6lo
Internet-Draft
Updates: 4944, 6282 (if approved)
Intended status: Standards Track
Expires: April 21, 2016

S. Chakrabarti
Ericsson
G. Montenegro
Microsoft
R. Droms
Cisco
J. Woodyatt
Nest

October 19, 2015

IANA Registry for 6lowpan ESC Dispatch Code points
draft-chairs-6lo-dispatch-iana-registry-01

Abstract

RFC4944 defines ESC dispatch type for additional dispatch bytes in the 6lowpan header. The value of ESC byte has been updated by RFC6282. However, the usage of ESC extension byte has not been defined in RFC6282 and RFC4944. The purpose of this document is to define the ESC extension byte code points and to request corresponding IANA actions.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2016.

Copyright Notice

Table of Contents

1. Introduction 3
2. Terminology 3
3. Usage of ESC dispatch bytes 3
3.1. Interaction with other RFC4944 implementations 4
3.2. ESC Extension Bytes Typical Sequence 5
3.3. Example: ITU-T G.9903 ESC type usage 5
3.4. NALP Usage 6
4. IANA Considerations 6
5. Security Considerations 7
6. Acknowledgements 7
7. References 7
7.1. Normative References 7
7.2. Informative References 7
Authors' Addresses 8

1. Introduction

[RFC4944] section 5.1 defines the dispatch header and types. The ESC type is defined for using additional dispatch bytes in the 6lowpan header. RFC 6282 modifies the value of the ESC dispatch type and it is recorded in IANA registry [6LOWPAN-IANA]. However, the bytes and usage following the ESC byte are not defined in either [RFC4944] and [RFC6282]. However, in recent years with 6lowpan deployments, the implementations and Standards organizations have started using the ESC extension bytes and a co-ordination between the respective organizations and IETF/IANA are needed.

The following sections record the ITU-T specification for ESC dispatch byte code points as an existing known usage and propose the definition of ESC extension bytes for future applications. The document also requests IANA actions for the first extension byte following the ESC byte.

2. Terminology

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].

3. Usage of ESC dispatch bytes

RFC 4944 [RFC4944] first introduces this "ESC" dispatch header type for extension of dispatch bytes. RFC 6282 [RFC6282] subsequently modified its value to [01 000000].

This document specifies that the first octet following the ESC byte be used for extension type(extended dispatch values). Subsequent octets are left unstructured for the specific use of the extension type:

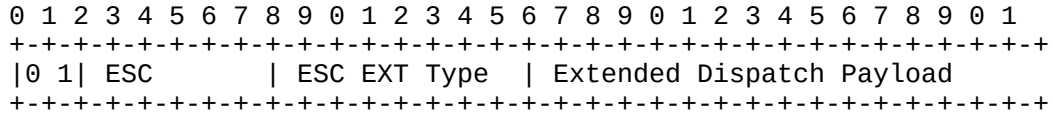


Figure 1: Frame Format with ESC Byte

ESC: The left-most byte is the ESC dispatch type containing ’0100000’

ESC Extension Type(EET): It is the first byte following the ESC byte. Extension type defines the payload for the additional dispatch bytes. The values are from 0 to 255. Value 0 and 255 are reserved for future use. These values are assigned by IANA. The EET values are similar to dispatch values in the 6lowpan header except they are preceeded by the ESC byte. Thus, ESC extension types and dispatch values are using orthogonal code spaces. Though not desirable, multiple ESC bytes MAY appear in a 6lowpan header. Section 3.1 describes how to handle unknown ESC dispatch type.

Extended Dispatch Payload(EDP): This part of frame format must be defined by the corresponding extension type. A specification is required to define each usage of extension type and its corresponding Extension Payload.

Note that section 5.1 in RFC4944 indicates that the Extension Type field may contain additional dispatch values larger than 63 [4944-ERRATA]. Note that the new dispatch type MUST NOT modify the behavior of existing dispatch types for the sake of interoperability.

3.1. Interaction with other RFC4944 implementations

It is expected that RFC4944 existing implementations are not capable of processing ESC extension data bytes as defined in this document. However, implementors have to assume that existing implementation that attempt to process an EET unknown to them will simply drop the packet or ignore the ESC dispatch bytes.

If an implementation following this document, during processing of the received packet reaches the ESC byte for which it does not understand the extension bytes (EET), it MUST drop that packet. However, it is important to clarify that a router node SHOULD forward a 6lowpan packet with the EET bytes as long as it does not attempt to process any ESC extension bytes.

Sequence Of dispatch bytes and ESC bytes: Multiple ESC extension bytes may appear in a packet. Could a 6lowpan packet start with a ESC dispatch type? In another word, should ESC extension always be preceeded by non-ESC dispatch bytes?

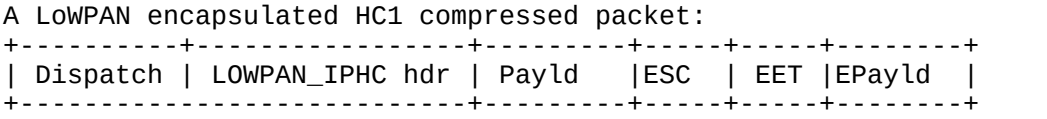
gab: I think the answer is no. But per the previous sentence, you have to assume that your packet will get dropped immediately by any node that does not understand the EET at the beginning of the packet. The closer to the end of the packet are the EET’s, the higher chance there is that a legacy node will recognize and successfully process some dispatch type before the EET and then ignore the EET instead of dropping the entire packet. Unless you know for sure that all nodes in your network understand a given EET (by definition a private and

non-standard deployment), placing it at the beginning is a good way to guarantee that the packet will get dropped.

3.2. ESC Extension Bytes Typical Sequence

The following diagram provides an example when ESC extension bytes might be used:

A LoWPAN encapsulated HC1 compressed packet:



A LoWPAN_IPHC Header, Mesh header and an ESC extenstion byte:

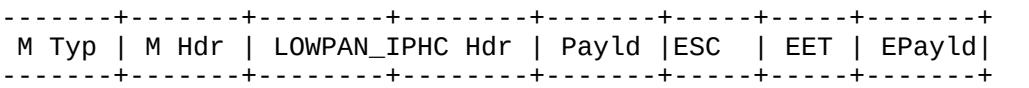


Figure 2: A 6lowpan packet with ESC Bytes

3.3. Example: ITU-T G.9903 ESC type usage

[G3-PLC] provides native mesh-under functionalities. The ESC dispatch type is used with the command frames specified in figure 9-12 and Table 9-35 in [G3-PLC] . The command ID values are 0x01 to 0x1F.

The frame format is defined as follows:

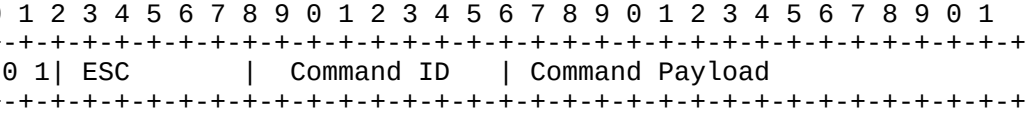


Figure 3: G.9903 Frame Format with ESC Byte

3.4. NALP Usage

There were several comments on 00 draft -- that this draft should provide guidance on NALP usage as there was no clear distinction between ITU-T command mode usage and NALP usage. In order to avaoid such confusion, a NALP usage guidance should be provided. This is a space holder section in order to decide whether NALP usage indeed should belong here.

gab: I don’t think we need to say anything beyond what we already say in 4944: it is not a 6lowpan frame. This was done recognizing that some SDO’s would also define their own frame structure, in particular, Zigbee. There was some effort to agree with them on some way for our definitions to not collide. So prescribing usage of NALP, beyond saying it is not 6lowpan nor the subject of any IETF document, would defeat the purpose.

4. IANA Considerations

This document requests IANA to register the ’ESC Extension Type’ values as per the policy ’Specification Required’[RFC5226] as specified in this document which follows the same policy as in the IANA section of [RFC4944]. For each Extension Type(except the Reserved values)the specification MUST define corresponding Extended Dispatch Payload frame bytes for the receiver implementation to read the ESC bytes with interoperability.

The initial values for the ’ESC Extension Type’ fields are:

Value	Description	Reference
0	Reserved for future use	This document
1-31	Used by ITU-T G.9903 and G.9905 Command IDs	ITU-T G.9903 & ITU-T G.9905
32-254	Unassigned (Reserved for future IANA Assignment-- Spec Required)	This document
255	Reserved for future use	This document

Figure 4: Initial Values for IANA Registry

5. Security Considerations

There is no additional security threats due to the assignments of ESC byte usage described in this document. However, this document forbids defining any extended dispatch values or extension types that modifies the behavior of existing Dispatch types.

6. Acknowledgements

The authors would like to thank the members of the 6lo WG members for the comments in the mailing list. Many thanks to Carsten Bormann, Ralph Droms, Thierry Lys, Cedric Lavenu, Pascal Thubert for their discussions regarding resolving the bits allocation issues which led to this document. Jonathan Hui and Robert Cregie provided extensive reviews and guidance for interoperability. The authors acknowledges the comments from the following people for shaping this document: Paul Duffy, Don Sturek, Michael Richardson, Xavier Vilajosana and Scott Mansfield.

7. References

7.1. Normative References

[4944-ERRATA]
"https://www.rfc-editor.org/errata_search.php?rfc=4944".

[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>.

[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>.

[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>.

7.2. Informative References

[6LOWPAN-IANA]
"https://www.iana.org/assignments/_6lowpan-parameters/_6lowpan-parameters.xhtml".

[G3-PLC] "http://www.itu.int/rec/T-REC-G.9903-201402-I".

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

Authors' Addresses

Samita Chakrabarti
Ericsson
300 Holger Way
San Jose, CA
US

Phone: +1 408 750 5843
Email: samita.chakrabarti@ericsson.com

Gabriel Montenegro
Microsoft
Seattle
US

Email: gabriel.montenegro@microsoft.com

Ralph Droms
Cisco
USA

Email: rdroms@cisco.com

James Woodyatt
Nest
Mountain View, CA
USA

Email: jhw@netstlabs.com

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

L. Del Carpio Vega
M. Robles
R. Morabito
Ericsson

October 19, 2015

IPv6 over 802.11ah
draft-delcarpio-6lo-wlanah-01

Abstract

IEEE 802.11 is an established Wireless LAN (WLAN) technology which provides radio connectivity to a wide range of devices. The IEEE 802.11ah amendment defines a WLAN system operating at sub 1 GHz license-exempt bands designed to operate with low-rate/low-power consumption. This amendment supports large number of stations and extends the radio coverage to several hundreds of meters. This document describes how IPv6 is transported over 802.11ah using 6LoWPAN techniques.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology and Language Requirements 3
3. Overview of 802.11ah 3
3.1. Link Layer Topology of 802.11ah 4
3.2. Device Addressing and Frame Structure 5
3.3. Protocol Version 0 6
3.4. Protocol Version 1 6
3.5. Link Layer Control 7
3.6. Ad Hoc Mode and Extended Service Set 8
3.7. Relation with other 802.11 Versions 9
4. Uses Cases 9
5. 6LoWPAN over 802.11ah 9
6. Stateless Address Autoconfiguration 11
7. Neighbour Discovery in 802.11ah 12
8. Header Compression 12
9. Fragmentation 13
10. Multicast at IP Level 13
11. Internet Connection 13
12. Management of the Network 13
13. IANA Considerations 14
14. Security Considerations 14
15. Acknowledgements 14
16. References 14
16.1. Normative References 14
16.2. Informative References 15
Authors' Addresses 17

1. Introduction

IEEE 802.11 [IEEE802.11], also known as Wi-Fi, is an established Wireless LAN (WLAN) technology operating in unlicensed Industrial, Scientific and Medical (ISM) bands. Its IEEE 802.11ah [IEEE802.11ah] amendment is tailored for Internet of Things (IoT) use-cases and at the moment of writing this draft it is in the final stages of IEEE standardization.

IEEE 802.11ah operates in the Sub-1 GHz spectrum which helps reducing the power consumption. It also supports a larger number of stations on a single Basic Service Set (BSS) and it provides power-saving mechanisms that allow radio stations to sleep in order to save power.

However, the system achieves lower throughput compared to 802.11n/ac amendments.

IEEE 802.11 specifies only the MAC and PHY layers of the radio technology. In other words, 802.11 does not specify a networking layer but it is compatible with commonly used internet protocol such as IPv4 and IPv6. As 802.11ah is a low-rate/low-power technology, the communication protocols used above MAC should also take power-efficiency into consideration. This motivates the introduction of 6LoWPAN techniques [RFC4944] [RFC6282] for efficient transport of IPv6 packets over IEEE 802.11ah radio networks.

This document specifies how to use 6LoWPAN techniques for 802.11ah.

2. Terminology and Language Requirements

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].

Terminology from 802.11ah:

Station (STA): defined in 802.11-2012 [IEEE802.11-2012] as a wireless station which is an addressable unit.

Sensor-STA: defined in 802.11ah as a device having low-power consumption requirements. This device might be a battery operated device.

Non-sensor STA: defined in 802.11ah as device which usually does not have low-power consumption requirements.

In this document, any type STA (sensor STA/non-sensor STA) is associated with a 6LoWPAN Node(6LN).

Access Point (AP): entity maintaining the WLAN Basic Service Set (BSS) and it is associated with the 6LoWPAN Border Router (6LBR). It is assumed that APs are connected to the power-line.

The terms 6LoWPAN Router (6LR) and 6LoWPAN Border Router (6LBR) are defined as in [RFC6775] and in this context 6LoWPAN Nodes (6LN) do not refer to a router (Access Point), just to a host (STA).

3. Overview of 802.11ah

The IEEE 802.11 technology uses the unlicensed spectrum in different ISM bands, using CSMA/CA techniques. Specifically 802.11ah is designed to operate in ISM band below Sub-1 Ghz with a basic

bandwidth of 1Mhz/2Mhz (depending of configuration). The system is formed by an Access Point (AP) which maintains a Basic Service Set (BSS) and stations (STAs). STAs are connected to the AP in a star topology.

The 802.11ah is more energy efficient compared to other conventional 802.11 technologies because of it uses mechanisms which allow STAs to doze periodically and STAs request downlink data when switching to active mode i.e. Traffic Indication Map (TIM) operation, non-TIM operation, Target Wakeup Time (TWT)

An exemplary deployment of a 802.11ah BSS may include a large number of STAs associated to a BSS where STAs are sleeping (dozing) most of the time and they may monitor periodic beacon-frame transmissions containing Traffic Indication Maps (TIM). Data packets intended to STAs cannot be delivered when STAs sleep, thus the TIM indicates which STAs have downlink data buffered at the AP. After reading the TIM, STAs request their buffered data by transmitting a Power-Saving Poll (PS-Poll) frame to the AP. After the downlink data is delivered, STAs enter into sleep mode again. For uplink data delivery, STAs might transmit as soon as their data is available.

There might be STAs that do not monitor constantly the TIM and request downlink data sporadically after waking up.

3.1. Link Layer Topology of 802.11ah

The 802.11ah defines a star topology at L2 link connectivity, where the STAs are connected to the AP and any communication between STAs passes through the AP. It also includes L2 relays to extend the range of the system. As in other 802.11 amendments, the ad-hoc topology is also suported. Finally, the 802.11 standard does not define its own networking layer but is compatible with commonly used protocols e.g. IPv4, IPv6 via the Link Layer Control.

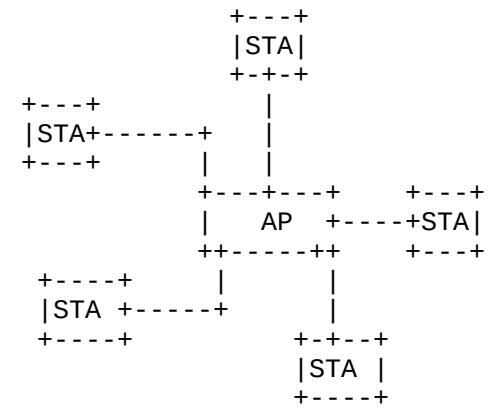


Figure 1: Star Link Layer Topology

It is important to note that the communication link is unidirectional at any given point in time and that the medium is shared by CSMA/CA techniques which avoid that two or more STAs utilize the medium simultaneously.

3.2. Device Addressing and Frame Structure

The 802.11 physical transmission is composed by a preamble which is used to prepare a receiver for frame decoding, basic physical layer information, and the physical layer payload which encapsulates the MAC Protocol Data Unit (MPDU).

There can be different classes of MAC frames in 802.11, the MAC data frame is the only one carrying higher layer data. Other frames are control and management frames which are used to maintain MAC layer functions. In general in 802.11 MAC addresses use the EUI-48 bit address space.

A MAC data frame in 802.11 is composed by a MAC header, a MAC payload and a Frame Check Sequence (FCS) which are encoded in an MPDU. The MAC payload carries Link Layer Control PDUs which encapsulates, for example, IP packets. There are two protocol versions for MAC frame formats, the Protocol Version 0 (PV0) which is the default format of 802.11 and it is inherited to 802.11ah and the Protocol Version 1 (PV1) which has less overhead that PV0 and can be optionally supported by 802.11ah non-sensor STA and it is mandatory supported for 802.11ah sensor STA.

In 802.11ah, the maximum size of the MSDU (MAC payload) is given by the maximum size of a A-MSDU which is constrained by the maximum size

of the A-MPDU of 7991 bytes. This maximum of the A-MPDU is independent of Protocol Version.

In addition, segmentation at 802.11 MAC layer level is supported if required.

3.3. Protocol Version 0

The elements of the MAC data frame with PV0 are defined in 802.11-2012, Section 8.2 [IEEE802.11-2012] and are depicted in the picture below.

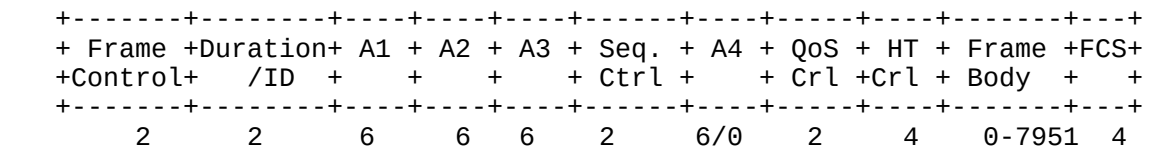


Figure 2: MAC frame PV0

Frame Control: contains information relevant in link layer such as the Protocol Version, frame type and subtype, Power Management, Fragmentation Information, among others.

A1, A2, A3: indicate the recipient, the transmitter and the BSSID which in infraestructure mode is the value of the STA contained in the AP (AP MAC address in practice). They follow 48-bits MAC address format.

A4, Sequence control, QoS control, HT control: The meaning of these field are out of scope of this draft. Please refer to 802.11-2012, Section 8.2.4 [IEEE802.11-2012] for further information.

Frame Body: is of variable-length field and contains the MAC payload for example L3 packets.

FCS: The Frame Check Sequence field is a 32-bit field containing a 32-bit CRC which is calculated over all the fields of the MAC header and the Frame Body field

3.4. Protocol Version 1

The MAC header for the PV1 format is at least formed by a Frame Control field and the address fields. Other fields are optional. Please refer to 802.11-2012, Section 8.8.1 [IEEE802.11ah] for further information.

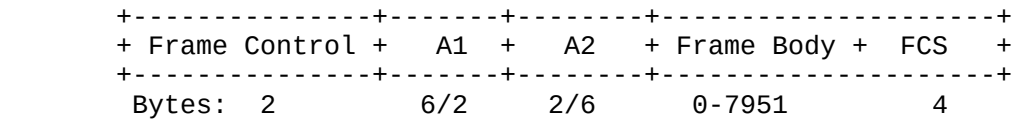


Figure 3: MAC frame PV1 of 802.11ah

Frame control: see above.

A1, A2: indicates the recipient and the transmitter respectively of the frame and it contains the 6-bytes MAC address or the Short ID (2-bytes) provided by the AP after association in a given BSS. Short ID includes the Association Identifier (AID) field which is used in TIM and power-saving mode.

Frame Body: The minimum length for non-data frames is 0 bytes. The maximum length of A-MSDU is constrained by the maximum size of the A-MPDU of 7991 bytes.

3.5. Link Layer Control

The Logical Link Control (LLC) layers works as the interface between higher layers, for example IP, and the 802.11 MAC. It supports higher layer protocol discrimination via the EtherType value utilizing the LLC SNAP or RFC1042.

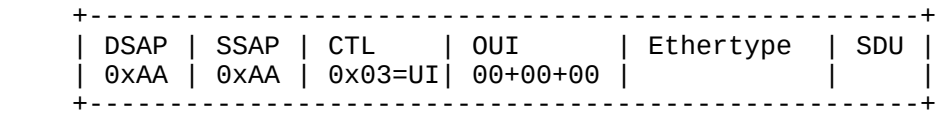


Figure 4: Format of LPD compatible with current 802.11 recommendations

Examples of EtherTypes are 0x0800 and 0x8DD, which are used to identify IPv4 and IPv6, respectively.

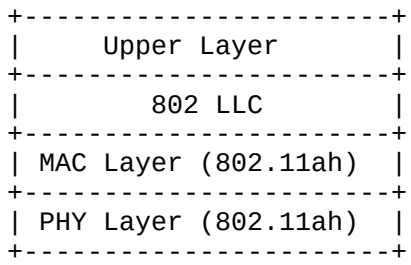


Figure 5: WLAN Protocol Stack

3.6. Ad Hoc Mode and Extended Service Set

The standard allows to connect devices through ad-hoc mechanisms. In this mode the devices are connected using implementation specific protocols e.g. between two STAs or between two APs and the power-saving mechanism of 802.11ah cannot be used (as AP-STA hierarchy is required). The following figure describes STAs connected to AP through 802.11ah and connections between APs are not based on 802.11ah, but are implementation specific.

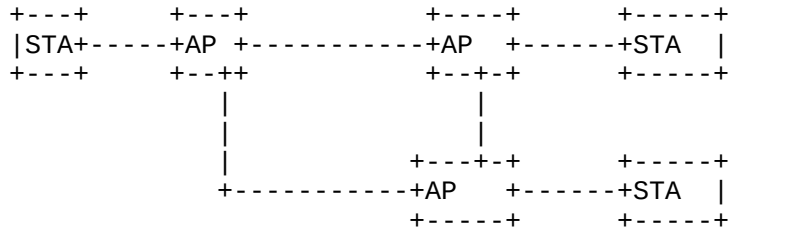


Figure 6: WLAN Ad Hoc Mode

In an Extented Service Set(ESS), the connections between Base Service Station (BSS) happen through a distribution system. The distribution system (DS) maybe realised by a different technology or it can be composed by AP connections.

Figure 7: WLAN Protocol Stack

3.7. Relation with other 802.11 Versions

In principle, the 6Lo stack might be used for other 802.11 versions such as 802.11b, 802.11n and 802.11ac, due to these standards support LLC compatibility. LLC 6lo indentifier would be the same for all mentioned WiFi versions.

4. Uses Cases

[RFC7548] defines use cases for the management of constrained networks: Environmental Monitoring, Infrastructure Monitoring, Industrial Applications, Energy Management, Medical Applications, Building Automation, Home Automation, Transport Applications, Community Network Applications and Field Operations. These uses cases are apply as well to 802.11ah.

As a starting point in 802.11ah specification work, the Task Group AH proposed the following use-case categories [ReferenceUseCase802.11ah]:

- Sensor and Meters, where large number of sensor deliver data through 802.11ah connectivity

- Backhaul Sensor and meter data, where 802.11ah STA can be either directly integrated with a sensor or it will aggregate data from other tree of wireless sensors and then deliver 802.11ah connectivity

- Extended Range Wi-Fi, where the typical range of the Wi-Fi connection will extended due to the use of lower frequencies and other techniques.

5. 6LoWPAN over 802.11ah

IPv4 and IPv6 are compatible with 802.11ah via the LLC. However, 802.11ah technology presents a trade-off between energy consumption and link bitrate. Consequently, 6LoWPAN techniques are beneficial to reduce the overhead of transmissions, save energy and improve throughput. With 6LoWPAN, the nodes, i.e. 6LN, 6LBR, are co-located on the same devices with 802.11 features. The typical 802.11ah network uses a star topology where the 6LBR functionally is co-located with the AP. 6LNs are co-located with STAs and are connected to the 6LBR through 802.11ah links. As mesh topology at MAC level is not defined by the 802.11ah standard, 6LBR is the only router present in the network. Thus, there is no presence of 6LR.

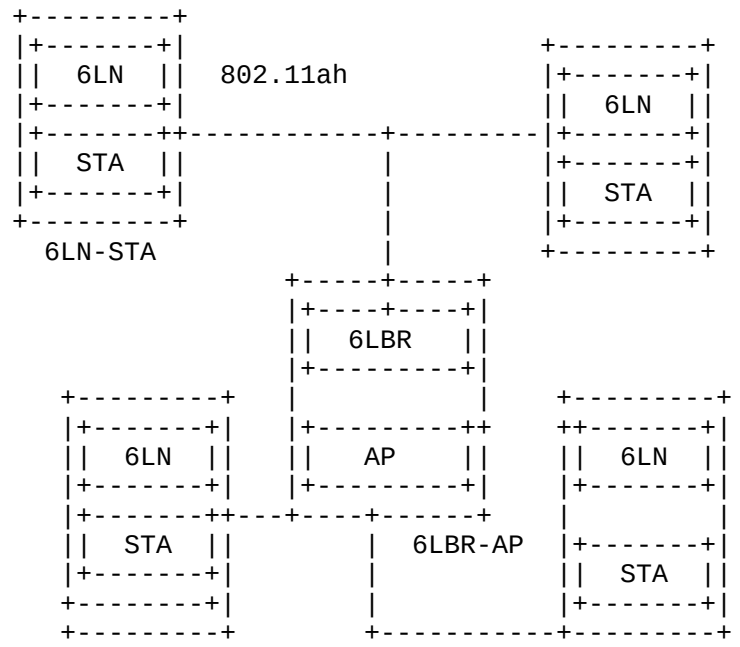


Figure 8: Network Topology

There exists the possibility to have a 802.11ah relay node at L2 to extend the range of an AP. This however is an L2 feature and it is experienced as a single hop by the 6LoWPAN network. In case there is need to connect wirelessly several APs and ad hoc solution needs to be considered.

Devices in this kind of networks, not necessarily have constrained resources (memory, CPU, etc), but the radio link capacity is limited. It might be that APs are connected to mains power and STAs might be for example battery operated sensors. Therefore 6LoWPAN techniques might be good to support transmission of IPv6 packets over 802.11ah battery operated devices. Related to performance gain, a reduction in air-time is achieved if the stack is compressed. The communication 6LN-6LN is not supported directly using link-local addresses, it is done through the 6LBR using the shared prefix used on the subnet. This specification requires IPv6 header compression format specified in [RFC6282].

The Figure below shows the stack for PHY/MAC and IPv6 including 6LoWPAN

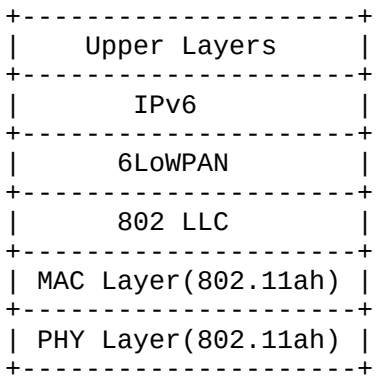


Figure 9: Protocol Stack with 6LoWPAN

6. Stateless Address Autoconfiguration

The IPv6 link local address follows Section 5.3 of [RFC4862] based on the 48-bit MAC device address.

To get the 64-bit Interface Identifier (IID) RFC 7136 [RFC7136] MUST be followed. Section 5 of this RFC states:

"For all unicast addresses, except those that start with the binary value 000, Interface IDs are required to be 64 bits long. If derived from an IEEE MAC-layer address, they must be constructed in Modified EUI-64 format."

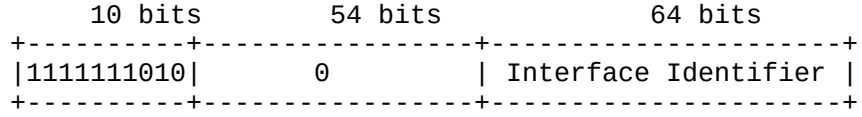


Figure 10: IPv6 link local address

Following Appendix-A of RFC 4291 [RFC4291] the IID is formed inserting two octets, with hexadecimal values of 0xFF and 0xFE in the middle of the 48-bit MAC. The IID would be as follow where "a" is a bit of the 48 MAC address.

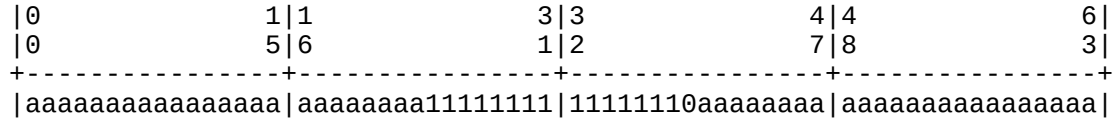


Figure 11: Modified EUI-64 format

For non-link-local addresses a 64-bit IID MAY be formed by utilizing the 48-bit MAC device address. Random IID can be generated for 6LN using alternative methods such as [I-D.ietf-6man-default-iids].

7. Neighbour Discovery in 802.11ah

Neighbour Discovery approach for 6LoWPAN [RFC6775] is applicable to 802.11ah topologies. Related to Host-initiated process, use of Address Registration Option (ARO), through the Neighbour Solicitation (NS) and Neighbour Advertisement (NA). Router Solicitation and Router Advertisement are applicable as well following [RFC6775].

As the topology is star, Multihop Distribution of prefix and 6LoWPAN header compression; and Multihop Duplicated Address Detection (DAD) mechanism are not applicable, since this technology does not cover multihop topology.

8. Header Compression

For header compression, the rules proposed in [RFC6282] are applicable. Section 3.1.1 mentions the base Encoding principle applicable to 802.11ah.

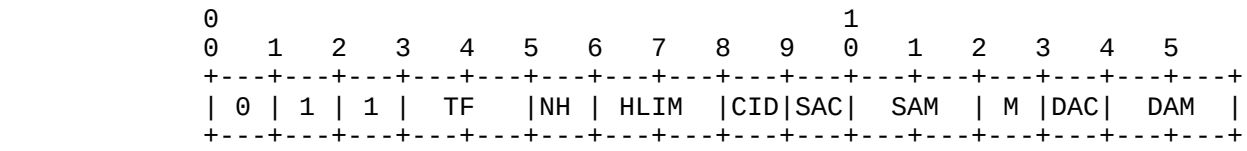


Figure 12: LOWPAN_IPHC base Encoding

TF: Traffic Class; Flow Label; For 802.11ah case would apply this field as defined in [RFC6282].

NH: Next Header; as defined in [RFC6282].

HLIM: Hop Limit; as star topology the common value would be HLIM=1.

CID: Context Identifier Extension; as defined in [RFC6282].

SAC: Source Address Compression; as defined in [RFC6282].

SAM: Source Address Mode; In this case, the combinations for 16-bits are not applicable to this technology since 802.11 uses 48-bits for addresses.

M: Multicast Compression; as defined in [RFC6282].

DAC: Destination Address Compression; as defined in [RFC6282].

DAM: Destination Address Mode. In this case, the combinations for 16-bits are not applicable to this technology since 802.11 uses 48-bits for addresses.

9. Fragmentation

802.11ah perform fragmentation at L2, thus the fragmentation at L3 would be not necessary.

10. Multicast at IP Level

802.11ah supports broadcast and multicast at link layer level, both can be used to carry multicast IP transmission depending on the system's configuration. TBD: add an example.

11. Internet Connection

For Internet connection, the 6LBR acts as router and forwarding packets between 6LNs to and from Internet.

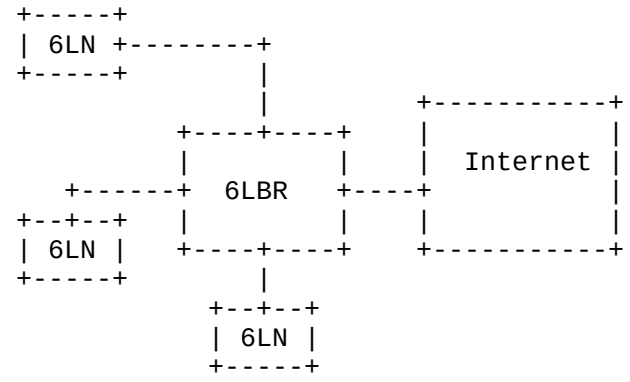


Figure 13: Internet connection of 6Lo network

12. Management of the Network

TBD: how LightWeight Machine to Machine (LWM2M) or CoAP Management Interface (COMI) [I-D.vanderstok-core-comi] aspects can be applied to this technology, considering [RFC7547]

13. IANA Considerations

There are no IANA considerations related to this document.

14. Security Considerations

The security considerations defined in [RFC4944] and its update [RFC6282] can be assumed valid for the 802.11ah case as well. Indeed, the transmission of IPv6 over 802.11ah links meets all the requirements for security as for IEEE 802.15.4. The standard IEEE 802.11ah defines all those aspects related with Link Layer security. As well as for other existing WiFi solutions, 802.11ah Link Layer supports security mechanism such as WPA, WPS, 802.1X. To have a deeper understanding on how the Key Management processes are handled in 802.11ah, please refer to [TBD]

Implementations defined in [I-D.ietf-6man-default-iids], [RFC3972], [RFC4941], or [RFC5535], can be considered, for example, as methods to support non-link local addresses.

For what concerns privacy issues, the draft [I-D.thaler-6lo-privacy-considerations] introduces a series of recommendations which can be applied in order to overcome possible privacy threats in the particular case of technologies designed for IPv6 over networks of resource-constrained nodes.

15. Acknowledgements

This work is partially funded by the FP7 Marie Curie Initial Training Network (ITN) METRICS project (grant agreement No. 607728).

The authors are thankful to the members of IEEE Task Group AH for their valuable comments.

16. References

16.1. Normative References

[IEEE802.11ah] Institute of Electrical and Electronics Engineers (IEEE), "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment- Sub 1 GHz License-Exempt Operation", January 2015.

[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>.

[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>.

16.2. Informative References

[I-D.ietf-6lo-btle] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", draft-ietf-6lo-btle-17 (work in progress), August 2015.

[I-D.ietf-6man-default-iids] Gont, F., Cooper, A., Thaler, D., and S. LIU, "Recommendation on Stable IPv6 Interface Identifiers", draft-ietf-6man-default-iids-08 (work in progress), October 2015.

[I-D.thaler-6lo-privacy-considerations] Thaler, D., "Privacy Considerations for IPv6 over Networks of Resource-Constrained Nodes", draft-thaler-6lo-privacy-considerations-01 (work in progress), October 2015.

[I-D.vanderstok-core-comi] Stok, P., Bierman, A., Schoenwaelder, J., and A. Sehgal, "CoAP Management Interface", draft-vanderstok-core-comi-08 (work in progress), October 2015.

[IEEE802-2014]
Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", 2014.

[IEEE802.11]
Institute of Electrical and Electronics Engineers (IEEE), "Wireless LAN", 2011.

[IEEE802.11-2012]
Institute of Electrical and Electronics Engineers (IEEE), "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2012.

[ReferenceUseCase802.11ah]
Institute of Electrical and Electronics Engineers (IEEE), "Potential compromise of 80211ah use case", 2012.

[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>.

[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>.

[RFC7547] Ersue, M., Ed., Romascanu, D., Schoenwaelder, J., and U. Herberg, "Management of Networks with Constrained Devices: Problem Statement and Requirements", RFC 7547, DOI 10.17487/RFC7547, May 2015, <http://www.rfc-editor.org/info/rfc7547>.

[RFC7548] Ersue, M., Ed., Romascanu, D., Schoenwaelder, J., and A. Sehgal, "Management of Networks with Constrained Devices: Use Cases", RFC 7548, DOI 10.17487/RFC7548, May 2015, <http://www.rfc-editor.org/info/rfc7548>.

Authors' Addresses

Luis Felipe Del Carpio Vega
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: felipe.del.carpio@ericsson.com

Maria Ines Robles
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: maria.ines.robles@ericsson.com

Roberto Morabito
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: roberto.morabito@ericsson.com

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

C. Gomez
S. Darroudi
UPC/i2cat
T. Savolainen
Nokia

October 19, 2015

IPv6 over BLUETOOTH(R) Low Energy Mesh Networks
draft-gomez-6lo-blemesh-00

Abstract

draft-ietf-6lo-btle describes the adaptation of 6LoWPAN techniques to enable IPv6 over Bluetooth low energy networks that follow the star topology. However, recent Bluetooth specifications allow the formation of extended topologies as well. This document defines how IPv6 is transported over Bluetooth low energy mesh networks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Terminology and Requirements Language 3
2. Bluetooth LE Mesh Networks 3
3. Specification of IPv6 over Bluetooth LE mesh networks 3
3.1. Protocol stack 3
3.2. Subnet model 4
3.3. Link model 5
3.3.1. Stateless address autoconfiguration 5
3.3.2. Neighbor Discovery 5
3.3.3. Header compression 6
3.3.4. Unicast and multicast mapping 7
4. IANA Considerations 7
5. Security Considerations 7
6. Acknowledgements 8
7. References 8
7.1. Normative References 8
7.2. Informative References 9
Authors' Addresses 10

1. Introduction

Bluetooth low energy (hereinafter, Bluetooth LE) was first introduced in the Bluetooth 4.0 specification. Bluetooth LE (which has been marketed as Bluetooth Smart) is a low-power wireless technology designed for short-range control and monitoring applications. Bluetooth LE is currently implemented in a wide range of consumer electronics devices, such as smartphones and wearable devices. Given the high potential of this technology for the Internet of Things, the Bluetooth Special Interest Group (Bluetooth SIG) and the IETF have produced specifications in order to enable IPv6 over Bluetooth LE, such as the Internet Protocol Support Profile (IPSP), and draft-ietf-6lo-btle, respectively. Bluetooth 4.0 only supports Bluetooth LE networks that follow the star topology. In consequence, draft-ietf-6lo-btle was specifically developed and optimized for that type of network topology. However, subsequent Bluetooth specifications allow the formation of extended topologies, such as the mesh topology. The functionality described in draft-ietf-6lo-btle is not sufficient and would fail to enable IPv6 over Bluetooth LE mesh networks. This document specifies the mechanisms needed to enable IPv6 over Bluetooth LE mesh networks. This specification also allows to run IPv6 over Bluetooth LE star topology networks, albeit without all the topology-specific optimizations contained in draft-ietf-6lo-btle.

1.1. Terminology and Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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

2. Bluetooth LE Mesh Networks

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

This document assumes a Bluetooth LE mesh network whereby link layer connections have been established between neighboring IPv6-enabled devices. In an IPv6-enabled Bluetooth LE mesh network, a node is a neighbor of another node, and vice versa, if a link layer connection has been established between both by using the IPSP functionality for discovery and link layer connection establishment for IPv6 packet transport.

3. Specification of IPv6 over Bluetooth LE mesh networks

3.1. Protocol stack

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

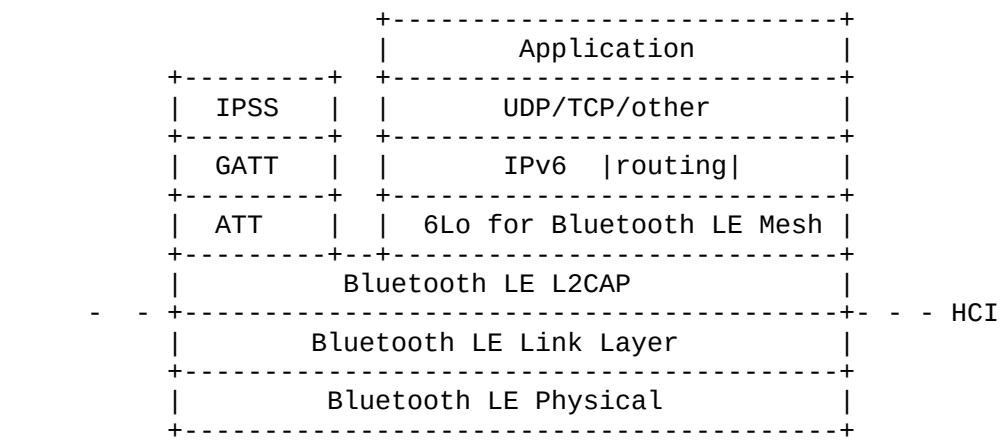
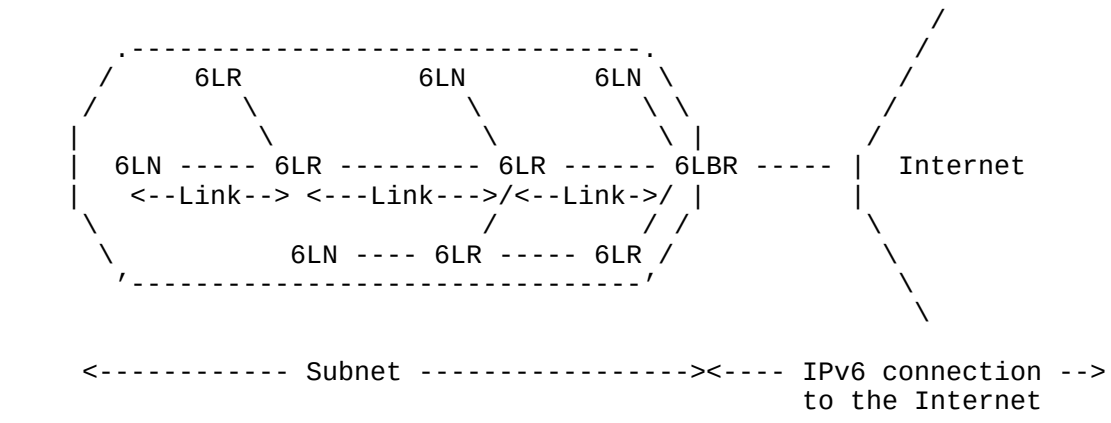


Figure 1: Protocol stack for IPv6-enabled Bluetooth LE mesh networks

3.2. Subnet model

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



to the Internet

Figure 2: Example of an IPv6-based Bluetooth LE mesh network connected to the Internet

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

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

3.3. Link model

3.3.1. Stateless address autoconfiguration

6LN, 6LR and 6LBR IPv6 addresses of a Bluetooth LE mesh network are configured as per section 3.2.2 of draft-ietf-6lo-btle.

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

3.3.2. Neighbor Discovery

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

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 its routers 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. The ARO option requires use of an EUI-64 identifier [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].

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

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

6LR TBD

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

3.3.3. Header compression

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

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

The specific optimizations of draft-ietf-6lo-btle for header compression, which exploit the star topology and ARO, cannot be generalized in a Bluetooth LE mesh network. Still, a subset of those optimizations can be applied in some cases in a Bluetooth LE mesh network. In particular, the latter comprise link-local interactions,

non-link-local packet transmissions originated and performed by a 6LN, and non-link-local packet transmissions originated by a 6LN neighbor and sent to a 6LN. For the rest of packet transmissions, context-based compression MAY be used.

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

When a 6LN transmits a packet, with a non-link-local source address that the 6LN has registered with ARO in the next-hop router for the indicated prefix, the source address MUST be fully elided if it is the latest address that the 6LN has registered for the indicated prefix (SAC=1, SAM=11). If the source non-link-local address is not the latest registered by the 6LN, then the 64-bits of the IID SHALL be fully carried in-line (SAC=1, SAM=01) or if the first 48-bits of the IID match with the latest address registered by the 6LN, then the last 16-bits of the IID SHALL be carried in-line (SAC=1, SAM=10).

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

3.3.4. Unicast and multicast mapping

TBD

4. IANA Considerations

There are no IANA considerations related to this document.

5. Security Considerations

The security considerations in draft-ietf-6lo-btle apply.

Further security considerations on additional threats due to ad-hoc routing. TBD.

6. Acknowledgements

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

The authors of this document are grateful to all draft-ietf-6lo-btle authors, since this document borrows many concepts (albeit, with necessary extensions) from draft-ietf-6lo-btle.

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

7. References

7.1. 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>.

[I-D.ietf-6lo-btle] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", draft-ietf-6lo-btle-17 (work in progress), August 2015.

[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>.

7.2. Informative References

[fifteendotfour] IEEE Computer Society, "IEEE Std. 802.15.4-2011 IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", June 2011.

[I-D.ietf-6man-default-iids] Gont, F., Cooper, A., Thaler, D., and S. LIU, "Recommendation on Stable IPv6 Interface Identifiers", draft-ietf-6man-default-iids-08 (work in progress), October 2015.

[IEEE802-2001] Institute of Electrical and Electronics Engineers (IEEE), "IEEE 802-2001 Standard for Local and Metropolitan Area Networks: Overview and Architecture", 2002.

[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

Carles Gomez
Universitat Politecnica de Catalunya/Fundacio i2cat
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: carlesgo@entel.upc.edu

Seyed Mahdi Darroudi
Universitat Politecnica de Catalunya/Fundacio i2cat
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: s.darroudi2014@yahoo.com

Teemu Savolainen
Nokia
Visiokatu 3
Tampere 33720
Finland

Email: teemu.savolainen@nokia.com

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2016

Y-G. Hong
Y-H. Choi
ETRI

October 17, 2015

Use cases for IPv6 over Networks of Resource-constrained Nodes
draft-hong-6lo-use-cases-00

Abstract

This document describes the characteristics of link layer technologies that are used at constrained node networks and typical use cases of IPv6 over networks of resource-constrained nodes. In addition to IEEE 802.15.4, various link layer technologies such as BLE, Z-wave, DECT-ULE, MS/TP, NFC, and IEEE 802.15.4e are widely used at constrained node networks for typical services. Based on these link layer technologies, IPv6 over networks of resource-constrained nodes has various and practical use cases. To efficiently implement typical services, the applicability and consideration of several design spaces are described.

Table of Contents

1. Introduction 2
2. Conventions and Terminology 3
3. 6lo Link layer technologies 4
3.1. ITU-T G.9959 4
3.2. Bluetooth Low Energy 4
3.3. DECT-ULE 4
3.4. Master-Slave/Token-Passing 5
3.5. NFC 5
3.6. IEEE 802.15.4e TSCH 6
4. Design Space 6
5. 6lo Use Cases 7
5.1. Use case of NFC: Alternative Secure Transfer 7
5.2. Use case of ITU-T G.9959 9
5.3. Use case of Bluetooth Low Energy 9
5.4. Use case of DECT-ULE 9
5.5. Use case of Master-Slave/Token-Passing 10
5.6. Use case of IEEE 802.15.4e TSCH 10
6. IANA Considerations 10
7. Security Considerations 10
8. Acknowledgements 10
9. References 10
9.1. Normative References 10
9.2. Informative References 11
Authors' Addresses 12

1. Introduction

Running IPv6 on constrained node networks has different features due to the characteristics of constrained node networks such as small packet size, short link-layer address, low bandwidth, network topology, low power, low cast, and large number of devices [RFC4919]. For example, because some IEEE 802.15.4 link layers have an MTU of 127 octets and IPv6 requires 1280 bytes, an appropriate fragmentation and reassembly adaptation layer must be provided at the layer of below IPv6. Also, due to the limited size of IEEE 802.15.4 frame and the length shortage of data delivery, it makes the need for header compression. IETF 6lowpan (IPv6 over low power and WPAN) working group published [RFC4944], an adaptation layer for sending IPv6 packets over low power WPAN, [RFC6282], compression format for IPv6

datagrams over IEEE 802.15.4-based networks, and [RFC6775], Neighbor Discovery Optimization for 6lowpan.

As IoT (Internet of Things) services becomes more popular, various link layer technologies such as BLE, Z-wave, DECT-ULE, MS/TP, NFC, and IEEE 802.15.4e are actively used. And the need of transmission of IPv6 packets over these link layer technologies is required. A number of IPv6-over-foo documents have been developed in the IETF 6lo (IPv6 over Networks of Resource-constrained Nodes) and 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) working group.

In the 6lowpan working group, the [RFC6568], "Design and Application Spaces for 6LoWPANs" was published and it describes potential application scenarios and use cases for low-power wireless personal area networks. In this document, various design spaces such as deployment, network size, power source, connectivity, multi-hop communication, traffic pattern, security level, mobility, and QoS were analyzed. And it described a fundamental set of 6lowpan application scenarios and use cases; Industrial monitoring-Hospital storage rooms, Structural monitoring-Bridge safety monitoring, Connected home-Home Automation, Healthcare-Healthcare at home by tele-assistance, Vehicle telematics-telematics, and Agricultural monitoring-Automated vineyard.

Even though the [RFC6568] describes some potential application scenarios and use cases and it lists the design space in the context of 6lowpan, it needs a different use cases and design space in the context of the 6lo working group to provide practical information of 6lo technologies. To do this, the use case of 6lo is required to consider the followings;

- 6lo use cases SHOULD be uniquely different to the 6lowpan use cases.

- 6lo use cases SHOULD cover various IoT related wire/wireless link layer technology including the IEEE 802.15.4.

- 6lo use cases MAY describe characteristics of each link layer technologies and typical use case of each link layer technology and then 6lo use cases’s applicability.

2. Conventions and Terminology

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].

3. 6lo Link layer technologies

3.1. ITU-T G.9959

The ITU-T G.9959 recommendation G. [G.9959] targets low-power Personal Area Networks (PANs). 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 [RFC7428].

3.2. Bluetooth Low Energy

Bluetooth LE was introduced in Bluetooth 4.0, enhanced in Bluetooth 4.1, and developed even further in successive versions. Bluetooth SIG has also published Internet Protocol Support Profile (IPSP), which includes Internet Protocol Support Service (IPSS). The IPSP enables discovery of IP-enabled devices and establishment of link-layer connection for transporting IPv6 packets. IPv6 over Bluetooth LE is dependent on both Bluetooth 4.1 and IPSP 1.0 or newer.

Devices such as mobile phones, notebooks, tablets and other handheld computing devices which will include Bluetooth 4.1 chipsets will also have the low-energy functionality of Bluetooth. Bluetooth LE will also 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 the mobile phone to a server on the Internet [I-D.ietf-6lo-btle].

3.3. DECT-ULE

DECT ULE is a low power air interface technology that is designed to support both circuit switched for service, such as voice communication, and for packet mode data services at modest data rate.

The DECT ULE protocol stack consists of the PHY layer operating at frequencies in the 1880 - 1920 MHz frequency band depending on the region and uses a symbol rate of 1.152 Mbps. Radio bearers are allocated by use of FDMA/TDMA/TDD technics.

In its generic network topology, DECT is defined as a cellular network technology. However, the most common configuration is a star network with a single FP defining the network with a number of PP attached. The MAC layer supports both traditional DECT as this is used for services like discovery, pairing, security features etc. All these features have been reused from DECT.

The DECT ULE device can switch to the ULE mode of operation, utilizing the new ULE MAC layer features. The DECT ULE Data Link Control (DLC) provides multiplexing as well as segmentation and re-assembly for larger packets from layers above. The DECT ULE layer also implements per-message authentication and encryption. The DLC layer ensures packet integrity and preserves packet order, but delivery is based on best effort.

The current DECT ULE MAC layer standard supports low bandwidth data broadcast. However the usage of this broadcast service has not yet been standardized for higher layers [I-D.ietf-6lo-dect-ule].

3.4. Master-Slave/Token-Passing

Master-Slave/Token-Passing (MS/TP) is a contention-free access method for the RS-485 physical layer, which is used extensively in building automation networks. This specification defines the frame format for transmission of IPv6 [RFC2460] packets and the method of forming link-local and statelessly autoconfigured IPv6 addresses on MS/TP networks. The general approach is to adapt elements of the 6LoWPAN [RFC4944] specification to constrained wired networks.

An MS/TP device is typically based on a low-cost microcontroller with limited processing power and memory. Together with low data rates and a small address space, these constraints are similar to those faced in 6LoWPAN networks and suggest some elements of that solution might be leveraged. MS/TP differs significantly from 6LoWPAN in at least three respects: a) MS/TP devices typically have a continuous source of power, b) all MS/TP devices on a segment can communicate directly so there are no hidden node or mesh routing issues, and c) recent changes to MS/TP provide support for large payloads, eliminating the need for link-layer fragmentation and reassembly.

MS/TP is designed to enable multidrop networks over shielded twisted pair wiring. It can support a data rate of 115,200 baud on segments up to 1000 meters in length, or segments up to 1200 meters in length at lower baud rates. An MS/TP link requires only a UART, an RS-485 transceiver with a driver that can be disabled, and a 5ms resolution timer. These features make MS/TP a cost-effective field bus for the most numerous and least expensive devices in a building automation network [I-D.ietf-6lo-6lobac].

3.5. NFC

NFC technology enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC complements many popular consumer level

wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and it enables a consumer to utilize one device across different systems.

Extending the capability of contactless card technology, NFC also enables devices to share information at a distance that is less than 10 cm with a maximum communication speed of 424 kbps. Users can share business cards, make transactions, access information from a smart poster or provide credentials for access control systems with a simple touch.

NFC's bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch. In addition to the easy connection and quick transactions, simple data sharing is also available [I-D.ietf-6lo-nfc].

3.6. IEEE 802.15.4e TSCH

[TBD]

4. Design Space

The [RFC6568] lists the dimensions used to describe the design space of wireless sensor networks in the context of the 6LoWPAN working group. The design space is already limited by the unique characteristics of a LoWPAN (e.g., low power, short range, low bit rate). In the RFC 6558, the following design space is described; Deployment, Network size, Power source, Connectivity, Multi-hop communication, Traffic pattern, Mobility, Quality of Service (QoS).

The design space of 6lo is a little different to those of the RFC 6558 due to the different characteristics of 6lo link layer technologies. The following design space can be considered.

- Network access/Bootstrapping: 6lo nodes can be connected randomly, or in an organized manner. The bootstrapping has different characteristics of each link layer technologies.

- Topology: Topology of 6lo networks may inherently follow the characteristics of each link layer technologies. A star topology can be configured or point-to-point or mesh topology can be configured.

- L2-Mesh or L3-Mesh: L2-mesh and L3-mesh may inherently follow the characteristics of each link layer technologies. Some link layer technologies may support L2-mesh and some may not support.

- Multi-link subnet, single subnet: The selection of multi-link subnet and single subnet depends on connectivity and the number of 6lo nodes.

- Data rate: Originally, the link layer technologies of 6lo has low rate of data transmission. But, by adjusting the MTU, it can deliver higher data rate.

- Buffering requirements: Some 6lo use case may require more data rate than the link layer technology support. In this case, a buffering mechanism to manage the date is required.

- Security Requirements: Some 6lo use case can transfer some important and personal data between 6lo nodes. In this case, high-level security support is required.

- Mobility across 6lo networks and subnets: The movement of 6lo nodes is dependent on the 6lo use case. If the 6lo nodes can move or moved around, it requires the mobility management mechanism.

- Time synchronization requirements: The requirement of time synchronization is dependent on the 6lo use case. For some 6lo use case related to health service, the measured data must be recorded with exact time and must be transferred with time synchronization.

- Reliability and QoS: Some 6lo use case requires high reliability, for example real-time service or health-related services.

- Data models: 6lo use case may various data models. Some 6lo use case may require short data length and randomly. Some 6lo use case may require continuous data and periodic data transmission.

- Security Bootstrapping: Without the external operations, 6lo nodes must have the security bootstrapping mechanism.

5. 6lo Use Cases

5.1. Use case of NFC: Alternative Secure Transfer

According to applications, various secured data can be handled and transferred. Depending on security level of the data, methods for transfer can be alternatively selected. The personal data having serious issues should be transferred securely, but data transfer by using Wi-Fi and Bluetooth connections cannot always be secure because of their a little long radio frequency range. Hackers can overhear the personal data transfer behind hidden areas. Therefore, methods need to be alternatively selected to transfer secured data. Voice

and video data, which are not respectively secure and requires long transmission range, can be transferred by 3G/4G technologies, such as WCDMA, GSM, and LTE. Big size data, which are not secure and requires high speed and broad bandwidth, can be transferred by Wi-Fi and wired network technologies. However, the person data, which are serious issues so requires secure transfer in wireless area, can be securely transferred by NFC technology. It has very short frequency range ? nearly single touch communication.

Example: Secure Transfer by Using NFC in Healthcare Services with Tele-Assistance

A senior citizen who lives alone wears one to several wearable 6lo devices to measure heartbeat, pulse rate, etc. The 6lo devices are densely installed at home for movement detection. An LoWPAN Border Router (LBR) at home will send the sensed information to a connected healthcare center. Portable base stations with LCDs may be used to check the data at home, as well. Data is gathered in both periodic and event-driven fashion. In this application, event-driven data can be very time-critical. In addition, privacy also becomes a serious issue in this case, as the sensed data is very personal.

While the senior citizen is provided audio and video healthcare services by a tele-assistance based on LTE connections, the senior citizen can alternatively use NFC connections to transfer the personal sensed data to the tele-assistance. At this moment, hidden hackers can overhear the data based on the LTE connection, but they cannot gather the personal data over the NFC connection.

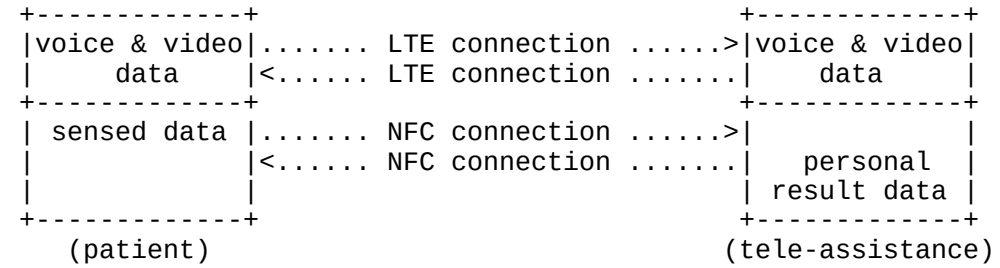


Figure 1: Alternative Secure Transfer in Healthcare Services

Dominant parameters in secure transfer by using NFC in healthcare services:

- Network access/Bootstrapping: Pre-planned. MP2P/P2MP (data collection), P2P (local diagnostic).

- Topology: Small, NFC-enabled device connected to the Internet.
- L2-mesh or L3-mesh: NFC does not support L2-mesh, L3-mesh can be configured.
- Multi-link subnet, single subnet: a Single-hop for gateway; patient’s body network is mesh topology.
- Data rate: Small data rate.
- Buffering requirements: Low requirement.
- Security requirements: Data privacy and security must be provided. Encryption is required.
- Mobility: Moderate (patient’s mobility).
- Time Synchronization: Highly required.
- Reliability and QoS: High level of reliability support (life-or-death implication), role-based.
- Data models: Short data length and periodic (randomly).
- Security Bootstrapping: Highly required.
- Other Issues: Plug-and-play configuration is required for mainly non-technical end-users. Real-time data acquisition and analysis are important. Efficient data management is needed for various devices that have different duty cycles, and for role-based data control. Reliability and robustness of the network are also essential.

5.2. Use case of ITU-T G.9959

[TBD]

5.3. Use case of Bluetooth Low Energy

[TBD]

5.4. Use case of DECT-ULE

[TBD]

5.5. Use case of Master-Slave/Token-Passing

[TBD]

5.6. Use case of IEEE 802.15.4e TSCH

[TBD]

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

[TBD]

8. Acknowledgements

[TBD]

9. References

9.1. Normative References

[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>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <http://www.rfc-editor.org/info/rfc4919>.

[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>.

[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>.

[RFC6568] Kim, E., Kaspar, D., and JP. Vasseur, "Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6568, DOI 10.17487/RFC6568, April 2012, <http://www.rfc-editor.org/info/rfc6568>.

[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>.

[RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015, <http://www.rfc-editor.org/info/rfc7428>.

9.2. Informative References

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[I-D.ietf-6lo-btle] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", draft-ietf-6lo-btle-17 (work in progress), August 2015.

[I-D.ietf-6lo-dect-ule] Mariager, P., Petersen, J., Shelby, Z., Logt, M., and D. Barthel, "Transmission of IPv6 Packets over DECT Ultra Low Energy", draft-ietf-6lo-dect-ule-03 (work in progress), September 2015.

[I-D.ietf-6lo-6lobac] Lynn, K., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over MS/TP Networks", draft-ietf-6lo-6lobac-02 (work in progress), July 2015.

[I-D.ietf-6lo-nfc] Youn, J. and Y. Hong, "Transmission of IPv6 Packets over Near Field Communication", draft-ietf-6lo-nfc-01 (work in progress), July 2015.

[G.9959] "International Telecommunication Union, "Short range narrow-band digital radiocommunication transceivers - PHY and MAC layer specifications", ITU-T Recommendation", January 2015.

Authors' Addresses

Yong-Geun Hong
ETRI
161 Gajeong-Dong Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 6557
Email: yghong@etri.re.kr

Younghwan Choi
ETRI
218 Gajeongno, Yuseong
Daejeon 305-700
Korea

Phone: +82 42 860 1429
Email: yhc@etri.re.kr

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2016

Y-G. Hong
Y-H. Choi
ETRI
J-S. Youn
DONG-EUI Univ
D-K. Kim
KNU
J-H. Choi
Samsung Electronics Co.,
October 17, 2015

Transmission of IPv6 Packets over Near Field Communication
draft-ietf-6lo-nfc-02

Abstract

Near field communication (NFC) is a set of standards for smartphones and portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than 10 cm. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum. The NFC technology has been widely implemented and available in mobile phones, laptop computers, and many other devices. This document describes how IPv6 is transmitted over NFC using 6LowPAN techniques.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 19, 2016.

Table of Contents

1. Introduction 3
2. Conventions and Terminology 4
3. Overview of Near Field Communication Technology 4
3.1. Peer-to-peer Mode of NFC 4
3.2. Protocol Stacks of NFC 5
3.3. NFC-enabled Device Addressing 6
3.4. NFC MAC PDU Size and MTU 6
4. Specification of IPv6 over NFC 8
4.1. Protocol Stacks 8
4.2. Link Model 9
4.3. Stateless Address Autoconfiguration 10
4.4. IPv6 Link Local Address 10
4.5. Neighbor Discovery 11
4.6. Dispatch Header 11
4.7. Header Compression 12
4.8. Fragmentation and Reassembly 12
4.9. Unicast Address Mapping 13
4.10. Multicast Address Mapping 13
5. Internet Connectivity Scenarios 14
5.1. NFC-enabled Device Connected to the Internet 14
5.2. Isolated NFC-enabled Device Network 15
6. IANA Considerations 15
7. Security Considerations 15
8. Acknowledgements 15
9. References 15
9.1. Normative References 15
9.2. Informative References 17
Authors' Addresses 17

1. Introduction

NFC is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is possible, provided both devices are powered. NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only. It has been used in devices such as mobile phones, running Android operating system, named with a feature called "Android Beam". In addition, it is expected for the other mobile phones, running the other operating systems (e.g., iOS, etc.) to be equipped with NFC technology in the near future.

Considering the potential for exponential growth in the number of heterogeneous air interface technologies, NFC would be widely used as one of the other air interface technologies, such as Bluetooth Low Energy (BT-LE), Wi-Fi, and so on. Each of the heterogeneous air interface technologies has its own characteristics, which cannot be covered by the other technologies, so various kinds of air interface technologies would be existing together. Therefore, it is required for them to communicate each other. NFC also has the strongest point (e.g., secure communication distance of 10 cm) to prevent the third party from attacking privacy.

When the number of devices and things having different air interface technologies communicate each other, IPv6 is an ideal internet protocols owing to its large address space. Also, NFC would be one of the endpoints using IPv6. Therefore, This document describes how IPv6 is transmitted over NFC using 6LoWPAN techiques with following scopes.

- Overview of NFC technologies;
- Specifications for IPv6 over NFC;
  - Neighbor Discovery;
  - Addressing and Configuration;
  - Header Compression;
  - Fragmentation & Reassembly for a IPv6 datagram;

RFC4944 [1] specifies the transmission of IPv6 over IEEE 802.15.4. The NFC link also has similar characteristics to that of IEEE 802.15.4. Many of the mechanisms defined in the RFC4944 [1] can be applied to the transmission of IPv6 on NFC links. This document specifies the details of IPv6 transmission over NFC links.

2. Conventions and Terminology

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 [2].

3. Overview of Near Field Communication Technology

NFC technology enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and it enables a consumer to utilize one device across different systems.

Extending the capability of contactless card technology, NFC also enables devices to share information at a distance that is less than 10 cm with a maximum communication speed of 424 kbps. Users can share business cards, make transactions, access information from a smart poster or provide credentials for access control systems with a simple touch.

NFC’s bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch. In addition to the easy connection and quick transactions, simple data sharing is also available.

3.1. Peer-to-peer Mode of NFC

NFC-enabled devices are unique in that they can support three modes of operation: card emulation, peer-to-peer, and reader/writer. Peer-to-peer mode enables two NFC-enabled devices to communicate with each other to exchange information and share files, so that users of NFC-enabled devices can quickly share contact information and other files with a touch. Therefore, a NFC-enabled device can securely send IPv6 packets to any corresponding node on the Internet when a NFC-enabled gateway is linked to the Internet.

3.2. Protocol Stacks of NFC

The IP protocol can use the services provided by Logical Link Control Protocol (LLCP) in the NFC stack to provide reliable, two-way transport of information between the peer devices. Figure 1 depicts the NFC P2P protocol stack with IPv6 bindings to the LLCP.

For data communication in IPv6 over NFC, an IPv6 packet SHALL be received at LLCP of NFC and transported to an Information Field in Protocol Data Unit (I PDU) of LLCP of the NFC-enabled peer device. Since LLCP does not support fragmentation and reassembly, upper layers SHOULD support fragmentation and reassembly. For IPv6 addressing or address configuration, LLCP SHALL provide related information, such as link layer addresses, to its upper layer. LLCP to IPv6 protocol Binding SHALL transfer the SSAP and DSAP value to the IPv6 over NFC protocol. SSAP stands for Source Service Access Point, which is 6-bit value meaning a kind of Logical Link Control (LLC) address, while DSAP means a LLC address of destination NFC-enabled device.

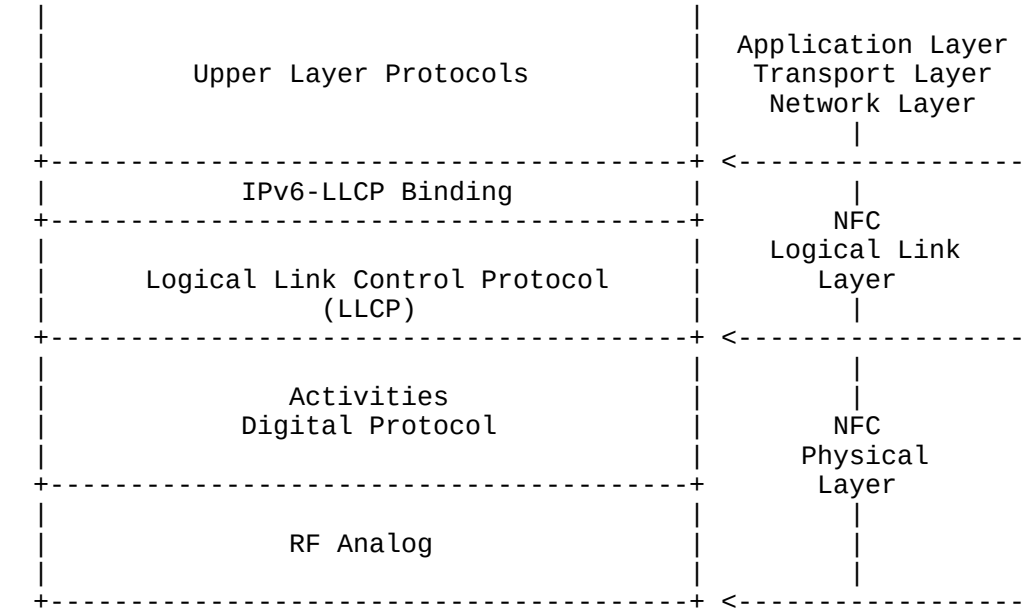


Figure 1: Protocol Stacks of NFC

The LLCP consists of Logical Link Control (LLC) and MAC Mapping. The MAC Mapping integrates an existing RF protocol into the LLCP architecture. The LLC contains three components, such as Link Management, Connection-oriented Transport, and Connection-less

Transport. The Link Management component is responsible for serializing all connection-oriented and connectionless LLC PDU (Protocol Data Unit) exchanges and for aggregation and disaggregation of small PDUs. This component also guarantees asynchronous balanced mode communication and provides link status supervision by performing the symmetry procedure. The Connection-oriented Transport component is responsible for maintaining all connection-oriented data exchanges including connection set-up and termination. The Connectionless Transport component is responsible for handling unacknowledged data exchanges.

3.3. NFC-enabled Device Addressing

NFC-enabled devices are identified by 6-bit LLC address. In other words, Any address SHALL be usable as both an SSAP and a DSAP address. According to NFCForum-TS-LLCP_1.1 [3], address values between 0 and 31 (00h - 1Fh) SHALL be reserved for well-known service access points for Service Discovery Protocol (SDP). Address values between 32 and 63 (20h - 3Fh) inclusively, SHALL be assigned by the local LLC as the result of an upper layer service request.

3.4. NFC MAC PDU Size and MTU

As mentioned in Section 3.2, an IPv6 packet SHALL be received at LLCP of NFC and transported to an Unnumbered Information Protocol Data Unit (UI PDU) and an Information Field in Protocol Data Unit (I PDU) of LLCP of the NFC-enabled peer device. The format of the UI PDU and I PDU SHALL be as shown in Figure 2 and Figure 3.

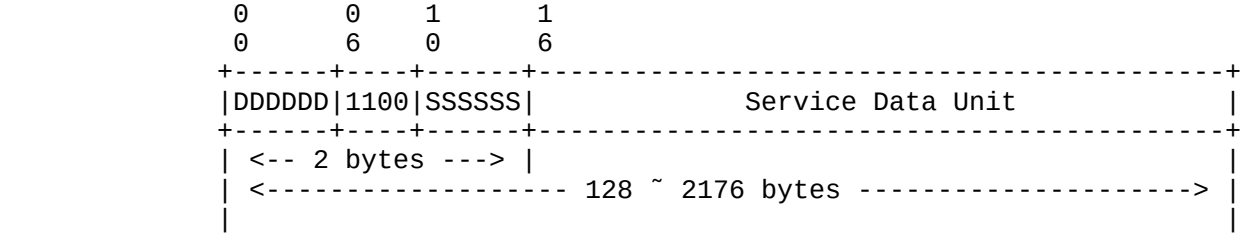


Figure 2: Format of the UI PDU in NFC

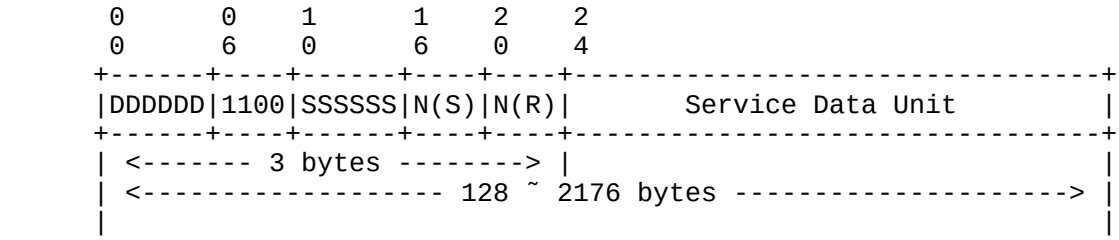


Figure 3: Format of the I PDU in NFC

The I PDU sequence field SHALL contain two sequence numbers: The send sequence number N(S) and the receive sequence number N(R). The send sequence number N(S) SHALL indicate the sequence number associated with this I PDU. The receive sequence number N(R) value SHALL indicate that I PDUs numbered up through N(R) - 1 have been received correctly by the sender of this I PDU and successfully passed to the senders SAP identified in the SSAP field. These I PDUs SHALL be considered as acknowledged.

The information field of an I PDU SHALL contain a single service data unit. The maximum number of octets in the information field SHALL be determined by the Maximum Information Unit (MIU) for the data link connection. The default value of the MIU for I PDUs SHALL be 128 octets. The local and remote LLCs each establish and maintain distinct MIU values for each data link connection endpoint. Also, An LLC MAY announce a larger MIU for a data link connection by transmitting an MIUX extension parameter within the information field. If no MIUX parameter is transmitted, the default MIU value of 128 SHALL be used. Otherwise, the MTU size in NFC LLCP SHALL calculate the MIU value as follows:

$$MIU = 128 + MIUX.$$

According to NFCForum-TS-LLCP_1.1 [3], format of the MIUX parameter TLV is as shown in Figure 4.

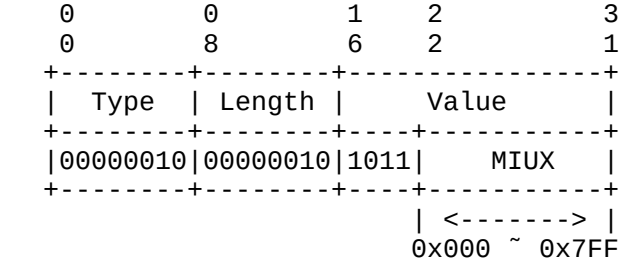


Figure 4: Format of the MIUX Parameter TLV

When the MIUX parameter is encoded as a TLV, the TLV Type field SHALL be 0x02 and the TLV Length field SHALL be 0x02. The MIUX parameter SHALL be encoded into the least significant 11 bits of the TLV Value field. The unused bits in the TLV Value field SHALL be set to zero by the sender and SHALL be ignored by the receiver. However, a maximun value of the TLV Value field can be 0x7FF, and a maximum size of the MTU in NFC LLCP SHALL calculate 2176 bytes.

4. Specification of IPv6 over NFC

NFC technology sets also has considerations and requirements owing to low power consumption and allowed protocol overhead. 6LoWPAN standards RFC4944 [1], RFC6775 [4], and RFC6282 [5] provide useful functionality for reducing overhead which can be applied to BT-LE. This functionality comprises of link-local IPv6 addresses and stateless IPv6 address auto-configuration (see Section 4.3), Neighbor Discovery (see Section 4.5) and header compression (see Section 4.7).

One of the differences between IEEE 802.15.4 and NFC is that the former supports both star and mesh topology (and requires a routing protocol), whereas NFC can support direct peer-to-peer connection and simple mesh-like topology depending on NFC application scenarios because of very short RF distance of 10 cm or less.

4.1. Protocol Stacks

Figure 5 illustrates IPv6 over NFC. Upper layer protocols can be transport protocols (TCP and UDP), application layer, and the others capable running on the top of IPv6.

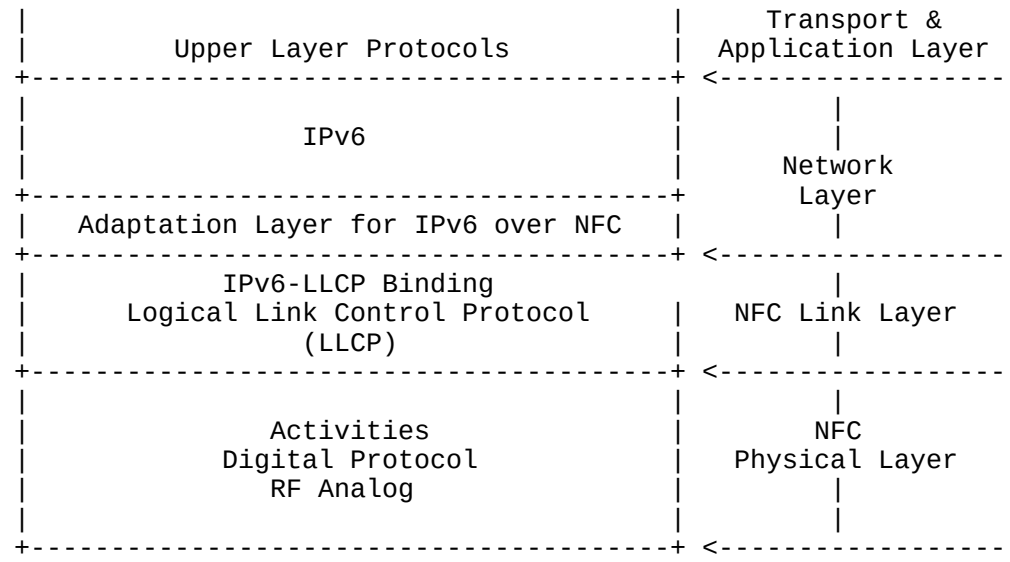


Figure 5: Protocol Stacks for IPv6 over NFC

Adaptation layer for IPv6 over NFC SHALL support neighbor discovery, address auto-configuration, header compression, and fragmentation & reassembly.

4.2. Link Model

In the case of BT-LE, Logical Link Control and Adaptation Protocol (L2CAP) supports fragmentation and reassembly (FAR) functionality; therefore, adaptation layer for IPv6 over BT-LE does not have to conduct the FAR procedure. The NFC LLCP, by contrast, does not support the FAR functionality, so IPv6 over NFC needs to consider the FAR functionality, defined in RFC4944 [1]. However, MTU on NFC link can be configured in a connection procedure and extended enough to fit the MTU of IPv6 packet.

The NFC link between two communicating devices is considered to be a point-to-point link only. Unlike in BT-LE, NFC link does not consider star topology and mesh network topology but peer-to-peer topology and simple multi-hop topology. Due to this characteristics, 6LoWPAN functionality, such as addressing and auto-configuration, and header compression, is specialized into NFC.

4.3. Stateless Address Autoconfiguration

A NFC-enabled device (i.e., 6LN) performs stateless address autoconfiguration as per RFC4862 [6]. A 64-bit Interface identifier (IID) for a NFC interface MAY be formed by utilizing the 6-bit NFC LLCP address (i.e., SSAP or DSAP) (see Section 3.3). In the viewpoint of address configuration, such an IID MAY guarantee a stable IPv6 address because each data link connection is uniquely identified by the pair of DSAP and SSAP included in the header of each LLC PDU in NFC.

Following the guidance of RFC7136 [10], interface Identifiers of all unicast addresses for NFC-enabled devices are formed on the basis of 64 bits long and constructed in a modified EUI-64 format as shown in Figure 6.

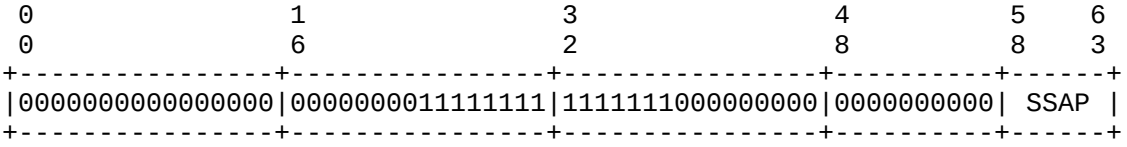


Figure 6: Formation of IID from NFC-enabled device adddress

In addition, the "Universal/Local" bit in the case of NFC-enabled device address MUST be set to 0 RFC4291 [7].

4.4. IPv6 Link Local Address

Only if the NFC-enabled device address is known to be a public address the "Universal/Local" bit can be set to 1. The IPv6 link-local address for a NFC-enabled device is formed by appending the IID, to the prefix FE80::/64, as depicted in Figure 7.

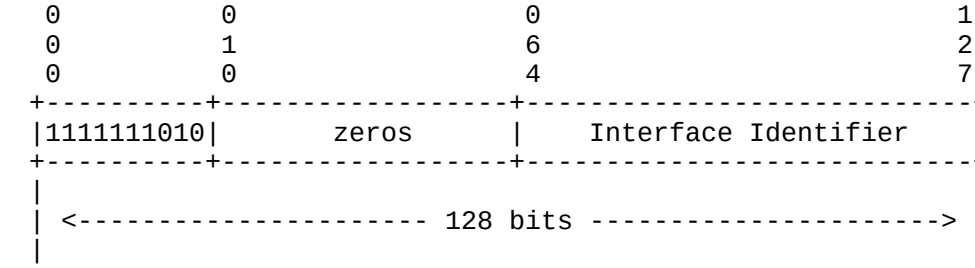


Figure 7: IPv6 link-local address in NFC

The tool for a 6LBR to obtain an IPv6 prefix for numbering the NFC network is can be accomplished via DHCPv6 Prefix Delegation (RFC3633 [8]).

4.5. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs (RFC6775 [4]) describes the neighbor discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC does not consider complicated mesh topology but simple multi-hop network topology or directly connected peer-to-peer network. Therefore, the following aspects of RFC6775 are applicable to NFC:

1. In a case that a NFC-enabled device (6LN) is directly connected to 6LBR, A NFC 6LN MUST register its address with the 6LBR by sending a Neighbor Solicitation (NS) message with the Address Registration Option (ARO) and process the Neighbor Advertisement (NA) accordingly. In addition, DHCPv6 is used to assigned an address, Duplicate Address Detection (DAD) is not required.

2. For sending Router Solicitations and processing Router Advertisements the NFC 6LNs MUST follow Sections 5.3 and 5.4 of the RFC6775.

4.6. Dispatch Header

All IPv6-over-NFC encapsulated datagrams transmitted over NFC are prefixed by an encapsulation header stack consisting of a Dispatch value followed by zero or more header fields. The only sequence currently defined for IPv6-over-NFC is the LOWPAN_IPHC header followed by payload, as depicted in Figure 8.

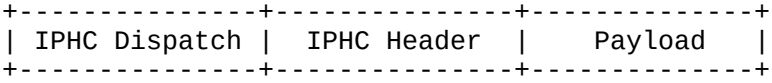


Figure 8: A IPv6-over-NFC Encapsulated 6LOWPAN_IPHC Compressed IPv6 Datagram

The dispatch value may be treated as an unstructured namespace. Only a single pattern is used to represent current LoBAC functionality.

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

Figure 9: Dispatch Values

Other IANA-assigned 6LoWPAN Dispatch values do not apply to this specification.

4.7. Header Compression

Header compression as defined in RFC6282 [5] , which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, is REQUIRED in this document as the basis for IPv6 header compression on top of NFC. All headers MUST be compressed according to RFC6282 encoding formats.

Therefore, IPv6 header compression in RFC6282 [5] MUST be implemented. Further, implementations MAY also support Generic Header Compression (GHC) of RFC7400 [11]. A node implementing GHC MUST probe its peers for GHC support before applying GHC.

If a 16-bit address is required as a short address of IEEE 802.15.4, it MUST be formed by padding the 6-bit NFC link-layer (node) address to the left with zeros as shown in Figure 10.

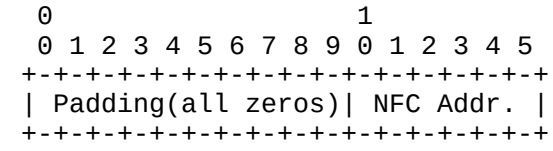


Figure 10: NFC short adress format

4.8. Fragmentation and Reassembly

NFC provides fragmentation and reassembly (FAR) for payloads from 128 bytes up to 2176 bytes as mention in Section 3.4. The MTU of a general IPv6 packet can fit into a sigle NFC link frame. Therefore, the FAR functionality as defined in RFC4944, which specifies the fragmentation methods for IPv6 datagrams on top of IEEE 802.15.4, is NOT REQUIRED in this document as the basis for IPv6 datagram FAR on top of NFC. The NFC link connection for IPv6 over NFC MUST be configured with an equivalent MIU size to fit the MTU of IPv6 Packet. However, the default configuration of MIUX value is 0x480 in order to fit the MTU (1280 bytes) of a IPv6 packet.

4.9. Unicast Address Mapping

The address resolution procedure for mapping IPv6 non-multicast addresses into NFC link-layer addresses follows the general description in Section 7.2 of RFC4861 [9], unless otherwise specified.

The Source/Target link-layer Address option has the following form when the addresses are 6-bit NFC link-layer (node) addresses.

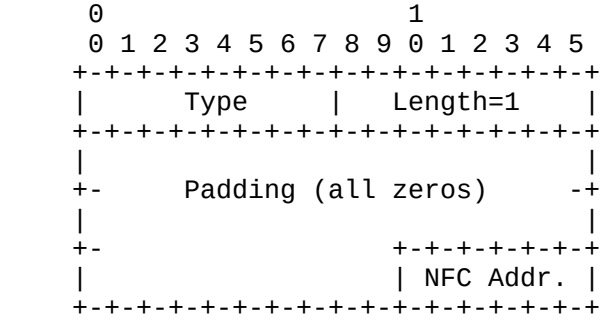


Figure 11: Unicast address mapping

Option fields:

Type:

1: for Source Link-layer address.

2: for Target 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 1 for 6-bit NFC node addresses.

NFC address:

The 6-bit address in canonical bit order. This is the unicast address the interface currently responds to.

4.10. Multicast Address Mapping

All IPv6 multicast packets MUST be sent to NFC Destination Address, 0x3F (broadcast) and filtered at the IPv6 layer. When represented as a 16-bit address in a compressed header, it MUST be formed by padding

on the left with a zero. In addition, the NFC Destination Address, 0x3F, MUST not be used as a unicast NFC address of SSAP or DSAP.

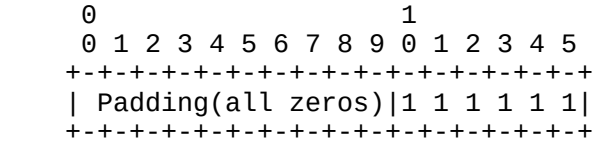


Figure 12: Multicast address mapping

5. Internet Connectivity Scenarios

As two typical scenarios, the NFC network can be isolated and connected to the Internet.

5.1. NFC-enabled Device Connected to the Internet

One of the key applications by using adaptation technology of IPv6 over NFC is the most securely transmitting IPv6 packets because RF distance between 6LN and 6LBR SHOULD be within 10 cm. If any third party wants to hack into the RF between them, it MUST come to nearly touch them. Applications can choose which kinds of air interfaces (e.g., BT-LE, Wi-Fi, NFC, etc.) to send data depending characteristics of data. NFC SHALL be the best solution for secured and private information.

Figure 13 illustrates an example of NFC-enabled device network connected to the Internet. Distance between 6LN and 6LBR SHOULD be 10 cm or less. If there is any of close laptop computers to a user, it SHALL becomes the 6LBR. Additionally, When the user mounts a NFC-enabled air interface adapter (e.g., portable small NFC dongle) on the close laptop PC, the user’s NFC-enabled device (6LN) can communicate the laptop PC (6LBR) within 10 cm distance.

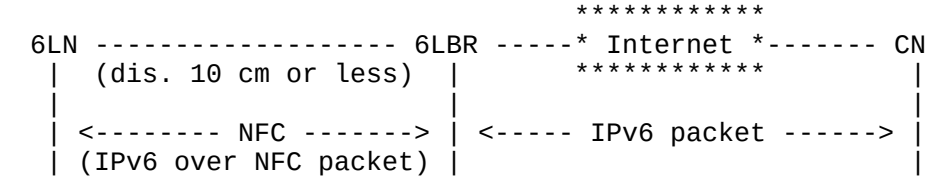


Figure 13: NFC-enabled device network connected to the Internet

5.2. Isolated NFC-enabled Device Network

In some scenarios, the NFC-enabled device network may transiently be a simple isolated network as shown in the Figure 14.

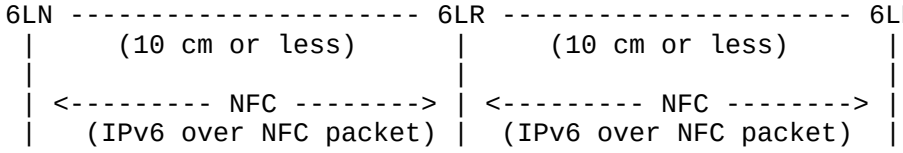


Figure 14: Isolated NFC-enabled device network

In mobile phone markets, applications are designed and made by user developers. They may image interesting applications, where three or more mobile phones touch or attach each other to accomplish outstanding performance. For instance, three or more mobile phones can play multi-channel sound of music together. In addition, attached three or more mobile phones can make an extended banner to show longer sentences in a concert hall.

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

The method of deriving Interface Identifiers from 6-bit NFC Link layer addresses is intended to preserve global uniqueness when it is possible. Therefore, it is to required to protect from duplication through accident or forgery.

8. Acknowledgements

We are grateful to the members of the IETF 6lo working group.

Michael Richardson, Suresh Krishnan, Pascal Thubert, Carsten Bormann, and Alexandru Petrescu have provided valuable feedback for this draft.

9. References

9.1. Normative References

[1] 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>.

[2] 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>.

[3] "Logical Link Control Protocol version 1.1", NFC Forum Technical Specification , June 2011.

[4] 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>.

[5] 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>.

[6] 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>.

[7] 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>.

[8] 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>.

[9] 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>.

[10] 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>.

[11] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <http://www.rfc-editor.org/info/rfc7400>.

9.2. Informative References

[12] "Near Field Communication - Interface and Protocol (NFCIP-1) 3rd Ed.", ECMA-340 , June 2013.

Authors' Addresses

Yong-Geun Hong
ETRI
161 Gajeong-Dong Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 6557
Email: yghong@etri.re.kr

Younghwan Choi
ETRI
218 Gajeongno, Yuseong
Daejeon 305-700
Korea

Phone: +82 42 860 1429
Email: yhc@etri.re.kr

Joo-Sang Youn
DONG-EUI University
176 Eomgwangno Busan_jin_gu
Busan 614-714
Korea

Phone: +82 51 890 1993
Email: joosang.youn@gmail.com

Dongkyun Kim
Kyungpook National University
80 Daehak-ro, Buk-gu
Daegu 702-701
Korea

Phone: +82 53 950 7571
Email: dongkyun@knu.ac.kr

JinHyouk Choi
Samsung Electronics Co.,
129 Samsung-ro, Youngdong-gu
Suwon 447-712
Korea

Phone: +82 2 2254 0114
Email: jinchoe@samsung.com

6lo
Internet-Draft
Intended status: Informational
Expires: January 4, 2016

R. Kelsey
Silicon Labs

July 3, 2015

Mesh Link Establishment
draft-kelsey-6lo-mesh-link-establishment-00

Abstract

This document defines the mesh link establishment (MLE) protocol for establishing and configuring secure radio links in IEEE 802.15.4 radio mesh networks. MLE extends IEEE 802.15.4 for use in multihop mesh networks by adding three capabilities: 1) dynamically configuring and securing radio links, 2) enabling network-wide changes to radio parameters, and 3) determining link quality prior to link configuration MLE operates below the routing layer, insulating it from the details of configuring, securing, and maintaining individual radio links within a larger mesh network.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 4, 2016.

Table of Contents

1. Introduction 3
1.1. Requirements Language 3
2. Terminology 4
3. Applicability 4
4. Overview 4
4.1. Link Configuration 5
4.2. Parameter Dissemination 5
4.3. Link Quality Determination 5
5. Security Formats 6
6. Command Format 7
7. TLV Formats 7
7.1. Source Address 8
7.2. Mode 8
7.3. Timeout 8
7.4. Challenge 9
7.5. Response 9
7.6. Link-layer Frame Counter 9
7.7. Link Quality 9
7.8. Network Parameter 11
7.9. MLE Frame Counter 12
8. Message transmission 12
9. Processing of incoming messages 13
10. Link Configuration 14
11. Parameter Dissemination 15
12. Neighbor Detection 15
13. Acknowledgements 16
14. IANA Considerations 16
14.1. Security Suites 16
14.2. Command Types 17
14.3. TLV Types 17
14.4. Network Parameters 17
15. Security Considerations 18
16. References 18
16.1. Normative References 18
16.2. Informative References 19
Author's Address 19

1. Introduction

The configuration of individual links in IEEE 802.15.4 mesh networks falls into a gap between standards. The IEEE 802.15.4 standard provides for static point-to-point and star topologies while the routing (L3) protocols used in multi-hop mesh networks assume that the L2 links are already up and running. Effective mesh networking using IEEE 802.15.4 requires identifying, configuring, and securing usable links to neighboring devices as the network's membership and physical environment change. Newly usable links need to be identified and configured automatically, where configuration values can include link-layer addresses, transmit and receive modes, security parameters, and so forth.

Security configuration is particularly important, as IEEE 802.15.4's replay protection applies only between a joining device and the IEEE 802.15.4 coordinator via which it joins the network. Replay protection with other neighbors requires a synchronization step that is not specified by IEEE 802.15.4.

MLE can also be used to distribute configuration values that are shared across a network, such as the channel and PAN ID. Network-wide configuration uses multicasts and requires some form of multi-hop multicast forwarding. These messages are sent infrequently, so forwarding with simple flooding is sufficient.

One of the most important properties of a radio link, how reliably the two neighbors can communicate, often cannot be determined unilaterally by either neighbor. Many 802.15.4 links are asymmetric, where messages traveling one way across the link are received more or less reliably than messages traveling in the opposite direction. There is a chicken and egg problem here. It is a waste of effort to configure a link that does not have sufficient two-way reliability to be useful, but the two-way reliability cannot be determined without exchanging messages over the link. MLE resolves this by allowing a node to periodically multicast an estimate of the quality of its links. This allows a node to determine if it has a usable radio link to a neighbor without first configuring that link.

MLE was developed as part of the ZigBee IP networking standard [ZigBeeIP]. This document describes the protocol as it was used in that standard.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and

"OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Terminology

ETX	Expected Transmission Count [RFC6551]; the number of transmission attempts required to send a packet over a particular link. Defined to be the product of the IDR values for both directions. A perfect link has an ETX of 1, less than perfect links have higher ETX values.
Frame counter	A value that is incremented with each new secured message and used to detect replayed messages.
IDR	Inverse Delivery Ratio; the number of transmission attempts divided by the number of successful transmissions in a given direction over a link. Used in computing the ETX value for a link.

3. Applicability

This protocol provides configuration and management mechanisms for using IEEE 802.15.4 links in IP-based multi-hop mesh networks. The protocol is designed to be easily extended to add additional features. It could also be adapted for use with other single-hop link protocols that have some of the same features (message encryption, one-hop multicast) and omissions (listed at the start of Section 4) as IEEE 802.15.4.

4. Overview

MLE adds three capabilities to IEEE 802.15.4:

- Dynamically configuring and securing radio links.
- Enabling network-wide changes to radio parameters.
- Determining link quality, prior to link configuration.

The first two are mutually independent; either one can be used without the other. The purpose of the third, determining link quality, is to make link management more efficient by detecting unreliable links before any effort is spent configuring them.

All MLE messages are sent using UDP. While UDP is not an obvious choice for a protocol used for L2 configuration, it was chosen to simplify integration of MLE into existing systems.

4.1. Link Configuration

Link configuration is done using link-local unicasts to exchange IEEE 802.15.4 radio parameters (addresses, node capabilities, and frame counters) between neighbors. Link configuration messages are either a request that the link be configured, or an acceptance or rejection of such a request.

IEEE 802.15.4 security uses frame counters to detect replayed messages. MLE uses a two-message challenge and response protocol to ensure that the MLE message containing a neighbor’s frame counter is not itself a replayed message.

4.2. Parameter Dissemination

Network-wide changes to radio parameters, such as moving the network to a new channel, is done by multicasting the new value(s) to all devices in the network. Along with the values themselves, the multicast messages include a delay value indicating when the new value takes effect. The delay avoids having the parameters change while the multicast is still propagating.

In addition to network wide dissemination, a device that does not have the current network values, either because it has just joined the network or for any other reason, can send a unicast request to a neighbor. The neighbor will respond by sending the current network values.

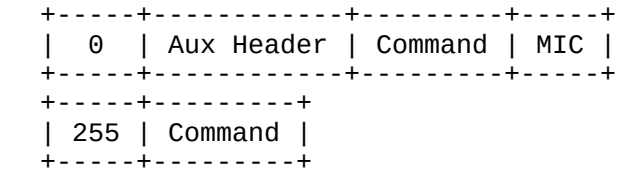
4.3. Link Quality Determination

802.15.4 links can be asymmetric in that a link between neighboring devices may be much more reliable in one direction than in the other. This limits the usefulness of unilateral link quality detection: a link that looks strong to one device may not be usable because it works poorly in the other direction. To avoid wasting effort configuring unusable links, devices can use MLE to send link-local multicasts containing their local link quality estimates. Neighboring nodes can then form an estimate of the two-way quality of their link to the sender.

5. Security Formats

One of the main functions of MLE is to initialize link-layer security. This means that MLE itself cannot rely on link-layer security. To avoid the cost and complexity of adding a second security suite, MLE reuses that of 802.15.4. [AES] in Counter with CBC-MAC Mode [CCM] as described in [IEEE802154]. Later extensions may include other security suites for use with other radio standards.

An MLE message begins with single byte indicating the security suite used in that message. If that initial byte is "255" no security is used and the messages has no additional security data. An initial byte of "0" indicates that the message is secured (encrypted and authenticated) as described in [IEEE802154]. MLE messages thus have one of the two following formats:



Aux Header Auxiliary Security Header as described in [IEEE802154].

Command MLE command; see Section 6.

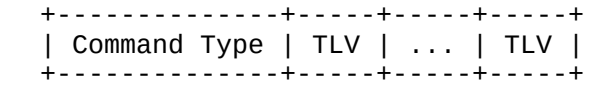
MIC Message Integrity Code as described in [IEEE802154].

MLE security MUST NOT use any key that is being used by the link (or any other) layer. [CCM] requires that each key and nonce pair be used exactly once, which is most easily achieved by using different keys.

If MLE security is in use each device MUST maintain an outgoing MLE frame counter for use in securing outgoing packets in compliance with [CCM]. This MAY be the same frame counter used for securing 802.15.4 frames. Other than the above requirements, the distribution or derivation of the key(s) used for MLE security is outside the scope of this document. The outgoing MLE frame counter MUST be handled as required by [CCM]. In particular, frame counters MUST NOT be reused for any given key; if the outgoing MLE frame counter reaches its maximum value (0xFFFFFFFF), secured MLE messages MUST NOT be sent until a new key is available, at which point the outgoing MLE frame counter MAY be set back to zero.

6. Command Format

MLE messages consist of a command type and a series of type-length-value parameters.



Command Type An eight-bit unsigned integer identifying the type of message. This document defines the following commands:

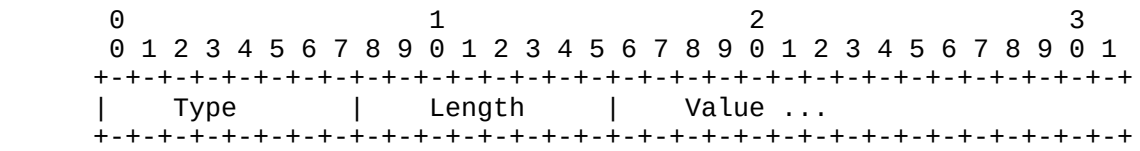
- 0 Link Request. A request to establish a link to a neighbor.
- 1 Link Accept. Accept a requested link.
- 2 Link Accept and Request. Accept a requested link and request a link with the sender of the original request.
- 3 Link Reject. Reject a link request.
- 4 Advertisement. Inform neighbors of a device’s link state.
- 5 Update. Informs of changes to link parameters shared by all nodes in a network.
- 6 Update Request. Request that an Update message be sent.

The first four (Link Request, Link Accept, Link Accept and Request, and Link Reject) are collectively referred to as link configuration messages.

TLVs Zero or more TLV frames. These are described in Section 7.

7. TLV Formats

Values are encoded using a type-length-value format, where the type and length are one byte each and the length field contains the length of the value in bytes. TLVs are stored serially with no padding between them. They are byte-aligned but are not aligned in any other way such as on 2 or 4 byte boundaries. All values in TLVs are in network byte order.



Type	An eight-bit unsigned integer giving the type of the value, from IANA registry Section 14.3.
Length	An eight-bit unsigned integer giving the length of the Value field in bytes.
Value	Length bytes of value, formatted as defined for the Type.

With the exceptions of the Source Address TLV and Parameter TLV, an MLE message MUST NOT contain two or more TLVs of the same type. To allow devices to have multiple source addresses, an MLE message MAY contain two or more Source Address TLVs.

7.1. Source Address

The Source Address TLV (TLV Type 0) has a Value containing a byte string representing a link-layer address assigned to the source of the message. A given radio interface may have multiple link-layer addresses. This TLV is used to communicate any source address(es) that is not included in the message by the link layer itself.

7.2. Mode

The Mode TLV (TLV Type 1) has a Value containing a byte string representing the mode in which this link is used by the source of the message. The format of the value is that of the Capability Information field in the 802.15.4 Associate command as described in [IEEE802154].

7.3. Timeout

The Timeout TLV (TLV Type 2) has a Value containing a 32-bit unsigned integer. The value is the expected maximum interval between transmissions by the sender, in seconds. This allows the receiver to more accurately timeout a link to a neighbor that polls for its incoming messages.

7.4. Challenge

The Challenge TLV (TLV Type 3) has a Value containing a randomly-chosen byte string that is used to determine the freshness of any reply to this message. The recommendations in [RFC4086] apply with regard to generation of the challenge value. The byte string MUST be at least 4 bytes in length and a new value MUST be chosen for each Challenge TLV transmitted. An important part of replay protection is determining if a newly-heard neighbor is actually present or is a set of recorded messages. This is done by sending a random challenge value to the neighbor and then receiving that same value in a Response TLV sent by the neighbor.

7.5. Response

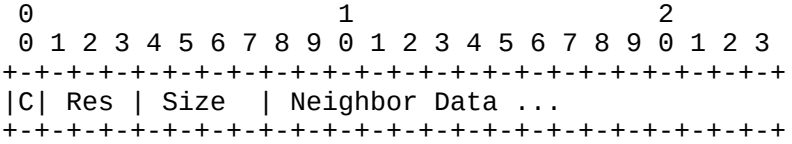
The Response TLV (TLV Type 4) has a Value containing a byte string copied from a Challenge TLV.

7.6. Link-layer Frame Counter

The Link-layer Frame Counter TLV (TLV Type 5) has a Value containing the sender’s current outgoing link-layer Frame Counter, encoded as an N-byte unsigned integer. For 802.15.4 this is a 4-byte value.

7.7. Link Quality

The Link Quality TLV (TLV Type 6) reports the sender’s measured link quality for messages received from its neighbors. The format of the Link Quality value is as follows:

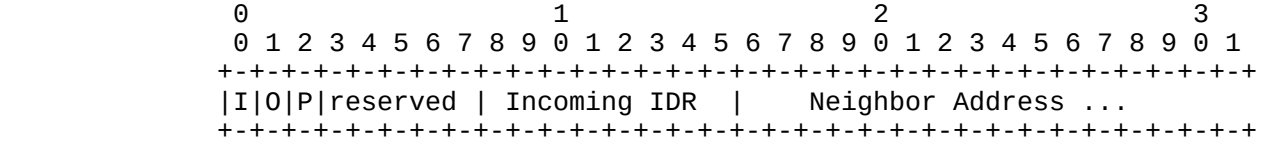


C — Complete: "1" if the message includes all neighboring routers for which the source has link quality data. Multicast Link Quality TLVs normally contain complete information; a unicast to a particular neighbor would normally contain only that neighbor’s link quality and would have the C flag set to "0".

Res — Reserved; MUST be set to 000 and SHOULD be ignored on receipt.

Size	The size in bytes of the included neighbor link-layer addresses, minus 1. This supports addresses of lengths 1 to 16 bytes.
Neighbor Data	A sequence of neighbor records, each containing receive and transmit state flags, the estimated incoming link reliability (IDR), and the neighbor's link-layer address.

The neighbor data in a Link Quality TLV is formatted as follows:



I(ncoming)	"1" if the sender's Receive State for this neighbor is true, "0" if not.
O(utgoing)	"1" if the sender's Transmit State for this neighbor is true, "0" if not.
P(riority)	"1" if the sender expects to use this link for sending messages, "0" if not. Given limited resources, the P flag MAY be used in deciding which links should be maintained.
Incoming IDR	The estimated inverse delivery ratio of messages sent by the neighbor to the source of this message. This is an eight-bit unsigned integer. To allow for fractional IDR, the value encoded is multiplied by 32. A perfect link, with an actual IDR of 1, would have an Incoming IDR of 0x20. A value of 0xFF indicates that the link is unusable.
Address	A link-layer address of a neighbor.

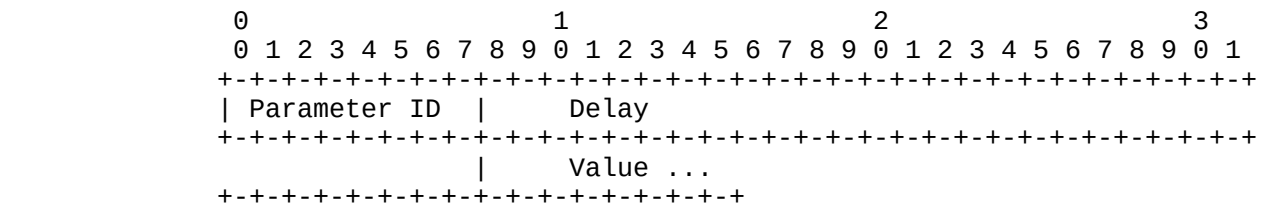
The I and O flags are used to facilitate the two-way use of links between neighboring routers.

A node that does not have a link configured to a neighbor but receives a Link Quality TLV from that neighbor with the node's O flag set to "1" SHOULD send an MLE message with a Link Quality TLV with that neighbor's I bit set to "0". This message may either be a

regular multicast Advertisement or a unicast to that neighbor containing only a single Neighbor Data record.

7.8. Network Parameter

The Parameter TLV (TLV Type 7) specifies the value of a link-layer parameter shared across the network (as opposed to a parameter specific to a particular link). The Value contains three fields:



Parameter ID — The ID of the parameter to be changed.

Delay — The delay before setting the parameter, in milliseconds. This is a four-byte unsigned integer. Having a delay gives time for the new value to propagate throughout the network. It may also be used for limiting the time a particular parameter setting is in use, by including two different values for a single parameter, with two different delays.

Value — A byte string containing the new value of the parameter. The format of this value is determined by the particular parameter

Update messages MUST contain only Network Parameter TLVs. Update messages with new parameter settings are normally multicast to the entire MLE domain. They may also be unicast to nodes that have just joined the network or otherwise do not have up-to-data parameter information.

The defined Network Parameters are:

0 Channel

1 PAN ID

2 Permit Joining

3 Beacon Payload

7.9. MLE Frame Counter

The MLE Frame Counter TLV (TLV Type 8) has a Value containing the sender's current outgoing MLE Frame Counter, encoded as an 32-bit unsigned integer.

8. Message transmission

MLE messages SHOULD be sent using the assigned UDP port number (19788) as both the source and destination port. Link configuration and advertisement messages MUST be sent with an IP Hop Limit of 255, either to a link-local unicast address or to the link-local all-nodes (FF02::1) or all-routers (FF02::2) multicast addresses. Update messages MAY be sent as above, or MAY be sent to a site-local all-MLE-nodes multicast address (to be assigned by IANA).

Outgoing link configuration and advertisement messages SHOULD be secured using the procedure specified in [AES] and [CCM] using the auxiliary security header as described in [IEEE802154]. The one exception to this is messages sent to or from a device that is joining the network and does not yet have the necessary keys; such unsecured messages MUST NOT contain Challenge, Response, or Link-Layer Frame Counter TLVs.

The authenticated data consists of the following three values concatenated together:

IP source address
IP destination address
auxiliary security header

The secured data consists of the messages body following the auxiliary security header (the command ID and TLVs). The security suite identifier is not included in either the authenticated data or the secured data. Key choice is outside the scope of this document.

In order to allow update messages to be forwarded multiple hops, outgoing update messages, MUST be secured at the link layer, if link layer security is in use, and MUST NOT be secured by MLE.

A message sent in response to a multicast request, such as a multicast Link Request, MUST be delayed by a random time between 0 and MAX_RESPONSE_DELAY_TIME seconds, with a resolution of at least 1ms.

MAX_RESPONSE_DELAY_TIME 1 second

If no response is received to a unicast request, the request MAY be retransmitted using a simple timeout mechanism. This is based on the retransmission mechanism used in DHCPv6 RFC 3315 [RFC3315], simplified to use a single, fixed timeout. Unicast requests are not relayed, which avoids the need for a more elaborate mechanism.

Parameter	Default	Description
URT	1 sec	Unicast Retransmission timeout.
MRT	5 sec	Multicast Retransmission timeout.
MRC	3	Maximum retransmission count.

For each transmission the appropriate URT or MRT value is multiplied by a random number chosen with a uniform distribution between 0.9 and 1.1 with a resolution of at least 1ms. The randomization factor is included to minimize synchronization of messages transmitted.

9. Processing of incoming messages

Any incoming link configuration or advertisement message, or an incoming update sent to a link-local address, whose IP Hop Limit is not 255 may have been forwarded by a router and MUST be discarded.

Incoming messages whose Command Type is a reserved value MUST be ignored. Any TLVs in an incoming message whose TLV Type has a reserved value MUST be ignored.

Incoming messages that are not secured with either MLE or link-layer security SHOULD be ignored. The one exception to this is messages sent to or from a device that is joining the network and does not yet have the necessary keys. Secured incoming messages are decrypted and authenticated using the procedures specified in [AES] and [CCM], with security material obtained from the auxiliary security header as described in [IEEE802154]. The key source may be obtained either from the link layer source address or from the auxiliary security header.

A device MUST maintain a separate incoming MLE frame counter for each neighbor with which it establishes a link. Any MLE message received with a frame counter the same or lower than that of a previously received and authenticated message from the same source MUST be discarded. Messages for which no previous frame counter are available MAY be processed, but their counter value MUST be saved for comparison with later messages.

10. Link Configuration

The values that may need to be communicated to configure an 802.15.4 link are:

- Long (64-bit) and short (16-bit) addresses.
- Capability Information, as in the 802.15.4 Association command in [IEEE802154], especially the Device Type and Receiver On When Idle fields.
- Initialization of AES-CCM frame counters.

A device wishing to establish a link to a neighbor MUST send a Link Request message containing the following:

- Source Address TLV, containing the sender's short (16-bit) MAC address. The sender's long (64-bit) MAC address MUST used as the MAC source address of the message.
- Mode TLV, containing the sender's Capability data byte.
- Timeout TLV, if the sender is an rxOffWhenIdle device.
- Challenge TLV, whose size is determined by the network configuration.

The neighbor SHOULD respond with a Link Accept message containing the same TLVs (with its own values), but with a Response TLV in place of the Challenge TLV and with added Link-layer Frame Counter and MLE Frame Counter TLVs. If large numbers of Link Request messages arrive a device MAY reduce or completely suspend sending Link Accept messages, and MAY send Link Reject messages instead. The MLE Frame Counter TLV MAY be omitted if the sender uses the same counter for both MLE and 802.15.4 messages. If the neighbor also requires a liveness check, it MAY include its own challenge, and use the Link Accept And Request message type.

If a node receives a secured 802.15.4 unicast from a neighbor for whom it does not have link configuration data, the receiving node SHOULD respond with a Link Reject message to inform the neighbor that the link is not configured. If large numbers of such messages arrive a device MAY reduce or completely suspend sending Link Reject messages.

Link Configuration messages are used to establish 802.15.4 security and so MUST NOT be secured at the 802.15.4 layer.

11. Parameter Dissemination

Update messages may be sent to change the channel, PAN ID, and/or permit joining flags on all nodes. Determining when these values should be changed is beyond the scope of this document.

To make a network-wide change to one of these parameters, an MLE update messages SHOULD be sent to an appropriate multicast address, such as the site-local all-node, all-routers or all-MLE-nodes multicast address (to be assigned by IANA). Alternatively, MLE update messages MAY be unicast to individual devices, either to avoid the cost of a multicast or to have the parameter change apply to only a subset of devices. This requires some form of multi-hop multicast forwarding; these messages are sent infrequently, so forwarding with simple flooding is sufficient.

A single update message MAY contain multiple values for the same parameter with different time delays. In particular, the permit joining flag can be enabled for a limited time by including both on and off values in a single update message.

A device that does not have the current network values, either because it has just joined the network or for any other reason, MAY send a unicast Update Request to a neighbor. The neighbor responds by sending an Update message containing the current values of the parameters.

12. Neighbor Detection

Nodes MAY send out periodic advertisements containing the incoming IDR values for their neighbors. The primary purpose of these messages is to allow nodes to choose likely candidates for link establishment. They can also be used to determine if existing links continue to provide sufficient two-way reliability.

A node maintains two boolean values for each known neighbor:

Receive State True if the node will accept incoming non-MLE messages from that neighbor.

Transmit State A local cache of the neighbor’s Receive State corresponding to this node.

Both values default to false.

The Receive State is set to true when the node receives a valid incoming link accept from the neighbor, and set to false when the

link configuration information is discarded for any reason (link failure or timeout, for example).

The Transmit State is set to true when a link accept message is sent to the neighbor. When an advertisement message is received from the neighbor the Transmit State is set to the Receive State as reported in the advertisement. If the advertisement's C flag is 1 and the receiving node's address is not included in the advertisement, the recipient's Transmit State for the sender is set to false.

These states are advisory only; a node may send a message to a neighbor regardless of its Transmit State for that neighbor. Similarly, a node may unilaterally change its Receive State (and discard any link configuration data) without first informing the neighbor of its intention. The change in Receive State will be reflected in the next advertisement sent by the node.

Advertisement messages are used prior to establishing 802.15.4 security and thus SHOULD NOT be secured at the 802.15.4 layer.

13. Acknowledgements

The author would like to acknowledge the helpful comments of Thomas Clausen, Robert Cragie, Colin O'Flynn, Edward Hill, Matteo Paris, Kundok Park, Joseph Reddy, and Dario Tedeschi, which greatly improved the document.

14. IANA Considerations

IANA has assigned UDP port 19788 to MLE.

IANA is requested to establish a new top-level registry, called "MLE: Mesh Link Establishment", to contain all MLE objects, codepoints, and sub-registries.

The allocation policy for each new registry is by IETF review: new values are assigned through the IETF review process .

14.1. Security Suites

IANA is requested to create a subregistry, called "Security Suites". Values range from 0 to 255.

Value	Meaning	Reference
0	802.15.4 Security	This document
255	No Security	This document

Values 1-254 are currently unassigned.

14.2. Command Types

IANA is requested to create a subregistry, called "Command Types". Values range from 0 to 255.

Value	Meaning	Reference
0	Link Request	This document
1	Link Accept	This document
2	Link Accept and Request	This document
3	Link Reject	This document
4	Advertisement	This document
5	Update	This document
6	Update Request	This document

Values 7-255 are currently unassigned.

14.3. TLV Types

IANA is requested to create a subregistry, called "TLV Types". Values range from 0 to 255.

Value	Meaning	Reference
0	Source Address	This document
1	Mode	This document
2	Timeout	This document
3	Challenge	This document
4	Response	This document
5	Link-layer Frame Counter	This document
6	Link Quality	This document
7	Network Parameter	This document
8	MLE Frame Counter	This document

Values 9-255 are currently unassigned.

14.4. Network Parameters

IANA is requested to create a subregistry, called "Network Parameters". Values range from 0 to 255.

Value	Meaning	Reference
0	Channel	This document
1	PAN ID	This document
2	Permit Joining	This document
3	Beacon Payload	This document

Values 4-255 are currently unassigned.

15. Security Considerations

In general MLE has the strengths and weaknesses of the link layer security that it inherits. The one exception is that MLE's operation requires accepting and acting on incoming Advertisements and Link Requests messages for which the receiver has no prior knowledge of the sender's MLE frame counter. Because of this, implementers must be careful in how they use information obtained from these possibly-replayed messages. For example, information from unsecured messages should not be used to modify any stored information obtained from secured messages.

The Hop Limit field of received packets other than multihop update messages is verified to contain 255, the maximum legal value. Because routers decrement the Hop Limit on all packets they forward, received packets containing a Hop Limit of 255 must have originated from a neighbor. This technique is borrowed from IPv6 ND [RFC4861].

16. References

16.1. Normative References

[AES] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", FIPS 197, November 2001.

[CCM] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", SP 800-38C, May 2004.

[IEEE802154] Institute of Electrical and Electronics Engineers, "Wireless Personal Area Networks", IEEE Standard 802.15.4-2006, 2006.

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

[RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

16.2. Informative References

[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.

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

[RFC6551] Vasseur, JP., Kim, M., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, March 2012.

[ZigBeeIP] ZigBee Alliance, "ZigBee IP Specification", 2014, <http://www.zigbee.org/non-menu-pages/zigbee-ip-download>.

Author’s Address

Richard Kelsey
Silicon Labs
343 Congress St
Boston, Massachusetts 02210
USA

Phone: +1 617 951 1225
Email: richard.kelsey@silabs.com

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: April 20, 2016

Y. Ohba, Ed.
Toshiba

October 18, 2015

An Extension to Mesh Link Establishment (MLE) for Host Identity Protocol Diet Exchange (HIP DEX) draft-ohba-6lo-mle-hip-dex-01

Abstract

This document defines an extension of MLE (Mesh Link Establishment) protocol to encapsulate HIP DEX key exchange protocol messages.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 20, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirement Language 3
1.2. Acronyms 3
1.3. Convention 3
2. Overview 3
3. Key Establishment Phase 4
4. Key Update Phase 6
5. Key Materials 7
5.1. Pair-wise Key 7
5.2. Group Keys 7
6. MLE Security 8
7. Certificate Revocation 8
8. Security Considerations 9
9. IANA Considerations 9
9.1. MLE TLV Types 9
9.2. HIP Parameter 9
10. Acknowledgments 10
11. References 10
11.1. Normative References 10
11.2. External Informative References 11
Author's Address 11

1. Introduction

HIP DEX (Host Identity Protocol Diet EXchange) [I-D.moskowitz-hip-dex] is a light-weight key exchange protocol designed for constrained devices. HIP DEX builds on the HIP Base EXchange (HIP BEX) [I-D.ietf-hip-rfc5201-bis] and inherits the transport-agnostic property of HIP BEX.

MLE (Mesh Link Establishment) [I-D.kelsey-6lo-mesh-link-establishment] is defined for establishing and configuring secure links in IEEE 802.15.4 mesh networks. MLE assumes that shared keys to secure link-layer frames and MLE messages exchanged between a pair of nodes are pre-configured between the nodes. Therefore, a key exchange protocol is required in order to dynamically configure the required shared keys. While such a key exchange protocol can be run outside MLE, sequentially running a key exchange protocol and MLE as separate protocols requires more message roundtrips. For example, running a HIP DEX 4-way handshake followed by an MLE 3-way handshake requires 3.5 message roundtrips.

In this document, an extension to the MLE protocol for encapsulating HIP DEX messages is defined in order to realize optimized key exchange and link establishment for IEEE 802.15.4 mesh networks.

1.1. Requirement Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Acronyms

DEX-I1, DEX-R1, DEX-I2, DEX-R2: HIP DEX I1, R1, I2, R2 messages

ECDH: Elliptic Curve Diffie-Hellman

EI: HIP DEX Key Establishment Initiator

ER: HIP DEX Key Establishment Responder

LLFC: Link-Layer Frame Counter

MIC: MLE Message Integrity Code

MLFC: MLE Frame Counter

UI: HIP DEX Key Update Initiator

UR: HIP DEX Key Update Responder

1.3. Convention

In the figures of this document, MLE messages marked with '*' are those secured by the MLE protocol.

In the key material formats in this document, '|' denotes concatenation operator.

2. Overview

HIP DEX over MLE consists of two phases, i.e., Key Establishment Phase and Key Update Phase. In Key Establishment Phase, a HIP DEX 4-way handshake using I1, R1, I2 and R2 messages is conducted to establish a secure channel between an EI and an ER based on an ECDH shared secret and exchange session key materials over the secure channel.

In Key Update Phase, HIP DEX Update messages encrypting session key materials are exchanged between a UI and each UR using an MLE Update Request and Update exchange, followed by a multicast MLE Update message for triggering each UR to simultaneously activate new key

materials and reset the associated link-layer frame counters. The UI and UR roles for a pair of nodes may be determined independently of the EI and ER roles that have been taken by the nodes.

All MLE messages used for the extension defined in this document SHOULD NOT be protected by link-layer so that a key exchange can be done regardless of the security state of the link-layer. A node that implements this specification MUST allow sending and receiving MLE messages not secured by the link-layer.

Secured 802.15.4 MAC frames and MLE messages that use keys established via HIP DEX MUST use a 5-octet Frame Counter so that the Frame Counter does not reach its maximum value throughout the lifetime of a node. An MLE Frame Counter is always carried in the Frame Counter field in the Aux Header of any secured MLE frame.

Other than the rules described in this document, the rules defined in [I-D.kelsey-6lo-mesh-link-establishment] are preserved.

3. Key Establishment Phase

A message exchange diagram for Key Establishment Phase is shown in Figure 1.

```
(EI)  (ER)
  -->    Advertisement [HIP{DEX-I1}, Link Quality]

  <--    Advertisement [HIP{DEX-R1}, Link Quality]

  -->    Link Request  [HIP{DEX-I2}, Source Address, Mode,
                        Timeout, Challenge]*

  <--    Link Accept and Request
                       [HIP{DEX-R2}, LLFC, MLFC, Source Address, Mode,
                        Timeout, Response, Challenge]*

  -->    Link Accept   [LLFC, MLFC, Response]*
```

Figure 1: Key Establishment Phase

An EI sends an MLE Advertisement message containing a HIP TLV and a Link Quality TLV to an ER. The HIP TLV carries a DEX-I1 packet. How an EI discovers an ER is outside the scope of this document.

The ER receives the MLE Advertisement message containing a DEX-I1 packet from the EI and sends an MLE Advertisement message containing a HIP TLV and a Link Quality TLV to the EI. The HIP TLV carries a DEX-R1 packet. The DEX-R1 packet MUST contain mandatory R1

parameters specified in [I-D.moskowitz-hip-dex]. The DEX-R1 packet MAY contain optional R1 parameters specified in [I-D.moskowitz-hip-dex] and a CERT parameter defined in [RFC6253].

The EI receives the MLE Advertisement message from the ER and sends a secured MLE Link Request message containing HIP, Source Address, Mode, Timeout and Challenge TLVs to the ER. The HIP TLV carries a DEX-I2 packet. The DEX-I2 packet MUST contain mandatory I2 parameters specified in [I-D.moskowitz-hip-dex] including an ENCRYPTED_KEY parameter wrapping a session key material of the EI. The DEX-I2 packet MUST also contain an ENCRYPTED parameter wrapping group key materials of the EI. The DEX-I2 packet MAY contain optional I2 parameters specified in [I-D.moskowitz-hip-dex] and a CERT parameter defined in [RFC6253]. The MLE Link Request message is protected by the EI's group MLE key (see section Section 5.2) derived from the EI's group key materials.

The ER receives the MLE Link Request message from the EI and extracts the EI's session key material wrapped in the ENCRYPTED_KEY parameter and the EI's group key materials wrapped in the ENCRYPTED parameter. Then the ER sends a secured MLE Link Accept and Request message containing HIP, LLFC, MLFC, Source Address, Mode Timeout, Response and Challenge TLVs to the EI. The HIP TLV carries a DEX-R2 packet. The DEX-R2 packet MUST contain R2 parameters specified in [I-D.moskowitz-hip-dex] including an ENCRYPTED_KEY parameter wrapping a session key material of the ER. The DEX-R2 packet MUST also contain an ENCRYPTED parameter wrapping group key materials of the ER. The DEX-R2 packet MAY contain optional R2 parameters specified in [I-D.moskowitz-hip-dex]. Note that the MIC field of the MLE Link Request message is verified after the ER successfully extracts the EI's group key materials.

The EI receives the MLE Link Accept and Request message from the ER and extracts the ER's session key material wrapped in the ENCRYPTED_KEY parameter and the ER's group key materials wrapped in the ENCRYPTED parameter. Then the EI sends a secured MLE Link Accept message containing LLFC TLV, MLFC and Response TLVs to the ER. If a pair-wise key is used by the link-layer, the EI also creates a Pair-wise Key SA with the session key generated by the pair of session key materials of the EI and ER as specified in [I-D.moskowitz-hip-dex]. Note that the MIC field of the MLE Link Accept and Request message is verified after the EI successfully extracts the ER's group key materials.

The ER receives the MLE Link Accept message from the EI. If a pair-wise key is used by the link-layer, the EI creates a Pair-wise Key SA with the session key generated by the pair of session key materials of the EI and ER as specified in [I-D.moskowitz-hip-dex].

4. Key Update Phase

In Key Update Phase, group key materials are updated.

Since the 5-octet Frame Counter space is large enough considering the maximum bandwidth of 250Kbps in 802.15.4 [IEEE802154] to make an assumption that a Frame Counter does not reach its maximum value throughout the lifetime of a node, a mechanism for updating a pair-wise key is not defined in this document. Both link-layer Frame Counters and MLE Frame Counters are not reset in the Key Update Phase.

Updating a group key may happen when a node that shares the group key is revoked. A message exchange diagram for group key update is shown in Figure 2.

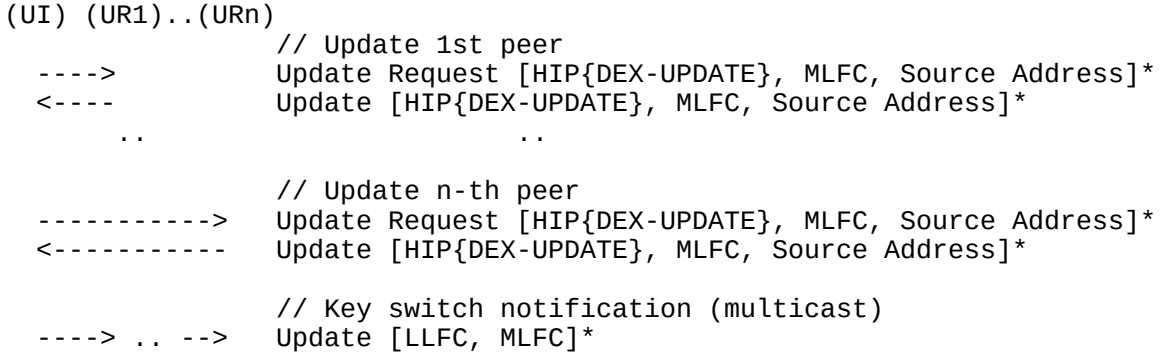


Figure 2: Group Key Update

First, a UI performs the following exchange for each UR:

- The UI sends an MLE Update Request message containing HIP, MLFC, Source Address and MIC TLVs to a UR. The HIP TLV carries a DEX-UPDATE packet containing SEC, MAC and ENCRYPTED parameters. The ENCRYPTED parameter wraps new group key materials of the UI.

- The UR receives the MLE Update Request message from the UI, extracts UI’s new group key materials from the ENCRYPTED parameter, activates the UI’s new group key materials for incoming frames, and sends an MLE Update message containing HIP, MLFC and Source Address TLVs, where the HIP TLV carries a DEX-UPDATE packet containing ACK and MAC parameters. Note that the MIC field of the MLE Update message is verified after the UR successfully extracts the UI’s new group key materials.

Once MLE Update Request and Update exchange is completed for all URs, the UI activates the UI's new group key materials for outgoing frames by multicasting an MLE Update message containing LLFC and MLFC TLVs. The MLE Update message is protected by the UI's group MLE key (see section Section 5.2) derived from the UI's new group key materials.

When a UR receives the multicast MLE Update message, If the received message is valid, the UR deactivates the UI's old group key materials for incoming frames.

A UR that did not receive the multicast MLE Update message may deactivate the UI's old group key materials for incoming frames when it receives a valid MAC frame protected by the link-layer key derived from the UI's new group key materials.

5. Key Materials

5.1. Pair-wise Key

The first 16 octets of the session key corresponding to the HIP DEX Pair-wise SA [I-D.moskowitz-hip-dex] is used as the pairwise link-layer key used for securing unicast link-layer frames with Key Identifier Mode 0x00.

An encrypted session key material is contained in an ENCRYPTED_KEY parameter of HIP when the session key is distributed during Key Establishment Phase.

5.2. Group Keys

Group key materials are created by a node and distributed to peer nodes.

The group key materials consist of a 1-octet key identifier (KeyId) and a 16-octet group master key (GroupMasterKey), and encoded as follows:

Group Key Materials = KeyId | GroupMasterKey

A 16-octet group link-layer key (GroupL2Key), and a 16-octet group MLE key (GroupMLEKey) are derived from GroupMasterKey as follows:

GroupL2Key = The first 16-octet of HMAC_SHA256(GroupMasterKey, KeyId).

GroupMLEKey = The last 16-octet of HMAC_SHA256(GroupMasterKey, KeyId).

A GroupL2Key is used for securing link-layer frames with Key Identifier Mode 0x03 sent by the node that created the group key material. GroupL2Key MUST be used for securing broadcast link-layer frames and MAY also be used for securing unicast link-layer frames.

A GroupMLEKey MUST be used for securing MLE messages with Key Identifier Mode 0x03 sent by the node that created the group key material.

The group key materials are contained in an GROUP_KEY_MATERIALS parameter of HIP, where the GROUP_KEY_MATERIALS parameter MUST be encrypted in an ENCRYPTED parameter of HIP.

6. MLE Security

As described in [I-D.kelsey-6lo-mesh-link-establishment], MLE security reuses that of IEEE 802.15.4, i.e., AES-CCM* [IEEE802154]. Since some of the MLE messages (i.e., MLE Link Accept and Request and MLE Accept messages carrying DEX-I2 and DEX-R2 packets, respectively, and unicast MLE Update Request and Update messages carrying a DEX-UPDATE packet) require to be sent unencrypted and only authentication is needed, MIC-64 (Security Level 2) or MIC-128 (Security Level 3) is used to secure MLE messages. MIC-64 is the default security level for securing MLE messages used in this document. GroupMLEKey (see section Section 5.2) with Key Identifier Mode 0x03 and a 5-octet Frame Counter MUST be used for any secured MLE message.

7. Certificate Revocation

Any MLE message used in this document MAY also contain a CRL (Certificate Revocation List) TLV in which CertificateList defined in [RFC5280] is encoded in the Value field. A node that receives a valid MLE message containing a CRL TLV revokes certificates specified in the TLV and deletes all pair-wise and group keys associated with the revoked certificates. A node MUST reject a CERT parameter for a revoked certificate in Key Establishment Phase.

When a CRL TLV is carried in a multicast Update message and forwarded multiple hops, MPL [I-D.ietf-roll-trickle-mcast] MAY be used. In this case, the multicast Update message MUST be secured at the link layer and MUST NOT be secured by MLE as specified in [I-D.kelsey-6lo-mesh-link-establishment]. Detailed MPL parameters for the multicast-based CRL distribution are out of the scope of this document.

8. Security Considerations

The MLE extension defined in this document uses HIP DEX for key management of computation or memory constrained sensor/actuator devices, and thus it inherits all security considerations made for HIP DEX [I-D.moskowitz-hip-dex].

In order to mitigate security weakness caused by lack of Perfect Forward Secrecy (PFS) in HIP DEX, it is RECOMMENDED to use this MLE extension in conjunction with an additional mechanism to update public/private key pairs and renew HIP DEX SAs using new public/ private key pairs whenever necessary.

In both Key Establishment Phase and Key Update Phase, MLE messages are secured using a group key instead of a pairwise key in order to optimize message roundtrips since a group key establishment requires only a half roundtrip. As a result, a Denial of Service (DoS) attack from an insider sharing the group key is possible over MLE TLVs.

Due to integration of HIP DEX into MLE, secured MLE messages are authenticated but not encrypted because decryption can be done only after establishing a key. As a result, Source Address, Mode, Timeout, Challenge, Response LLFC and MLFC TLVs are sent in clear, and the cleartext information may be used by attackers for the DoS attack described above. Note that authentication of the MLE message carrying a DEX-I2, DEX-R2 or DEX-UPDATE packet is possible by validating MIC of the MLE message after extracting the authentication key (i.e., GroupMLEKey) from the HIP DEX packet.

9. IANA Considerations

9.1. MLE TLV Types

The following MLE TLV types are to be assigned by IANA based on the policy described in [I-D.kelsey-6lo-mesh-link-establishment]:

- HIP-DEX (Value: 9, Length: Variable, Meaning: HIP DEX packet, Reference: this document).

- CRL (Value: 10, Length: Variable, Meaning: Certificate Revocation List, Reference: this document).

9.2. HIP Parameter

The following HIP Parameter is assigned based on the policy described in [I-D.ietf-hip-rfc5201-bis]:

- o GROUP_KEY_MATERIALS, (Value: 65530, Length: 33, Meaning: Group key materials for MLE and link-layer, Reference: this document).

10. Acknowledgments

The author would like to acknowledge the helpful comments of Randy Turner, Robert Cragie and Subir Das.

11. References

11.1. Normative References

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC6253] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", RFC 6253, DOI 10.17487/RFC6253, May 2011, <http://www.rfc-editor.org/info/rfc6253>.

[I-D.moskowitz-hip-dex] Moskowitz, R. and R. Hummen, "HIP Diet EXchange (DEX)", draft-moskowitz-hip-dex-04 (work in progress), July 2015.

[I-D.ietf-hip-rfc5201-bis] Moskowitz, R., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", draft-ietf-hip-rfc5201-bis-20 (work in progress), October 2014.

[I-D.kelsey-6lo-mesh-link-establishment] Kelsey, R., "Mesh Link Establishment", draft-kelsey-6lo-mesh-link-establishment-00 (work in progress), July 2015.

[I-D.ietf-roll-trickle-mcast] Hui, J. and R. Kelsey, "Multicast Protocol for Low power and Lossy Networks (MPL)", draft-ietf-roll-trickle-mcast-12 (work in progress), June 2015.

11.2. External Informative References

[IEEE802154]
IEEE standard for Information Technology, "IEEE std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks", June 2011.

Author's Address

Yoshihiro Ohba (editor)
Toshiba Electronics Asia
20 Pasir Panjang Road, #12-25/28, Mapletree Business City
117439
Singapore

Phone: +65 6278 5252
Email: yoshihiro.ohba@toshiba.co.jp

6lo
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

B. Sarikaya, Ed.
Huawei USA
P. Thubert, Ed.
Cisco

October 19, 2015

Address Protected Neighbor Discovery for Low-power and Lossy Networks
draft-sarikaya-6lo-ap-nd-01

Abstract

This document defines an extension of 6LoWPAN Neighbor Discovery for application in low-power and lossy networks. The protocol is specified to be protected and to support multi-hop operation. A node computes its Cryptographic, Unique Interface ID, and associates one or more of its Registered Addresses with that Cryptographic ID in place of the EUI-64 that is used in RFC 6775 to uniquely identify the interface of the Registered Address. Once an address is registered with a Cryptographic ID, only the owner of that ID can modify the state in the 6LR and 6LBR regarding the Registered Address.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. Requirements 4
4. Protocol Interactions 4
4.1. Overview 4
4.2. Protocol Operations 7
4.2.1. Calculation of Cryptographic Identifier 8
4.3. Multihop Operation 10
5. Security Considerations 11
6. IANA considerations 12
7. Acknowledgements 12
8. References 12
8.1. Normative References 12
8.2. Informative references 13
Authors' Addresses 14

1. Introduction

Neighbor discovery for IPv6 [RFC4861] and stateless address autoconfiguration [RFC4862], together referred to as neighbor discovery protocols (NDP), are defined for regular hosts operating with wired/wireless links. These protocols are not suitable and require optimizations for resource constrained, low power hosts operating with LLN for low-power and lossy networks. Neighbor Discovery optimizations for 6LoWPAN networks include simple optimizations such as a host address registration feature using the address registration option (ARO) which is sent in unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages [RFC6775]. With 6LoWPAN ND [RFC6775], the ARO option includes a EUI-64 address to uniquely identify the interface of the Registered Address on the registering device, so as to correlate further registrations for the same address and avoid address duplication. The EUI-64 address is not secured and its ownership cannot be verified. It results that any device claiming the same EUI-64 address may take over a registration and attract the traffic for that address.

In this document, we extend 6LoWPAN ND to protect the address ownership with cryptographic material, but as opposed to Secure Neighbor Discovery (SEND) [RFC3971], [RFC3972], the cryptographic material is not embedded in the Interface ID (IID) in an IPv6 address

but used as a correlator associated to the registration of the IPv6 address. This approach is made possible with 6LoWPAN ND [RFC6775], where the 6LR and the 6LBR maintain a state for each Registered Address. If a cryptographic ID is associated with an original 6LoWPAN ND registration and stored in the registration state, then it can be used to validate that any update to the registration state is made by the owner of that ID.

To achieve this, this specification replaces the EUI-64 address, that is used in 6LoWPAN ND to avoid address duplication, with cryptographic material whose ownership can be verified; it also provides new means for the 6LR to validate ownership of the registration thus that of the registered address by the registering device. The resulting protocol is called Protected address autoconfiguration and registration protocol (ND-PAAR).

A node generates one 64-bit cryptographic ID and uses it as Unique Interface ID in the registration of (one or more of) its addresses with the 6LR, which it attaches to and uses as default router. The 6LR validates ownership of the cryptographic ID typically upon creation or update of a registration state, for instance following an apparent movement from a point of attachment to another. The ARO option is modified to carry the Unique Interface ID, and through the DAR/DAC exchange, the 6LBR is kept aware that this is the case, i.e. unique and whether the 6LR has verified the claim.

2. Terminology

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].

Readers are expected to be familiar with all the terms and concepts that are discussed in [RFC3971], [RFC3972], "neighbor Discovery for IP version 6" [RFC4861], "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919], neighbor Discovery Optimization for Low-power and Lossy Networks [RFC6775] where the 6LoWPAN Router (6LR) and the 6LoWPAN Border Router (6LBR) are introduced, and [I-D.chakrabarti-nordmark-6man-efficient-nd], which proposes an evolution of [RFC6775] for a larger applicability.

The document also conforms to the terms and models described in [RFC5889] and uses the vocabulary and the concepts defined in [RFC4291] for the IPv6 Architecture.

This document uses [RFC7102] for Terminology in Low power And Lossy Networks.

3. Requirements

In this section we state requirements of a secure neighbor discovery protocol for low-power and lossy networks.

The protocol MUST be based on the Neighbor Discovery Optimization for Low-power and Lossy Networks protocol defined in [RFC6775] due to the host-initiated interactions to allow for sleeping hosts, elimination of multicast-based address resolution for hosts, etc.

New options to be added to Neighbor Solicitation messages MUST lead to small packet sizes. Smaller packet sizes facilitate low-power transmission by resource constrained nodes on lossy links.

The support of the registration mechanism SHOULD be extended to more LLN links than IEEE 802.15.4, matching at least the LLN links for which a 6lo "IPv6 over foo" specification exists, as well as Low-Power Wi-Fi.

As part of this extension, a mechanism to compute a unique Identifier should be provided, with the capability to form a Link Local Address that SHOULD be unique at least within the LLN connected to a 6LBR discovered by ND in each node within the LLN.

The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of Unique Interface IDentifier.

The Neighbour Discovery should specify the formation of a site-local address that follows the security recommendations from [RFC7217].

4. Protocol Interactions

Protected address autoconfiguration and registration neighbor discovery protocol (ND-PAAR) modifies Neighbor Discovery Optimization for Low-power and Lossy Networks [RFC6775] as explained in this section.

4.1. Overview

The scope of the present work is a 6LoWPAN Low Power Lossy Network (LLN), typically a stub network connected to a larger IP network via a Border Router called a 6LBR per [RFC6775].

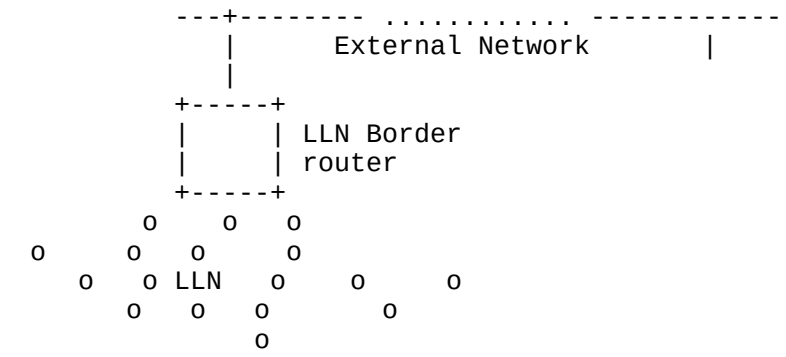


Figure 1: Basic Configuration

The 6LBR maintains a registration state for all devices in the attached LLN, and, in conjunction with the first-hop router (the 6LR), is in position to validate uniqueness and grant ownership of an IPv6 address before it can be used in the LLN. This is a fundamental difference with a classical network that relies on IPv6 address auto-configuration [RFC4862], where there is no guarantee of ownership from the network, and any IPv6 Neighbor Discovery packet must be individually secured [RFC3971].

In a route-over mesh network, the 6LR is directly connected to the host device; this specification expects that peer-wise Layer-2 security is deployed so that all the packets from a particular host are identified as such by the 6LR. The 6LR may be multiple hops away from the 6LBR. Packets are routed between the 6LR and the 6LBR via other 6LRs; this specification expects that a chain of trust is established so that a packet that was validated by the first 6LR can be safely routed by the next 6LRs and 6LBR.

The [I-D.ietf-6tisch-architecture] suggests to use RPL [RFC6550] as the routing protocol between the 6LRs and the 6LBR, and to leverage [I-D.chakrabarti-nordmark-6man-efficient-nd] to extend the LLN in a larger multilink subnet [RFC4903]. In that model, a registration flow happens as shown in Figure 2:

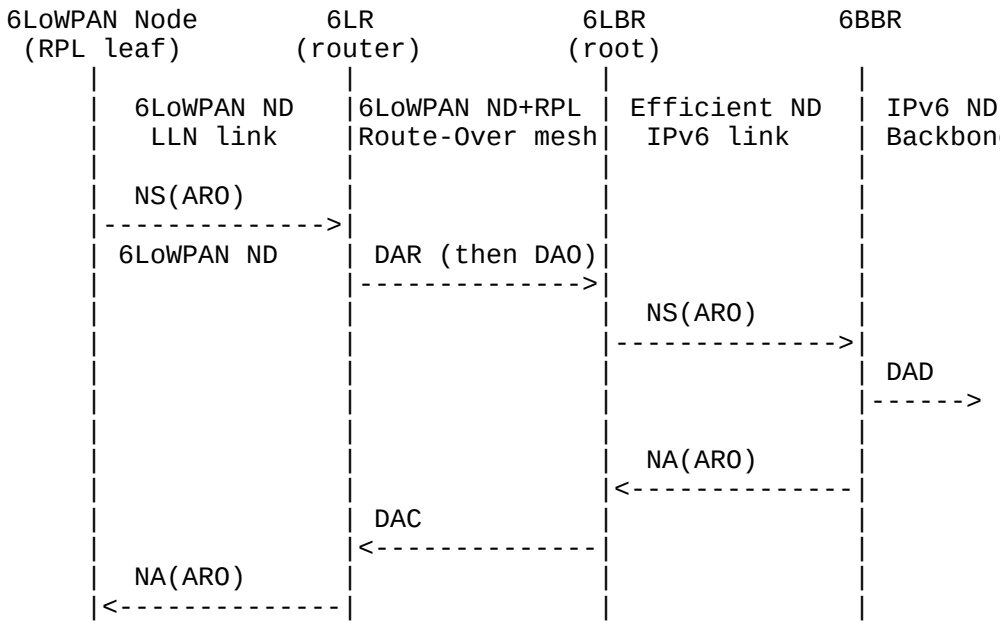


Figure 2: (Re-)Registration Flow over Multi-Link Subnet

A new device that joins the network auto-configures an address and performs an initial registration to an on-link 6LR with an NS message that carries a new Address Registration Option (ARO) [RFC6775]. The 6LR validates the address with the central 6LBR using a DAR/DAC exchange, and the 6LR confirms (or infirms) the address ownership with an NA message that also carries an Address Registration Option.

The registration mechanism in [RFC6775] was created for the original purpose of Duplicate Address Detection (DAD), whereby use of an address would be granted as long as the address is not already present in the subnet. But [RFC6775] does not require that the 6LR use the registration for source address validation (SAVI).

In order to validate address ownership, that mechanism enables the 6LBR to correlate further claims for a registered address with the device to which it is granted, based on a Unique Interface IDentifier (UID) that is derived from the MAC address of the device (EUI-64).

The limitation of the mechanism in [RFC6775] is that it does not enable to prove the UID itself, so any node connected to the subnet and aware of the address/UID mapping may effectively fake the same UID and steal an address.

This draft uses a randomly generated value as an alternate UID for the registration. Proof of ownership of the UID is passed with the first registration to a given 6LR, and enforced at the 6LR, which validates the proof. With this new operation, the 6LR allows only packets from a connected host if the connected host owns the registration of the source address of the packet.

If a chain of trust is present between the 6LR and the 6LBR, then there is no need to propagate the proof of ownership to the 6LBR. All the 6LBR need to know is that this particular UID is randomly generated, so as to enforce that any update via a different 6LR is also random.

4.2. Protocol Operations

Protocol interactions are as defined in Figure 2. The crypto ID is calculated as described in Section 4.2.1.

The Target Address field in NS message is set to the prefix concatenated with the node’s address. This address does not need duplicate address detection as crypto ID is globally unique. So a host cannot steal an address that is already registered unless it has the key for the crypto ID. The same crypto ID can thus be used to protect multiple addresses e.g. when the node receives a different prefix.

Local or on-link protocol interactions are given in Figure 3. Crypto ID and ARO are passed to and stored by the 6LR/6LBR on the first NS and not sent again the in the next NS.

The 6LR/6LBR ensures first-come/first-serve by storing the ARO and the crypto ID correlated to the target being registered. Then, if the node is the first to claim any address it likes, then it becomes owner of that address and the address is bound to the crypto ID in the 6LR/6LBR registry. This procedure avoids the constrained device to compute multiple keys for multiple addresses. The registration process allows the node to tie all the addresses to the same crypto ID and have the 6LR/6LBR enforce first come first serve after that.

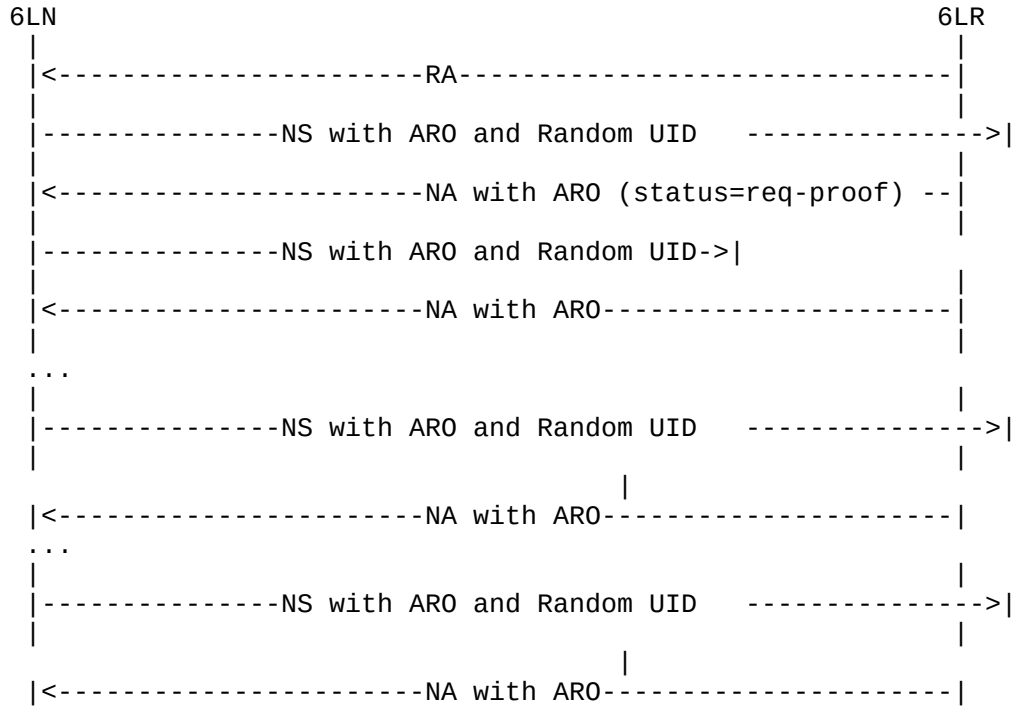


Figure 3: On-link Protocol Operation

4.2.1. Calculation of Cryptographic Identifier

Elliptic Curve Cryptography (ECC) is used in the calculation of cryptographical identifier. The digital signature is constructed by using the 6LN's private key over its EUI-64, i.e. its MAC address. The signature value is computed using the ECDSA signature algorithm and hash function used is SHA-256. Public Key is the most important parameter in CGA Parameters (sent by 6LN in an NS message). ECC Public Key could be in uncompressed form or in compressed form where the first octet of the OCTET STRING is 0x04 and 0x02 or 0x03, respectively. Point compression using secp256r1 reduces the key size by 32 octets.

After the calculation, 6LN sends it along with the CGA parameters in the first NS message, see Figure 3. In order to send Cryptographical Identifier a neighbor discovery option is defined in Figure 4. As defined in the figure this ID is variable length, varying between 64 to 128 bits. This ID is 128 bits long if it is used as IPv6 address.

6LN also sends some other parameters to enable 6LR or 6LBR to verify the crypto ID. One of them is 6LN's MAC address which is sent in Address Registration Option (ARO) as defined in [RFC6775]. The next

one is shown in Figure 5. In that figure, CGA Parameters field contains the public key, prefix and some other values. Digital signature option contains the signature of the CGA calculated using 6LN's private key.

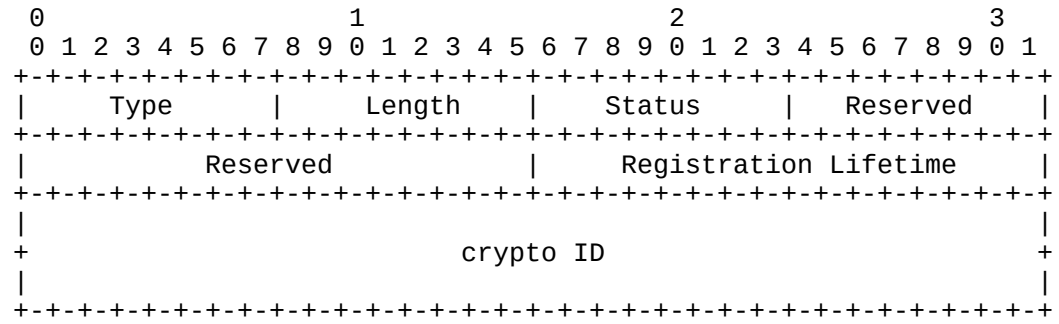


Figure 4: Crypto ID Option

Type: TBA

Length: 8-bit unsigned integer. The length of the option in units of 8 bytes. It is 2 or 3, if crypto ID is 128 bits.

Status: 8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. See below.

Reserved: This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Registration Lifetime: 16-bit unsigned integer. The amount of time in units of 60 seconds that the router should retain the NCE for the sender of the NS that includes this option.

Crypto ID Variable length field to carry the cryptographical identifier or random UID. This field is normally 64 bits long. It could be 128 bits long if IPv6 address is used as the crypto ID.

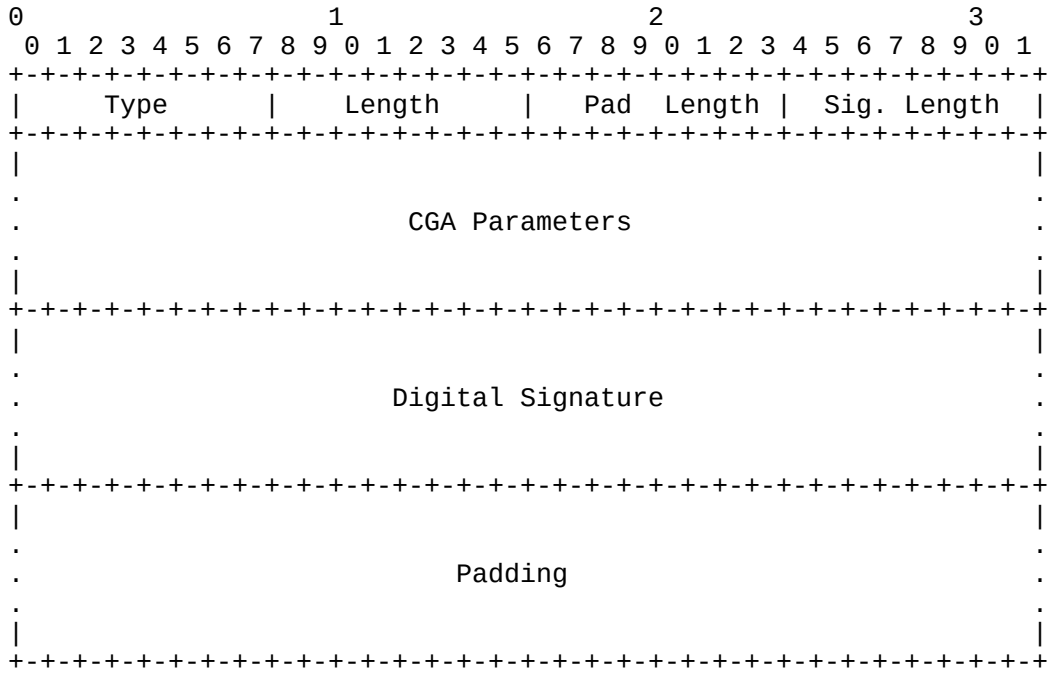


Figure 5: CGA Parameters Option

Type TBA

Length The length of the option in units of 8 octets.

Pad Length The length of the Padding field.

Sig Length The length of the Digital Signature field.

CGA Parameters The CGA Parameters field is variable-length containing the CGA Parameters data structure.

Digital Signature The Digital Signature field is a variable length field containing a Elliptic Curve Digital Signature Algorithm (ECDSA) signature (with SHA-256 and P-256 curve of [FIPS-186-3]).

4.3. Multihop Operation

In multihop 6LoWPAN, 6LBR sends RAs with prefixes downstream and it is the 6LR that receives and relays them to the nodes. 6LR and 6LBR communicate with the ICMPv6 Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC) messages. The DAR and DAC use

the same message format as NS and NA with different ICMPv6 type values.

In ND-PAAR we extend DAR/DAC messages to carry cryptographically generated UID.

In a multihop 6LoWPAN, the node exchanges the messages shown in Figure 2. The 6LBR must be aware of who owns an address (EUI-64) to defend the first user if there is an attacker on another 6LR. Because of this the content that the source signs and the signature needs to be propagated to the 6LBR in DAR message. For this purpose we need the DAR message sent by 6LR to 6LBR MUST contain CGA Parameters and Digital Signature Option carrying the CGA that the node calculates and its public key. DAR message also contains ARO.

It is possible that occasionally, 6LR may miss the node’s UID (that it received in ARO). 6LR should be able to ask for it again. This is done by restarting the exchanges shown in Figure 3. The result enables 6LR to refresh the information that was lost. 6LR MUST send DAR message with ARO to 6LBR. 6LBR as a reply forms a DAC message with the information copied from the DAR and the Status field is set to zero. With this exchange, the 6LBR can (re)validate and store the information to make sure that the 6LR is not a fake.

5. Security Considerations

The same considerations regarding the threats to the Local Link Not Covered (as in [RFC3971]) apply.

The threats discussed in Section 9.2 of [RFC3971] are countered by the protocol described in this document as well.

As to the attacks to the protocol itself, denial of service attacks that involve producing a very high number of packets are deemed unlikely because of the assumptions on the node capabilities in low-power and lossy networks.

A collision of ID in ND-PAAR is a really rare event that does not prevent the protocol operation though it opens a window for a node to hijack an address from another. The nodes would normally not be aware that they are in this situation, and the only thing they could do if they knew would be to steal addresses from one another, so the damage is limited to these 2 nodes.

6. IANA considerations

TBD.

7. Acknowledgements

TBD.

8. References

8.1. Normative References

[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>.

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, DOI 10.17487/RFC3756, May 2004, <http://www.rfc-editor.org/info/rfc3756>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <http://www.rfc-editor.org/info/rfc3971>.

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

[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>.

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

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <http://www.rfc-editor.org/info/rfc4919>.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, DOI 10.17487/RFC5480, March 2009, <http://www.rfc-editor.org/info/rfc5480>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <http://www.rfc-editor.org/info/rfc5889>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., 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, DOI 10.17487/RFC6550, March 2012, <http://www.rfc-editor.org/info/rfc6550>.

[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>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <http://www.rfc-editor.org/info/rfc7102>.

[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>.

[Guide] "Guidelines for 64-bit global Identifier (EUI-64TM)", November 2012, <http://standards.ieee.org/develop/regauth/tut/eui64.pdf>.

8.2. Informative references

[I-D.rafiee-6man-ssas] Rafiee, H. and C. Meinel, "A Simple Secure Addressing Scheme for IPv6 AutoConfiguration (SSAS)", draft-rafiee-6man-ssas-11 (work in progress), September 2014.

[I-D.chakrabarti-nordmark-6man-efficient-nd]
Chakrabarti, S., Nordmark, E., Thubert, P., and M. Wasserman, "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", draft-chakrabarti-nordmark-6man-efficient-nd-07 (work in progress), February 2015.

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-08 (work in progress), May 2015.

Authors' Addresses

Behcet Sarikaya (editor)
Huawei USA
5340 Legacy Dr. Building 3
Plano, TX 75024

Email: sarikaya@ieee.org

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis 06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

6lo
Internet-Draft
Updates: 4944 (if approved)
Intended status: Standards Track
Expires: February 7, 2016

P. Thubert, Ed.
Cisco
C. Bormann
Uni Bremen TZI
L. Toutain
IMT-TELECOM Bretagne
R. Cragie
ARM

August 06, 2015

A Routing Header Dispatch for 6LoWPAN
draft-thubert-6lo-routing-dispatch-06

Abstract

This specification introduces a new context switch mechanism for 6LoWPAN compression, expressed in terms of Pages. A new 6LoWPAN dispatch type is proposed in a new Page 1 for use in 6LoWPAN Route-Over topologies, that initially covers the needs of RPL (RFC6550) data packets compression. This specification defines a method to compress RPL Option (RFC6553) information and Routing Header type 3 (RFC6554), an efficient IP-in-IP technique and is extensible for more applications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 7, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 5
3. Updating RFC 4944 5
3.1. New Page1 Dispatch 6
3.2. New Routing Header Dispatch (6LoRH) 6
3.3. Sur-Compression Mechanisms 6
4. Placement Of The New Dispatch Types 7
4.1. Placement Of The Page1 Dispatch 7
4.2. Placement Of The 6LoRH 7
5. 6LoWPAN Routing Header General Format 8
5.1. Elective Format 8
5.2. Critical Format 9
6. The Routing Header Type 3 (RH3) 6LoRH 9
7. The RPL Packet Information 6LoRH 11
7.1. Compressing the RPLInstanceID 12
7.2. Compressing the SenderRank 12
7.3. The Overall RPI-6LoRH encoding 13
8. The IP-in-IP 6LoRH 15
9. The BIER 6LoRH 17
10. Security Considerations 18
11. IANA Considerations 18
12. Acknowledgments 19
13. References 19
13.1. Normative References 19
13.2. Informative References 20
Authors' Addresses 21

1. Introduction

The design of Low Power and Lossy Networks (LLNs) is generally focused on saving energy, which is the most constrained resource of all. The other constraints, such as the memory capacity and the duty cycling of the LLN devices, derive from that primary concern. Energy is often available from primary batteries that are expected to last for years, or is scavenged from the environment in very limited quantities. Any protocol that is intended for use in LLNs must be

designed with the primary concern of saving energy as a strict requirement.

Controlling the amount of data transmission is one possible venue to save energy. In a number of LLN standards, the frame size is limited to much smaller values than the IPv6 maximum transmission unit (MTU) of 1280 bytes. In particular, an LLN that relies on the classical Physical Layer (PHY) of IEEE 802.14.5 [IEEE802154] is limited to 127 bytes per frame. The need to compress IPv6 packets over IEEE 802.14.5 led to the 6LoWPAN Header Compression [RFC6282] work (6LoWPAN-HC).

Innovative Route-over techniques have been and are still being developed for routing inside a LLN. In a general fashion, such techniques require additional information in the packet to provide loop prevention and to indicate information such as flow identification, source routing information, etc.

For reasons such as security and the capability to send ICMP errors back to the source, an original packet must not be tampered with, and any information that must be inserted in or removed from an IPv6 packet must be placed in an extra IP-in-IP encapsulation. This is the case when the additional routing information is inserted by a router on the path of a packet, for instance a mesh root, as opposed to the source node. This is also the case when some routing information must be removed from a packet that will flow outside the LLN.

As an example, the Routing Protocol for Low Power and Lossy Networks [RFC6550] (RPL) is designed to optimize the routing operations in constrained LLNs. As part of this optimization, RPL requires the addition of RPL Packet Information (RPI) in every packet, as defined in Section 11.2 of [RFC6550].

The RPL Option for Carrying RPL Information in Data-Plane Datagrams [RFC6553] specification indicates how the RPI can be placed in a RPL Option for use in an IPv6 Hop-by-Hop header. This representation demands a total of 8 bytes when in most cases the actual RPI payload requires only 19 bits. Since the Hop-by-Hop header must not flow outside of the RPL domain, it must be removed from packets that leave the domain, and be inserted in packets entering the domain. In both cases, this operation implies an IP-in-IP encapsulation.

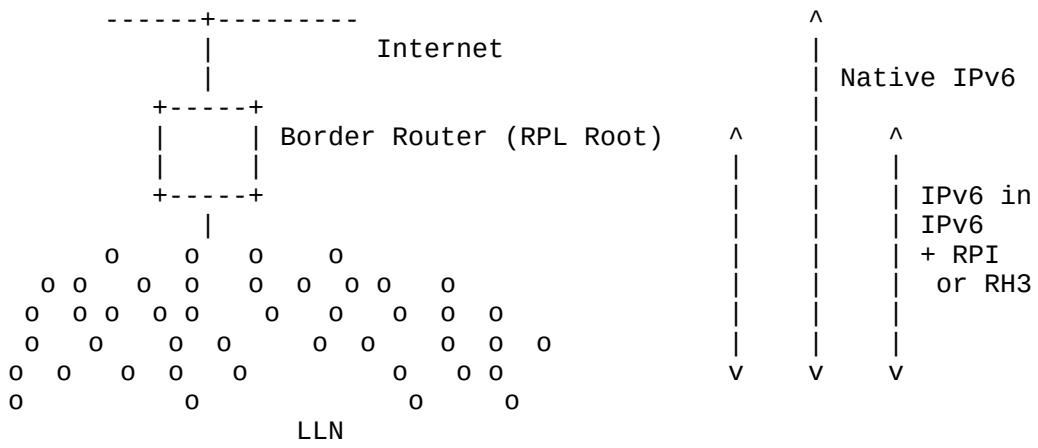


Figure 1: IP-in-IP Encapsulation within the LLN

Additionally, in the case of the Non-Storing Mode of Operation (MOP), RPL requires a Routing Header type 3 (RH3) as defined in the IPv6 Routing Header for Source Routes with RPL [RFC6554] specification, for all packets that are routed down a RPL graph. With Non-Storing RPL, even if the source is a node in the same LLN, the packet must first reach up the graph to the root so that the root can insert the RH3 to go down the graph. In any fashion, whether the packet was originated in a node in the LLN or outside the LLN, and regardless of whether the packet stays within the LLN or not, as long as the source of the packet is not the root itself, the source-routing operation also implies an IP-in-IP encapsulation at the root to insert the RH3.

6TiSCH [I-D.ietf-6tisch-architecture] specifies the operation of IPv6 over the TimeSlotted Channel Hopping [I-D.ietf-6tisch-tsch] (TSCH) mode of operation of IEEE 802.14.5. The architecture requires the use of both RPL and the 6lo adaptation layer framework ([RFC4944], [RFC6282]) over IEEE 802.14.5. Because it inherits the constraints on the frame size from the MAC layer, 6TiSCH cannot afford to spend 8 bytes per packet on the RPI. Hence the requirement for a 6LoWPAN header compression of the RPI.

The type of information that needs to be present in a packet inside the LLN but not outside of the LLN varies with the routing operation, but there is overall a need for an extensible compression technique that would simplify the IP-in-IP encapsulation, when needed, and optimally compress existing routing artifacts found in LLNs.

This specification extends 6LoWPAN [RFC4944] and in particular reuses the Mesh Header formats that are defined for the Mesh-under use cases so as to carry routing information for Route-over use cases. The

specification includes the formats necessary for RPL and is extensible for additional formats.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The Terminology used in this document is consistent with and incorporates that described in ‘Terminology in Low power And Lossy Networks’ [RFC7102] and [RFC6550].

The terms Route-over and Mesh-under are defined in [RFC6775].

Other terms in use in LLNs are found in [RFC7228].

The term "byte" is used in its now customary sense as a synonym for "octet".

3. Updating RFC 4944

This draft adapts 6LoWPAN while maintaining backward compatibility with IPv6 over IEEE 802.15.4 [RFC4944] by introducing a concept of context in the 6LoWPAN parser, a context being identified by a Page number, and defines 16 Pages.

Pages are delimited in a 6LoWPAN packet by a dispatch value that indicates the next current Page. The Page number is encoded in a Dispatch Value Bit Pattern of 1111xxxx where xxxx is the Page number, 0 to 15, as follows:

Figure 2: Page encoding

Values of the Dispatch byte defined in [RFC4944] are considered as belonging to a Page 0 parsing context, which is the default and does not need to be signaled explicitly at the beginning of a 6LoWPAN packet. That way, backward compatibility with existing implementations in ensured.

Note: This specification does not use the Escape Dispatch, which extends Page 0 to more values, but rather allocates another Dispatch Bit Pattern (1111xxxx), in all Pages including Page 0 and Pages defined in future specifications, to indicate the next parsing context represented by its Page number.

3.1. New Page1 Dispatch

This draft defines a new Page1 Dispatch with a Dispatch Value of 11110001 that indicates a context switch in the 6LoWPAN parser to a Page 1.

The Dispatch bits defined in Page 0 by [RFC4944] are free to be reused in Page 1.

On the other hand, the Dispatch bits defined in Page 0 for the Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks [RFC6282] are defined with the same values in Page 1 so there is no need to switch context back from Page 1 to Page 0 to address LOWPAN_IPHC and LOWPAN_NHC.

3.2. New Routing Header Dispatch (6LoRH)

This specification introduces a new 6LoWPAN Routing Header (6LoRH) to carry IPv6 routing information. The 6LoRH may contain source routing information such as a compressed form of RH3, as well as other sorts of routing information such as the RPL Packet Information and IP-in-IP encapsulation.

The 6LoRH is expressed in a 6loWPAN packet as a Type-Length-Value (TLV) field, which is extensible for future uses. The proposed BIER bitmap encoding in Section 9 is an example of extension.

Section 5.1 of the [RFC4944] specification defines various Dispatch Types and Headers, and in particular a Mesh Header that corresponds to a bit pattern 10xxxxxx (in Page 0).

This specification uses the same bit pattern 10xxxxxx in Page 1 for the canonical form of 6LoRH Dispatch that is detailed in Section 5

3.3. Sur-Compression Mechanisms

It is expected that virtual-link-specific sur-compression mechanisms may be applied in the future that merge Dispatch values from multiple Pages into a single octet, attempting to keep the dispatch bits settings in their canonical form as much as possible.

Considering that the Mesh-Under and the Route-Over modes are generally mutually exclusive, it is expected that the new 6LoRH Dispatch introduced in this specification can be left in its canonical form through sur-compression technique.

A dispatch space of equivalent size to the Mesh Header was reserved in [RFC4944] for external specifications, Not A LowPan (NALP), hoping that such specification could coexist harmlessly on a same network as a early 6LoWPAN.

A sur-compression technique may alternatively use the NALP space for 6LoRH, in which case bit patterns represented as 10xxxxxx in this specification will be mapped directly to 00xxxxxx.

4. Placement Of The New Dispatch Types

4.1. Placement Of The Page1 Dispatch

In a zone of a packet where Page 1 is active, which means once a Page1 Dispatch is parsed, and as long as no other Page Dispatch is parsed, the parsing of the packet MUST follow this specification if the 6LoRH Bit Pattern [Section 5] is found.

Mesh Headers represent Layer-2 information and are processed before any Layer-3 information that is encoded in Page 1. If a 6LoWPAN packet requires a Mesh header, the Mesh Header MUST always be placed in the packet before the first Page1 Dispatch, if any.

For the same reason, Fragments Headers as defined in [RFC4944] MUST always be placed in the packet before the first Page1 Dispatch, if any.

It must be noted that the NALP Dispatch Bit Pattern as defined in [RFC4944] is only defined for the first octet in the packet. Switching back to Page 0 for NALP inside a 6LoWPAN packet appears non-sensical.

It results that there is no need so far for restoring the Page 0 parsing context after a context was switched to Page 1, so the value for the Page0 Dispatch of 11110000 may not actually be seen in packets following the 6LoWPAN specifications that are available at the time of this writing.

4.2. Placement Of The 6LoRH

With this specification, the 6LoRH [Section 5] is only defined in Page 1, so it MUST be placed in the packet in a zone where the Page 1 context is active.

One or more 6LoRHs MAY be placed in a 6LoWPAN packet and MUST always be placed before the LOWPAN_IPHC [RFC6282].

A 6LoRH being placed in a Page 1 context, it MUST always be placed after any Fragmentation Header and/or Mesh Header [RFC4944], even if a sur-compression mechanism is used that elides the Page Dispatches.

5. 6LoWPAN Routing Header General Format

In its canonical form, the 6LoRH reuses in Page 1 the Dispatch Value Bit Pattern of 10xxxxxx that is defined in Page 0 for the Mesh Header in [RFC4944].

The Dispatch Value Bit Pattern is split in two forms of 6LoRH:

Elective (6LoRHE) that may skipped if not understood

Critical (6LoRHC) that may not be ignored

5.1. Elective Format

In its canonical form, the 6LoRHE uses the Dispatch Value Bit Pattern of 101xxxxx.
A 6LoRHE may be ignored and skipped in parsing.
If it is ignored, the 6LoRHE is forwarded with no change inside the LLN.

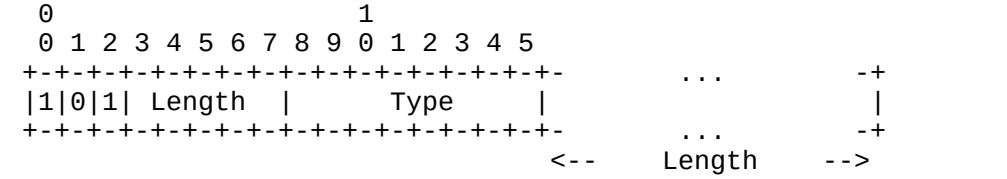


Figure 3: Elective 6LoWPAN Routing Header

Length:
Length of the 6LoRHE expressed in bytes, excluding the first 2 bytes. This is done to enable a node to skip a 6LoRH that it does not support and/or cannot parse, for instance if the Type is not known.

Type:
Type of the 6LoRHE

5.2. Critical Format

In its canonical form, the 6LoRHC uses the Dispatch Value Bit Pattern of 100xxxxx.

A node which does not support the 6LoRHC Type MUST silently discard the packet.

Note: there is no provision for the exchange of error messages; such a situation should be avoided by judicious use of administrative control and/or capability indications.

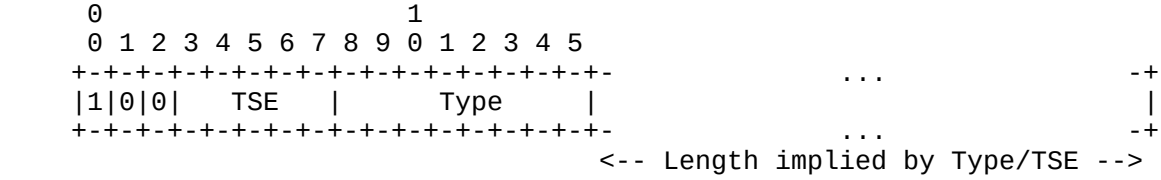


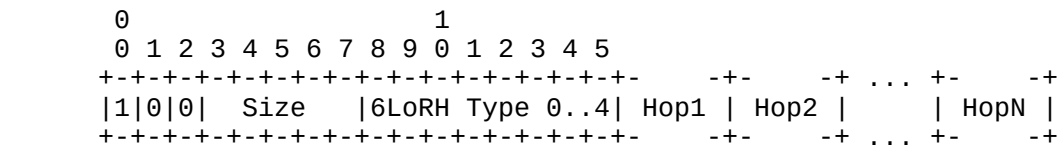
Figure 4: Critical 6LoWPAN Routing Header

TSE:
Type Specific Extension. The meaning depends on the Type, which must be known in all of the nodes. The interpretation of the TSE depends on the Type field that follows. For instance, it may be used to transport control bits, the number of elements in an array, or the length of the remainder of the 6LoRHC expressed in a unit other than bytes.

Type:
Type of the 6LoRHC

6. The Routing Header Type 3 (RH3) 6LoRH

The Routing Header type 3 (RH3) 6LoRH (RH3-6LoRH) is a Critical 6LoWPAN Routing Header that provides a compressed form for the RH3, as defined in [RFC6554] for use by RPL routers. Routers that need to forward a packet with a RH3-6LoRH are expected to be RPL routers and expected to support this specification. If a non-RPL router receives a packet with a RPI-6LoRH, this means that there was a routing error and the packet should be dropped so the Type cannot be ignored.



Size indicates the number of compressed addresses

Figure 5: The RH3-6LoRH

The values for the RH3-6LoRH Type are an enumeration, 0 to 4. The form of compression is indicated by the Type as follows:

Type	Size Unit
0	1
1	2
2	4
3	8
4	16

Figure 6: The RH3-6LoRH Types

In the case of a RH3-6LoRH, the TSE field is used as a Size, which encodes the number of hops minus 1; so a Size of 0 means one hop, and the maximum that can be encoded is 32 hops. (If more than 32 hops need to be expressed, a sequence of RH3-6LoRH can be employed.)

The next Hop is indicated in the first entry of the first RH3-6LoRH. Upon reception, the entry is checked whether it refers to the processing router itself. If it so, the entry is removed from the RH3-6LoRH and the Size is decremented. If the Size is now zero, the whole RH3-6LoRH is removed. If there is no more RH3-6LoRH, the processing node is the last router on the way, which may or may not be collocated with the final destination.

The last hop in the last RH3-6LoRH is the last router prior to the destination in the LLN. So even when there is a RH3-6LoRH in the frame, the address of the final destination is in the LoWPAN_IPHC [RFC6282].

If some bits of the first address in the RH3-6LoRH can be derived from the final destination is in the LoWPAN_IPHC, then that address may be compressed, otherwise is is expressed in full. Next addresses only need to express the delta from the previous address.

All addresses in a RH3-6LoRH are compressed in a same fashion, down to the same number of bytes per address. In order to get different forms of compression, multiple consecutive RH3-6LoRH must be used.

7. The RPL Packet Information 6LoRH

[RFC6550], Section 11.2, specifies the RPL Packet Information (RPI) as a set of fields that are to be added to the IP packets for the purpose of Instance Identification, as well as Loop Avoidance and Detection.

In particular, the SenderRank, which is the scalar metric computed by an specialized Objective Function such as [RFC6552], indicates the Rank of the sender and is modified at each hop. The SenderRank allows to validate that the packet progresses in the expected direction, either upwards or downwards, along the DODAG.

RPL defines the RPL Option for Carrying RPL Information in Data-Plane Datagrams [RFC6553] to transport the RPI, which is carried in an IPv6 Hop-by-Hop Options Header [RFC2460], typically consuming eight bytes per packet.

With [RFC6553], the RPL option is encoded as six Octets; it must be placed in a Hop-by-Hop header that consumes two additional octets for a total of eight. In order to limit its range to the inside the RPL domain, the Hop-by-Hop header must be added to (or removed from) packets that cross the border of the RPL domain.

The 8-bytes overhead is detrimental to the LLN operation, in particular with regards to bandwidth and battery constraints. These bytes may cause a containing frame to grow above maximum frame size, leading to Layer 2 or 6LoWPAN [RFC4944] fragmentation, which in turn cause even more energy spending and issues discussed in the LLN Fragment Forwarding and Recovery [I-D.thubert-6lo-forwarding-fragments].

An additional overhead comes from the need, in certain cases, to add an IP-in-IP encapsulation to carry the Hop-by-Hop header. This is needed when the router that inserts the Hop-by-Hop header is not the source of the packet, so that an error can be returned to the router. This is also the case when a packet originated by a RPL node must be stripped from the Hop-by-Hop header to be routed outside the RPL domain.

This specification defines an IPinIP-6LoRH in Section 8 for that purpose, but it must be noted that stripping a 6LoRH does not require a manipulation of the packet in the LOWPAN_IPHC, and thus, if the

source address in the LOWPAN_IPHC is the node that inserted the IPinIP-6LoRH then this alone does not mandate an IPinIP-6LoRH.

As a result, a RPL packet may bear only a RPI-6LoRH and no IPinIP-6LoRH. In that case, the source and destination of the packet are located in the LOWPAN_IPHC.

As with [RFC6553], the fields in the RPI include an 'O', an 'R', and an 'F' bit, an 8-bit RPLInstanceID (with some internal structure), and a 16-bit SenderRank.

The remainder of this section defines the RPI-6LoRH, a Critical 6LoWPAN Routing Header that is designed to transport the RPI in 6LoWPAN LLNs.

7.1. Compressing the RPLInstanceID

RPL Instances are discussed in [RFC6550], Section 5. A number of simple use cases will not require more than one instance, and in such a case, the instance is expected to be the global Instance 0. A global RPLInstanceID is encoded in a RPLInstanceID field as follows:

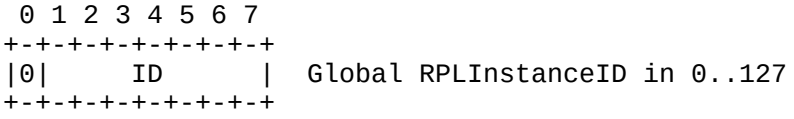


Figure 7: RPLInstanceID Field Format for Global Instances

For the particular case of the global Instance 0, the RPLInstanceID field is all zeros. This specification allows to elide a RPLInstanceID field that is all zeros, and defines a I flag that, when set, signals that the field is elided.

7.2. Compressing the SenderRank

The SenderRank is the result of the DAGRank operation on the rank of the sender; here the DAGRank operation is defined in [RFC6550], Section 3.5.1, as:

DAGRank(rank) = floor(rank/MinHopRankIncrease)

If MinHopRankIncrease is set to a multiple of 256, the least significant 8 bits of the SenderRank will be all zeroes; by eliding those, the SenderRank can be compressed into a single byte. This idea is used in [RFC6550] by defining DEFAULT_MIN_HOP_RANK_INCREASE as 256 and in [RFC6552] that defaults MinHopRankIncrease to DEFAULT_MIN_HOP_RANK_INCREASE.

This specification allows to encode the SenderRank as either one or two bytes, and defines a K flag that, when set, signals that a single byte is used.

7.3. The Overall RPI-6LoRH encoding

The RPI-6LoRH provides a compressed form for the RPL RPI. Routers that need to forward a packet with a RPI-6LoRH are expected to be RPL routers and expected to support this specification. If a non-RPL router receives a packet with a RPI-6LoRH, this means that there was a routing error and the packet should be dropped so the Type cannot be ignored.

Since the I flag is not set, the TSE field does not need to be a length expressed in bytes. The field is fully reused for control bits so as to encode the O, R and F flags from the RPI, and the I and K flags that indicate the compression that is taking place.

The Type for the RPI-6LoRH is 5.

The RPI-6LoRH is immediately followed by the RPLInstanceID field, unless that field is fully elided, and then the SenderRank, which is either compressed into one byte or fully in-lined as the whole 2 bytes. The I and K flags in the RPI-6LoRH indicate whether the RPLInstanceID is elided and/or the SenderRank is compressed and depending on these bits, the Length of the RPI-6LoRH may vary as described hereafter.

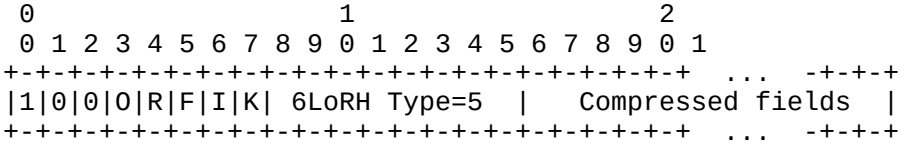


Figure 8: The Generic RPI-6LoRH Format

O, R, and F bits:
The O, R, and F bits as defined in [RFC6550], Section 11.2.

I bit:
If it is set, the Instance ID is elided and the RPLInstanceID is the Global RPLInstanceID 0. If it is not set, the octet immediately following the type field contains the RPLInstanceID as specified in [RFC6550] section 5.1.

K bit:

If it is set, the SenderRank is be compressed into one octet, and the lowest significant octet is elided. If it is not set, the SenderRank, is fully inlined as 2 octets.

In Figure 9, the RPLInstanceID is the Global RPLInstanceID 0, and the MinHopRankIncrease is a multiple of 256 so the least significant byte is all zeros and can be elided:

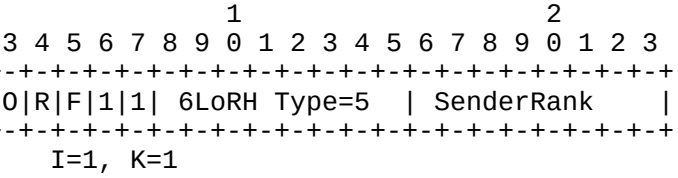


Figure 9: The most compressed RPI-6LoRH

In Figure 10, the RPLInstanceID is the Global RPLInstanceID 0, but both bytes of the SenderRank are significant so it can not be compressed:

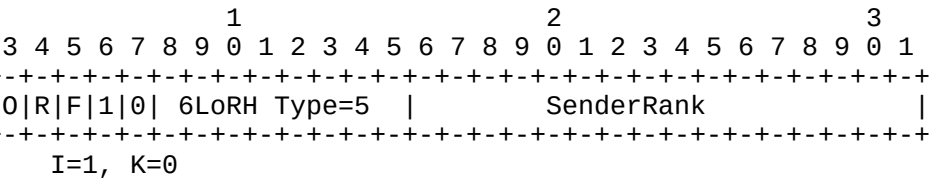


Figure 10: Eliding the RPLInstanceID

In Figure 11, the RPLInstanceID is not the Global RPLInstanceID 0, and the MinHopRankIncrease is a multiple of 256:

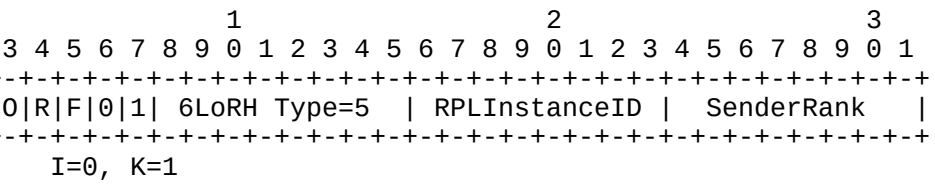


Figure 11: Compressing SenderRank

In Figure 12, the RPLInstanceID is not the Global RPLInstanceID 0, and both bytes of the SenderRank are significant:

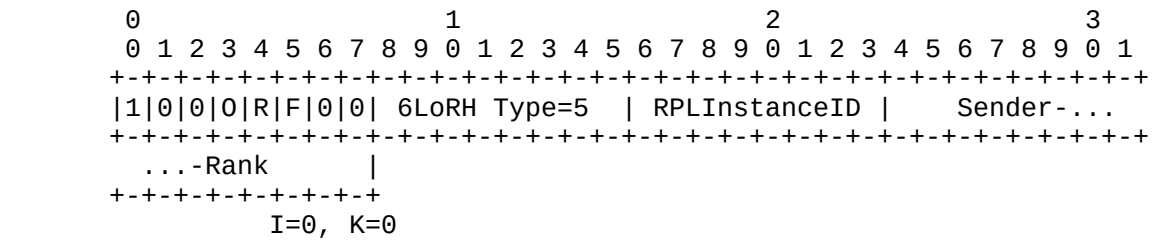


Figure 12: Least compressed form of RPI-6LoRH

A typical packet in RPL non-storing mode going down the RPL graph requires an IPinIP encapsulating the RH3, whereas the RPI is usually omitted, unless it is important to indicate the RPLInstanceID. To match this structure, an optimized IPinIP 6LoRH is defined in Section 8.

And the types include the setting of I and K as follows:

Type	I	K
5	0	0
6	0	1
7	1	0
8	1	1

Figure 13: The RPI-6LoRH Types

8. The IP-in-IP 6LoRH

The IP-in-IP 6LoRH (IPinIP-6LoRH) is an Elective 6LoWPAN Routing Header that provides a compressed form for the encapsulating IPv6 Header in the case of an IP-in-IP encapsulation.

An IPinIP encapsulation is used to insert a field such as a Routing Header or an RPI at a router that is not the source of the packet. In order to send an error back regarding the inserted field, the address of the router that performs the insertion must be provided.

The encapsulation can also enable a router down the path removing a field such as the RPI, but this can be done in the compressed form by removing the RPI-6LoRH, so an IPinIP-6LoRH encapsulation is not required for that sole purpose.

This field is not critical for routing so the Type can be ignored, and the TSE field contains the Length in bytes.

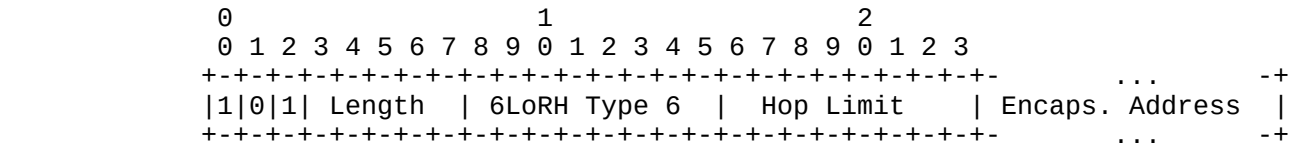


Figure 14: The IPinIP-6LoRH

The Length of an IPinIP-6LoRH is expressed in bytes and MUST be at least 1, to indicate a Hop Limit (HL), that is decremented at each hop. When the HL reaches 0, the packet is dropped per [RFC2460]

If the Length of an IPinIP-6LoRH is exactly 1, then the Encapsulator Address is elided, which means that the Encapsulator is a well-known router, for instance the root in a RPL graph.

If the Length of an IPinIP-6LoRH is strictly more than 1, then an Encapsulator Address is placed in a compressed form after the Hop Limit field. The value of the Length indicates which compression is performed on the Encapsulator Address. For instance, a Size of 3 indicates that the Encapsulator Address is compressed to 2 bytes.

When it cannot be elided, the destination IP address of the IP-in-IP header is transported in a RH3-6LoRH as the first address of the list.

With RPL, the destination address in the IP-in-IP header is implicitly the root in the RPL graph for packets going upwards, and the destination address in the IPHC for packets going downwards. If the implicit value is correct, the destination IP address of the IP-in-IP encapsulation can be elided.

If the final destination of the packet is a leaf that does not support this specification, then the chain of 6LoRH must be stripped by the RPL/6LR router to which the leaf is attached. In that example, the destination IP address of the IP-in-IP header cannot be elided.

In the special case where the 6LoRH is used to route 6LoWPAN fragments, the destination address is not accessible in the IPHC on all fragments and can be elided only for the first fragment and for packets going upwards.

9. The BIER 6LoRH

(Note that the current contents of this section is a proof of concept only; the details for this encoding need to be developed in parallel with defining the semantics of a constrained version of BIER.)

The Bit Index Explicit Replication (BIER) 6LoRH (BIER-6LoRH) is an Elective 6LoWPAN Routing Header that provides a variable-size container for a BIER Bitmap. BIER can be used to route downwards a RPL graph towards one or more LLN node, as discussed in the BIER Architecture [I-D.wijnands-bier-architecture] specification. The capability to parse the BIER Bitmap is necessary to forward the packet so the Type cannot be ignored.

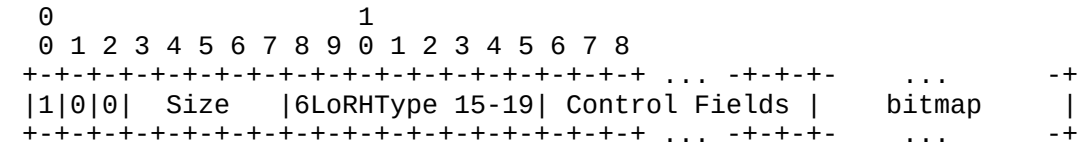


Figure 15: The BIER-6LoRH

The Type for a BIER-6LoRH indicates the size of words used to build the bitmap and whether the bitmap is operated as an uncompressed bit-by-bit mapping, or as a Bloom filter.

In the bit-by-bit case, each bit is mapped in an unequivocal fashion with a single addressable resource in the network. This may rapidly lead to large bitmaps, and BIER allows to divide a network into groups that partition the network so that a given bitmap is locally significant to one group only. This specification allows to encode a 1-byte Group ID in the BIER-6LoRH Control Fields.

A Bloom Filter can be seen as a compression technique for the bitmap. A Bloom Filter may generate false positives, which, in the case of BIER, result in undue forwarding of a packet down a path where no listener exists.

As an example, the Constrained-Cast [I-D.bergmann-bier-ccast] specification employs Bloom Filters as a compact representation of a match or non-match for elements in a large set.

In the case of a Bloom Filter, a number of Hash functions must be run to obtain a multi-bit signature of an encoded element. This specification allows to signal an Identifier of the Hash functions being used to generate a certain bitmap, so as to enable a migration scenario where Hash functions are renewed. A Hash ID is signaled as

a 1-byte value, and, depending on the Type, there may be up to 2 or up to 8 Hash IDs passed in the BIER-6LoRH Control Fields associated with a Bloom Filter bitmap, as follows:

Type	encoding	Control Fields	Word Size
15	bit-by-bit	none	32 bits
16	Bloom filter	2* 1-byte HashID	32 bits
17	bit-by-bit	none	128 bits
18	Bloom filter	8* 1-byte HashID	128 bits
19	bit-by-bit	1-byte GroupID	128 bits

Figure 16: The BIER-6LoRH Types

In order to address a potentially large number of devices, the bitmap may grow very large. Yet, the maximum frame size for a given MAC layer may limit the number of bits that can be dedicated to routing. The Size indicates the number of words in the bitmap minus one, so a size of 0 means one word, a Size of 1 means 64 2 words, up to a size of 31 which means 32 words.

10. Security Considerations

The security considerations of [RFC4944], [RFC6282], and [RFC6553] apply.

Using a compressed format as opposed to the full in-line format is logically equivalent and does not create an opening for a new threat when compared to [RFC6550], [RFC6553] and [RFC6554].

11. IANA Considerations

This document creates a IANA registry for the 6LoWPAN Routing Header Type, and assigns the following values:

0..4 : RH3-6LoRH [RFCthis]

5 : RPI-6LoRH [RFCthis]

6 : IPinIP-6LoRH [RFCthis]

15..19 : BIER-6LoRH [RFCthis]

12. Acknowledgments

The authors wish to thank Martin Turon, James Woodyatt, Samita Chakrabarti, Jonathan Hui, Gabriel Montenegro and Ralph Droms for constructive reviews to the design in the 6lo Working Group. The overall discussion involved participants to the 6MAN, 6TiSCH and ROLL WGs, thank you all. Special thanks to the chairs of the ROLL WG, Michael Richardson and Ines Robles, and Brian Haberman, Internet Area A-D, and Adrian Farrel, Routing Area A-D, for driving this complex effort across Working Groups and Areas.

13. References

13.1. Normative References

[IEEE802154] IEEE standard for Information Technology, "IEEE std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks", 2015.

[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>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[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>.

[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>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., 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, DOI 10.17487/RFC6550, March 2012, <http://www.rfc-editor.org/info/rfc6550>.

[RFC6552] Thubert, P., Ed., "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6552, DOI 10.17487/RFC6552, March 2012, <http://www.rfc-editor.org/info/rfc6552>.

[RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, DOI 10.17487/RFC6553, March 2012, <http://www.rfc-editor.org/info/rfc6553>.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, DOI 10.17487/RFC6554, March 2012, <http://www.rfc-editor.org/info/rfc6554>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <http://www.rfc-editor.org/info/rfc7102>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <http://www.rfc-editor.org/info/rfc7228>.

13.2. Informative References

[I-D.bergmann-bier-ccast]
Bergmann, O., Bormann, C., and S. Gerdes, "Constrained-Cast: Source-Routed Multicast for RPL", draft-bergmann-bier-ccast-00 (work in progress), November 2014.

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-08 (work in progress), May 2015.

[I-D.ietf-6tisch-tsch]
Watteyne, T., Palattella, M., and L. Grieco, "Using IEEE802.15.4e TSCH in an IoT context: Overview, Problem Statement and Goals", draft-ietf-6tisch-tsch-06 (work in progress), March 2015.

[I-D.thubert-6lo-forwarding-fragments]
Thubert, P. and J. Hui, "LLN Fragment Forwarding and Recovery", draft-thubert-6lo-forwarding-fragments-02 (work in progress), November 2014.

[I-D.wijnands-bier-architecture]
Wijnands, I., Rosen, E., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast using Bit Index Explicit Replication", draft-wijnands-bier-architecture-05 (work in progress), March 2015.

[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>.

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems
Village d'Entreprises Green Side
400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Phone: +33 4 97 23 26 34
Email: pthubert@cisco.com

Carsten Bormann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.org

Laurent Toutain
Institut MINES TELECOM; TELECOM Bretagne
2 rue de la Chataigneraie
CS 17607
Cesson-Sevigne Cedex 35576
France

Email: Laurent.Toutain@telecom-bretagne.eu

Robert Cragie
ARM Ltd.
110 Fulbourn Road
Cambridge CB1 9NJ
UK

Email: robert.cragie@gridmerge.com