Internet Engineering Task Force (IETF)
Request for Comments: 7428
Category: Standards Track
ISSN: 2070-1721
February 2015

A. Brandt
J. Buron
Sigma Designs

Transmission of IPv6 Packets over ITU-T G.9959 Networks

Abstract

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

Status of This Memo

Copyright Notice

Table of Contents

1. 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 [RFC4944] to G.9959 networks. G.9959 provides a Segmentation and Reassembly (SAR) layer for transmission of datagrams larger than the G.9959 Media Access Control Protocol Data Unit (MAC PDU).

[RFC6775] updates [RFC4944] by specifying IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) optimizations for IPv6 Neighbor Discovery (ND) (originally defined by [RFC4861]). This document limits the use of [RFC6775] to prefix and Context ID assignment. An Interface Identifier (IID) may be constructed from a G.9959 link-layer address, leading to a "link-layer-derived IPv6 address". If using that method, Duplicate Address Detection (DAD) is not needed. Alternatively, IPv6 addresses may be assigned centrally via DHCP, leading to a "non-link-layer-derived IPv6 address". Address registration is only needed in certain cases.

In addition to IPv6 application communication, the frame format defined in this document may be used by IPv6 routing protocols such as the Routing Protocol for Low-Power and Lossy Networks (RPL) [RFC6550] or Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks (P2P-RPL) [RFC6997] to implement IPv6 routing over G.9959 networks.

The encapsulation frame defined by this specification may optionally be transported via mesh routing below the 6LoWPAN layer. Mesh-under and route-over routing protocol specifications are out of scope for this document.

1.1. Terms Used

6LoWPAN: IPv6 over Low-Power Wireless Personal Area Network

ABR: Authoritative 6LoWPAN Border Router (Authoritative 6LBR) [RFC6775]

Ack: Acknowledgement

AES: Advanced Encryption Standard

CID: Context Identifier [RFC6775]

DAD: Duplicate Address Detection [RFC6775]

DHCPv6: Dynamic Host Configuration Protocol for IPv6 [RFC3315]

EUI-64: Extended Unique Identifier [EUI64]

G.9959: Short range narrow-band digital radiocommunication transceiver [G.9959]

GHC: Generic Header Compression [RFC7400]

HomeID: G.9959 Link-Layer Network Identifier

IID: Interface Identifier

Link-layer-derived address: IPv6 address constructed on the basis of link-layer address information

MAC: Media Access Control

Mesh-under: Forwarding via mesh routing below the 6LoWPAN layer

MTU: Maximum Transmission Unit

ND: Neighbor Discovery [RFC4861] [RFC6775]

NodeID: G.9959 Link-Layer Node Identifier

Non-link-layer-derived address: IPv6 address assigned by a managed process, e.g., DHCPv6

P2P-RPL: Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks [RFC6997]

PAN: Personal Area Network

PDU: Protocol Data Unit

PHY: Physical Layer

RA: Router Advertisement [RFC4861] [RFC6775]

Route-over: Forwarding via IP routing above the 6LoWPAN layer

RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks [RFC6550]

SAR: G.9959 Segmentation and Reassembly

ULA: Unique Local Address [RFC4193]

1.2. 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].

2. G.9959 Parameters to Use for IPv6 Transport

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

2.1. 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 to each node. NodeIDs are unique within the network identified by the HomeID. The G.9959 HomeID represents an IPv6 subnet that is identified by one or more IPv6 prefixes.

An IPv6 host MUST construct its link-local IPv6 address from the link-layer-derived IID in order to facilitate IP header compression as described in [RFC6282].

A node interface MAY support the M flag of the RA message for the construction of routable IPv6 addresses. A cost-optimized node implementation may save memory by skipping support for the M flag. The M flag MUST be interpreted as defined in Figure 1.

M flag support	M flag value	Required node behavior
No	(ignore)	Node MUST use link-layer-derived addressing
Yes	0	Node MUST use link-layer-derived addressing
	1	Node MUST use DHCPv6-based addressing, and node MUST comply fully with [RFC6775]

Figure 1: RA M Flag Support and Interpretation

A node that uses DHCPv6-based addressing MUST comply fully with the text of [RFC6775].

If DHCPv6-based addressing is used, the DHCPv6 client must use a DHCPv6 Unique Identifier (DUID) of type DUID-UUID, as described in [RFC6355]. The Universally Unique Identifier (UUID) used in the DUID-UUID must be generated as specified in [RFC4122], Section 4.5, starting at the third paragraph in that section (the 47-bit random number-based UUID). The DUID must be stored persistently by the node as specified in Section 3 of [RFC6355].

A word of caution: since HomeIDs and NodeIDs are handed out by a network controller function during inclusion, identifier validity and uniqueness are limited by the lifetime of the network membership. This can be cut short by a mishap occurring at the network controller. Having a single point of failure at the network controller suggests that high-reliability network deployments may benefit from a redundant network controller function.

This warning applies to link-layer-derived addressing as well as to non-link-layer-derived addressing deployments.

2.2. 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 6LoWPAN layer. Routing protocol specifications are out of scope for 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 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 network identified by the HomeID.

2.3. G.9959 MAC PDU Size and IPv6 MTU

IPv6 packets MUST be transmitted using G.9959 transmission profile R3 or higher.

[RFC2460] specifies that any link that cannot convey a 1280-octet packet in one piece must provide link-specific fragmentation and reassembly at a layer below IPv6.

G.9959 provides segmentation and reassembly for payloads up to 1350 octets. IPv6 header compression [RFC6282] improves the chances that a short IPv6 packet can fit into a single G.9959 frame. Therefore, Section 3 of this document specifies that [RFC6282] MUST be supported. With the mandatory link-layer security enabled, a G.9959 R3 MAC PDU may accommodate 6LoWPAN datagrams of up to

130 octets without triggering G.9959 segmentation and reassembly. Longer 6LoWPAN datagrams will lead to the transmission of multiple G.9959 PDUs.

2.4. 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. An IPv6 routing stack communicating over G.9959 may utilize link-layer status indications such as delivery confirmation and Ack timeout from the MAC layer.

2.5. Transmission Security

Implementations claiming conformance with this document MUST enable G.9959 shared network key security.

The shared network key is intended to address security requirements in the home at the normal level of security requirements. For applications with high or very high requirements for confidentiality and/or integrity, additional application-layer security measures for end-to-end authentication and encryption may need to be applied. (The availability of the network relies on the security properties of the network key in any case.)

3. 6LoWPAN Adaptation Layer and Frame Format

The 6LoWPAN encapsulation formats defined in this section are carried as payload in the G.9959 MAC PDU. IPv6 header compression [RFC6282] MUST be supported by implementations of this specification. Further, implementations MAY support Generic Header Compression (GHC) [RFC7400]. A node implementing [RFC7400] MUST probe its peers for GHC support before applying GHC.

All 6LoWPAN datagrams transported over G.9959 are prefixed by a 6LoWPAN encapsulation header stack. The 6LoWPAN payload follows this encapsulation header stack. 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 6LoWPAN header format is structured the same way. Currently, only one payload option is defined for the G.9959 6LoWPAN header format.

The definition of 6LoWPAN 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 6LoWPAN adaptation layer, it is not intended to provide general-purpose extensibility.

An example of a complete G.9959 6LoWPAN datagram can be found in Appendix A.

3.1. Dispatch Header

The Dispatch Header is shown below:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 6LoWPAN CmdCls|   Dispatch    |  Type-specific header         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Dispatch Type and Header

6LoWPAN CmdCls: 6LoWPAN Command Class identifier. This field MUST carry the value 0x4F [G.9959]. The value is assigned by the ITU-T and specifies that the following bits are a 6LoWPAN encapsulated datagram. 6LoWPAN protocols MUST ignore the G.9959 frame if the 6LoWPAN Command Class identifier deviates from 0x4F.

Dispatch: 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 6LoWPAN 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.

Pattern	Header Type	Reference
01 1xxxxx	6LoWPAN_IPHC	[RFC6282]

Other IANA-assigned 6LoWPAN dispatch values do not apply to this document.

Figure 3: Dispatch Values

6LoWPAN_IPHC: IPv6 Header Compression. Refer to [RFC6282].

4. 6LoWPAN Addressing

IPv6 addresses may be autoconfigured from IIDs that may again be constructed from link-layer address information to save memory in devices and to facilitate efficient IP header compression as per [RFC6282]. Link-layer-derived addresses have a static nature and may involuntarily expose private usage data on public networks. Refer to Section 7.

A NodeID is mapped into an IEEE EUI-64 identifier as follows:

IID = 0000:00ff:fe00:YYXX

Figure 4: Constructing a Compressible IID

where XX carries the G.9959 NodeID and YY is a 1-byte value chosen by the individual node. The default YY value MUST be zero. A node MAY use values of YY other than zero to form additional IIDs in order to instantiate multiple IPv6 interfaces. The YY value MUST be ignored when computing the corresponding NodeID (the XX value) from an IID.

The method of constructing IIDs from the link-layer address obviously does not support addresses assigned or constructed by other means. A node MUST NOT compute the NodeID from the IID if the first 6 bytes of the IID do not comply with the format defined in Figure 4. In that case, the address resolution mechanisms of [RFC6775] apply.

4.1. 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.

4.2. IPv6 Link-Local Address

The IPv6 link-local address [RFC4291] for a G.9959 interface is formed by appending the IID defined above 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 5: IPv6 Link-Local Address

4.3. 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   |
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    |     0x00      |    NodeID     |
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    |            Padding            |
                    +-                             -+
                    |          (All zeros)          |
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: 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.

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

4.4. On the Use of Neighbor Discovery Technologies

[RFC4861] specifies how IPv6 nodes may resolve link-layer addresses from IPv6 addresses via the use of link-local IPv6 multicast. [RFC6775] is an optimization of [RFC4861], specifically targeting 6LoWPAN networks. [RFC6775] defines how a 6LoWPAN node may register IPv6 addresses with an authoritative border router (ABR). Mesh-under networks MUST NOT use [RFC6775] address registration. However, [RFC6775] address registration MUST be used if the first 6 bytes of the IID do not comply with the format defined in Figure 4.

4.4.1. Prefix and CID Management (Route-Over)

In route-over environments, IPv6 hosts MUST use [RFC6775] address registration. A node implementation for route-over operation MAY use [RFC6775] mechanisms for obtaining IPv6 prefixes and corresponding header compression context information [RFC6282]. [RFC6775] route-over requirements apply with no modifications.

4.4.2. Prefix and CID Management (Mesh-Under)

An implementation for mesh-under operation MUST use [RFC6775] mechanisms for managing IPv6 prefixes and corresponding header compression context information [RFC6282]. [RFC6775] Duplicate Address Detection (DAD) MUST NOT be used, since the link-layer inclusion process of G.9959 ensures that a NodeID is unique for a given HomeID.

With this exception and the specific redefinition of the RA Router Lifetime value 0xFFFF (refer to Section 4.4.2.3), the text of the following subsections is in compliance with [RFC6775].

4.4.2.1. Prefix Assignment Considerations

As stated by [RFC6775], an ABR is responsible for managing prefix(es). Global routable prefixes may change over time. It is RECOMMENDED that a ULA prefix is assigned to the 6LoWPAN subnet to facilitate stable site-local application associations based on IPv6 addresses. A node MAY support the M flag of the RA message. This influences the way IPv6 addresses are assigned. Refer to Section 2.1 for details.

4.4.2.2. Robust and Efficient CID Management

The 6LoWPAN Context Option (6CO) is used according to [RFC6775] in an RA to disseminate Context IDs (CIDs) to use for compressing prefixes. One or more prefixes and corresponding Context IDs MUST be assigned during initial node inclusion.

When updating context information, a CID may have its lifetime set to zero to obsolete it. The CID MUST NOT be reused immediately; rather, the next vacant CID should be assigned. Header compression based on CIDs MUST NOT be used for RA messages carrying context information. An expired CID and the associated prefix MUST NOT be reset but rather must be retained in receive-only mode if there is no other current need for the CID value. This will allow an ABR to detect if a sleeping node without a clock uses an expired CID, and in response, the ABR MUST return an RA with fresh context information to the originator.

4.4.2.3. Infinite Prefix Lifetime Support for Island-Mode Networks

Nodes MUST renew the prefix and CID according to the lifetime signaled by the ABR. [RFC6775] specifies that the maximum value of the RA Router Lifetime field MAY be up to 0xFFFF. This document further specifies that the value 0xFFFF MUST be interpreted as infinite lifetime. This value MUST NOT be used by ABRs. Its use is only intended for a sleeping network controller -- for instance, a battery-powered remote control being master for a small island-mode network of light modules.

5. Header Compression

IPv6 header compression [RFC6282] MUST be implemented, and GHC [RFC7400] compression for higher layers MAY be implemented. This section will simply identify substitutions that should be made when interpreting the text of [RFC6282] and [RFC7400].

In general, the following substitutions should be made:

- Replace "802.15.4" with "G.9959".
- Replace "802.15.4 short address" with "<Interface><G.9959 NodeID>".
- 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 prepending an Interface label byte to the G.9959 NodeID:

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

A transmitting node may be sending to an IPv6 destination address that can be reconstructed from the link-layer destination address. If the Interface number is zero (the default value), all IPv6 address bytes may be elided. Likewise, the Interface number of a fully elided IPv6 address (i.e., SAM/DAM=11) may be reconstructed to the value zero by a receiving node.

64-bit 802.15.4 address details do not apply.

6. Security Considerations

The method of derivation of Interface Identifiers from 8-bit NodeIDs preserves uniqueness within the 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 shared key. Doing so will alleviate the majority of threats stated above. A sizable 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, Transport Layer Security (TLS), etc.).

7. Privacy Considerations

IP addresses may be used to track devices on the Internet; such devices can in turn be linked to individuals and their activities. Depending on the application and the actual use pattern, this may be undesirable. To impede tracking, globally unique and non-changing characteristics of IP addresses should be avoided, e.g., by frequently changing the global prefix and avoiding unique link-layer-derived IIDs in addresses.

Some link layers use a 48-bit or 64-bit link-layer address that uniquely identifies the node on a global scale, regardless of global prefix changes. The risk of exposing a G.9959 device from its link-layer-derived IID is limited because of the short 8-bit link-layer address.

While intended for central address management, DHCPv6 address assignment also decouples the IPv6 address from the link-layer address. Addresses may be made dynamic by the use of a short DHCP lease period and an assignment policy that makes the DHCP server hand out a fresh IP address every time. For enhanced privacy, the DHCP-assigned addresses should be logged only for the duration of the lease, provided the implementation also allows logging for longer durations as per the operational policies.

It should be noted that privacy and frequently changing address assignments come at a cost. Non-link-layer-derived IIDs require the use of address registration. Further, non-link-layer-derived IIDs cannot be compressed; this leads to longer datagrams and increased link-layer segmentation. Finally, frequent prefix changes necessitate more Context Identifier updates; this not only leads to increased traffic but also may affect the battery lifetime of sleeping nodes.

8. References

8.1. Normative References

[G.9959] International Telecommunication Union, "Short range narrow-band digital radiocommunication transceivers - PHY and MAC layer specifications", ITU-T Recommendation G.9959, January 2015, <http://www.itu.int/rec/T-REC-G.9959>.

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, July 2005, <http://www.rfc-editor.org/info/rfc4122>.

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

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, 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, September 2007, <http://www.rfc-editor.org/info/rfc4861>.

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

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

[RFC6355] Narten, T. and J. Johnson, "Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)", RFC 6355, August 2011, <http://www.rfc-editor.org/info/rfc6355>.

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

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, November 2014, <http://www.rfc-editor.org/info/rfc7400>.

8.2. Informative References

[EUI64] IEEE, "Guidelines for 64-bit Global Identifier (EUI-64TM)", November 2012, <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>.

[KW03] Karlof, C. and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", Elsevier Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, issues 2-3, September 2003.

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

[RFC3587] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global Unicast Address Format", RFC 3587, August 2003, <http://www.rfc-editor.org/info/rfc3587>.

[RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004, <http://www.rfc-editor.org/info/rfc3756>.

[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, <http://www.rfc-editor.org/info/rfc3819>.

[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, <http://www.rfc-editor.org/info/rfc6550>.

[RFC6997] Goyal, M., Baccelli, E., Philipp, M., Brandt, A., and J. Martocci, "Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks", RFC 6997, August 2013, <http://www.rfc-editor.org/info/rfc6997>.

Appendix A. G.9959 6LoWPAN Datagram Example

This example outlines each individual bit of a sample IPv6 UDP packet arriving to a G.9959 node from a host in the Internet via a PAN border router.

In the G.9959 PAN, the complete frame has the following fields.

G.9959:

```
+------+---------+----------+---+-----+----------...
|HomeID|SrcNodeID|FrmControl|Len|SeqNo|DestNodeID|
+------+---------+----------+---+-----+----------+-...
```

6LoWPAN:

```
...+--------------+---------------+----------------------...
   |6LoWPAN CmdCls|6LoWPAN_IPHC Hdr|Compressed IPv6 headers|
  ...-------------+---------------+----------------------+-...
```

IPv6, TCP/UDP, App payload:

```
...+-----------------------+-----------+----------+
   |Uncompressed IPv6 headers|TCP/UDP/ICMP|App payload|
  ...----------------------+-----------+----------+
```

The frame comes from the source IPv6 address 2001:0db8:ac10:ef01::ff:fe00:1206. The source prefix 2001:0db8:ac10:ef01/64 is identified by the IPHC CID = 3.

The frame is delivered in direct range from the gateway that has source NodeID = 1. The Interface Identifier (IID) ff:fe00:1206 is recognized as a link-layer-derived address and is compressed to the 16-bit value 0x1206.

The frame is sent to the destination IPv6 address 2001:0db8:27ef:42ca::ff:fe00:0004. The destination prefix 2001:0db8:27ef:42ca/64 is identified by the IPHC CID = 2.

The IID ff:fe00:0004 is recognized as a link-layer-derived address.

Thanks to the link-layer-derived addressing rules, the sender knows that this is to be sent to G.9959 NodeID = 4, targeting the IPv6 interface instance number 0 (the default).

To reach the 6LoWPAN stack of the G.9959 node (skipping the G.9959 header fields), the first octet must be the 6LoWPAN Command Class (0x4F).

```
        0
        0 1 2 3 4 5 6 7 8
       +-+-+-+-+-+-+-+-+-...
       |     0x4F      |
       +-+-+-+-+-+-+-+-+-+-...
```

The Dispatch Header bits '011' advertise a compressed IPv6 header.

```
        0                   1
        0 1 2 3 4 5 6 7 8 9 0
       +-+-+-+-+-+-+-+-+-+-+-+-...
       |     0x4F      |0 1 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-...
```

The following bits encode the first IPv6 header fields:

```
TF = '11'   : Traffic Class and Flow Label are elided
NH = '1'    : Next Header is elided
HLIM = '10' : Hop limit is 64
```

```
         0                   1
         0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
        |     0x4F      |0 1 1 1 1 1 1 0|
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
```

```
CID = '1'   : CI data follows the DAM field
SAC = '1'   : Src addr uses stateful, context-based compression
SAM = '10'  : Use src CID and 16 bits for link-layer-derived addr
M = '0'     : Dest addr is not a multicast addr
DAC = '1'   : Dest addr uses stateful, context-based compression
DAM = '11'  : Use dest CID and dest NodeID to link-layer-derived addr
```

```
        0                   1                   2
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
       |     0x4F      |0 1 1 1 1 1 1 0|1 1 1 0 0 1 1 1|
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
```

Address compression context identifiers:

SCI = 0x3
DCI = 0x2

```
     2           3
     4 5 6 7 8 9 0 1
  ...+-+-+-+-+-+-+-+-...
    |  0x3  |  0x2  |
    ...+-+-+-+-+-+-+-+-...
```

IPv6 header fields:
(skipping "version" field)
(skipping "Traffic Class")
(skipping "flow label")
(skipping "payload length")

IPv6 header address fields:

SrcIP = 0x1206 : Use SCI and 16 least significant bits of link-layer-derived address

```
(skipping DestIP ) - completely reconstructed from dest NodeID
                     and DCI
```

```
     2           3                   4
     4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7
  ...+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
    |  0x3  |  0x2  |     0x12      |     0x06      |
    ...+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
```

Next Header encoding for the UDP header:

```
Dispatch = '11110': Next Header dispatch code for UDP header
C =      '0'      : 16-bit checksum carried inline
P =      '00'     : Both src port and dest port are carried in-line
```

```
     4   5
     8 9 0 1 2 3 4 5
  ...+-+-+-+-+-+-+-+-...
    |1 1 1 1 0|0|0 0|
    ...+-+-+-+-+-+-+-+-...
```

```
 UDP header fields:

 src port  = 0x1234
 dest port = 0x5678

     5       6                   7                   8
     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 2 3 4 5 6 7
 ...+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
    |     0x12      |     0x34      |     0x56      |     0x78      |
   ...+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-..


 (skipping "length")
 checksum = ....  (actual checksum value depends on
                   the actual UDP payload)


                               1
        8   9                  0
        8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
    ...+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
       |         (UDP checksum)        |
      ...+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...


 Add your own UDP payload here...
```

Acknowledgements

Thanks to the authors of RFC 4944 and RFC 6282, and members of the IETF 6LoWPAN working group; this document borrows extensively from their work. Thanks to Erez Ben-Tovim, Erik Nordmark, Kerry Lynn, Michael Richardson, and Tommas Jess Christensen for useful comments. Thanks to Carsten Bormann for extensive feedback that improved this document significantly. Thanks to Brian Haberman for pointing out unclear details.

Authors' Addresses

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

EMail: anders_brandt@sigmadesigns.com

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

EMail: jakob_buron@sigmadesigns.com