            Transmission of IPv6 packets over ITU-T G.9959 Networks
                       draft-brandt-6man-lowpanz-00

Abstract

   This document describes the frame format for transmission of IPv6
   packets and a method of forming IPv6 link-local addresses and
   statelessly autoconfigured IPv6 addresses on ITU-T G.9959 networks.

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 [RFC2119].

Status of this Memo

Copyright Notice

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. Author's notes

   This chapter MUST be deleted before going for last call.

1.1. Reader's guidance

   This document borrows heavily from RFC4944, "Transmission of IPv6
   Packets over IEEE 802.15.4 Networks". The process of creating this
   document was mainly a simplification; removing the following topics:

   o EUI-64 link-layer addresses

   o Fragmentation layer

   o Mesh routing

   The 16-bit short addresses of 802.15.4 have been changed to 8-bit
   G.9959 NodeIDs.

2. Introduction

   The ITU-T G.9959 recommendation [G.9959] targets low-power Personal
   Area Networks (PANs). This document defines the frame format for
   transmission of IPv6 [RFC2460] packets as well as the formation of
   IPv6 link-local addresses and statelessly autoconfigured IPv6
   addresses on G.9959 networks.

   The general approach is to adapt elements of the 6LoWPAN [RFC4944]
   specification to G.9959 networks. G.9959 provides a Segmentation and
   Reassembly (SAR) layer for transmission of datagrams larger than the
   G.9959 MAC PDU.

   In addition to IPv6 application communication, the frame format
   defined in this specification may be used by IPv6 routing protocols
   such as RPL [RFC6550] or P2P-RPL [P2P-RPL] to implement IPv6 routing
   over G.9959 networks.

   G.9959 networks may implement mesh routing between nodes below the IP
   layer. Mesh routing is out of scope of this document.

2.1. Terms used

   AES: Advanced Encryption Scheme

   EUI-64: Extended Unique Identifier

   HomeID: Link-Layer Network Identifier

    IID: Interface IDentifier

    MAC: Media Access Control

    MTU: Maximum Transmission Unit

    NodeID: Link-Layer Node Identifier (Short Address)

    PAN: Personal Area Network

    PDU: Protocol Data Unit

    SAR: Segmentation And Reassembly

    ULA: Unique Local Address

3. ITU-T G.9959 parameters to use for IPv6 transport

    This chapter outlines properties applying to the PHY and MAC of
    G.9959 and how to use these for IPv6 transport.

3.1. Addressing mode

    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. NodeIDs are unique within the logical
    network identified by the HomeID. The logical network identified by
    the HomeID maps directly to an IPv6 subnet identified by one or more
    IPv6 prefixes.

    An IPv6 host SHOULD construct its link-local IPv6 address and
    routable IPv6 addresses from the G.9959 NodeID in order to facilitate
    IP header compression as described in [RFC6282].

    A word of caution: since HomeIDs and NodeIDs are handed out by a
    network controller function during inclusion, identifier validity and
    uniqueness is limited by the lifetime of the logical network
    membership. This can be cut short by a mishap occurring to the
    network controller. Having a single point of failure at the network
    controller suggests that deployers of high-reliability applications
    should carefully consider adding redundancy to the network controller
    function.

3.2. IPv6 Multicast support

    [RFC3819] recommends that IP subnetworks support (subnet-wide)
    multicast. G.9959 supports direct-range IPv6 multicast while subnet-

wide multicast is not supported natively by G.9959. Subnet-wide
multicast may be provided by an IP routing protocol or a mesh routing
protocol operating below the LoWPAN layer. Mesh routing is out of
scope of this document.

IPv6 multicast packets MUST be carried via G.9959 broadcast.

As per [G.9959], this is accomplished as follows:

1. The destination HomeID of the G.9959 MAC PDU MUST be the HomeID
    of the logical network

2. The destination NodeID of the G.9959 MAC PDU MUST be the
    broadcast NodeID (0xff)

G.9959 broadcast MAC PDUs are only intercepted by nodes within the
logical network identified by the G.9959 HomeID.

3.3. G.9959 MAC PDU size and IPv6 MTU

IPv6 packets MUST use G.9959 transmission profiles which support MAC
PDU payload sizes of 150 bytes or higher, e.g. the R3 profile.

[RFC2460] specifies that IPv6 packets may be up to 1280 octets.
However, a full IPv6 packet does not fit in an G.9959 MAC PDU. The
maximum G.9959 R3 MAC PDU payload size is 158 octets. G.9959 link-
layer security imposes an overhead, which in the extreme case leaves
130 octets available.

G.9959 provides Segmentation And Reassembly for payloads up to 1350
octets. Segmentation however adds further overhead. It is therefore
desirable that datagrams can fit into a single G.9959 MAC PDU. IPv6
Header Compression [RFC6282] improves the chances that a short IPv6
packet can fit into a single G.9959 frame.

3.4. Transmission status indications

The G.9959 MAC layer provides native acknowledgement and
retransmission of MAC PDUs. The G.9959 SAR layer does the same for
larger datagrams. A mesh routing layer may provide a similar feature
for routed communication. Acknowledgment and retransmission improves
the transmission success rate and frees higher layers from the burden
of implementing individual retransmission schemes. The feature may
however introduce challenges to existing TCP rate control algorithms
and it may mask problematic links from IP routing protocols.

3.4.1. IPv6 Socket interface considerations

   An IPv6 socket implementation communicating over G.9959 MUST have
   access to status indications such as link-layer delivery confirmation
   and Ack timeout from the MAC layer. If there is a mesh routing layer
   below the LoWPAN layer, the IPv6 socket implementation MUST have
   access to status indications such as delivery confirmation and Ack
   timeout from the mesh routing layer. This will allow the IPv6 socket
   implementation to adjust its transmissions to the available bandwidth
   of the G.9959 network; transmitting a new IPv6 packet only when it
   positively knows that the previous transmission ended (with fail or
   success).

3.4.2. IPv6 Routing protocol interface considerations

   An IPv6 routing stack communicating over G.9959 MUST have access to
   delivery status indications such as link-layer delivery confirmation
   and Ack timeout from the MAC layer. This will allow the IP routing
   stack to adjust its routing decisions or alternatively initiate route
   rediscovery based on status indications from the link layer.

3.5. Transmission security

   G.9959 provides link-layer security based on a common network key.
   Mission critical applications such as door locks and meters SHOULD
   deploy additional application layer security measures for end-to-end
   authentication and encryption.

   Implementations claiming conformance with this specification MUST
   enable G.9959 common network key security.

4. LoWPAN Adaptation Layer and Frame Format

   The LoWPAN encapsulation formats defined in this chapter are the
   payload in the G.9959 MAC PDU or the G.9959 SAR PDU. IPv6 header
   compression [RFC6282] MUST be supported by implementations of this
   specification.

   All LoWPAN datagrams transported over G.9959 are prefixed by a LoWPAN
   encapsulation header stack. The LoWPAN payload (e.g. an IPv6 packet)
   follows this encapsulation header. Each header in the header stack
   contains a header type followed by zero or more header fields. An
   IPv6 header stack may contain, in the following order, addressing,
   hop-by-hop options, routing, fragmentation, destination options, and
   finally payload [RFC2460]. The LoWPAN header format is structured
   the same way. Currently only payload options are defined for the
   LoWPAN header format.

The definition of LoWPAN headers consists of the dispatch value, the
definition of the header fields that follow, and their ordering
constraints relative to all other headers. Although the header stack
structure provides a mechanism to address future demands on the
LoWPAN adaptation layer, it is not intended to provide general
purpose extensibility. This document specifies a small set of
6LoWPAN header types using the 6LoWPAN header stack for clarity,
compactness, and orthogonality.

4.1. Dispatch Type and Header

The dispatch type is defined by a zero bit as the first bit and a one
bit as the second bit. The dispatch type and header are shown here:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| LoWPAN CmdCls |0 1| Dispatch  |   Type-specific header        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
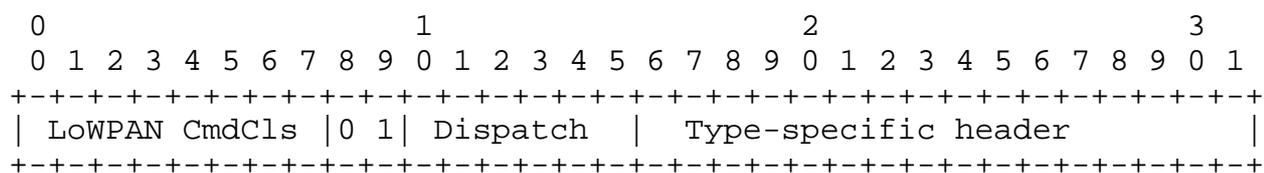
Figure 1: Dispatch Type and Header

LoWPAN CmdCls: LoWPAN Command Class identifier, [G.9959]. Specifies
that the following bits are a LoWPAN encapsulated datagram. Non-
LoWPAN protocols MUST ignore the contents following the LoWPAN
Command Class identifier. TBD: Explicit value to be assigned by
Z-Wave Alliance before last call of this Internet Draft. Refer to
Section 8.

Dispatch: 6-bit selector. Identifies the header type immediately
following the Dispatch Header.

Type-specific header: A header determined by the Dispatch Header.

The dispatch value may be treated as an unstructured namespace. Only
a few symbols are required to represent current LoWPAN functionality.
Although some additional savings could be achieved by encoding
additional functionality into the dispatch byte, these measures would
tend to constrain the ability to address future alternatives.

Dispatch values used in this specification are compatible with the
dispatch values defined by [RFC4944] and [RFC6282].

```
+-----------+---------------------------------------------+-----------+
| Pattern   | Header Type                                 | Reference |
+-----------+---------------------------------------------+-----------+
| 01  000000 | ESC         - Dispatch octet #2 follows    | [RFC6282] |
| 01  000001 | IPv6        - Uncompressed IPv6 Addresses  | [RFC4944] |
|    ...     | reserved    - Defined or reserved          | [RFC4944] |
| 01  1xxxxx | LoWPAN_IPHC - LoWPAN_IPHC compressed IPv6  | [RFC6282] |
| 1x  xxxxxx | reserved    - Defined or reserved          | [RFC4944] |
+-----------+---------------------------------------------+-----------+
```

                     Figure 2: Dispatch Value Bit Pattern

   IPv6: Specifies that the following header is an uncompressed IPv6
   header.

   ESC: Specifies that the following header is a single 8-bit field for
   an additional Dispatch value. It allows support for Dispatch values
   larger than 63. Note: [RFC4944] assigns the value 01 111111 for ESC.
   That assignment was deprecated by [RFC6282].

   LoWPAN_IPHC: IPv6 Header Compression. Refer to [RFC6282].

5. LoWPAN addressing

   IPv6 addresses are derived from link-layer address information to
   save memory in devices and to facilitate efficient IP header
   compression.

   A G.9959 NodeID is 8 bits in length. NodeIDs are mapped into the
   restricted space of IEEE EUI-64 addresses by setting the middle 16
   bits to 0xfffe, the bottom 8 bits to the NodeID, and all other bits
   to zero. As a result, an Interface Identifier (IID) generated from a
   NodeID has the form:

      IID = 0000:00ff:fe00:00XX

   where XX carries the G.9959 NodeID. The universal/local bit is zero
   to indicate local scope.

   This mapping differs from that presented in Appendix A of [RFC4291].
   Using the restricted space ensures that there is no overlap with IIDs
   generated from unrestricted IEEE EUI-64 addresses. Also, including
   0xfffe in the middle of the IID helps avoid overlap with other
   locally managed IIDs. Further, the mapping enables efficient IP
   Header Compression as per [RFC6282].

5.1. Stateless Address Autoconfiguration of routable IPv6 addresses

   The IID defined above MUST be used whether autoconfiguring a ULA IPv6
   address [RFC4193] or a globally routable IPv6 address [RFC3587] in
   G.9959 subnets.

5.2. IPv6 Link Local Address

   The IPv6 link-local address [RFC4291] for a G.9959 interface is
   formed by appending the IID to the IPv6 link local prefix FE80::/64.

   The "Universal/Local" (U/L) bit MUST be set to zero in keeping with
   the fact that this is not a globally unique value [EUI64].

   The resulting link local address is formed as follows:

```
        10 bits            54 bits                    64 bits
      +----------+----------------------+---------------------------+
      |1111111010|       (zeros)        | Interface Identifier (IID)|
      +----------+----------------------+---------------------------+
```
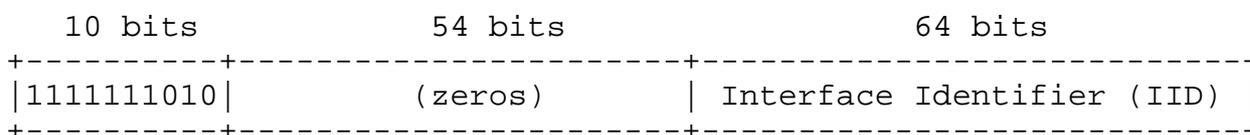
                   Figure 3: IPv6 Link Local Address

5.3. Unicast Address Mapping

   The address resolution procedure for mapping IPv6 unicast addresses
   into G.9959 link-layer addresses follows the general description in
   Section 7.2 of [RFC4861]. The Source/Target Link-layer Address
   option MUST have the following form when the link layer is G.9959.

```
                    0                   1
                    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |     Type      |   Length=1    |
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   | HomeID1 (MS)  | HomeID2       |
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   | HomeID3       | HomeID4 (LS)  |
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   | 0x00          | NodeID        |
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
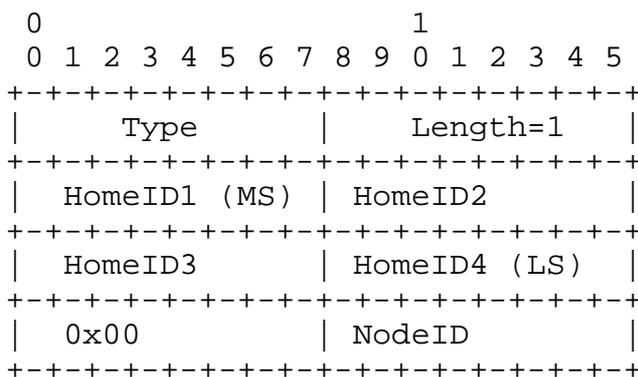
                 Figure 4: IPv6 Unicast Address Mapping

   Option fields:

Type: The value 1 signifies the Source Link-layer address. The value
2 signifies the Destination Link-layer address.

Length: This is the length of this option (including the type and
length fields) in units of 8 octets. The value of this field is
always 1 for G.9959 NodeIDs.

HomeID: This is the G.9959 HomeID the actual interface currently
responds to. The link-layer address may change if the interface
joins another network at a later time.

NodeID: This is the G.9959 NodeID the actual interface currently
responds to. The link-layer address may change if the interface
joins another network at a later time.

6. Header Compression

IPv6 header fields SHOULD be compressed. If IPv6 header compression
is used, it MUST be according to [RFC6282]. This section will simply
identify substitutions that should be made when interpreting the text
of [RFC6282].

In general the following substitutions should be made:

o Replace "802.15.4" with "G.9959"

o Replace "802.15.4 short address" with "G.9959 NodeID"

o Replace "802.15.4 PAN ID" with "G.9959 HomeID"

When a 16-bit address is called for (i.e., an IEEE 802.15.4 "short
address") it MUST be formed by padding the G.9959 NodeID to the left
with zeros:

```
                          0                   1
                          0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
                         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         |      0x00     |     NodeID     |
                         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

64 bit 802.15.4 address details should be ignored. This document
only specifies the use of short addresses.

7. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an
RFC.

8. Z-Wave Allliance Considerations

This document requests that the Z-Wave Alliance assigns a Command
Class identifier for the LoWPAN Command Class; refer to Section 4.1.

Note to RFC Editor: this section may be removed on publication as an
RFC.

9. Security Considerations

The method of derivation of Interface Identifiers from 8-bit NodeIDs
preserves uniqueness within the logical network. However, there is
no protection from duplication through forgery. Neighbor Discovery
in G.9959 links may be susceptible to threats as detailed in
[RFC3756]. G.9959 networks may feature mesh routing. This implies
additional threats due to ad hoc routing as per [KW03]. G.9959
provides capability for link-layer security. G.9959 nodes MUST use
link-layer security with a common key. Doing so will alleviate the
majority of threats stated above. A sizeable portion of G.9959
devices is expected to always communicate within their PAN (i.e.,
within their subnet, in IPv6 terms). In response to cost and power
consumption considerations, these devices will typically implement
the minimum set of features necessary. Accordingly, security for
such devices may rely on the mechanisms defined at the link layer by
G.9959. G.9959 relies on the Advanced Encryption Standard (AES) for
authentication and encryption of G.9959 frames and further employs
challenge-response handshaking to prevent replay attacks.

It is also expected that some G.9959 devices (e.g. billing and/or
safety critical products) will implement coordination or integration
functions. These may communicate regularly with IPv6 peers outside
the subnet. Such IPv6 devices are expected to secure their end-to-
end communications with standard security mechanisms (e.g., IPsec,
TLS, etc).

10. Acknowledgements

Thanks to the authors of RFC 4944 and RFC6282 and members of the IETF
6LoWPAN working group; this document borrows extensively from their
work. Thanks to Kerry Lynn, Tommas Jess Christensen and Erez Ben-
Tovim for useful discussions which helped shape this document.

11. References

11.1. Normative References

   [EUI64]   "GUIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64)
              REGISTRATION AUTHORITY".

   [G.9959]   "ITU-T G.9959: Low-Power, narrowband radio for control
              applications", January 2012.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", RFC 2460, December 1998.

   [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet
              Networks", RFC 2464, December 1998.

   [RFC3587] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global
              Unicast Address Format", RFC 3587, August 2003.

   [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast
              Addresses", RFC 4193, October 2005.

   [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
              Architecture", RFC 4291, February 2006.

   [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
              "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
              September 2007.

   [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler,
              "Transmission of IPv6 Packets over IEEE 802.15.4
              Networks", RFC 4944, September 2007.

   [RFC6282] Hui, J. and P. Thubert, "Compression Format for IPv6
              Datagrams over IEEE 802.15.4-Based Networks", RFC 6282,
              September 2011.

11.2. Informative References

   [P2P-RPL] Goyal, M., Baccelli, E., Philipp, M., Brandt, A., and J.
              Martocci, "IETF, I-D.ietf-roll-p2p-rpl-15, Reactive
              Discovery of Point-to-Point Routes in Low Power and Lossy
              Networks", December 2012.

   [RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor

              Discovery (ND) Trust Models and Threats", RFC 3756,
              May 2004.

   [RFC3819] Karn, P., Bormann, C., Fairhurst, G., Grossman, D.,
              Ludwig, R., Mahdavi, J., Montenegro, G., Touch, J., and L.
              Wood, "Advice for Internet Subnetwork Designers", BCP 89,
              RFC 3819, July 2004.

   [RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R.,
              Levis, P., Pister, K., Struik, R., Vasseur, JP., and R.
              Alexander, "RPL: IPv6 Routing Protocol for Low-Power and
              Lossy Networks", RFC 6550, March 2012.

Authors' Addresses

   Anders Brandt
   Sigma Designs
   Emdrupvej 26A, 1.
   Copenhagen O,   2100
   Denmark

   Phone:
   Fax:
   Email: anders_brandt@sigmadesigns.com

   Jakob Buron
   Sigma Designs
   Emdrupvej 26A, 1.
   Copenhagen O,   2100
   Denmark

   Phone:
   Fax:
   Email: jakob_buron@sigmadesigns.com