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
		1. MLME-PRIV-ADDR-LIST.request

This primitive is used by the device to send Address List command.

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.

Table 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 | IEEE address | An extended IEEE address | DI 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 command to the destination.

IncludeSenderId, IncludeAddressListSequenceNumber, IncludeNewPanId, IncludeShortAddresses and IncludeExtendedAddresses parameters specify whether Sender ID field, Address List Sequence Number field, PAN ID field, List of Short Address field and List of Extended Addresses field are included in the Address List command. If present those fields shall be filled with values from the SenderId, AddressListSequenceNumber, NewPanId, ListOfShortAddresses and ListOfExtendedAddresses parameters respectively.

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 multicast or broadcast address, as sender does not know which of the recipients are up to date with its source addresses.

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

If the number of items in ListOfShortAddresses list is zero, then this indicates that device does not use short addresses.

If the number of items in ListOfExtendedAddresses list is zero, then this indicates that the device does not use privacy addresses anymore.

* + 1. MLME-PRIV-ADDR-LIST.indication

This primitive reports the reception of the Address List 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 2

Table 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 | IEEE address | An extended IEEE address | DI 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 command is received.

Parameters contain the values copied directly from the fields from the frame.

If the ConfirmationRequested is TRUE, then MLME-PRIV-ADDR-LIST.response may be used to send Address List Confirm command back.

* + 1. MLME-PRIV-ADDR-LIST.response

This primitive responds to the Address List command by sending Address List Confirm command.

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 3.

Table 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 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 command back to the sender of Address List command.

If IncludeAddressListSequenceNumber is TRUE then Address List Sequence Number Present field of Address List Confirm command is set to one.

If the ErrorCode parameter is zero, then Error Code Present field of the Address List Confirm command shall be set to zero, and no Error Code field is included in the frame.

If present the Error Code field, and the Address List Sequence Number field of the Address List Confirm command are filled with the values of ErrorCode and AddressListSequenceNumber parameters.

* + 1. MLME-PRIV-ADDR-LIST.confirm

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.confirm (
 SrcAddrMode,
 DstAddrMode,
 DstPanId,
 DstAddr,
 Status
 )

The primitive parameters are defined in Table 4.

Table 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 command to the destination.

* 1. MLME-PRIV-ADDR-LIST-CONFIRM
		1. MLME-PRIV-ADDR-LIST-CONFIRM.indication

This primitive reports the reception of the Address List Confirm 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 5.

Table 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 command is received.

ErrorCode, AddressListSequenceNumberPresent and AddressListSequenceNumber parameters contain the values copied directly from the fields from the frame.

* 1. MLME-PRIV-REQ-ADDR
		1. MLME-PRIV-REQ-ADDR.request

This primitive is used by the device to send Request Addresses command.

The semantics of this primitive are as follows:

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

The primitive parameters are defined in Table 6.

Table 6—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 | IEEE address | An extended IEEE address | DI 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 | IEEE address | An extended IEEE address | DI of the recipient. Ignored if the IncludeRecipientId is FALSE. |

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

IncludeSenderId, and IncludeRecipientId parameters specify whether Sender ID field, Recipient ID field are included in the Request Addresses command. If present those fields shall be filled with values from the SenderId, and RecipientId parameters respectively.

* + 1. MLME-PRIV-REQ-ADDR.indication

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

The semantics of this primitive are as follows:

MLME-PRIV-REQ-ADDR.indication (
 SrcAddrMode,
 SrcAddr,
 DstAddrMode,
 DstPanId,
 DstAddr,
 SecurityParams,
 SenderIdPresent,
 SenderId,
 RecipientIdPresent,
 RecipientId
 )

The primitive parameters are defined in Table 7.

Table 7—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 | IEEE address | An extended IEEE address | DI 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 | IEEE address | An extended IEEE address | DI of the recipient. Valid only of RecipientIdPresent is TRUE. |

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

Parameters contain the values copied directly from the fields from the frame.

* + 1. MLME-PRIV-REQ-ADDR.confirm

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

The semantics of this primitive are as follows:

MLME-PRIV-REQ-ADDR.confirm (
 SrcAddrMode,
 DstAddrMode,
 DstPanId,
 DstAddr,
 Status
 )

The primitive parameters are defined in Table 8.

Table 8—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-REQ-ADDR.confirm primitive is issued the MAC has sent out the Request Addresses command to the destination.

* 1. MLME-PRIV-ADDR-ASSIGN
		1. MLME-PRIV-ADDR-ASSIGN.request

This primitive is used by the device to send Assign Addresses command.

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-ASSIGN.request (
 SrcAddrMode,
 DstAddrMode,
 DstPanId,
 DstAddr,
 SecurityParams,
 IncludeSenderId,
 SenderId,
 IncludeRecipientId,
 RecipientId,
 IncludeNewPanId,
 NewPanId,
 ListOfShortAddresses,
 ConfirmationRequested
 )

The primitive parameters are defined in Table 9.

Table 9—MLME-PRIV-ADDR-ASSIGN.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 | IEEE address | An extended IEEE address | DI of the sender. Ignored if the IncludeSenderId is FALSE. |
| IncludeRecipientId | Boolean | TRUE, FALSE | Specifies whether the RecipientId is included in the frame. |
| RecipientId | IEEE address | An extended IEEE address | DI of the recipient. Ignored if the IncludeRecipientId 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. |
| ListOfShortAddresses | List of short addresses | — | List of short addresses to be transmitted. Ignored if IncludeShortAddresses is FALSE. |
| ConfirmationRequested | Boolean | TRUE, FALSE | Specifies whether the confirmation from the is requested. |

When MLME-PRIV-ADDR-ASSIGN.request primitive is issued the MAC will send Assign Addresses command to the destination.

IncludeSenderId, IncludeRecipientId, and IncludeNewPanId parameters specify whether Sender ID field, Recipient ID field, and PAN ID field are included in the Assign Addresses command. If present those fields shall be filled with values from the SenderId, RecipientId, and NewPanId parameters respectively.

If SrcAddrMode is NONE, and the IncludeSenderId is FALSE, then MAC shall fail the transmission with Status set to INVALID\_PARAMETER.

If the number of items in ListOfShortAddresses list is zero, then this indicates that device shall not be assigned any short addresses.

XXX Short addresses are tied to the primary extended privacy address. We can either add primary extended privacy address to this MLME call and Assign Addresses command, or we might require that device shall only assign short addresses to someone who has already sent Address List command and included one primary extended privacy address.

* + 1. MLME-PRIV-ADDR-ASSIGN.indication

This primitive reports the reception of the Assign Addresses command.

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-ASSIGN.indication (
 SrcAddrMode,
 SrcAddr,
 DstAddrMode,
 DstPanId,
 DstAddr,
 SecurityParams,
 SenderIdPresent,
 SenderId,
 RecipientIdPresent,
 RecipientId,
 NewPanIdPresent,
 NewPanId,
 ListOfShortAddresses,
 ConfirmationRequested
 )

The primitive parameters are defined in Table 10.

Table 10—MLME-PRIV-ADDR-ASSIGN.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 | IEEE address | An extended IEEE address | DI 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 | IEEE address | An extended IEEE address | DI of the recipient. Valid only of RecipientIdPresent 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. |
| ListOfShortAddresses | List of short addresses | — | List of short addresses to be transmitted. Valid only if the ShortAddressesPresent is TRUE. |
| ConfirmationRequested | Boolean | TRUE, FALSE | Specifies whether the confirmation from the is requested. |

The MLME-PRIV-ADDR-ASSIGN.indication primitive is issued from the MAC when the Assign Addresses command is received.

Parameters contain the values copied directly from the fields from the frame.

If the ConfirmationRequested is TRUE, then MLME-PRIV-ADDR-ASSIGN.response may be used to send Assign Addresses Confirm command back.

* + 1. MLME-PRIV-ADDR-ASSIGN.response

This primitive responds to the Assign Addresses command by sending Assign Addresses Confirm command.

The semantics of this primitive are as follows:

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

The primitive parameters are defined in Table 11.

Table 11—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 Error Code field should not be included in the frame. |

When MLME-PRIV-ADDR-ASSIGN.response primitive is issued then the MAC shall transmit the Assign Addresses Confirm command back to the sender of Assign Addresses command.

If the ErrorCode parameter is zero, then Error Code Present field of the Assign Addresses Confirm command shall be set to zero, and no Error Code field is included in the frame. Otherwise the Error Code field is filled with the ErrorCode parameter value.

* + 1. MLME-PRIV-ADDR-ASSIGN.confirm

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

The semantics of this primitive are as follows:

MLME-PRIV-ADDR-ASSIGN.confirm (
 SrcAddrMode,
 DstAddrMode,
 DstPanId,
 DstAddr,
 Status
 )

The primitive parameters are defined in Table 12.

Table 12—MLME-PRIV-ADDR-ASSIGN.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-ASSIGN.confirm primitive is issued the MAC has sent out the Assign Addresses command to the destination.

* 1. MLME-PRIV-ADDR-ASSIGN-CONFIRM
		1. MLME-PRIV-ADDR-ASSIGN-CONFIRM.indication

This primitive reports the reception of the Assign Addresses Confirm command.

The semantics of this primitive are as follows:

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

The primitive parameters are defined in Table 13.

Table 13—MLME-PRIV-ADDR-ASSIGN-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. |

The MLME-PRIV-ADDR-ASSIGN-CONFIRM.indication primitive is issued from the MAC when the Assign Addresses Confirm command is received.

ErrorCode parameters contain the values copied directly from the fields from the frame.

* 1. MLME-PRIV-UPDATE-KEY-ID
		1. MLME-PRIV-UPDATE-KEY-ID.request

This primitive is used by the device to send Key Identifier Update command.

The semantics of this primitive are as follows:

MLME-PRIV-UPDATE-KEY-ID.request (
 SrcAddrMode,
 DstAddrMode,
 DstPanId,
 DstAddr,
 SecurityParams,
 IncludeSenderId,
 SenderId,
 KeyIdMode
 IncludeOldKeyIdentifier,
 OldKeySource
 OldKeyIndex,
 NewKeySource,
 NewKeyIndex,
 ConfirmationRequested
 )

The primitive parameters are defined in Table 14.

Table 14—MLME-PRIV-UPDATE-KEY-ID.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 | IEEE address | An extended IEEE address | DI of the sender. Ignored if the IncludeSenderId is FALSE. |
| KeyIdMode | Integer | 0x01-0x03 | The mode used to identify the key. Same mode is used for both old and new key ID. |
| IncludeOldKeyIdentifier | Boolean | TRUE, FALSE | Specifies whether the OldKeyIdentifier field is included in the frame.  |
| OldKeySource | Set of Octets | As specified by the KeyIdMode parameter | The originator of the key to be replaced, as described in 9.4.4.2. This parameter is ignored if KeyIdMode is set to 0x01. |
| OldKeyIndex | Integer | 0x01-0xff | The index of the key to be replaced, as described in 9.4.4.3. |
| NewKeySource | Set of Octets | As specified by the KeyIdMode parameter | The originator of the replacement key, as described in 9.4.4.2. This parameter is ignored if KeyIdMode is set to 0x01. |
| NewKeyIndex | Integer | 0x01-0xff | The index of the replacement key, as described in 9.4.4.3. |
| ConfirmationRequested | Boolean | TRUE, FALSE | Specifies whether the confirmation from the is requested. |

When MLME-PRIV-UPDATE-KEY-ID.request primitive is issued the MAC will send Key Identifier Update command to the destination.

IncludeSenderId, and IncludeOldKeyIdentifier parameters specify whether Sender ID field, and Old Key Identifier field are included in the Key Identifier Update command. If Sender ID field is present it shall be filled with value of the SenderId parameter.

If SrcAddrMode is NONE, and the IncludeSenderId is FALSE, then MAC shall fail the transmission with Status set to INVALID\_PARAMETER.

The length of the Old Key Identifier and New Key Identifier fields in the Key Identifier Update command depends on the KeyIdMode. If the IncludeOldKeyIdentifier is FALSE, then key ID to replaced is taken from the SecurityParams parameter.

The Old and New Key Identifier fields are generated from KeySource and KeyIndex parameters as specified in the 9.4.4.

NOTE—The KeyIdMode of 0x00 does not have any key identification except the source address of the frame, thus there is nothing to update there.

* + 1. MLME-PRIV-UPDATE-KEY-ID.indication

This primitive reports the reception of the Key Identifier Update command.

The semantics of this primitive are as follows:

MLME-PRIV-UPDATE-KEY-ID.indication (
 SrcAddrMode,
 SrcAddr,
 DstAddrMode,
 DstPanId,
 DstAddr,
 SecurityParams,
 SenderIdPresent,
 SenderId,
 KeyIdMode,
 OldKeyIdentifierPresent,
 OldKeySource
 OldKeyIndex,
 NewKeySource,
 NewKeyIndex,
 ConfirmationRequested
 )

The primitive parameters are defined in Table 15.

Table 15—MLME-PRIV-UPDATE-KEY-ID.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 | IEEE address | An extended IEEE address | DI of the sender. Valid only of SenderIdPresent is TRUE. |
| KeyIdMode | Integer | 0x01-0x03 | The mode used to identify the key. Same mode is used for both old and new key ID. |
| OldKeyIdentifierPresent | Boolean | TRUE, FALSE | Specifies whether the OldKeyIdentifier is included in the frame.  |
| OldKeySource | Set of Octets | As specified by the KeyIdMode parameter | The originator of the key to be replaced, as described in 9.4.4.2. This parameter is ignored if KeyIdMode is set to 0x01. |
| OldKeyIndex | Integer | 0x01-0xff | The index of the key to be replaced, as described in 9.4.4.3. |
| NewKeySource | Set of Octets | As specified by the KeyIdMode parameter | The originator of the replacement key, as described in 9.4.4.2. This parameter is ignored if KeyIdMode is set to 0x01. |
| NewKeyIndex | Integer | 0x01-0xff | The index of the replacement key, as described in 9.4.4.3. |
| ConfirmationRequested | Boolean | TRUE, FALSE | Specifies whether the confirmation from the is requested. |

The MLME-PRIV-UPDATE-KEY-ID.indication primitive is issued from the MAC when the Key Identifier Update command is received.

Parameters contain the values copied directly from the fields from the frame.

If the ConfirmationRequested is TRUE, then MLME-PRIV-UPDATE-KEY-ID.response may be used to send Key Identifier Update Confirm command back.

* + 1. MLME-PRIV-UPDATE-KEY-ID.response

This primitive responds to the Key Identifier Update command by sending Key Identifier Update Confirm command.

The semantics of this primitive are as follows:

MLME-PRIV-UPDATE-KEY-ID.response (
 SrcAddrMode,
 SrcAddr,
 DstAddrMode,
 DstPanId,
 DstAddr,
 SecurityParams,
 KeyIdMode,
 IncludeOldKeyIdentifier,
 OldKeySource
 OldKeyIndex
 )

The primitive parameters are defined in Table 16.

Table 16—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. |
| KeyIdMode | Integer | 0x01-0x03 | The mode used to identify the key. Same mode is used for both old and new key ID. |
| IncludeOldKeyIdentifier | Boolean | TRUE, FALSE | Specifies whether the OldKeyIdentifier is included in the frame.  |
| OldKeySource | Set of Octets | As specified by the KeyIdMode parameter | The originator of the key to be replaced, as described in 9.4.4.2. This parameter is ignored if KeyIdMode is set to 0x01. |
| OldKeyIndex | Integer | 0x01-0xff | The index of the key to be replaced, as described in 9.4.4.3. |

When MLME-PRIV-UPDATE-KEY-ID.response primitive is issued then the MAC shall transmit the Key Identifier Update Confirm command back to the sender of Key Identifier Update command.

The KeyIdMode, OldKeySource and OldKeyIndex parameters are copied from the MLME-PRIV-UPDATE-KEY-ID.indication. If the IncludeOldKeyIdentifier is set TRUE then Old Key Identifier field of the Key Identifier Update command is omitted and the KeyIdMode parameter shall be ignored and KeyIdMode of SecurityParams is used instead when filling in the Key Identifier Mode of Key Identifier Update Confirm command.

* + 1. MLME-PRIV-UPDATE-KEY-ID.confirm

This primitive reports the results of the MLME-PRIV-UPDATE-KEY-ID.request transmission.

The semantics of this primitive are as follows:

MLME-PRIV-UPDATE-KEY-ID.confirm (
 SrcAddrMode,
 DstAddrMode,
 DstPanId,
 DstAddr,
 Status
 )

The primitive parameters are defined in Table 17.

Table 17—MLME-PRIV-UPDATE-KEY-ID.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-UPDATE-KEY-ID.confirm primitive is issued the MAC has sent out the Key Identifier Update command to the destination.

* 1. MLME-PRIV-UPDATE-KEY-ID-CONFIRM
		1. MLME-PRIV-UPDATE-KEY-ID-CONFIRM.indication

This primitive reports the reception of the Key Identifier Update Confirm command.

The semantics of this primitive are as follows:

MLME-PRIV-UPDATE-KEY-ID-CONFIRM.indication (
 SrcAddrMode,
 SrcAddr,
 DstAddrMode,
 DstPanId,
 DstAddr,
 SecurityParams,
 KeyIdMode,
 OldKeyIdentifierPresent,
 OldKeySource
 OldKeyIndex
 )

The primitive parameters are defined in Table 18.

Table 18—MLME-PRIV-UPDATE-KEY-ID-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. |
| KeyIdMode | Integer | 0x01-0x03 | The mode used to identify the key. Same mode is used for both old and new key ID. |
| OldKeyIdentifierPresent | Boolean | TRUE, FALSE | Specifies whether the OldKeyIdentifier is included in the frame.  |
| OldKeySource | Set of Octets | As specified by the KeyIdMode parameter | The originator of the key to be replaced, as described in 9.4.4.2. This parameter is omitted if KeyIdMode is set to 0x01 or OldKeyIdentifierPresent is FALSE. |
| OldKeyIndex | Integer | 0x01-0xff | The index of the key to be replaced, as described in 9.4.4.3. This parameter is omitted if OldKeyIdentifierPresent is FALSE. |

The MLME-PRIV-UPDATE-KEY-ID-CONFIRM.indication primitive is issued from the MAC when the Key Identifier Update Confirm command is received.

KeyIdMode, OldKeyIdentifierPresent parameters contain the values copied directly from the fields from the frame. The OldKeySource and OldKeyIndex parameters are extracted from the Old Key Identifier field of the Key Identifier Update Confirm command.

* 1. MLME-PRIV-NET-VERIFIER-GENERATE
		1. MLME-PRIV-NET-VERIFIER-GENERATE.request

This primitive is used to generate the contents of the Encrypted Verifier field of the Net Announcement or Net Request IEs.

The semantics of this primitive are as follows:

MLME-PRIV-NET-VERIFIER-GENERATE.request (
 SecurityLevel,
 AlgorithmId,
 NetworkIdentifier,
 ExtendedPrivacyAddress,
 AnnouncementNonce,
 SequenceNumber
 )

The primitive parameters are defined in Table 19.

Table 19—MLME-PRIV-NET-VERIFIER-GENERATE.request parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SecurityLevel | Integer | 0x05-0x07 | The security level of the verifier to be generated, as defined in the Table 9-6. |
| AlgorithmId | Integer | As defined in Table 9-9 | The AEAD algorithm to be used generating verifier. |
| NetworkIdentifier | IEEE address | An extended IEEE address | The network ID of the network for which the verifier is to be generated. |
| ExtendedPrivacyAddress | IEEE address | An extended IEEE address | Extended Address used as source address of the frame sending this IE out. |
| AnnouncementNonce | Set of Octets | 64-bit octet string. | Random announcement nonce used when generating the verifier. |
| SequenceNumber | Integer | 0x00000000-0xffffffff | Sequence number of the announcement. Sequence number should be incremented by the next higher layer every time Net Announcement IE or Net Request IE is generated for each network.  |

This primitive generates Encrypted verifier field value and issue MLME-PRIV-NET-VERIFIER-GENERATE.confirm to return the generated value back to the higher layer, so higher layer can include it in IE to be sent out.

* + 1. MLME-PRIV-NET-VERIFIER-GENERATE.confirm

This primitive is used to return the generated contents of the Encrypted Verifier field for the Net Announcement or Net Request IEs.

The semantics of this primitive are as follows:

MLME-PRIV-NET-VERIFIER-GENERATE.confirm (
 EncryptedVerifier,
 Status
 )

The primitive parameters are defined in Table 20.

Table 20—MLME-PRIV-NET-VERIFIER-GENERATE.confirm parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| EncryptedVerifier | Set of Octets | Octet string. | Generated Encrypted Verifier field value. The length of the verifier depends on the algorithm used to generate it. |
| Status | Enumeration | SUCCESS, XXX. Also see 8.2.2 | The status of the request. |

This primitive returns the generated Encrypted verifier field value to next higher layer.

* 1. MLME-PRIV-NET-VERIFIER-VERIFY
		1. MLME-PRIV-NET-VERIFIER-VERIFY.request

This primitive is used to find the matching network and verify the contents of the Encrypted Verifier field of the received Net Announcement or Net Request IEs.

The semantics of this primitive are as follows:

MLME-PRIV-NET-VERIFIER-VERIFY.request (
 SecurityLevel,
 AlgorithmId,
 ExtendedPrivacyAddress,
 AnnouncementNonce,
 EncryptedVerifier
 )

The primitive parameters are defined in Table 21.

Table 21—MLME-PRIV-NET-VERIFIER-VERIFY.request parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| SecurityLevel | Integer | 0x05-0x07 | The security level of the verifier to be generated, as defined in the Table 9-6. |
| AlgorithmId | Integer | As defined in Table 9-9 | The AEAD algorithm to be used generating verifier. |
| ExtendedPrivacyAddress | IEEE address | An extended IEEE address | Extended Address used as source address of the frame sending this IE out. |
| AnnouncementNonce | Set of Octets | 64-bit octet string. | Random announcement nonce used when generating the verifier. |
| EncryptedVerifier | Set of Octets | Octet string. | Encrypted Verifier field value received. The length of the verifier depends on the algorithm used to generate it. |

This primitive searches the network key that authenticates the received Encrypted Verifier and issues MLME-PRIV-NET-VERIFIER-VERIFY.confirm to return the network ID and SequenceNumber to next higher layer, or an error if no network key that verifies this is not found.

* + 1. MLME-PRIV-NET-VERIFIER-VERIFY.confirm

This primitive is used to return the network ID and sequence number from the authenticated Encrypted Verifier field of the Net Announcement or Net Request IEs to next higher layer.

The semantics of this primitive are as follows:

MLME-PRIV-NET-VERIFIER-VERIFY.confirm (
 NetworkIdentifier,
 SequenceNumber,
 Status
 )

The primitive parameters are defined in Table 22.

Table 22—MLME-PRIV-NET-VERIFIER-GENERATE.confirm parameters

| **Name** | **Type** | **Valid range** | **Description** |
| --- | --- | --- | --- |
| NetworkIdentifier | IEEE address | An extended IEEE address | The network ID of the network for which the verifier is to be generated. |
| SequenceNumber | Integer | 0x00000000-0xffffffff | Sequence number of the announcement. Sequence number should be incremented by the next higher layer every time Net Announcement IE or Net Request IE is generated for each network.  |
| Status | Enumeration | SUCCESS or NETWORK\_KEY\_NOT\_FOUND, SEQUENCE\_NUMBER\_ERROR. Also see 8.2.2 | The status of the request. |

If none of the network keys configured to the system could authenticate the EncryptedVerifier then the Status of the primitive shall indicate NETWORK\_KEY\_NOT\_FOUND.

If network key was found then NetworkIdentifier shall be set to indicate the matching network ID, and the SequenceNumber is set to contain the decrypted Sequence Number field of the EncryptedVerifier.

If sequence number field inside the EncryptedVerifier is less than or equal than the sequence number associated with the network ID then the Status of the primitive shall indicate SEQUENCE\_NUMBER\_ERROR.

If the network key was found and the sequence number field check passed, then the Status of the primitive shall indicate SUCCESS, and the received decrypted sequence number shall be stored to sequence number associated with the network ID.