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

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.

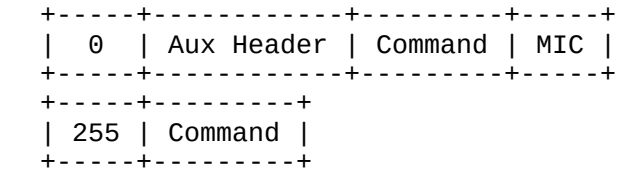
4.3. Link Quality Determination

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.

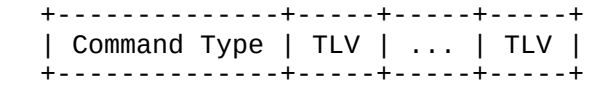
MIC Message Integrity Code as described in [IEEE802154].

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:

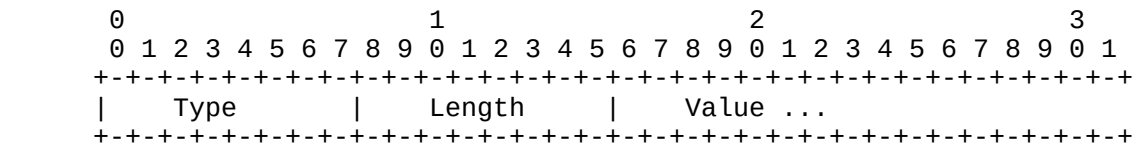
- 0 Link Request. A request to establish a link to a neighbor.
- 1 Link Accept. Accept a requested link.
- 2 Link Accept and Request. Accept a requested link and request a link with the sender of the original request.
- 3 Link Reject. Reject a link request.
- 4 Advertisement. Inform neighbors of a device’s 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

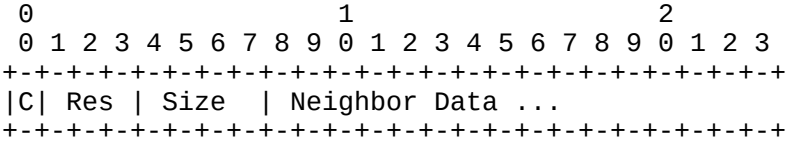
The Response TLV (TLV Type 4) has a Value containing a byte string copied from a Challenge TLV.

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:

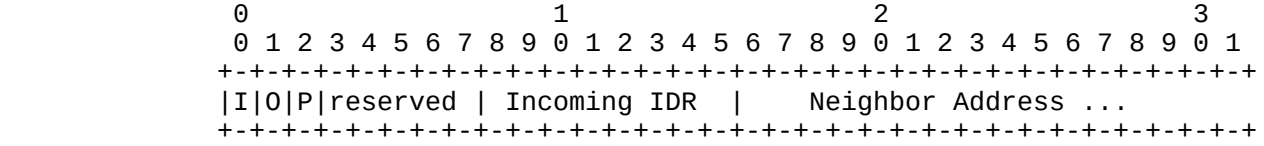


C — Complete: "1" if the message includes all neighboring routers for which the source has link quality data. Multicast Link Quality TLVs normally contain complete information; a unicast to a particular neighbor would normally contain only that neighbor’s link quality and would have the C flag set to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

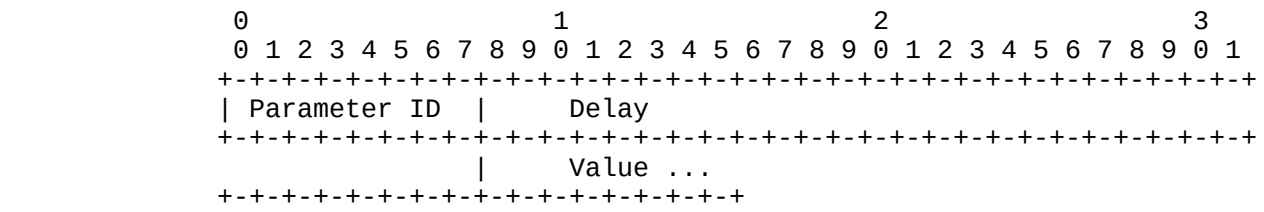
The I and O flags are used to facilitate the two-way use of links between neighboring routers.

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