carried as a standalone header in a message that is sent back to the 6LoWPAN endpoint that was the source of the fragments, as known by its MAC address. The process ensures that at every hop, the source MAC address and the datagram_tag in the received fragment are enough information to send the RFRAG Acknowledgment back towards the source 6LoWPAN endpoint.

The 6LoWPAN endpoint that fragments the packets at 6LoWPAN level (the sender) also controls the RFRAG Acknowledgments by setting the Ack Requested flag in the RFRAG packets. It may set the Ack Requested flag on any fragment so as to implement its own policy or perform congestion control by limiting the number of fragments in the air, if fragments that have been sent but for which reception or loss was not positively confirmed by the other 6LoWPAN endpoint. When the sender of the fragment knows that an underlying link-layer mechanism protects the Fragments already it may refrain from using the RFRAG Acknowledgment mechanism, and never set the Ack Requested bit. When it receives a fragment with the ACK Request flag set, the 6LoWPAN endpoint that reassembles the packets at 6LoWPAN level (the receiver) sends back an RFRAG Acknowledgment to confirm reception of all the fragments it has received so far, though it may slightly defer it to let additional packets in.

The sender transfers a controlled number of fragments and MAY flag the last fragment of a series with an RFRAG Acknowledgment Request. The received MUST acknowledge a fragment with the acknowledgment request bit set. If any fragment immediately preceding an acknowledgment request is still missing, the receiver MAY intentionally delay its acknowledgment to allow in-transit fragments to arrive. delaying the acknowledgment might defeat the round trip delay computation so it should be configurable and not enabled by default.

The receiver interacts with the sender using an Acknowledgment message with a bitmap that indicates which fragments were actually received. The bitmap is a 32bit bitstring (a DWORD), which accommodates up to 32 fragments and is sufficient to transport 2028 bytes over an IEEE Std. 802.15.4 MAC payload. For all \( n \) in \([0..31]\), bit \( n \) is set to 1 in the bitmap to indicate that fragment with
sequence n was received, otherwise the bit is set to 0. All 0s is a NULL bitmap that indicates that the fragmentation process was canceled by the receiver for that datagram.

The receiver MAY issue unsolicited acknowledgments. An unsolicited acknowledgment enables the sender endpoint to resume sending if it had reached its maximum number of outstanding fragments or indicate that the receiver has cancelled the process of an individual datagram. Note that acknowledgments might consume precious resources so the use of unsolicited acknowledgments should be configurable and not enabled by default.

The sender arms a retry timer to cover the fragment that carries the Acknowledgment request. Upon time out, the sender assumes that all the fragments on the way are received or lost. The process must have completed within an acceptable time that is within the boundaries of upper layer retries. The method detailed in [RFC6298] is recommended for the computation of the retry timer. It is expected that the upper layer retries obey the same or friendly rules in which case a single round of fragment recovery should fit within the upper layer recovery timers.

Fragments are sent in a round robin fashion: the sender sends all the fragments for a first time before it retries any lost fragment; lost fragments are retried in sequence, oldest first. This mechanism enables the receiver to acknowledge fragments that were delayed in the network before they are actually retried.

When the sender decides that a packet should be dropped and the fragmentation process canceled, it sends a pseudo fragment with the fragment_offset, sequence and fragment_size all set to 0, and no data. Upon reception of this message, the receiver should clean up all resources for the packet associated to the datagram_tag. If an acknowledgment is requested, the receiver responds with a NULL bitmap.

The receiver might need to cancel the process of a fragmented packet for internal reasons, for instance if it is out of reassembly buffers, or considers that this packet is already fully reassembled and passed to the upper layer. In that case, the receiver SHOULD indicate so to the sender with a NULL bitmap. Upon an acknowledgment with a NULL bitmap, the sender MUST drop the datagram.

6. Forwarding Fragments

   It is assumed that the first Fragment is large enough to carry the IPv6 header and make routing decisions. If that is not so, then this specification MUST NOT be used.
This specification enables intermediate routers to forward fragments with no intermediate reconstruction of the entire packet. Upon the first fragment, the routers lay an label along the path that is followed by that fragment (that is IP routed), and all further fragments are label switched along that path. As a consequence, alternate routes not possible for individual fragments. The datagram_tag is used to carry the label, that is swapped at each hop.

6.1. Upon the first fragment

In Route-Over mode, the MAC address changes at each hop. The label that is formed and placed in the datagram_tag is associated to the source MAC and only valid (and unique) for that source MAC. Say the first fragment has:

Source IPv6 address = IP_A (maybe hops away)
Destination IPv6 address = IP_B (maybe hops away)
Source MAC = MAC_prv (prv as previous)
Datagram_tag= DT_prv

The intermediate router that forwards individual fragments does the following:

a route lookup to get Next hop IPv6 towards IP_B, which resolves as IP_nxt (nxt as next)
a MAC address resolution to get the MAC address associated to IP_nxt, which resolves as MAC_nxt

Since it is a first fragment of a packet from that source MAC address MAC_prv for that tag DT_prv, the router:

cleans up any leftover resource associated to the tuple (MAC_prv, DT_prv)
allocates a new label for that flow, DT_nxt, from a Least Recently Used pool or some similar procedure.
allocates a Label swap structure indexed by (MAC_prv, DT_prv) that contains (MAC_nxt, DT_nxt)
allocates a Label swap structure indexed by (MAC_nxt, DT_nxt) that contains (MAC_prv, DT_prv)
swaps the MAC info to from self to MAC_nxt
Swaps the datagram_tag to DT_nxt

At this point the router is all set and can forward the packet to nxt.

6.2. Upon the next fragments

Upon next fragments (that are not first fragment), the router expects to have already Label swap structure indexed by (MAC_prv, DT_prv). The router:

- lookups up the Label swap entry for (MAC_prv, DT_prv), which resolves as (MAC_nxt, DT_nxt)
- swaps the MAC info to from self to MAC_nxt;
- Swaps the datagram_tag to DT_nxt

At this point the router is all set and can forward the packet to nxt.

if the Label swap entry for (MAC_prv, DT_prv) is not found, the router builds an RFRAG-ACK to indicate the error. The resulting message has the following information:

- MAC info set to from self to MAC_prv as found in the fragment
- Swaps the datagram_tag set to DT_prv
- Bitmap of all 0es to indicate the error

At this point the router is all set and can send the RFRAG-ACK back ot the previous router.

6.3. Upon the RFRAG Acknowledgments

Upon an RFRAG Acknowledgment, the router expects to have already Label swap structure indexed by (MAC_nxt, DT_nxt), which are respectively the source MAC address of the received frame and the received datagram_tag. DT_nxt should have been computed by this router and this router should have assigned it to this particular datagram. The router:

- lookups up the Label swap entry for (MAC_nxt, DT_nxt), which resolves as (MAC_prv, DT_prv)
- swaps the MAC info to from self to MAC_prv;
Swaps the datagram_tag to DT_prv

At this point the router is all set and can forward the RFRAG-ACK to prv.

if the Label swap entry for (MAC_nxt, DT_nxt) is not found, it simply drops the packet.

if the RFRAG-ACK indicates either an error or that the fragment was fully receive, the router schedules the Label swap entries for recycling. If the RFRAG-ACK is lost on the way back, the source may retry the last fragments, which will result as an error RFRAG-ACK from the first router on the way that has already cleaned up.

7. Security Considerations

The process of recovering fragments does not appear to create any opening for new threat compared to "Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [RFC4944].

8. IANA Considerations

Need extensions for formats defined in "Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [RFC4944].

9. Acknowledgments

The author wishes to thank Jay Werb, Christos Polyzois, Soumitri Kolavennu, Pat Kinney, Margaret Wasserman, Richard Kelsey, Carsten Bormann and Harry Courtice for their contributions and review.

10. References

10.1. Normative References


10.2. Informative References


Appendix A. Rationale

There are a number of uses for large packets in Wireless Sensor Networks. Such usages may not be the most typical or represent the largest amount of traffic over the LLN; however, the associated functionality can be critical enough to justify extra care for ensuring effective transport of large packets across the LLN.

The list of those usages includes:

Towards the LLN node:

Packages of Commands: A number of commands or a full configuration can be packaged as a single message to ensure consistency and enable atomic execution or complete roll back. Until such commands are fully received and interpreted, the intended operation will not take effect.
Firmware update: For example, a new version of the LLN node software is downloaded from a system manager over unicast or multicast services. Such a reflashing operation typically involves updating a large number of similar LLN nodes over a relatively short period of time.

From the LLN node:

Waveform captures: A number of consecutive samples are measured at a high rate for a short time and then transferred from a sensor to a gateway or an edge server as a single large report.

Data logs: LLN nodes may generate large logs of sampled data for later extraction. LLN nodes may also generate system logs to assist in diagnosing problems on the node or network.

Large data packets: Rich data types might require more than one fragment.

Uncontrolled firmware download or waveform upload can easily result in a massive increase of the traffic and saturate the network.

When a fragment is lost in transmission, all fragments are resent, further contributing to the congestion that caused the initial loss, and potentially leading to congestion collapse.

This saturation may lead to excessive radio interference, or random early discard (leaky bucket) in relaying nodes. Additional queuing and memory congestion may result while waiting for a low power next hop to emerge from its sleeping state.

Considering that [RFC4944] defines an MTU is 1280 bytes and that in most incarnations (but 802.15.4G) a 802.15.4 frame can limit the MAC payload to as few as 74 bytes, a packet might be fragmented into at least 18 fragments at the 6LoWPAN shim layer. Taking into account the worst-case header overhead for 6LoWPAN Fragmentation and Mesh Addressing headers will increase the number of required fragments to around 32. This level of fragmentation is much higher than that traditionally experienced over the Internet with IPv4 fragments. At the same time, the use of radios increases the probability of transmission loss and Mesh-Under techniques compound that risk over multiple hops.

Mechanisms such as TCP or application-layer segmentation could be used to support end-to-end reliable transport. One option to support bulk data transfer over a frame-size-constrained LLN is to set the Maximum Segment Size to fit within the link maximum frame size. Doing so, however, can add significant header overhead to each
802.15.4 frame. In addition, deploying such a mechanism requires that the end-to-end transport is aware of the delivery properties of the underlying LLN, which is a layer violation, and difficult to achieve from the far end of the IPv6 network.

Appendix B. Requirements

For one-hop communications, a number of Low Power and Lossy Network (LLN) link-layers propose a local acknowledgment mechanism that is enough to detect and recover the loss of fragments. In a multihop environment, an end-to-end fragment recovery mechanism might be a good complement to a hop-by-hop MAC level recovery. This draft introduces a simple protocol to recover individual fragments between 6LoWPAN endpoints that may be multiple hops away. The method addresses the following requirements of a LLN:

Number of fragments

The recovery mechanism must support highly fragmented packets, with a maximum of 32 fragments per packet.

Minimum acknowledgment overhead

Because the radio is half duplex, and because of silent time spent in the various medium access mechanisms, an acknowledgment consumes roughly as many resources as data fragment.

The new end-to-end fragment recovery mechanism should be able to acknowledge multiple fragments in a single message and not require an acknowledgment at all if fragments are already protected at a lower layer.

Controlled latency

The recovery mechanism must succeed or give up within the time boundary imposed by the recovery process of the Upper Layer Protocols.

Support for out-of-order fragment delivery

Forwarding over a mesh network with rerouting and load balancing can introduce out-of-sequence packets.

The recovery mechanism must account for packets that appear lost but are actually only delayed over a different path.

Optional congestion control
The aggregation of multiple concurrent flows may lead to the saturation of the radio network and congestion collapse.

The recovery mechanism should provide means for controlling the number of fragments in transit over the LLN.

Appendix C. Considerations On Flow Control

Considering that a multi-hop LLN can be a very sensitive environment due to the limited queuing capabilities of a large population of its nodes, this draft recommends a simple and conservative approach to congestion control, based on TCP congestion avoidance.

Congestion on the forward path is assumed in case of packet loss, and packet loss is assumed upon time out. The draft allows to control the number of outstanding fragments, that have been transmitted but for which an acknowledgment was not received yet. It must be noted that the number of outstanding fragments should not exceed the number of hops in the network, but the way to figure the number of hops is out of scope for this document.

Congestion on the forward path can also be indicated by an Explicit Congestion Notification (ECN) mechanism. Though whether and how ECN [RFC3168] is carried out over the LoWPAN is out of scope, this draft provides a way for the destination endpoint to echo an ECN indication back to the source endpoint in an acknowledgment message as represented in Figure 5 in Section 4.2.

It must be noted that congestion and collision are different topics. In particular, when a mesh operates on a same channel over multiple hops, then the forwarding of a fragment over a certain hop may collide with the forwarding of a next fragment that is following over a previous hop but in a same interference domain. This draft enables an end-to-end flow control, but leaves it to the sender stack to pace individual fragments within a transmit window, so that a given fragment is sent only when the previous fragment has had a chance to progress beyond the interference domain of this hop. In the case of 6TiSCH [I-D.ietf-6tisch-architecture], which operates over the TimeSlotted Channel Hopping [RFC7554] (TSCH) mode of operation of IEEE802.14.5, a fragment is forwarded over a different channel at a different time and it make full sense to fire a next fragment as soon as the previous fragment has had its chance to be forwarded at the next hop, retry (ARQ) operations included.

From the standpoint of a source 6LoWPAN endpoint, an outstanding fragment is a fragment that was sent but for which no explicit acknowledgment was received yet. This means that the fragment might be on the way, received but not yet acknowledged, or the
acknowledgment might be on the way back. It is also possible that
either the fragment or the acknowledgment was lost on the way.

Because a meshed LLN might deliver frames out of order, it is
virtually impossible to differentiate these situations. In other
words, from the sender standpoint, all outstanding fragments might
still be in the network and contribute to its congestion. There is
an assumption, though, that after a certain amount of time, a frame
is either received or lost, so it is not causing congestion anymore.
This amount of time can be estimated based on the round trip delay
between the 6LoWPAN endpoints. The method detailed in [RFC6298] is
recommended for that computation.

The reader is encouraged to read through "Congestion Control
Principles" [RFC2914]. Additionally [RFC2309] and [RFC5681] provide
deeper information on why this mechanism is needed and how TCP
handles Congestion Control. Basically, the goal here is to manage
the amount of fragments present in the network; this is achieved by
to reducing the number of outstanding fragments over a congested path
by throttling the sources.

Section 5 describes how the sender decides how many fragments are
(re)sent before an acknowledgment is required, and how the sender
adapts that number to the network conditions.

Authors’ Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes – BP1200
MOUGINS – Sophia Antipolis 06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Jonathan W. Hui
Nest Labs
3400 Hillview Ave
Palo Alto, California 94304
USA

Email: jonhui@nestlabs.com