IPv6 over Networks of Resource-constrained Nodes (6lo) WG
Internet-Draft
Intended status: Standards Track
Expires: July 25, 2014
January 21, 2014

A. Brandt
J. Buron
Sigma Designs

Transmission of IPv6 packets over ITU-T G.9959 Networks
draft-ietf-6lo-lowpanz-01

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

Table of Contents

1. Author's notes 2
  1.1. Reader's guidance 2
2. Introduction 3
  2.1. Terms used 3
3. G.9959 parameters to use for IPv6 transport 4
  3.1. Addressing mode 4
  3.2. IPv6 Multicast support 4
  3.3. G.9959 MAC PDU size and IPv6 MTU 5
  3.4. Transmission status indications 5
  3.5. Transmission security 6
4. LoWPAN Adaptation Layer and Frame Format 6
  4.1. Dispatch Header 6
5. LoWPAN addressing 8
  5.1. Stateless Address Autoconfiguration of routable IPv6 addresses 8
  5.2. IPv6 Link Local Address 8
  5.3. Unicast Address Mapping 9
  5.4. On the use of Neighbor Discovery technologies 9
    5.4.1. Prefix and CID management (Route-over) 10
    5.4.2. Prefix and CID management (Mesh-under) 10
6. Header Compression 11
7. IANA Considerations 12
8. Security Considerations 12
9. Acknowledgements 13
10. References 13
  10.1. Normative References 13
  10.2. Informative References 14
Authors' Addresses 14

1. Author's notes

This chapter MUST be deleted before going for document 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 [RFC4944] to G.9959 networks. G.9959 provides a Segmentation and Reassembly (SAR) layer for transmission of datagrams larger than the G.9959 MAC PDU.

[RFC6775] updates [RFC4944] by specifying 6LoWPAN optimizations for IPv6 Neighbor Discovery (ND) (originally defined by [RFC4861]). This document limits the use of [RFC6775] to prefix and Context ID assignment. It is described how to construct an IID from a G.9959 link-layer address. Refer to Section 5. If using that method, Duplicate Address Detection (DAD) is not needed. 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 RPL [RFC6550] or 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. Actual routing protocols are out of scope of this document.

2.1. Terms used

ABR: Authoritative Border Router ([RFC6775])

AES: Advanced Encryption Scheme

EUI-64: Extended Unique Identifier

HomeID: G.9959 Link-Layer Network Identifier

IID: Interface IDentifier

MAC: Media Access Control

MTU: Maximum Transmission Unit

NodeID: G.9959 Link-Layer Node Identifier (Short Address)

PAN: Personal Area Network

PDU: Protocol Data Unit

SAR: Segmentation And Reassembly

ULA: Unique Local Address

3. 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 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 6LoWPAN layer. Routing protocol specifications are 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 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. G.9959 profiles R1 and R2 only supports MPDU payloads around 40 bytes and the transmission speed is down to 9.6kbit/s.

[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. 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 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. Therefore, section Section 4 specifies that [RFC6282] MUST be supported.

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. 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.

3.5. 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 security requirements level. For applications with high or very high requirements on 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.

4. LoWPAN Adaptation Layer and Frame Format

The 6LoWPAN encapsulation formats defined in this chapter are the payload in the G.9959 MAC PDU. IPv6 header compression [RFC6282] MUST be supported by implementations of this specification.

All 6LoWPAN datagrams transported over G.9959 are prefixed by a 6LoWPAN encapsulation header stack. The 6LoWPAN 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 6LoWPAN header format is structured the same way. Currently only payload options are defined for the 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. This document specifies a small set of 6LoWPAN header types using the 6LoWPAN header stack for clarity, compactness, and orthogonality.

4.1. 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 1: Dispatch Type and Header

6LoWPAN CmdCls: 6LoWPAN Command Class identifier. This field MUST carry the value 0x4F [G.9959]. The value specifies that the following bits are a 6LoWPAN encapsulated datagram. Non-6LoWPAN protocols MUST ignore the contents following the 6LoWPAN Command Class identifier.

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.

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

Pattern	Header Type	Reference
01 000001	IPv6 - Uncompressed IPv6 Addresses	[RFC4944]
01 1xxxxx	6LoWPAN_IPHC - 6LoWPAN_IPHC compressed IPv6	[RFC6282]

All other Dispatch values are unassigned in this document.

Figure 2: Dispatch values

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

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

5. LoWPAN addressing

IPv6 addresses are autoconfigured from IIDs which are again constructed from link-layer address information to save memory in devices and to facilitate efficient IP header compression as per [RFC6282].

A G.9959 NodeID is 8 bits in length. A NodeID is mapped into an IEEE EUI-64 identifier as follows:

```
IID = 0000:00ff:fe00:YYXX
```

Figure 3: Constructing a compressible IID

where XX carries the G.9959 NodeID and YY is a one byte value chosen by the individual node. The default YY value MUST be zero. A node MAY use other values of YY 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.

A 6LoWPAN network typically is used for M2M-style communication. 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 3. In that case, the address resolution mechanisms of RFC 6775 apply.

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 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 4: 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   |
                      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      |     0x00      |    NodeID     |
                      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      |            Padding            |
                      +-                             -+
                      |          (All zeros)          |
                      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: 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 the actual interface currently responds to. The link-layer address may change if the interface joins another network at a later time.

5.4. 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 SHOULD 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 3.

In route-over environments, IPv6 hosts MUST use [RFC6775] address registration. [RFC6775] Duplicate Address Detection (DAD) SHOULD NOT be used, since the link-layer inclusion process of G.9959 ensures that a NodeID is unique for a given HomeID.

5.4.1. Prefix and CID management (Route-over)

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.

5.4.2. 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]. Except for the specific redefinition of the RA Router Lifetime value 0xFFFF (refer to Section 5.4.2.3), the text of the following subsections is in compliance with [RFC6775].

5.4.2.1. Prefix assignment considerations

When using [RFC6775] mechanisms for sending RAs, the M flag MUST NOT be set. As stated by [RFC6775], an ABR is responsible for managing prefix(es). Global prefixes may change over time. It is RECOMMENDED that a ULA prefix is always assigned to the 6LoWPAN subnet to facilitate stable site-local application associations based on IPv6 addresses. Prefixes used in the 6LoWPAN subnet are distributed by normal RA mechanisms.

5.4.2.2. Robust and efficient CID management

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

CIDs SHOULD be used in a cyclic fashion to assist battery powered nodes with no real-time clock. When updating context information, a CID may have its lifetime set to zero to obsolete it. The CID SHOULD NOT be reused immediately; rather the next vacant CID should be

assigned. An ABR detecting the use of an obsoleted CID SHOULD immediately send an RA with updated Context Information. Header compression based on CIDs MUST NOT be used for RA messages carrying Context Information. An expired CID and the associated prefix SHOULD NOT be reset but rather 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 clock uses an expired CID and in response, the LBR SHOULD immediately return an RA with fresh Context Information to the originator.

5.4.2.3. 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 SHOULD 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.

6. Header Compression

IPv6 header compression [RFC6282] MUST be supported by implementations of this specification. IPv6 header fields SHOULD be compressed by default. When 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:

- 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 which 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 MUST 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. 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 shared 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).

9. 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, Kerry Lynn, Michael Richardson, Tommas Jess Christensen for useful comments. Thanks to Carsten Bormann for extensive feedback which improved this document significantly.

10. References

10.1. Normative References

[EUI64] IEEE, "communicationIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64) REGISTRATION AUTHORITY", IEEE Std http://standards.ieee.org/regauth/oui/tutorials/EUI64.html, November 2012.

[G.9959] "G.9959 (02/12) + G.9959 Amendment 1 (10/13): Short range, narrow-band digital radiocommunication transceivers", February 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.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, 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.

[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.

10.2. Informative References

[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.

[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.

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