IEEE P802.15

Wireless Personal Area Networks

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Privacy Frame Formats |
| Date Submitted | 16th May 2024 |
| Source | Tero Kivinen | E-mail: kivinen@iki.fi |
| Re: | TG4ac draft |
| Abstract | Frame formats 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. Frame formats
	1. Generic format

We are using MAC Commands for all of these messages.

* 1. Sending list of addresses (AddressListMessage)

This primitive is used to send list of addresses used by sender of this frame. This may be sent to unicast or multicast address. The source address of this may be either short private address, or extended private address. If this is sent to multicast address then Confirmation Required field shall be set to zero.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 1** | **0/8** | **0/1** | **0/2** | **0/1** | **0/varies** | **0/1** | **0/varies** |
| Flags | Sender ID | Address List Sequence Number | PAN ID | Number of Short Addresses | List of Short Addresses | Number of Extended Addresses | List of Extended Addresses |

**Figure 1— Format of the Address List MAC Command**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Bit: 0** | **1** | **2** | **3** | **4** | **5** | **6-7** |
| Sender ID Present | Address List Sequence Number Present | PAN ID Present | Short Address List Present | Extended Address List Present | Confirmation Required | Reserved |

**Figure 2— Flags of the Address List MAC Command**

The Sender ID Present, Address List Sequence Number Present, and PAN ID Present fields indicate whether the corresponding field in the Address List MAC Command is present. If the field is set to one, the field shall be present, and if it is set to zero, the field shall be omitted.

Sender ID field identifiers the actual sender using senders Device identifier.

If the Address List Sequence Number field is present, it has the sequence number of the address list. The upper layer will manage the sequence numbers of the address lists. The upper layer can use Address List Sequence Number to detect Address List MAC Command replays.

The PAN ID Present field shall be set to one only if Short Address List Present field is also one.

If the Short Address List Present field is set to one, then both Number of Short Addresses and List of Short Addresses shall be present. If it set to zero, both are omitted.

List of Short Address contains the list of short addresses, and its length is Number of Short Addresses times two.

If the Extended Address List Present field is set to one, then both Number of Extended Addresses and List of Extended Addresses shall be present. If it set to zero, both are omitted.

List of Extended Address contains the list of extended addresses, and its length is Number of Extended Addresses times eight.

If the Confirmation Required field is set to one, then the sender of this frame requires the Address List Confirm MAC Command as a response to this command.

New list always replaces old one if the field is present.

If the Short Address List field is not present, the previous short address list is used. If the Short Address List field is present, but Number of Short Addresses field contains zero, then device is no longer using short addresses.

If the PAN ID field is not present, then PAN ID of the previous message is used. If no previous PAN ID is known, then PAN ID of 0xffff is used.

If the Extended Address List field is not present, the previous extended address list is used. If the Short Extended List field is present, but Number of Extended Addresses field contains zero, then device is no longer using extended addresses.

* 1. Confirmation of receipt of address list (AddressListConfirmMessage)

This frame shall be sent in unicast frame to the sender of the AddressListMessage. This shall not be sent if the destination address of the address list was not unicast address.

This is used to confirm the reception of the AddressListMessage.

|  |  |
| --- | --- |
| **Octets: 1** | **0/1** |
| Flags | Address List Sequence Number |

**Figure 3— Format of the Confirmation of Address List MAC Command**

|  |  |
| --- | --- |
| **Bit: 0** | **1-7** |
| Address List Sequence Number Present | Reserved |

**Figure 4— Flags of the Confirmation of Address List MAC Command**

The Address List Sequence Number Present field indicate whether the Address List Sequence Number field is present. If the field is set to one, the field shall be present, and if it is set to zero, the field shall be omitted.

Address List Sequence Number Present, and Address List Sequence Number fields of the oncoming Address List MAC Command shall be copied to the Address List Sequence Number field of the outgoing Confirmation of Address List MAC Command.

* 1. Request to get list of addresses (RequestAddressesMessage)

This frame may be sent to unicast or multicast address. This message is used when the device does not know the currently used private address for remote device, or where it thinks the list might be out of sync. Can be sent to last known unicast address, or to the multicast address. The source address is typically extended private address.

|  |  |  |  |
| --- | --- | --- | --- |
| **Octets: 1** | **0/8** | **0/8** | **0/1** |
| Flags | Sender ID | Recipient ID | Address List Sequence Number |

**Figure 5— Format of the Request Addresses MAC Command**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bit: 0** | **1** | **2** | **3-7** |
| Sender ID Present | Recipient ID Present | Sequence Number Present | Reserved |

**Figure 6— Flags of the Request Addresses MAC Command**

The Sender ID Present, Recipient ID Present, and Sequence Number Present fields indicate whether the corresponding field in the Request Addresses MAC Command is present. If the field is set to one, the field shall be present, and if it is set to zero, the field shall be omitted.

Sender ID field identifiers the actual sender using senders Device identifier.

Recipient ID field identifiers the actual receiver using receivers Device identifier. If frame is sent to multicast address then this field shall be included, and Recipient ID Present field shall be set to one.

Address List Sequence Number indicates the last address list the sending device has seen.

This message may be sent after or during oprhan scan, i.e., where the device things remote peer has changed address, and device do now know currently used addresses. The recipient of this will reply to that with Address List MAC Command.

* 1. Assignment of addresses to remote peer (AssignAddressesMessage)

This message may sent by the owner of the network to assign short addresses to devices. It is usually sent to the unicast address of the intended recipient, but if the network owner thinks remote peer might be out of sync it may also send this to multicast address.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Octets: 1** | **0/8** | **0/8** | **0/1** | **0/2** | **0/1** | **0/varies** |
| Flags | Sender ID | Recipient ID | Address List Sequence Number | PAN ID | Number of Short Addresses | List of Short Addresses |

**Figure 7— Format of the Addresses Assignment MAC Command**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Bit: 0** | **1** | **2** | **3** | **4** | **5-7** |
| Sender ID Present | Recipient ID Present | Address List Sequence Number Present | PAN ID Present | Confirmation Required | Reserved |

**Figure 8— Flags of the Addresses Assignment MAC Command**

The Sender ID Present, Recipient ID Present, Address List Sequence Number Present, and PAN ID Present fields indicate whether the corresponding field in the Address Assignment MAC Command is present. If the field is set to one, the field shall be present, and if it is set to zero, the field shall be omitted.

Sender ID field identifiers the actual sender using senders Device identifier.

Recipient ID field identifiers the actual receiver using receivers Device identifier. If frame is sent to multicast address then this field shall be included, and Recipient ID Present field shall be set to one.

If the Address List Sequence Number field is present, it has the sequence number of the address list. The upper layer will manage the sequence numbers of the address lists.

If the Confirmation Required field is set to one, then the sender of this frame requires the Confirmation of Address Assignment MAC Command as a response to this command.

If the PAN ID field is not present, then PAN ID of the previous message is used. If no previous PAN ID is known, then PAN ID of 0xffff is used.

List of Short Address contains the list of short addresses, and its length is Number of Short Addresses times two.

If device is assigned zero addresses, then it cannot use any short addresses anymore.

* 1. Confirmation of address assignment (AssignAddressesConfirmMessage)

This frame shall be sent in unicast frame to the sender of the Address Assignment MAC Command if confirmation was requested.

This is used to confirm the reception of the Address Assignment MAC Command.

|  |  |
| --- | --- |
| **Octets: 1** | **0/1** |
| Flags | Address List Sequence Number |

**Figure 9— Format of the Confirmation of Address Assignment MAC Command**

|  |  |
| --- | --- |
| **Bit: 0** | **1-7** |
| Address List Sequence Number Present | Reserved |

**Figure 10— Flags of the Confirmation of Address Assignment MAC Command**

The Address List Sequence Number Present field indicate whether the Address List Sequence Number field is present. If the field is set to one, the field shall be present, and if it is set to zero, the field shall be omitted.

Address List Sequence Number Present, and Address List Sequence Number fields of the oncoming Address Assignment MAC Command shall be copied to the Address List Sequence Number field of the outgoing Confirmation of Address Assignment MAC Command.

* 1. Updating key id (KeySourceUpdateMessage)

This may be sent as unicast or multicast message. If sent as multicast message there shall not be confirmations.

|  |  |  |  |
| --- | --- | --- | --- |
| **Octets: 1** | **0/8** | **0/1/5/9** | **1/5/9** |
| Flags | Sender ID | Old Key Id | New Key Id |

**Figure 11— Format of the Key Id Update MAC Command**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bit: 0** | **1** | **2-3** | **4** | **5-7** |
| Sender ID Present | Old Key Id Present | Key Id Mode | Confirmation Required | Reserved |

**Figure 12— Flags of the Key Id Update MAC Command**

The Sender ID Present, and Old Key Id Present fields indicate whether the corresponding field in the Key Id Update MAC Command is present. If the field is set to one, the field shall be present, and if it is set to zero, the field shall be omitted.

Sender ID field identifiers the actual sender using senders Device identifier.

If the Old Key Id Present is set to zero, then Key Id to be changed is taken from the MHR.

The Old and New Key Id fields are defined in 9.4.4.

Key Id Mode field is defined in 9.4.2.3.

If the Confirmation Required field is set to one, then the sender of this frame requires the Key Id Update Confirmation MAC Command as a response to this command.

When this frame is received the recipient will update the key id to the new value defined, but will keep the old key id also in security PIB. When the new key id is first time used, the old id is removed.

* 1. Confirmation of updating key id (KeySourceUpdateConfirmMessage)

This frame shall always sent in unicast frame to the sender of the KeySourceUpdateMessage.

This is used to confirm the reception of the Key Id Update MAC Command.

|  |  |
| --- | --- |
| **Octets: 1** | **1/5/9** |
| Flags | Old Key Id |

**Figure 13— Format of the Key Id Update Confirmation MAC Command**

|  |  |
| --- | --- |
| **Bit: 0-1** | **2-7** |
| Key Id Mode | Reserved |

**Figure 14— Flags of the Key Id Update Confirmation MAC Command**

The Old Key Id fields are defined in 9.4.4.

Key Id Mode field is defined in 9.4.2.3.

This sent as an reply to the Key Id Update MAC Command to confirm that key id update was successful. It is using the same key id than the Key Id Update MAC Command. The key id to updated will be identified inside the message, even the outer key id might be different.

1. Information Elements
	1. Network announcement (AnnouncementMessage)

This IE may be included in the mssage that is sent to multicast address, for example in Beacon frames. This IE is often sent without encryption, as this is used to find existing networks, and devices wanting to join might not have security context. Source address of such frame is extended private address of the sender.

|  |  |  |
| --- | --- | --- |
| **Octets: 1** | **8** | **16/20/28** |
| Flags | Announcement Nonce | Encrypted Verifier |

**Figure 15— Format of the Network Announcement IE**

|  |  |  |
| --- | --- | --- |
| **Bit: 0-2** | **3** | **4-7** |
| Security Level of Verifier | Reserved | Algorithm ID |

**Figure 16— Flags of the Network Announcement IE**

The Security Level fof the Verifier field contains the security level used when generating the Encrypted Verifier field as defined in Table 9-4. Only security levels 5-7 shall be allowed.

Algorithm ID indicates the algorithm used when generating Encrypted Verifier field, as defined in Table 9-9.

The Announcement Nonce field shall be filled with random 64-bit number.

The Encrypted Verifier is generated by taking the data defined in Figure 17, and encrypting it using the specified encryption algorithm, the Network key, and the security level specified in the Security Level of the Verifier field.

|  |  |
| --- | --- |
| **Octets: 8** | **4** |
| Announcement Nonce | Sequence Number |

**Figure 17— Nonce generation for Encrypted Verifier field of the Network Announcement IE**

The nonce used in encryption is defined in Figure 18.

|  |  |
| --- | --- |
| **Octets: 8** | **8** |
| Extended private address | Announcement Nonce |

**Figure 18— Nonce generation for Encrypted Verifier field of the Network Announcement IE**

The Encrypted Verifier field shall contain the output of the encryption process, meaning that the data in Figure 13 shall be used as m data and a data is set to empty (XXX TODO: Should we add additional data here, we could include rest of the beacon / frame, MHR etc to authenticate them too, this might make the frame generation more difficult), and the output c data is used as Encrypted Verifier field content.

Recipent of this message who know the Network key can decrypt and verify the Encrypted Verifier field inside the IE, and it can use it to verify that the Announcement Nonce inside matches that of outside, and that sequence number is not old.

If the device does not have security context with the network, it will start IEEE Std 802.15.9 KMP with the sender of this message to create security context, and join the network. This method requires that devices wanting to join the network needs to be configured with the 64-bit network identifier, and the 128-bit network key (if network key is used, if not only the network identifier is needed).

Devices who already have security context with the network, can use this message to find that network is available, and send RequestAddressesMessage to sender in case the source address used in this message was not already known to them.

* 1. Network request (AnnouncementRequestMessage)

This IE may be sent in frame that is sent to the multicast address to see if there is known network nearby. This is usually sent in clear, as this is used to find existing networks, and device sending this might not have addresses that are recognized by the network anymore. Can also be sent encrypted in case device assumes the network owner recognizes source address, and can find security context based on that. Source address is extended private address.

The contents of the Network request IE is exactly same as Network Announcement IE.

Processing is same as in the Network Announcement IE meaning if the recipient can verify the verifier, it can send AddressListMessage to the sender of this message to update the addresses.