6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2019
C. Gomez
S. Darroudi
Universitat Politecnica de Catalunya
T. Savolainen
DarkMatter
M. Spoerk
Graz University of Technology
March 9, 2019

IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP
draft-ietf-6lo-blemesh-05

Abstract

RFC 7668 describes the adaptation of 6LoWPAN techniques to enable IPv6 over Bluetooth low energy networks that follow the star topology. However, recent Bluetooth specifications allow the formation of extended topologies as well. This document specifies mechanisms that are needed to enable IPv6 mesh over Bluetooth Low Energy links established by using the Bluetooth Internet Protocol Support Profile. This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE links.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Bluetooth Low Energy (hereinafter, Bluetooth LE) was first introduced in the Bluetooth 4.0 specification. Bluetooth LE (which has been marketed as Bluetooth Smart) is a low-power wireless technology designed for short-range control and monitoring applications. Bluetooth LE is currently implemented in a wide range of consumer electronics devices, such as smartphones and wearable devices. Given the high potential of this technology for the Internet of Things, the Bluetooth Special Interest Group (Bluetooth SIG) and the IETF have produced specifications in order to enable IPv6 over Bluetooth LE, such as the Internet Protocol Support Profile (IPSP) [IPSP], and RFC 7668, respectively. Bluetooth 4.0 only supports Bluetooth LE networks that follow the star topology. In consequence, RFC 7668 was specifically developed and optimized for that type of network topology. However, the functionality described in RFC 7668 is not sufficient and would fail to enable an IPv6 mesh over Bluetooth LE

links. This document specifies mechanisms that are needed to enable IPv6 mesh over Bluetooth LE links. This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE links.

1.1. Terminology and Requirements Language

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].

The terms 6LoWPAN Node (6LN), 6LoWPAN Router (6LR) and 6LoWPAN Border Router (6LBR) are defined as in [RFC6775], with an addition that Bluetooth LE central and Bluetooth LE peripheral (see Section 2) can both be adopted by a 6LN, a 6LR or a 6LBR.

2. Bluetooth LE Networks and the IPSP

Bluetooth LE defines two Generic Access Profile (GAP) roles of relevance herein: the Bluetooth LE central role and the Bluetooth LE peripheral role. A device in the central role, which is called central from now on, has traditionally been able to manage multiple simultaneous connections with a number of devices in the peripheral role, called peripherals hereinafter. Bluetooth 4.1 (now deprecated) introduced the possibility for a peripheral to be connected to more than one central simultaneously, therefore allowing extended topologies beyond the star topology for a Bluetooth LE network. In addition, a device may simultaneously be a central in a set of link layer connections, as well as a peripheral in others. On the other hand, the IPSP enables discovery of IP-enabled devices and the establishment of a link layer connection for transporting IPv6 packets. The IPSP defines the Node and Router roles for devices that consume/originate IPv6 packets and for devices that can route IPv6 packets, respectively. Consistently with Bluetooth 4.1 and subsequent Bluetooth versions (e.g. Bluetooth 4.2 [BTCorev4.2] or subsequent), a device may implement both roles simultaneously.

This document assumes a mesh network composed of Bluetooth LE links, where link layer connections are established between neighboring IPv6-enabled devices (see Section 3.3.2, item 3.b)). The IPv6 forwarding devices of the mesh have to implement both Node and Router roles, while simpler leaf-only nodes can implement only the Node role. In an IPv6 mesh over Bluetooth LE links, a node is a neighbor of another node, and vice versa, if a link layer connection has been established between both by using the IPSP functionality for discovery and link layer connection establishment for IPv6 packet transport.

3. Specification of IPv6 mesh over Bluetooth LE links

3.1. Protocol stack

Figure 1 illustrates the protocol stack for IPv6 mesh over Bluetooth LE links. There are two main differences with the IPv6 over Bluetooth LE stack in RFC 7668: a) the adaptation layer below IPv6 (labelled as "6Lo for IPv6 mesh over Bluetooth LE") is now adapted for IPv6 mesh over Bluetooth LE links, and b) the protocol stack for IPv6 mesh over Bluetooth LE links includes IPv6 routing functionality.

```
                    +------------------------------------+
                    |             Application            |
       +---------+  +------------------------------------+
       |  IPSS   |  |             UDP/TCP/other          |
       +---------+  +------------------------------------+
       |  GATT   |  |             IPv6   |routing|       |
       +---------+  +------------------------------------+
       |  ATT    |  | 6Lo for IPv6 mesh over Bluetooh LE |
       +---------+--+------------------------------------+
       |                 Bluetooth LE L2CAP              |
  -  - +-------------------------------------------------+- - - HCI
       |               Bluetooth LE Link Layer           |
       +-------------------------------------------------+
       |                Bluetooth LE Physical            |
       +-------------------------------------------------+
```

Figure 1: Protocol stack for IPv6 mesh over Bluetooth LE links.

Bluetooth 4.2 defines a default MTU for Bluetooth LE of 251 bytes. Excluding the L2CAP header of 4 bytes, a protocol data unit (PDU) size of 247 bytes is available for the layer above L2CAP. (Note: earlier Bluetooth LE versions offered a maximum amount of 23 bytes for the layer atop L2CAP.) The L2CAP provides a fragmentation and reassembly solution for transmitting or receiving larger PDUs. At each link, the IPSP defines means for negotiating a link-layer connection that provides an MTU of 1280 octets or higher for the IPv6 layer [IPSP]. The link-layer MTU is negotiated separately for each direction. Implementations that require an equal link-layer MTU for the two directions SHALL use the smallest of the possibly different MTU values.

Note that this specification allows using different MTUs in different links. If an implementation requires use of the same MTU on every one of its links, and a new node with a smaller MTU is added to the network, a renegotiation of one or more links can occur. In the

worst case, the renegotiations could cascade network-wide. In that case, implementers need to assess the impact of such phenomenon.

Similarly to RFC 7668, fragmentation functionality from 6LoWPAN standards is not used for IPv6 mesh over Bluetooth LE links. Bluetooth LE's fragmentation support provided by L2CAP is used when necessary.

3.2. Subnet model

For IPv6 mesh over Bluetooth LE links, a multilink model has been chosen, as further illustrated in Figure 2. As IPv6 over Bluetooth LE is intended for constrained nodes, and for Internet of Things use cases and environments, the complexity of implementing a separate subnet on each peripheral-central link and routing between the subnets appears to be excessive. In this specification, the benefits of treating the collection of point-to-point links between a central and its connected peripherals as a single multilink subnet rather than a multiplicity of separate subnets are considered to outweigh the multilink model's drawbacks as described in [RFC4903].

```
                                                          /
       .--------------------------------.                /
      /     6LR           6LN       6LN \               /
     /         \             \          \ \            /
    |           \             \          \ |          /
    |  6LN ----- 6LR --------- 6LR ------ 6LBR ----- |  Internet
    |   <--Link--> <---Link--->/<--Link->/ |         |
     \                        /         / /           \
      \           6LN ---- 6LR ----- 6LR /             \
       '--------------------------------'               \
                                                         \


     <------------ Subnet ----------------><---- IPv6 connection -->
                                                  to the Internet
```

Figure 2: Example of an IPv6 mesh over a Bluetooth LE network connected to the Internet

One or more 6LBRs are connected to the Internet. 6LNs are connected to the network through a 6LR or a 6LBR. A prefix is used on the whole subnet.

IPv6 mesh over Bluetooth LE links MUST follow a route-over approach. This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth links.

3.3. Link model

3.3.1. Stateless address autoconfiguration

6LN, 6LR and 6LBR IPv6 addresses in an IPv6 mesh over Bluetooth LE links are configured as per section 3.2.2 of RFC 7668.

Multihop DAD functionality as defined in section 8.2 of RFC 6775 and updated by RFC 8505, or some substitute mechanism (see section 3.3.2), MUST be supported.

3.3.2. Neighbor Discovery

'Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)' [RFC6775], subsequently updated by 'Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery' [RFC8505], describes the neighbor discovery functionality adapted for use in several 6LoWPAN topologies, including the mesh topology. The route-over functionality of RFC 6775 and RFC 8505 MUST be supported.

The following aspects of the Neighbor Discovery optimizations for 6LoWPAN [RFC6775],[RFC8505] are applicable to Bluetooth LE 6LNs:

1. A Bluetooth LE host MUST register its non-link-local addresses with its routers by sending a Neighbor Solicitation (NS) message with the Extended Address Registration Option (EARO) and process the Neighbor Advertisement (NA) accordingly. The NS with the EARO option MUST be sent irrespective of the method used to generate the IID. The EARO option includes a Registration Ownership Verifier (ROVR) field [RFC8505]. In the case of Bluetooth LE, by default the ROVR field is filled with the 48-bit device address used by the Bluetooth LE node converted into 64-bit Modified EUI-64 format [RFC4291]. Optionally, a cryptographic ID (see [I-D.ietf-6lo-ap-nd] MAY be placed in the ROVR field. If a cryptographic ID is used, address registration and multihop DAD formats and procedures defined in [I-D.ietf-6lo-ap-nd] MUST be used, unless an alternative mechanism offering equivalent protection is used. As per RFC 8505, a 6LN MUST NOT register its link-local address.

If the 6LN registers for a same compression context multiple addresses that are not based on Bluetooth device address, the header compression efficiency will decrease.

2. For sending Router Solicitations and processing Router Advertisements the Bluetooth LE hosts MUST, respectively, follow Sections 5.3 and 5.4 of [RFC6775], and Section 5.6 of [RFC8505].

3. The router behavior for 6LRs and 6LBRs is described in Section 6 of RFC 6775, and updated by RFC 8505. However, as per this specification: a) Routers SHALL NOT use multicast NSs to discover other routers' link layer addresses. b) As per section 6.2 of RFC 6775, in a dynamic configuration scenario, a 6LR comes up as a non-router and waits to receive a Router Advertisement for configuring its own interface address first, before setting its interfaces to be advertising interfaces and turning into a router. In order to support such operation in an IPv6 mesh over Bluetooth LE links, a 6LR first uses the IPSP Node role only. Once the 6LR has established a connection with another node previously running as a router, and receives a Router Advertisement from that router, the 6LR configures its own interface address, it turns into a router, and it runs as an IPSP Router. A 6LBR uses the IPSP Router role since the 6LBR is initialized. See an example in the Appendix.

4. Border router behavior is described in Section 7 of RFC 6775, and updated by RFC 8505.

RFC 6775 defines substitutable mechanisms for distributing prefixes and context information (section 8.1 of RFC 6775), as well as for Duplicate Address Detection across a route-over 6LoWPAN (section 8.2 of RFC 6775). RFC 8505 updates those mechanisms and the related message formats. Implementations of this specification MUST support the features described in sections 8.1 and 8.2 of RFC 6775, as updated by RFC 8505, unless some alternative ("substitute") from some other specification is supported by the implementation.

3.3.3. Header compression

Header compression as defined in RFC 6282 [RFC6282], which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, is REQUIRED as the basis for IPv6 header compression on top of Bluetooth LE. All headers MUST be compressed according to RFC 6282 [RFC6282] encoding formats.

To enable efficient header compression, when the 6LBR sends a Router Advertisement it MUST include a 6LoWPAN Context Option (6CO) [RFC6775] matching each address prefix advertised via a Prefix Information Option (PIO) [RFC4861] for use in stateless address autoconfiguration.

The specific optimizations of RFC 7668 for header compression, which exploit the star topology and ARO, cannot be generalized in an IPv6 mesh over Bluetooth LE links. Still, a subset of those optimizations can be applied in some cases in such a network. In particular, the latter comprise link-local interactions, non-link- local packet transmissions originated and performed by a 6LN, and non-link-local

packets transmitted (but not necessarily originated) by the neighbor of a 6LN to that 6LN. For the rest of packet transmissions, context-based compression MAY be used.

When a device transmits a packet to a neighbor, the sender MUST fully elide the source IID if the source IPv6 address is the link-local address based on the sender's Bluetooth device address (SAC=0, SAM=11). The sender also MUST fully elide the destination IPv6 address if it is the link-local address based on the neighbor's Bluetooth device address (DAC=0, DAM=11).

A 6LN SHOULD register its non-link-local address with ARO in the next-hop router. Note that in some cases (e.g. very short-lived connections) it may not be worthwhile for a 6LN to send an NS with ARO for registering its address. When a 6LN transmits a packet, with a non-link-local source address that the 6LN has registered with ARO in the next-hop router for the indicated prefix, the source address MUST be fully elided if it is the latest address that the 6LN has registered for the indicated prefix (SAC=1, SAM=11). If the source non-link-local address is not the latest registered by the 6LN, then the 64 bits of the IID SHALL be fully carried in-line (SAC=1, SAM=01) or if the first 48 bits of the IID match with the latest address registered by the 6LN, then the last 16 bits of the IID SHALL be carried in-line (SAC=1, SAM=10).

When a router transmits a packet to a neighboring 6LN, with a non-link-local destination address, the router MUST fully elide the destination IPv6 address if the destination address is the latest registered by the 6LN with ARO for the indicated context (DAC=1, DAM=11). If the destination address is a non-link-local address and not the latest registered, then the 6LN MUST either include the IID part fully in-line (DAM=01) or, if the first 48 bits of the IID match to the latest registered address, then elide those 48 bits (DAM=10).

3.3.4. Unicast and multicast mapping

The Bluetooth LE Link Layer does not support multicast. Hence, traffic is always unicast between two Bluetooth LE neighboring nodes. If a node needs to send a multicast packet to several neighbors, it has to replicate the packet and unicast it on each link. However, this may not be energy efficient, and particular care must be taken if the node is battery powered. A router (i.e. a 6LR or a 6LBR) MUST keep track of neighboring multicast listeners, and it MUST NOT forward multicast packets to neighbors that have not registered as listeners for multicast groups the packets belong to.

4. IANA Considerations

There are no IANA considerations related to this document.

5. Security Considerations

The security considerations in RFC 7668 apply.

IPv6 mesh over Bluetooth LE links requires a routing protocol to find end-to-end paths. Unfortunately, the routing protocol may generate additional opportunities for threats and attacks to the network.

RFC 7416 [RFC 7416] provides a systematic overview of threats and attacks on the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), as well as countermeasures. In that document, described threats and attacks comprise threats due to failures to authenticate, threats due to failure to keep routing information, threats and attacks on integrity, and threats and attacks on availability. Reported countermeasures comprise confidentiality attack, integrity attack, and availability attack countermeasures.

While this specification does not state the routing protocol to be used in IPv6 mesh over Bluetooth LE links, the guidance of RFC 7416 is useful when RPL is used in such scenarios. Furthermore, such guidance may partly apply for other routing protocols as well.

The ROVR can be derived from the Bluetooth device address. However, such a ROVR can be spoofed, and therefore, any node connected to the subnet and aware of a registered-address-to-ROVR mapping could perform address theft and impersonation attacks. Use of Address Protected Neighbor Discovery [I-D.ietf-6lo-ap-nd] provides protection against such attacks.

6. Contributors

Carlo Alberto Boano (Graz University of Technology) contributed to the design and validation of this document.

7. Acknowledgements

The Bluetooth, Bluetooth Smart and Bluetooth Smart Ready marks are registered trademarks owned by Bluetooth SIG, Inc.

The authors of this document are grateful to all RFC 7668 authors, since this document borrows many concepts (albeit, with necessary extensions) from RFC 7668.

The authors also thank Alain Michaud, Mark Powell, Martin Turon, Bilhanan Silverajan, Rahul Jadhav and Pascal Thubert for their comments, which helped improve the document.

Carles Gomez has been supported in part by the Spanish Government Ministerio de Economia y Competitividad through projects TEC2012-32531, TEC2016-79988-P and FEDER.

8. Appendix

This appendix provides an example of Bluetooth LE connection establishment and use of IPSP roles in an IPv6 mesh over Bluetooth LE links that uses dynamic configuration. The example follows text in Section 3.3.2, item 3.b).

The example assumes a network with one 6LBR, two 6LRs and three 6LNs, as shown in Figure 3. Connectivity between the 6LNs and the 6LBR is only possible via the 6LRs.

The following text describes the different steps as time evolves, in the example. Note that other sequences of events that may lead to the same final scenario are also possible.

At the beginning, the 6LBR starts running as an IPSP Router, whereas the rest of devices are not yet initialized (Step 1). Next, the 6LRs start running as IPSP Nodes, i.e., they use Bluetooth LE advertisement packets to announce their presence and support of IPv6 capabilities (Step 2). The 6LBR (already running as an IPSP Router) discovers the presence of the 6LRs and establishes one Bluetooth LE connection with each 6LR (Step 3). After establishment of those link layer connections (and after reception of Router Advertisements from the 6LBR), Step 4, the 6LRs start operating as routers, and also initiate the IPSP Router role (note: whether the IPSP Node role is kept running simultaneously is an implementation decision). Then, 6LNs start running the IPSP Node role (Step 5). Finally, the 6LRs discover presence of the 6LNs and establish connections with the latter (Step 6).

```
Step 1
******
                                     6LBR
                                (IPSP: Router)


                          6LR                   6LR
                   (not initialized)     (not initialized)
```

```
                6LN                 6LN                  6LN
       (not initialized)      (not initialized)     (not initialized)


   Step 2
   ******
                                                 6LBR
                                            (IPSP: Router)


                                      6LR                 6LR
                                 (IPSP: Node)         (IPSP: Node)



                6LN                 6LN                  6LN
       (not initialized)      (not initialized)     (not initialized)




   Step 3
   ******

                                                 6LBR
                                            (IPSP: Router)
     Bluetooth LE connection -->   /             \
                                  /               \
                                      6LR                 6LR
                                 (IPSP: Node)         (IPSP: Node)



                6LN                 6LN                  6LN
       (not initialized)      (not initialized)     (not initialized)






   Step 4
   ******

                                                 6LBR
                                            (IPSP: Router)
                                           /             \
```

```
                                  /              \
                              6LR                  6LR
                         (IPSP: Router)      (IPSP: Router)



                6LN                 6LN                  6LN
         (not initialized)      (not initialized)     (not initialized)
```

Step 5
******

```
                                        6LBR
                                   (IPSP: Router)
                                     /            \
                                    /              \
                                6LR                  6LR
                           (IPSP: Router)      (IPSP: Router)



                  6LN                    6LN                 6LN
              (IPSP: Node)          (IPSP: Node)        (IPSP: Node)
```

Step 6
******

```
                                        6LBR
                                   (IPSP: Router)
                                     /            \
                                    /              \
                                6LR                  6LR
                          (IPSP: Router)       (IPSP: Router)
                             /           \       /            \
                            /             \     /              \
                           /               \   /                \
                        6LN                  6LN                  6LN
                   (IPSP: Node)         (IPSP: Node)         (IPSP: Node)
```

Figure 3: An example of connection establishment and use of IPSP
          roles in an IPv6 mesh over Bluetooth LE links.

9. References

9.1. Normative References

[BTCorev4.2] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 4.2", December 2014, <https://www.bluetooth.com/specifications/archived-specifications>.

[IPSP] Bluetooth Special Interest Group, "Bluetooth Internet Protocol Support Profile Specification Version 1.0.0", December 2014, <https://www.bluetooth.org/en-us/specification/adopted-specifications>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

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

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

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

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <https://www.rfc-editor.org/info/rfc7668>.

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

9.2. Informative References

[BTCorev4.1] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 4.1", December 2013, <https://www.bluetooth.org/en-us/specification/adopted-specifications>.

[I-D.ietf-6lo-ap-nd] Thubert, P., Sarikaya, B., Sethi, M., and R. Struik, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-11 (work in progress), February 2019.

[RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, DOI 10.17487/RFC4903, June 2007, <https://www.rfc-editor.org/info/rfc4903>.

[RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015, <https://www.rfc-editor.org/info/rfc7416>.

Authors' Addresses

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

Email: carlesgo@entel.upc.edu

Seyed Mahdi Darroudi
Universitat Politecnica de Catalunya
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: sm.darroudi@entel.upc.edu

Teemu Savolainen
DarkMatter LLC

Email: teemu.savolainen@darkmatter.ae

Michael Spoerk
Graz University of Technology
Inffeldgasse 16/I
Graz 8010
Austria

Email: michael.spoerk@tugraz.at