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

Most of the messages are delivered using MAC commands, but the net announcement and request feature uses IEs so they can be included in the Beacon or other frames.

* 1. Address List command

The Address List MAC command frame is used to announce list of addresses used by the sender of the frame. This may be sent to unicast or multicast address. The source address of this should be either short address, or extended privacy address. If this is sent to multicast address then Confirmation Required field shall be set to zero.

Address List MAC Command frame shall be formatted as illustrated in Figure 1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 frame

Flags field shall be formatted as illustrated in Figure 2.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 field of the Address List MAC Command frame

The Sender ID Present, Address List Sequence Number and PAN ID Present fields specify whether the corresponding fields in the Address List MAC Command frame are 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, and contains the Device identifier of the sender.

The Address List Sequence Number field contains a sequence number maintained by the next higher layer and it specifies the sequence number of the address list contained in the frame. Address List Sequence Number field is associated with the address list generated by the next higher layer. If the next higher layer uses the Address List Sequence Number fields it shall increment it by one every time address list changes. If the short address list and extended address list updates are split in two different MAC Command frames, they may still share the same Address List Sequence Number field value. If next higher layer uses separate address list for each recipient, it may share the sequence numbers.

If device resends the same address list again, it should include same address list sequence number.

The recipient may use the Address List Sequence Number to detect whether the address list in the Address List MAC Command frame is replayed. If only one extended privacy address is used then the replay protection of the security layer will already filter out replays, but if sender uses multiple different extended privacy addresses at the same time then each of those extended privacy addresses is associated with separate frame counter in security layer, thus old frames not seen by the receiving end using one extended privacy address may be replayed to destination after newer frames is already received using another extended privacy address. The same extended privacy address shall not be in address list where the address list sequence number is more than 127 from each other.

Address List Sequence Number wraps to zero upon reaching maximum value.

The PAN ID Present field shall be set to one only if Short Address List Present field is also set to 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 expects the Address List Confirm MAC Command frame as a response to this command.

When the device sends a list the new list received in this message replaces the old address list if the address list 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 short list is used. If the PAN ID field is not present, and this frame was sent using short address then PAN ID of the MHR 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 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 (Address List Confirm MAC Command frame)

This frame shall be sent in unicast frame to the sender of the Address List MAC Command frame as a response to the Address List MAC Command frame. This shall not be sent if the destination address of the address list was not unicast address.

Address List Confirm MAC Command frame shall be formatted as illustrated in Figure 3.

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

Figure 3—Format of the Address List Confirm MAC Command **frame**

Flags field of the Address List Confirm MAC Command frame shall be formatted as illustrated in Figure 4.

|  |  |  |
| --- | --- | --- |
| **Bit: 0** | **1** | **2-7** |
| Address List Sequence Number Present | Error Code Present | Reserved |

Figure 4—Flags of the Address List Confirm MAC Command frame

The Address List Sequence Number, and Error Code Present fields specifies whether the Address List Sequence Number field and Error Code Present field are 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 field shall only be present if the Address List MAC Command contained Address List Sequence Number field. If Address List Sequence Number field is present it shall contain the same value as the Address List Sequence number field of the Address List MAC Command frame to what this is response to.

If the Error Code field is present it shall contain values listed in Table 1. If the Error Code field is not present the address list was successfully updated.

Table 1—List of Error Codes

|  |  |  |
| --- | --- | --- |
| Error Code | Name | Description |
| 0 | Success | Address list was successfully updated. |
| 1 | Unknown Source Address | The source address was not recognized, thus device could not find the device to update addresses to.  |
| 2 | Out of resources | Device could not update the list because it run out of resources. |
| 3-255 | Reserved |  |

* 1. Request to get list of addresses (Request Addresses MAC Command frame)

This frame may be sent to unicast or multicast address. This message is used when the device does not know the currently used privacy 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 privacy address.

Request Addresses MAC Command frame shall be formatted as illustrated in Figure 5.

|  |  |  |
| --- | --- | --- |
| **Octets: 1** | **0/8** | **0/8** |
| Flags | Sender ID | Recipient ID |

Figure 5— Format of the Request Addresses MAC Command from

Flags field of the Request Addresses MAC Command frame shall be formatted as illustrated in Figure 6.

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

Figure 6—Flags of the Request Addresses MAC Command from

The Sender ID Present, and Recipient ID Present fields specify whether the corresponding field in the Request Addresses MAC Command frame 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.

This message may be sent after or during orphan scan, i.e., where the device thinks 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 (Assign Addresses MAC Command frame)

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.

Assign Addresses MAC Command frame shall be formatted as illustrated in Figure 7.

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

Figure 7—Format of the Assign Addresses MAC Command frame

Flags field of the Assign Addresses MAC Command frame shall be formatted as illustrated in Figure 8.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bit: 0** | **1** | **2** | **3** | **4-7** |
| Sender ID Present | Recipient ID Present | PAN ID Present | Confirmation Required | Reserved |

Figure 8—Flags of the Assign Addresses MAC Command frame

The Sender ID Present, Recipient ID Present, and PAN ID Present fields specify whether the corresponding field in the Assign Addresses MAC Command frame are 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 Confirmation Required field is set to one, then the sender of this frame requires the Assign Addresses Confirm MAC Command frame as a response to this command.

If the PAN ID field is not present, then PAN ID of the previous short list is used. If the PAN ID field is not present, and this frame was sent using short address then PAN ID of the MHR 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 (Assign Addresses Confirm MAC Command frame)

This frame shall be sent in unicast frame to the sender of the Assign Addresses Confirm MAC Command frame if confirmation was requested.

This is used to confirm the reception of the Assign Addresses MAC Command frame.

Assign Addresses Confirm MAC Command frame shall be formatted as illustrated in Figure 9.

|  |  |
| --- | --- |
| **Octets: 1** | **0/1** |
| Flags | Error Code |

Figure 9—Format of the Assign Addresses Confirm MAC Command frame

Flags field of the Assign Addresses Confirm MAC Command frame shall be formatted as illustrated in Figure 10.

|  |  |
| --- | --- |
| **Bit: 0** | **1-7** |
| Error Code Present | Reserved |

Figure 10—Flags of the Assign Addresses Confirm MAC Command frame

The Error Code Present field specifies whether the Error Code 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.

If the Error Code field is present it shall contain values listed in Table 2. If the Error Code field is not present the address list was successfully updated.

Table 2—List of Error Codes

|  |  |  |
| --- | --- | --- |
| Error Code | Name | Description |
| 0 | Success | Address list was successfully updated. |
| 1 | Unknown ID | The Sender ID or the Recipient ID is unknown, i.e., the Recipient ID does not match the recipient of this message, or the Sender ID does not match the owner of the network. |
| 2 | Out of resources | Device could not update the list because it run out of resources. |
| 3 | Unsupported operation | The device does not support short address assignments. |
| 4-255 | Reserved |  |

* 1. Updating key id (Key Id Update MAC Command frame)

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

Key Id Update MAC Command frame shall be formatted as illustrated in Figure 11.

|  |  |  |  |
| --- | --- | --- | --- |
| **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 frame

Flags field of the Key Id Update MAC Command frame shall be formatted as illustrated in Figure 12.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 frame

The Sender ID Present, and Old Key Id Present fields specify whether the corresponding field in the Key Id Update MAC Command are 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 Confirm 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. Before taking new key id to use, the device should take new set of addresses in use, i.e., make sure old and new key id do not use same short addresses or extended privacy addresses.

* 1. Confirmation of updating key id (Key Id Update Confirm MAC Command frame)

This frame shall always sent in unicast frame to the sender of the Key Id Update MAC Command frame.

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

Key Id Update Confirm MAC Command frame shall be formatted as illustrated in Figure 13.

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

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

Flags field of the Key Id Update Confirm MAC Command frame shall be formatted as illustrated in Figure 14.

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

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

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 frame to confirm that key id update was successful. Key Id Mode and Old Key Id fields of the received Key Id Update MAC Command frame shall be copied to the this Key Id Update Confirm MAC Command frame.

1. Information Elements
	1. Network announcement (Net Announcement IE)

This IE may be included in the frame 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 this frame shall be extended privacy address of the sender.

Net Announcement IE shall be formatted as illustrated in Figure 15.

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

Figure 15—Format of the Net Announcement IE

Flags field of the Net Announcement IE shall be formatted as illustrated in Figure 16.

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

Figure 16—Flags of the Net Announcement IE

The Security Level of 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 specifies 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—Verifier generation for Encrypted Verifier field of the Net Announcement IE

When encrypting the data in Figure 17 the nonce used shall be generated illustrated in Figure 18.

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

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

The Encrypted Verifier field shall contain the output of the encryption process, meaning that the data in Figure 17 shall be used as m data and a data is set to empty, and the output c data is used as Encrypted Verifier field content.

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.

Recipient 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 see that network is available, and send Request Addresses MAC Command frame to sender in case the source address used in this message was not already known to them.

* 1. Network request (Net Request IE)

The Net Request IE may be sent in frame that is sent to the multicast address to see if there is known network nearby. This frame 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. Typically source address is extended privacy address.

The contents of the Net Request IE is exactly same as Net Announcement IE.

Processing is same as in the Net Announcement IE meaning if the recipient can verify the verifier, it can send Address List MAC Command frame to the sender of this message to update the addresses.