                    IPv6 over BLUETOOTH(R) Low Energy

Abstract

   Bluetooth Smart is the brand name for the Bluetooth low energy
   feature in the Bluetooth specification defined by the Bluetooth
   Special Interest Group. The standard Bluetooth radio has been widely
   implemented and available in mobile phones, notebook computers, audio
   headsets, and many other devices. The low-power version of Bluetooth
   is a specification that enables the use of this air interface with
   devices such as sensors, smart meters, appliances, etc. The low-
   power variant of Bluetooth has been standardized since revision 4.0
   of the Bluetooth specifications, although version 4.1 or newer is
   required for IPv6. This document describes how IPv6 is transported
   over Bluetooth low energy using IPv6 over Low-power Wireless Personal
   Area Network (6LoWPAN) techniques.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7668.

Copyright Notice

Table of Contents

1. Introduction

   Bluetooth Smart is the brand name for the Bluetooth low energy
   feature (hereinafter, "Bluetooth LE") in the Bluetooth specification
   defined by the Bluetooth Special Interest Group [BTCorev4.1].
   Bluetooth LE is a radio technology targeted for devices that operate
   with very low-capacity (e.g., coin cell) batteries or minimalistic
   power sources, which means that low power consumption is essential.
   Bluetooth LE is an especially attractive technology for Internet of
   Things applications, such as health monitors, environmental sensing,
   proximity applications, and many others.

   Considering the potential for the exponential growth in the number of
   sensors and Internet connected devices, IPv6 is an ideal protocol for
   communication with such devices due to the large address space it
   provides. In addition, IPv6 provides tools for stateless address
   autoconfiguration, which is particularly suitable for sensor network
   applications and nodes that have very limited processing power or
   lack a full-fledged operating system or a user interface.

   This document describes how IPv6 is transported over Bluetooth LE
   connections using IPv6 over Low-power Wireless Personal Area Network
   (6LoWPAN) techniques. RFCs 4944 [RFC4944], 6282 [RFC6282], and 6775
   [RFC6775] were developed for 6LoWPAN and specify the transmission of
   IPv6 over IEEE 802.15.4 [IEEE802.15.4]. The Bluetooth LE link, in
   many respects, has similar characteristics to that of IEEE 802.15.4,
   and many of the mechanisms defined for IPv6 over IEEE 802.15.4 can be
   applied to the transmission of IPv6 on Bluetooth LE links. This
   document specifies the details of IPv6 transmission 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 2.2) can both be either 6LN or 6LBR.

   The acronyms "DAC", "DAM", "SAC", "SAM", and "CID" are used in this
   document as defined in [RFC6282]. They are expanded as follows:

   o Destination Address Compression (DAC)

   o Destination Address Mode (DAM)

   o Source Address Compression (SAC)

   o Source Address Mode (SAM)

   o Context Identifier (CID)

2. Bluetooth Low Energy

   Bluetooth LE is designed for transferring small amounts of data
   infrequently at modest data rates with a very small energy
   expenditure per bit. The Bluetooth Special Interest Group (Bluetooth
   SIG) has introduced two trademarks: Bluetooth Smart for single-mode
   devices (a device that only supports Bluetooth LE) and Bluetooth
   Smart Ready for dual-mode devices (devices that support both
   Bluetooth and Bluetooth LE; note that Bluetooth and Bluetooth LE are
   different, non-interoperable radio technologies). In the rest of
   this document, the term "Bluetooth LE" is used regardless of whether
   this technology is supported by a single-mode or dual-mode device.

   Bluetooth LE was introduced in Bluetooth 4.0, enhanced in Bluetooth
   4.1 [BTCorev4.1], and developed even further in successive versions.
   Bluetooth SIG has also published the Internet Protocol Support
   Profile (IPSP) [IPSP], which includes the Internet Protocol Support
   Service (IPSS). The IPSP enables discovery of IP-enabled devices and
   establishment of a link-layer connection for transporting IPv6
   packets. IPv6 over Bluetooth LE is dependent on both Bluetooth 4.1
   and IPSP 1.0 or more recent versions of either specification to
   provide necessary capabilities.

   Devices such as mobile phones, notebooks, tablets, smartwatches, and
   other handheld computing devices that incorporate chipsets
   implementing Bluetooth 4.1 or later will also have the low energy
   functionality of Bluetooth. Bluetooth LE is also expected to 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 a mobile phone or smartwatch to a server
   on the Internet or sends data directly to the device.

2.1. Bluetooth LE Stack

   The lower layer of the Bluetooth LE stack consists of the Physical
   Layer (PHY), the Link Layer (LL), and a test interface called the
   Direct Test Mode (DTM). The Physical Layer transmits and receives
   the actual packets. The Link Layer is responsible for providing
   medium access, connection establishment, error control, and flow
   control. The Direct Test Mode is only used for testing purposes.
   The upper layer consists of the Logical Link Control and Adaptation

   Protocol (L2CAP), Attribute Protocol (ATT), Security Manager (SM),
   Generic Attribute Profile (GATT), and Generic Access Profile (GAP) as
   shown in Figure 1. The Host Controller Interface (HCI) separates the
   lower layers, often implemented in the Bluetooth controller, from
   higher layers, often implemented in the host stack. GATT and
   Bluetooth LE profiles together enable the creation of applications in
   a standardized way without using IP. L2CAP provides multiplexing
   capability by multiplexing the data channels from the above layers.
   L2CAP also provides fragmentation and reassembly for large data
   packets. The Security Manager defines a protocol and mechanisms for
   pairing, key distribution, and a security toolbox for the Bluetooth
   LE device.

```
      +--------------------------------------------------+
      |                   Applications                   |
      +----------------------------------------+---------+
      |        Generic Attribute Profile       | Generic |
      +--------------------+-------------------+ Access  |
      | Attribute Protocol | Security Manager  | Profile |
      +--------------------+-------------------+---------+
      |    Logical Link Control and Adaptation Protocol  |
 - - -+----------------------+---------------------------+- - - HCI
      |      Link Layer      |      Direct Test Mode      |
      +--------------------------------------------------+
      |                  Physical Layer                  |
      +--------------------------------------------------+
```
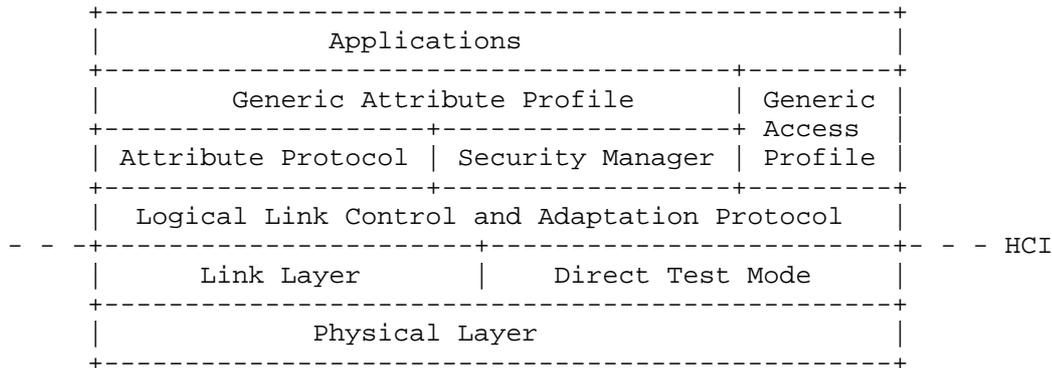
                 Figure 1: Bluetooth LE Protocol Stack

   As shown in Section 3.1, IPv6 over Bluetooth LE requires an adapted
   6LoWPAN layer that runs on top of Bluetooth LE L2CAP.

2.2. Roles and Topology for Link Layer

   Bluetooth LE defines two GAP roles of relevance herein: the Bluetooth
   LE central role and the Bluetooth LE peripheral role. A device in
   the central role (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" from now on).
   A peripheral is commonly connected to a single central, but with
   versions of Bluetooth from 4.1 onwards, it can also connect to
   multiple centrals at the same time. In this document, for IPv6
   networking purposes, the Bluetooth LE network (i.e., a Bluetooth LE
   piconet) follows a star topology shown in the Figure 2, where a
   router typically implements the Bluetooth LE central role and the
   rest of nodes implement the Bluetooth LE peripheral role. In the
   future, mesh networking and/or parallel connectivity to multiple
   centrals at a time may be defined for IPv6 over Bluetooth LE.

```
         Peripheral --.        .-- Peripheral
                       \      /
           Peripheral ---- Central ---- Peripheral
                       /      \
         Peripheral --'        '-- Peripheral
```
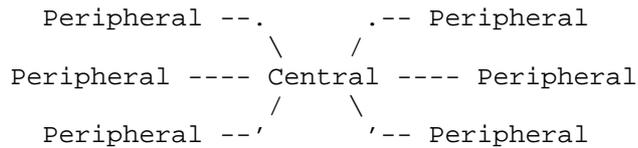
                Figure 2: Bluetooth LE Star Topology

   In Bluetooth LE, direct wireless communication only takes place
   between a central and a peripheral. This means that inherently the
   Bluetooth LE star represents a hub-and-spokes link model.
   Nevertheless, two peripherals may communicate through the central by
   using IP routing functionality per this specification.

2.3. Bluetooth LE Device Addressing

   Every Bluetooth LE device is identified by a 48-bit device address.
   The Bluetooth specification [BTCorev4.1] describes the device address
   of a Bluetooth LE device as follows: "Devices are identified using a
   device address. Device addresses may be either a public device
   address or a random device address". The public device addresses are
   based on the IEEE 802 standard [IEEE802]. Random device addresses
   and the Bluetooth LE privacy feature are described in the Bluetooth
   Generic Access Profile, Sections 10.8 and 10.7 of [BTCorev4.1],
   respectively. There are two types of random device addresses: static
   and private addresses. The private addresses are further divided
   into two sub-types: resolvable or non-resolvable addresses, which are
   explained in depth in the referenced Bluetooth specification. Once a
   static address is initialized, it does not change until the device is
   power cycled. The static address can be initialized to a new value
   after each power cycle, but that is not mandatory. The recommended
   time interval before randomizing new private address is 15 minutes,
   as determined by timer T_GAP(private_addr_int) in Table 17.1 of the
   Bluetooth Generic Access Profile [BTCorev4.1]. The selection of
   which device address types are used is implementation and deployment
   specific. In random addresses, the first 46 bits are randomized, and
   the last 2 bits indicate the random address type. Bluetooth LE does
   not support avoidance or detection of device address collisions.
   However, these 48-bit random device addresses have a very small
   probability of being in conflict within a typical deployment.

2.4. Bluetooth LE Packet Sizes and MTU

   The optimal MTU defined for L2CAP fixed channels over Bluetooth LE is
   27 octets, including the L2CAP header of 4 octets. The default MTU
   for Bluetooth LE is hence defined to be 27 octets. Therefore,
   excluding the L2CAP header of 4 octets, a protocol data unit (PDU)
   size of 23 octets is available for upper layers. In order to be able

to transmit IPv6 packets of 1280 octets or larger, a link-layer
fragmentation and reassembly solution is provided by the L2CAP layer.
The IPSP defines means for negotiating up 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.

3. Specification of IPv6 over Bluetooth Low Energy

   Bluetooth LE technology sets strict requirements for low power
   consumption and thus limits the allowed protocol overhead. 6LoWPAN
   standards [RFC6775] [RFC6282] provide useful functionality for
   reducing overhead, which is applied to Bluetooth LE. This
   functionality is comprised of link-local IPv6 addresses and stateless
   IPv6 address autoconfiguration (see Section 3.2.2), Neighbor
   Discovery (see Section 3.2.3), and header compression (see
   Section 3.2.4). Fragmentation features from 6LoWPAN standards are
   not used due to Bluetooth LE's link-layer fragmentation support (see
   Section 2.4).

   A significant difference between IEEE 802.15.4 and Bluetooth LE is
   that the former supports both star and mesh topologies (and requires
   a routing protocol), whereas Bluetooth LE does not currently support
   the formation of multihop networks at the link layer. However,
   inter-peripheral communication through the central is enabled by
   using IP routing functionality per this specification.

   In Bluetooth LE, a central node is assumed to be less resource
   constrained than a peripheral node. Hence, in the primary deployment
   scenario, central and peripheral will act as 6LoWPAN Border Router
   (6LBR) and a 6LoWPAN Node (6LN), respectively.

   Before any IP-layer communications can take place over Bluetooth LE,
   nodes enabled by Bluetooth LE such as 6LNs and 6LBRs have to find
   each other and establish a suitable link-layer connection. The
   discovery and Bluetooth LE connection setup procedures are documented
   by the Bluetooth SIG in the IPSP specification [IPSP].

   In the rare case of Bluetooth LE random device address conflict, a
   6LBR can detect multiple 6LNs with the same Bluetooth LE device
   address, as well as a 6LN with the same Bluetooth LE address as the
   6LBR. The 6LBR MUST ignore 6LNs with the same device address the
   6LBR has, and the 6LBR MUST have at most one connection for a given
   Bluetooth LE device address at any given moment. This will avoid
   addressing conflicts within a Bluetooth LE network.

3.1. Protocol Stack

   Figure 3 illustrates how the IPv6 stack works in parallel to the GATT
   stack on top of the Bluetooth LE L2CAP layer. The GATT stack is
   needed herein for discovering nodes supporting the Internet Protocol
   Support Service. UDP and TCP are provided as examples of transport
   protocols, but the stack can be used by any other upper-layer
   protocol capable of running atop of IPv6.

```
        +---------+   +----------------------------+
        |  IPSS   |   |       UDP/TCP/other         |
        +---------+   +----------------------------+
        |  GATT   |   |            IPv6             |
        +---------+   +----------------------------+
        |  ATT    |   |   6LoWPAN for Bluetooth LE  |
        +---------+--+----------------------------+
        |         Bluetooth LE L2CAP             |
 - - +----------------------------------------+- - - HCI
        |        Bluetooth LE Link Layer         |
        +----------------------------------------+
        |        Bluetooth LE Physical           |
        +----------------------------------------+
```
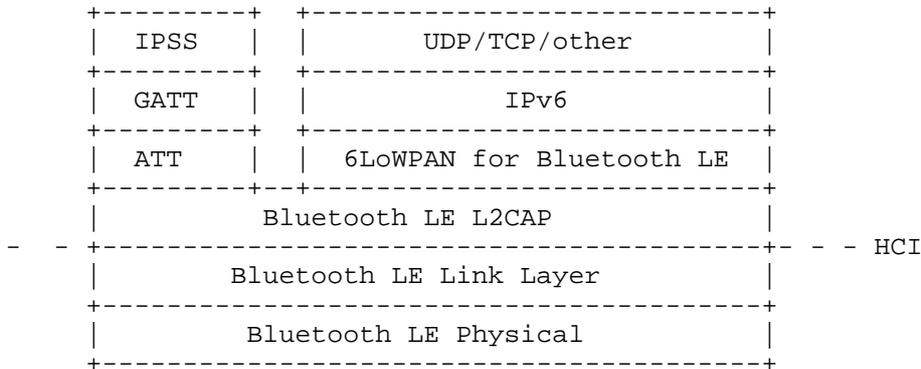
           Figure 3: IPv6 and IPSS on the Bluetooth LE Stack

3.2. Link Model

   The distinct concepts of the IPv6 link (layer 3) and the physical
   link (combination of PHY and Media Access Control (MAC)) need to be
   clear, and their relationship has to be well understood in order to
   specify the addressing scheme for transmitting IPv6 packets over the
   Bluetooth LE link. RFC 4861 [RFC4861] defines a link as "a
   communication facility or medium over which nodes can communicate at
   the link layer, i.e., the layer immediately below IP".

   In the case of Bluetooth LE, the 6LoWPAN layer is adapted to support
   transmission of IPv6 packets over Bluetooth LE. The IPSP defines all
   steps required for setting up the Bluetooth LE connection over which
   6LoWPAN can function [IPSP], including handling the link-layer
   fragmentation required on Bluetooth LE, as described in Section 2.4.
   Even though MTUs larger than 1280 octets can be supported, use of a
   1280-octet MTU is RECOMMENDED in order to avoid need for Path MTU
   discovery procedures.

   While Bluetooth LE protocols, such as L2CAP, utilize little-endian
   byte ordering, IPv6 packets MUST be transmitted in big-endian order
   (network byte order).

Per this specification, the IPv6 header compression format specified
in RFC 6282 [RFC6282] MUST be used. The IPv6 payload length can be
derived from the L2CAP header length and the possibly elided IPv6
address can be reconstructed from the link-layer address, used at the
time of Bluetooth LE connection establishment, from the HCI
Connection Handle during connection, compression context if any, and
address registration information (see Section 3.2.3).

Bluetooth LE connections used to build a star topology are point-to-
point in nature, as Bluetooth broadcast features are not used for
IPv6 over Bluetooth LE (except for discovery of nodes supporting
IPSS). After the peripheral and central have connected at the
Bluetooth LE level, the link can be considered up, and IPv6 address
configuration and transmission can begin.

3.2.1. IPv6 Subnet Model and Internet Connectivity

In the Bluetooth LE piconet model (see Section 2.2), peripherals each
have a separate link to the central and the central acts as an IPv6
router rather than a link-layer switch. As discussed in [RFC4903],
conventional usage of IPv6 anticipates IPv6 subnets spanning a single
link at the link layer. 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 the Bluetooth LE case, 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].

Hence, a multilink model has been chosen, as further illustrated in
Figure 4. Because of this, link-local multicast communications can
happen only within a single Bluetooth LE connection; thus, 6LN-to-6LN
communications using link-local addresses are not possible. 6LNs
connected to the same 6LBR have to communicate with each other by
using the shared prefix used on the subnet. The 6LBR ensures address
collisions do not occur (see Section 3.2.3) and forwards packets sent
by one 6LN to another.

In a typical scenario, the Bluetooth LE network is connected to the
Internet as shown in the Figure 4. In this scenario, the Bluetooth
LE star is deployed as one subnet, using one /64 IPv6 prefix, with
each spoke representing an individual link. The 6LBR is acting as
router and forwarding packets between 6LNs and to and from Internet.

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

        <------ Subnet -----><-- IPv6 connection -->
                                 to Internet
```
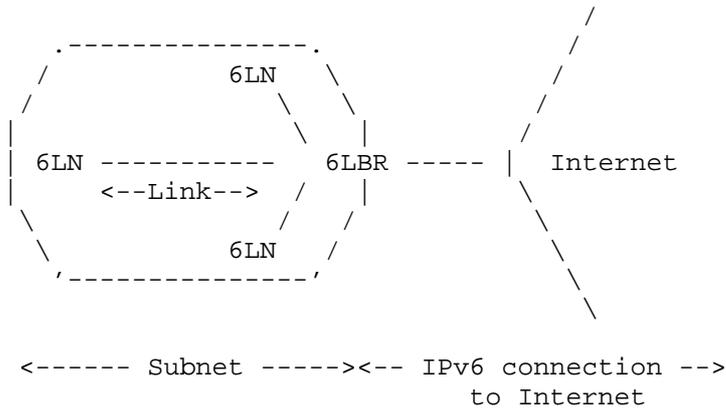
             Figure 4: Bluetooth LE Network Connected to the Internet

   In some scenarios, the Bluetooth LE network may transiently or
   permanently be an isolated network as shown in the Figure 5. In this
   case, the whole star consists of a single subnet with multiple links,
   where 6LBR is at central, routing packets between 6LNs. In the
   simplest case, the isolated network has one 6LBR and one 6LN.

```
            .-------------------.
           /                     \
          /    6LN       6LN       \
         /         \     /          \
        |           \   /            |
        |    6LN --- 6LBR --- 6LN    |
        |         /   \                |
         \       /     \              /
          \    6LN       6LN         /
           \                        /
            '-------------------'
         <--------- Subnet ---------->
```
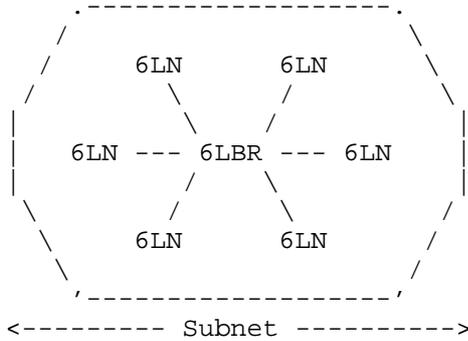
                 Figure 5: Isolated Bluetooth LE Network

3.2.2. Stateless Address Autoconfiguration

   At network interface initialization, both 6LN and 6LBR SHALL generate
   and assign to the Bluetooth LE network interface IPv6 link-local
   addresses [RFC4862] based on the 48-bit Bluetooth device addresses
   (see Section 2.3) that were used for establishing the underlying
   Bluetooth LE connection. A 6LN and a 6LBR are RECOMMENDED to use
   private Bluetooth device addresses. A 6LN SHOULD pick a different
   Bluetooth device address for every Bluetooth LE connection with a
   6LBR, and a 6LBR SHOULD periodically change its random Bluetooth

device address. Following the guidance of [RFC7136], a 64-bit
Interface Identifier (IID) is formed from the 48-bit Bluetooth device
address by inserting two octets, with hexadecimal values of 0xFF and
0xFE in the middle of the 48-bit Bluetooth device address as shown in
Figure 6. In the figure, letter 'b' represents a bit from the
Bluetooth device address, copied as is without any changes on any
bit. This means that no bit in the IID indicates whether the
underlying Bluetooth device address is public or random.

```
|0              1|1              3|3              4|4              6|
|0              5|6              1|2              7|8              3|
+----------------+----------------+----------------+----------------+
|bbbbbbbbbbbbbbbb|bbbbbbbb11111111|11111110bbbbbbbb|bbbbbbbbbbbbbbbb|
+----------------+----------------+----------------+----------------+
```
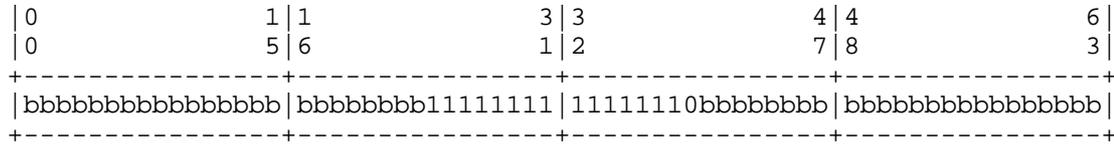
             Figure 6: Formation of IID from Bluetooth Device Address

The IID is then prepended with the prefix fe80::/64, as described in
RFC 4291 [RFC4291] and as depicted in Figure 7. The same link-local
address SHALL be used for the lifetime of the Bluetooth LE L2CAP
channel. (After a Bluetooth LE logical link has been established, it
is referenced with a Connection Handle in HCI. Thus, possibly
changing device addresses do not impact data flows within existing
L2CAP channels. Hence, there is no need to change IPv6 link-local
addresses even if devices change their random device addresses during
L2CAP channel lifetime).

```
        10 bits        54 bits                64 bits
     +----------+-----------------+----------------------+
     |1111111010|      zeros      | Interface Identifier |
     +----------+-----------------+----------------------+
```
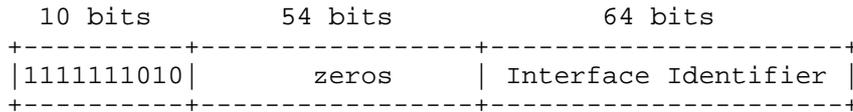
             Figure 7: IPv6 Link-Local Address in Bluetooth LE

A 6LN MUST join the all-nodes multicast address. There is no need
for 6LN to join the solicited-node multicast address, since 6LBR will
know device addresses and hence link-local addresses of all connected
6LNs. The 6LBR will ensure no two devices with the same Bluetooth LE
device address are connected at the same time. Detection of
duplicate link-local addresses is performed by the process on the
6LBR responsible for the discovery of IP-enabled Bluetooth LE nodes
and for starting Bluetooth LE connection establishment procedures.
This approach increases the complexity of 6LBR, but reduces power
consumption on both 6LN and 6LBR in the link establishment phase by
reducing the number of mandatory packet transmissions.

After link-local address configuration, the 6LN sends Router
Solicitation messages as described in [RFC4861], Section 6.3.7.

For non-link-local addresses, 6LNs SHOULD NOT be configured to embed
the Bluetooth device address in the IID by default. Alternative
schemes such as Cryptographically Generated Addresses (CGAs)
[RFC3972], privacy extensions [RFC4941], Hash-Based Addresses (HBAs)
[RFC5535], DHCPv6 [RFC3315], or static, semantically opaque addresses
[RFC7217] SHOULD be used by default. In situations where the
Bluetooth device address is known to be a private device address and/
or the header compression benefits of embedding the device address in
the IID are required to support deployment constraints, 6LNs MAY form
a 64-bit IID by utilizing the 48-bit Bluetooth device address. The
non-link-local addresses that a 6LN generates MUST be registered with
the 6LBR as described in Section 3.2.3.

The tool for a 6LBR to obtain an IPv6 prefix for numbering the
Bluetooth LE network is out of scope of this document, but can be,
for example, accomplished via DHCPv6 Prefix Delegation [RFC3633] or
by using Unique Local IPv6 Unicast Addresses (ULAs) [RFC4193]. Due
to the link model of the Bluetooth LE (see Section 3.2.1) the 6LBR
MUST set the "on-link" flag (L) to zero in the Prefix Information
Option in Neighbor Discovery messages [RFC4861] (see Section 3.2.3).
This will cause 6LNs to always send packets to the 6LBR, including
the case when the destination is another 6LN using the same prefix.

3.2.3. Neighbor Discovery

'Neighbor Discovery Optimization for IPv6 over Low-Power Wireless
Personal Area Networks (6LoWPANs)' [RFC6775] describes the neighbor
discovery approach as adapted for use in several 6LoWPAN topologies,
including the mesh topology. Bluetooth LE does not support mesh
networks; hence, only those aspects that apply to a star topology are
considered.

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

1. A Bluetooth LE 6LN MUST NOT register its link-local address. A
    Bluetooth LE 6LN MUST register its non-link-local addresses with
    the 6LBR by sending a Neighbor Solicitation (NS) message with the
    Address Registration Option (ARO) and process the Neighbor
    Advertisement (NA) accordingly. The NS with the ARO option MUST
    be sent irrespective of the method used to generate the IID. If
    the 6LN registers multiple addresses that are not based on
    Bluetooth device address for the same compression context, the
    header compression efficiency will decrease (see Section 3.2.4).

   2. For sending Router Solicitations and processing Router
       Advertisements, the Bluetooth LE 6LNs MUST follow Sections 5.3
       and 5.4 of [RFC6775], respectively.

3.2.4. 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 the encoding formats
   described in RFC 6282 [RFC6282].

   The Bluetooth LE's star topology structure and ARO can be exploited
   in order to provide a mechanism for address compression. The
   following text describes the principles of IPv6 address compression
   on top of Bluetooth LE.

   The ARO option requires use of a 64-bit Extended Unique Identifier
   (EUI-64) [RFC6775]. In the case of Bluetooth LE, the field SHALL be
   filled with the 48-bit device address used by the Bluetooth LE node
   converted into 64-bit Modified EUI-64 format [RFC4291].

   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.

   When a 6LN is sending a packet to a 6LBR, it MUST fully elide the
   source address if it is a link-local address. For other packets to
   or through a 6LBR with a non-link-local source address that the 6LN
   has registered with ARO to the 6LBR 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. If a source non-
   link-local address is not the latest registered, then the 64 bits of
   the IID SHALL be fully carried in-line (SAM=01), or if the first 48
   bits of the IID match with the latest registered address, then the
   last 16 bits of the IID SHALL be carried in-line (SAM=10). That is,
   if SAC=0 and SAM=11, the 6LN MUST be using the link-local IPv6
   address derived from the Bluetooth LE device address, and if SAC=1
   and SAM=11, the 6LN MUST have registered the source IPv6 address with
   the prefix related to the compression context, and the 6LN MUST be
   referring to the latest registered address related to the compression
   context. The IPv6 address MUST be considered to be registered only
   after the 6LBR has sent a Neighbor Advertisement with an ARO having
   its status field set to success. The destination IPv6 address MUST
   be fully elided if the destination address is the 6LBR's link-local
   address based on the 6LBR's Bluetooth device address (DAC=0, DAM=11).

The destination IPv6 address MUST be fully or partially elided if
context has been set up for the destination address, for example,
DAC=0 and DAM=01 when destination prefix is link-local, and DAC=1 and
DAM=01 if compression context has been configured for the destination
prefix used.

When a 6LBR is transmitting packets to a 6LN, it MUST fully elide the
source IID if the source IPv6 address is the link-local address based
on the 6LBR's Bluetooth device address (SAC=0, SAM=11), and it MUST
elide the source prefix or address if a compression context related
to the IPv6 source address has been set up. The 6LBR also MUST fully
elide the destination IPv6 address if it is the link-local address
based on the 6LN's Bluetooth device address (DAC=0, DAM=11), or 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).

3.2.4.1. Remote Destination Example

When a 6LN transmits an IPv6 packet to a remote destination using
global Unicast IPv6 addresses, if a context is defined for the 6LN's
global IPv6 address, the 6LN has to indicate this context in the
corresponding source fields of the compressed IPv6 header as per
Section 3.1 of RFC 6282 [RFC6282] and has to elide the full IPv6
source address previously registered with ARO (if using the latest
registered address; otherwise, part or all of the IID may have to be
transmitted in-line). For this, the 6LN MUST use the following
settings in the IPv6 compressed header: SAC=1 and SAM=11. The CID
may be set 0 or 1, depending on which context is used. In this case,
the 6LBR can infer the elided IPv6 source address since 1) the 6LBR
has previously assigned the prefix to the 6LNs; and 2) the 6LBR
maintains a Neighbor Cache that relates the device address and the
IID the device has registered with ARO. If a context is defined for
the IPv6 destination address, the 6LN has to also indicate this
context in the corresponding destination fields of the compressed
IPv6 header, and elide the prefix of or the full destination IPv6
address. For this, the 6LN MUST set the DAM field of the compressed
IPv6 header as DAM=01 (if the context covers a 64-bit prefix) or as
DAM=11 (if the context covers a full 128-bit address). DAC MUST be
set to 1. Note that when a context is defined for the IPv6
destination address, the 6LBR can infer the elided destination prefix
by using the context.

   When a 6LBR receives an IPv6 packet sent by a remote node outside the
   Bluetooth LE network, and the destination of the packet is a 6LN, if
   a context is defined for the prefix of the 6LN's global IPv6 address,
   the 6LBR has to indicate this context in the corresponding
   destination fields of the compressed IPv6 header. The 6LBR has to
   elide the IPv6 destination address of the packet before forwarding
   it, if the IPv6 destination address is inferable by the 6LN. For
   this, the 6LBR will set the DAM field of the IPv6 compressed header
   as DAM=11 (if the address is the latest 6LN has registered). DAC
   needs to be set to 1. If a context is defined for the IPv6 source
   address, the 6LBR needs to indicate this context in the source fields
   of the compressed IPv6 header and elide that prefix as well. For
   this, the 6LBR needs to set the SAM field of the IPv6 compressed
   header as SAM=01 (if the context covers a 64-bit prefix) or SAM=11
   (if the context covers a full 128-bit address). SAC is to be set to
   1.

3.2.4.2. Example of Registration of Multiple Addresses

   As described above, a 6LN can register multiple non-link-local
   addresses that map to the same compression context. From the
   multiple address registered, only the latest address can be fully
   elided (SAM=11, DAM=11), and the IIDs of previously registered
   addresses have to be transmitted fully in-line (SAM=01, DAM=01) or,
   in the best case, can be partially elided (SAM=10, DAM=10). This is
   illustrated in the example below:

   1. The 6LN registers first address 2001:db8::1111:2222:3333:4444 to
       a 6LBR. At this point the address can be fully elided using
       SAC=1/SAM=11 or DAC=1/DAM=11.

   2. The 6LN registers second address 2001:db8::1111:2222:3333:5555 to
       the 6LBR. As the second address is now the latest registered, it
       can be fully elided using SAC=1/SAM=11 or DAC=1/DAM=11. The
       first address can now be partially elided using SAC=1/SAM=10 or
       DAC=1/DAM=10, as the first 112 bits of the address are the same
       between the first and the second registered addresses.

   3. Expiration of registration time for the first or the second
       address has no impact on the compression. Hence, even if the
       most recently registered address expires, the first address can
       only be partially elided (SAC=1/SAM=10, DAC=1/DAM=10). The 6LN
       can register a new address, or re-register an expired address, to
       become able to again fully elide an address.

3.2.5. Unicast and Multicast Address Mapping

   The Bluetooth LE Link Layer does not support multicast. Hence,
   traffic is always unicast between two Bluetooth LE nodes. Even in
   the case where a 6LBR is attached to multiple 6LNs, the 6LBR cannot
   do a multicast to all the connected 6LNs. If the 6LBR needs to send
   a multicast packet to all its 6LNs, 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 central is
   battery powered. To further conserve power, the 6LBR MUST keep track
   of multicast listeners at Bluetooth LE link-level granularity (not at
   subnet granularity), and it MUST NOT forward multicast packets to
   6LNs that have not registered as listeners for multicast groups the
   packets belong to. In the opposite direction, a 6LN always has to
   send packets to or through the 6LBR. Hence, when a 6LN needs to
   transmit an IPv6 multicast packet, the 6LN will unicast the
   corresponding Bluetooth LE packet to the 6LBR.

4. Security Considerations

   The transmission of IPv6 over Bluetooth LE links and IPv6 over IEEE
   802.15.4 have similar requirements and concerns for security.
   Security considerations for the Bluetooth LE Link Layer are covered
   by the IPSP [IPSP].

   Bluetooth LE Link Layer supports encryption and authentication by
   using the Counter with CBC-MAC (CCM) mechanism [RFC3610] and a
   128-bit AES block cipher. Upper-layer security mechanisms may
   exploit this functionality when it is available. (Note: CCM does not
   consume octets from the maximum per-packet L2CAP data size, since the
   link-layer data unit has a specific field for them when they are
   used.)

   Key management in Bluetooth LE is provided by the Security Manager
   Protocol (SMP), as defined in [BTCorev4.1].

   The Direct Test Mode offers two setup alternatives: with and without
   accessible HCI. In designs with accessible HCI, the so-called upper
   tester communicates through the HCI (which may be supported by
   Universal Asynchronous Receiver Transmitter (UART), Universal Serial
   Bus (USB), and Secure Digital transports), with the Physical and Link
   Layers of the Bluetooth LE device under test. In designs without
   accessible HCI, the upper tester communicates with the device under
   test through a two-wire UART interface. The Bluetooth specification
   [BTCorev4.1] does not provide security mechanisms for the
   communication between the upper tester and the device under test in

either case. Nevertheless, an attacker needs to physically connect a
device (via one of the wired HCI types) to the device under test to
be able to interact with the latter.

The IPv6 link-local address configuration described in Section 3.2.2
only reveals information about the 6LN to the 6LBR that the 6LBR
already knows from the link-layer connection. This means that a
device using Bluetooth privacy features reveals the same information
in its IPv6 link-local addresses as in its device addresses.
Respectively, a device not using privacy at the Bluetooth level will
not have privacy at the IPv6 link-local address either. For non-
link-local addresses, implementations are recommended not to embed
the Bluetooth device address in the IID by default and instead
support, for example, [RFC3315], [RFC3972], [RFC4941], [RFC5535], or
[RFC7217].

A malicious 6LN may attempt to perform a denial-of-service attack on
the Bluetooth LE network, for example, by flooding packets. This
sort of attack is mitigated by the fact that link-local multicast is
not bridged between Bluetooth LE links and by 6LBR being able to
rate-limit packets sent by each 6LN by making smart use of the
Bluetooth LE L2CAP credit-based flow-control mechanism.

5. References

5.1. Normative References

   [BTCorev4.1]
            Bluetooth Special Interest Group, "Bluetooth Core
            Specification Version 4.1", December 2013,
            <https://www.bluetooth.org/en-us/specification/adopted-
            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,
            <http://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, <http://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,
              <http://www.rfc-editor.org/info/rfc4861>.

   [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
              Address Autoconfiguration", RFC 4862,
              DOI 10.17487/RFC4862, September 2007,
              <http://www.rfc-editor.org/info/rfc4862>.

   [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,
              <http://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,
              <http://www.rfc-editor.org/info/rfc6775>.

   [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6
              Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136,
              February 2014, <http://www.rfc-editor.org/info/rfc7136>.

5.2. Informative References

   [IEEE802] IEEE, "IEEE Standard for Local and Metropolitan Area
              Networks: Overview and Architecture", IEEE 802,
              DOI 10.1109/ieeestd.2002.93395,
              <http://ieeexplore.ieee.org/servlet/opac?punumber=7732>.

   [IEEE802.15.4]
              IEEE, "IEEE Standard for Local and metropolitan area
              networks--Part 15.4: Low-Rate Wireless Personal Area
              Networks (LR-WPANs)", IEEE 802.15.4,
              DOI 10.1109/ieeestd.2011.6012487,
              <http://ieeexplore.ieee.org/servlet/
              opac?punumber=6012485>.

   [RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins,
              C., and M. Carney, "Dynamic Host Configuration Protocol
              for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July
              2003, <http://www.rfc-editor.org/info/rfc3315>.

   [RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with
              CBC-MAC (CCM)", RFC 3610, DOI 10.17487/RFC3610, September
              2003, <http://www.rfc-editor.org/info/rfc3610>.

   [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic
              Host Configuration Protocol (DHCP) version 6", RFC 3633,
              DOI 10.17487/RFC3633, December 2003,
              <http://www.rfc-editor.org/info/rfc3633>.

   [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)",
              RFC 3972, DOI 10.17487/RFC3972, March 2005,
              <http://www.rfc-editor.org/info/rfc3972>.

   [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast
              Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005,
              <http://www.rfc-editor.org/info/rfc4193>.

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

   [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy
              Extensions for Stateless Address Autoconfiguration in
              IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007,
              <http://www.rfc-editor.org/info/rfc4941>.

   [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler,
              "Transmission of IPv6 Packets over IEEE 802.15.4
              Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007,
              <http://www.rfc-editor.org/info/rfc4944>.

   [RFC5535] Bagnulo, M., "Hash-Based Addresses (HBA)", RFC 5535,
              DOI 10.17487/RFC5535, June 2009,
              <http://www.rfc-editor.org/info/rfc5535>.

   [RFC7217] Gont, F., "A Method for Generating Semantically Opaque
              Interface Identifiers with IPv6 Stateless Address
              Autoconfiguration (SLAAC)", RFC 7217,
              DOI 10.17487/RFC7217, April 2014,
              <http://www.rfc-editor.org/info/rfc7217>.

Authors' Addresses

   Johanna Nieminen
   TeliaSonera

   Email: johannamaria.nieminen@gmail.com

   Teemu Savolainen
   Nokia
   Visiokatu 3
   Tampere 33720
   Finland

   Email: teemu.savolainen@nokia.com

Markus Isomaki
Nokia
Karaportti 2-4
Espoo 02610
Finland

Email: markus.isomaki@nokia.com

Basavaraj Patil
AT&T
1410 East Renner Road
Richardson, TX 75082
United States

Email: basavaraj.patil@att.com

Zach Shelby
ARM
150 Rose Orchard Way
San Jose, CA 95134
United States

Email: zach.shelby@arm.com

Carles Gomez
Universitat Politecnica de Catalunya/i2CAT
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: carlesgo@entel.upc.edu