IEEE P802.15

Wireless Personal Area Networks

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Privacy MLME primitives | |
| Date Submitted | 16th May 2024 | |
| Source | Tero Kivinen | E-mail: kivinen@iki.fi |
| Re: | TG4ac draft | |
| Abstract | MLME primitives needed to provide privacy on 802.15.4 | |
| Purpose | Create TG4ac draft | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend, or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

1. MLME primitives
   1. MLME-PRIV-ADDR-LIST (Address List MAC Command frame)
      1. Sending address list with confirmation
      2. MLME-PRIV-ADDR-LIST.request (Address List MAC Command frame)

This primitive is used by the device to send Address List MAC Command frame.

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-LIST.request (  
 SrcAddrMode,  
 DstAddrMode,  
 DstPanId,  
 DstAddr,  
 SecurityParams,  
 IncludeSenderId,  
 SenderId,  
 IncludeAddressListSequenceNumber,  
 AddressListSequenceNumber,  
 IncludeNewPanId,  
 NewPanId,  
 IncludeShortAddresses,  
 ListOfShortAddresses,  
 IncludeExtendedAddresses,  
 ListOfExtendedAddresses,   
 ConfirmationRequested  
 )

The primitive parameters are defined in Table 1-1.

Table 1-1‒MLME-PRIV-ADDR-LIST.request parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SrcAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The source addressing mode. |
| DstAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The destination addressing mode. |
| DstPanId | Integer | 0x0000-0xffff | The destination PAN ID of the frame. |
| DstAddr | — | As specified by the DstAddrMode parameter | Destination address of the frame. |
| SecurityParams | Structure | As defined in Table 8-29 | As defined in Table 8-29. |
| IncludeSenderId | Boolean | TRUE, FALSE | Specifies whether the SenderId is included to the frame or not. |
| SenderId | 64-bit Id | An Id | Id of the sender. Ignored if the IncludeSenderId is FALSE. |
| IncludeAddressListSequenceNumber | Boolean | TRUE, FALSE | Specifies whether the sequence number of the address list is included in the frame. |
| AddressListSequenceNumber | Integer | 0x00-0xff | Sequence number of the address list. Ignored if the IncludeAddressListSequenceNumber is FALSE. |
| IncludeNewPanId | Boolean | TRUE, FALSE | Specifies whether the NewPanId is included in the frame. |
| NewPanId | Integer | 0x0000-0xffff | The PAN ID associated to the new short addresses. Ignored if the IncludeNewPanId is FALSE. |
| IncludeShortAddresses | Boolean | TRUE, FALSE | Specifies whether the short addresses are included in the frame. If FALSE then the no short address list is included in the frame. |
| ListOfShortAddresses | List of short addresses | — | List of short addresses to be transmitted. Ignored if IncludeShortAddresses is FALSE. |
| IncludeExtendedAddresses | Boolean | TRUE, FALSE | Specifies whether the extended addresses are included in the frame. |
| ListOfExtendedAddresses | List of extended addresses | — | List of extended addresses to be transmitted. Ignored if IncludeExtendedAddresses is FALSE. |
| ConfirmationRequested | Boolean | TRUE, FALSE | Specifies whether the confirmation from the is requested. |

When MLME-PRIV-ADDR-LIST.request primitive is issued the MAC will send Address List MAC Command frame to the destination.

If the IncludeSenderId parameter is TRUE, then Address List MAC Command frame shall include Sender id field indicating the actual sender of the frame. Omitting Sender id field is useful when it is assumed that recipients already know it from the source addresses. If SrcAddrMode is NONE, and the IncludeSenderId is FALSE, then MAC shall fail the transmission with Status set to INVALID\_PARAMETER.

NOTE—Including SenderId is often needed when DstAddr is broadcast address, as sender does not know which of the recipients are up to date with its source addresses.

If the IncludeAddressListSequenceNumber is FALSE, then the Address list sequence number field is omitted from the frame.

If the IncludeNewPanId is FALSE, then PAN ID of the Address List Mac Command shall be omitted, and PAN ID from the MAC header is used.

If the IncludeShortAddresses list is FALSE, then the short address list is not present in the frame, meaning there is no changes in the the short addresses of the sender.

If the IncludeExtendedAddresses is FALSE, then the extended address list is not present in the frame, meaning there is no changes in the list of extended address of the sender.

Using IncludeShortAddresses and IncludeExtendedAddresses allows device to update its lists of addresses separately.

If the ListOfShortAddresses is empty then device does not use short addresses.

If the ListOfExtendedAddresses is empty then the device does not use extended addresses.

* + 1. MLME-PRIV-ADDR-LIST.indication (Address List MAC Command)

This primitive reports the reception of the Address List MAC Command.

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-LIST.indication (  
 SrcAddrMode,  
 SrcAddr,  
 DstAddrMode,  
 DstPanId,  
 DstAddr,  
 SecurityParams,  
 SenderIdPresent,  
 SenderId,  
 AddressListSequenceNumberPresent,  
 AddressListSequenceNumber,  
 NewPanIdPresent,  
 NewPanId,  
 ShortAddressesPresent,  
 ListOfShortAddresses,  
 ExtendedAddressesPresent,  
 ListOfExtendedAddresses,   
 ConfirmationRequested  
 )

The primitive parameters are defined in Table 1-2.

Table 1-2‒MLME-PRIV-ADDR-LIST.indication parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SrcAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The source addressing mode. |
| SrcAddr | — | As specified by the SrcAddrMode parameter | The source address. |
| DstAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The destination addressing mode. |
| DstPanId | Integer | 0x0000-0xffff | The PAN ID. |
| DstAddr | — | As specified by the DstAddrMode parameter | The destination address. |
| SecurityParams | Structure | As defined in Table 8-29 | As defined in Table 8-29. |
| SenderIdPresent | Boolean | TRUE, FALSE | Specifies whether the SenderId is included to the frame or not. |
| SenderId | 64-bit Id | An Id | Id of the sender. Valid only of SenderIdPresent is TRUE. |
| AddressListSequenceNumberPresent | Boolean | TRUE, FALSE | Specifies whether the sequence number of the address list is included in the frame. |
| AddressListSequenceNumber | Integer | 0x00-0xff | Sequence number of the address list. Valid only of the AddressListSequenceNumberPresent is TRUE. |
| NewPanIdPresent | Boolean | TRUE, FALSE | Specifies whether the NewPanId is included in the frame. |
| NewPanId | Integer | 0x0000-0xffff | The PAN ID associated to the new short addresses. Valid only if the NewPanIdPresent is TRUE. |
| ShortAddressesPresent | Boolean | TRUE, FALSE | Specifies whether the short addresses are included in the frame. |
| ListOfShortAddresses | List of short addresses | — | List of short addresses to be transmitted. Valid only if the ShortAddressesPresent is TRUE. |
| ExtendedAddressesPresent | Boolean | TRUE, FALSE | Specifies whether the extended addresses are included in the frame. |
| ListOfExtendedAddresses | List of extended addresses | — | List of extended addresses to be transmitted. Valid only if the ExtendedAddressesPresent is TRUE. |
| ConfirmationRequested | Boolean | TRUE, FALSE | Specifies whether the confirmation from the is requested. |

The MLME-PRIV-ADDR-LIST.indication primitive is issued from the MAC when the Address List MAC Command is received.

If the ConfirmationRequested is TRUE, then MLME-PRIV-ADDR-LIST.response is used to send Address List Confirm MAC Command frame back.

* + 1. MLME-PRIV-ADDR-LIST.response (Address List MAC Command)

This primitive responds to the Address List MAC Command frame by sending Address List Confirm MAC Command frame.

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-LIST.response (  
 SrcAddrMode,  
 SrcAddr,  
 DstAddrMode,  
 DstPanId,  
 DstAddr,  
 SecurityParams,  
 ErrorCode,  
 IncludeAddressListSequenceNumber,  
 AddressListSequenceNumber  
 )

The primitive parameters are defined in Table 1-3.

Table 1-3‒MLME-PRIV-ADDR-LIST.response parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SrcAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The source addressing mode. |
| SrcAddr | — | As specified by the SrcAddrMode parameter | The source address |
| DstAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The destination addressing. |
| DstPanId | Integer | 0x0000-0xffff | The PAN ID. |
| DstAddr | — | As specified by the DstAddrMode parameter | The destination address. |
| SecurityParams | Structure | As defined in Table 8-29 | As defined in Table 8-29. |
| ErrorCode | Integer | 0x00-0xff | Error code to send to the other end. If zero then no Error Code field should not be included in the frame. |
| IncludeAddressListSequenceNumber | Boolean | TRUE, FALSE | Specifies whether the sequence number of the address list is included in the frame. |
| AddressListSequenceNumber | Integer | 0x00-0xff | Sequence number of the address list. Valid only of the IncludeAddressListSequenceNumber is TRUE. |

When MLME-PRIV-ADDR-LIST.response primitive is issued then the MAC shall transmit the Address List Confirm MAC Command back to the sender of Address List MAC Command frame.

* + 1. MLME-PRIV-ADDR-LIST.confirm (Address List MAC Command)

This primitive reports the results of the MLME-PRIV-ADDR-LIST.request transmission.

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-LIST.request (  
 SrcAddrMode,  
 DstAddrMode,  
 DstPanId,  
 DstAddr,  
 Status  
 )

The primitive parameters are defined in Table 1-4.

Table 1-4‒MLME-PRIV-ADDR-LIST.confirm parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SrcAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The source addressing mode. |
| DstAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The destination addressing mode. |
| DstPanId | Integer | 0x0000-0xffff | The PAN ID. |
| DstAddr | — | As specified by the DstAddrMode parameter | Destination address. |
| Status | Enumeration | SUCCESS. Also see 8.2.2 | The status of the request. |

The MLME-PRIV-ADDR-LIST.confirm primitive is issued the MAC has sent out the Address List MAC command frame to the destination.

* 1. MLME-PRIV-ADDR-LIST-CONFIRM (Address List Confirm MAC Command frame)
     1. MLME-PRIV-ADDR-LIST-CONFIRM.indication (Address List Confirm MAC Command frame)

This primitive reports the reception of the Address List Confirm MAC Command.

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-LIST-CONFIRM.indication (  
 SrcAddrMode,  
 SrcAddr,  
 DstAddrMode,  
 DstPanId,  
 DstAddr,  
 SecurityParams,  
 ErrorCode,  
 AddressListSequenceNumberPresent,  
 AddressListSequenceNumber,  
 )

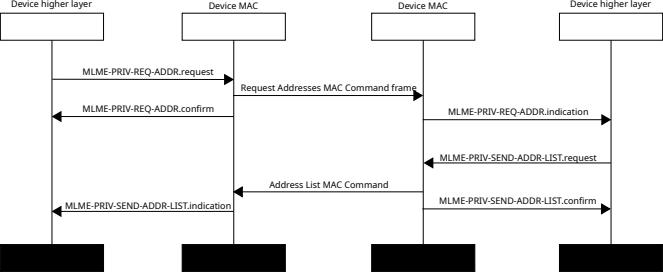
The primitive parameters are defined in Table 1-5.

Table 1-5‒MLME-PRIV-ADDR-LIST-CONFIRM.indication parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SrcAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The source addressing mode. |
| SrcAddr | — | As specified by the SrcAddrMode parameter | The source address. |
| DstAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The destination addressing mode. |
| DstPanId | Integer | 0x0000-0xffff | The PAN ID. |
| DstAddr | — | As specified by the DstAddrMode parameter | The destination address. |
| SecurityParams | Structure | As defined in Table 8-29 | As defined in Table 8-29. |
| ErrorCode | Integer | 0x00-0xff | Error Code field received from the other end. If the Error Code field was not present then ErrorCode shall be set to zero to indicate success. |
| AddressListSequenceNumberPresent | Boolean | TRUE, FALSE | Specifies whether the sequence number of the address list is included in the frame. |
| AddressListSequenceNumber | Integer | 0x00-0xff | Sequence number of the address list. Valid only of the AddressListSequenceNumberPresent is TRUE. |

The MLME-PRIV-ADDR-LIST-CONFIRM.indication primitive is issued from the MAC when the Address List Confirm MAC Command is received.

* 1. MLME-PRIV-REQ-ADDR (Request Addresses MAC Command frame)
     1. Requesting address list

Figure 1—Requesting address list from the device

* + 1. MLME-PRIV-REQ-ADDR.request (Request Addresses MAC Command frame)

This primitive is used by the device to send Request Addresses MAC Command frame.

The semantics of this primitive are as follows:

MLME-PRIV-REQ-ADDR.request (  
 SrcAddrMode,  
 DstAddrMode,  
 DstPanId,  
 DstAddr,  
 SecurityParams,  
 IncludeSenderId,  
 SenderId,  
 IncludeRecipientId,  
 RecipientId,  
 IncludeAddressListSequenceNumber,  
 AddressListSequenceNumber,  
 )

The primitive parameters are defined in Table 1-1.

Table 1-1‒MLME-PRIV-REQ-ADDR.request parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SrcAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The source addressing mode. |
| DstAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The destination addressing mode. |
| DstPanId | Integer | 0x0000-0xffff | The destination PAN ID of the frame. |
| DstAddr | — | As specified by the DstAddrMode parameter | Destination address of the frame. |
| SecurityParams | Structure | As defined in Table 8-29 | As defined in Table 8-29. |
| IncludeSenderId | Boolean | TRUE, FALSE | Specifies whether the SenderId is included to the frame or not. |
| SenderId | 64-bit Id | An Id | Id of the sender. Ignored if the IncludeSenderId is FALSE. |
| IncludeRecipientId | Boolean | TRUE, FALSE | Specifies whether the RecipientId is included to the frame or not. |
| RecipientId | 64-bit Id | An Id | Id of the recipient. Ignored if the IncludeRecipientId is FALSE. |
| IncludeAddressListSequenceNumber | Boolean | TRUE, FALSE | Specifies whether the sequence number of the address list is included in the frame. |
| AddressListSequenceNumber | Integer | 0x00-0xff | Sequence number of the address list. Ignored if the IncludeAddressListSequenceNumber is FALSE. |

When MLME-PRIV-REQ-ADDR.request primitive is issued the MAC will send Request Addresses MAC Command frame to the destination.

If the IncludeSenderId parameter is TRUE, then Request Addresses MAC Command frame shall include Sender id field indicating the actual sender of the frame.

If the IncludeRecipientId parameter is TRUE, then Request Addresses MAC Command frame shall include Recipient id field indicating the intended recipient of the frame.

If the IncludeAddressListSequenceNumber is FALSE, then the Address list sequence number field is omitted from the frame.

* + 1. MLME-PRIV-REQ-ADDR.indication (Request Addresses MAC Command frame)

This primitive is used by the MAC when it receives Request Addresses MAC Command frame.

The semantics of this primitive are as follows:

MLME-PRIV-REQ-ADDR.indication (  
 SrcAddrMode,

SrcAddr,  
 DstAddrMode,  
 DstPanId,  
 DstAddr,  
 SecurityParams,  
 SenderIdPresent,  
 SenderId,  
 RecipientIdPresent,  
 RecipientId,  
 AddressListSequenceNumberPresent,  
 AddressListSequenceNumber,  
 )

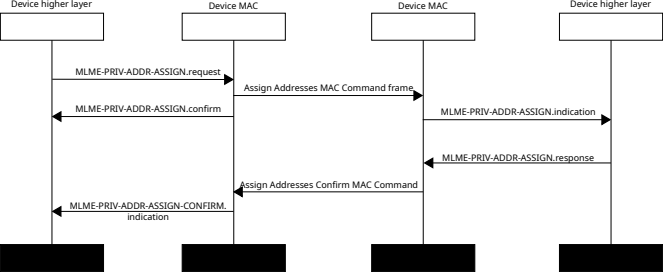
The primitive parameters are defined in Table 1-1.

Table 1-1‒MLME-PRIV-REQ-ADDR.indication parameters

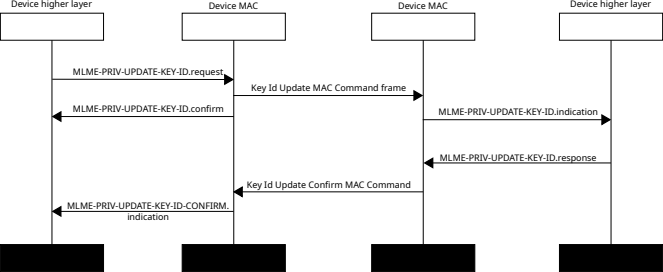
| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SrcAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The source addressing mode. |
| SrcAddr | — | As specified by the SrcAddrMode parameter | The source address of the frame. |
| DstAddrMode | Enumeration | NONE, SHORT,  EXTENDED | The destination addressing mode. |
| DstPanId | Integer | 0x0000-0xffff | The destination PAN ID of the frame. |
| DstAddr | — | As specified by the DstAddrMode parameter | Destination address of the frame. |
| SecurityParams | Structure | As defined in Table 8-29 | As defined in Table 8-29. |
| SenderIdPresent | Boolean | TRUE, FALSE | Specifies whether the SenderId is included to the frame or not. |
| SenderId | 64-bit Id | An Id | Id of the sender. Valid only of SenderIdPresent is TRUE. |
| RecipientIdPresent | Boolean | TRUE, FALSE | Specifies whether the RecipientId is included to the frame or not. |
| RecipientId | 64-bit Id | An Id | Id of the recipient. Valid only of RecipientIdPresent is TRUE. |
| AddressListSequenceNumberPresent | Boolean | TRUE, FALSE | Specifies whether the sequence number of the address list is included in the frame. |
| AddressListSequenceNumber | Integer | 0x00-0xff | Sequence number of the address list. Valid only of the AddressListSequenceNumberPresent is TRUE. |

MLME-PRIV-REQ-ADDR.indication primitive is issued by the MAC when it receives Request Addresses MAC Command frame.

* + 1. MLME-PRIV-REQ-ADDR.confirm (Request Addresses MAC Command frame)
  1. MLME-PRIV-ADDR-ASSIGN (Assign Addresses MAC Command frame)
     1. Assign addresses with confirmation

Figure 2—Assigning addresses with confirmation

* + 1. MLME-PRIV-ADDR-ASSIGN.request (Assign Addresses MAC Command frame)
    2. MLME-PRIV-ADDR-ASSIGN.indication (Assign Addresses MAC Command frame)
    3. MLME-PRIV-ADDR-ASSIGN.response (Assign Addresses MAC Command frame)
    4. MLME-PRIV-ADDR-ASSIGN.confirm (Assign Addresses MAC Command frame)
  1. MLME-PRIV-ADDR-ASSIGN-CONFIRM (Assign Addresses Confirm MAC Command frame)
     1. MLME-PRIV-ADDR-ASSIGN-CONFIRM.indication (Assign Addresses Confirm MAC Command frame)
  2. MLME-PRIV-UPDATE-KEY-ID (Key Id Update MAC Command frame)
     1. Updating key source with confirmation

Figure 3—Updating the key source with confirmation

* + 1. MLME-PRIV-UPDATE-KEY-ID.request (Key Id Update MAC Command frame)
    2. MLME-PRIV-UPDATE-KEY-ID.indication (Key Id Update MAC Command frame)
    3. MLME-PRIV-UPDATE-KEY-ID.response (Key Id Update MAC Command frame)
    4. MLME-PRIV-UPDATE-KEY-ID.confirm (Key Id Update MAC Command frame)
  1. MLME-PRIV-UPDATE-KEY-ID-CONFIRM (Key Id Update Confirm MAC Command frame)
     1. MLME-PRIV-UPDATE-KEY-ID-CONFIRM.indication (Key Id Update Confirm MAC Command frame)
  2. MLME-PRIV-NET-VERIFIER (Net Announcement IE and Net Request IE Encrypted Verifier)
     1. MLME-PRIV-NET-VERIFIER.request (Net Announcement IE and Net Request IE Encrypted Verifier)
     2. MLME-PRIV-NET-VERIFIER.confirm (Net Announcement IE and Net Request IE Encrypted Verifier)