IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB282 CR for CID225 and CID255 | | | | |
| Date: 2024-01-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  | okan.mutgan@nokia-sbell.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions and discussions for CID225 and CID255 on 802.11bh D2.0:

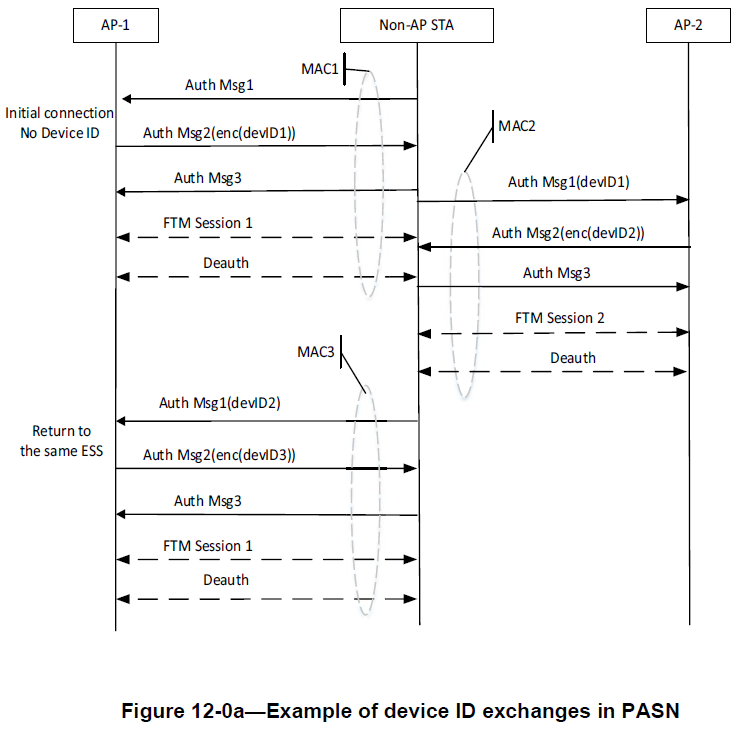
R0. Initial Version.

R1. Modification on text and figures for PASN case based on 11/24-0044r8.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 225 | 30 | 44 | Draw example figures of the signaling for IRM and device ID, preferably each mechanism with identifier recognized or not recognized. (Previous letter ballot consists of several comments that are not completely clear about the signaling procedures) | As in comment. | REVISED. |
| 255 | 32 | 23 | In addition to no "Device ID" (the protocol element), there is no "device ID" (the concept), yet, for the initial connection in Figure 12-0a. | In the label on the left of "AP-1" line, change "No Device ID" to "No device ID" (lower-case 'd'). | REVISED. |

**Discussion**

This is the current figure of device ID exchange in PASN:



This document proposes additional figures and also some modification for the current figure 12-0a.

**Proposed Changes**

**1) CID225, CID255**

*Add the following sentence in 12.2.12 Identifying a non-AP STA with changing MAC address:*

The two mechanisms, device ID and IRM, both allow the network to recognize the STA while mitigating the abilities of third parties to do traffic analysis and tracking of the non-AP STA.

The two mechanisms, device ID and IRM, may be used concurrently.

Annex AX provides illustrative examples of the usage of device ID and IRM.

*Remove the following paragraph and Figure 12-0a—Example of device ID exchanges in PASN:*

Figure 12-0a (Example of device ID exchanges in PASN) shows an example of a device ID exchange in

PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS

containing AP1 and AP2. The non-AP STA with a MAC address of MAC1 first initiates the connection with AP1 by sending the first PASN frame with the Device ID Active field in the RSNXE set to 1. Upon receiving the first PASN frame, AP1 assigns a device ID (devID1) and sends it to the non-AP STA in the second PASN frame. The non-AP STA then continues to establish an FTM session with AP1. When the non-AP STA with a MAC address of MAC2 (non-AP STA changing its MAC from MAC1 to MAC2) performs PASN with AP2 to establish another FTM session, the non-AP STA sends previously assigned device ID (devID1) to AP2 in the first PASN frame. Upon receiving the device ID (devID1) in first PASN frame, AP2 assigns another device ID (devID2) and sends it to the non-AP STA in the second PASN frame. The non-AP STA then proceeds to establish the FTM session. Similarly, when the non-AP STA with a MAC address of MAC3 returns to AP1, it sends the previously assigned device ID (devID2) and is assigned another device ID (devID3) that will be used in the subsequent PASN for another FTM session.

A diagram of a device exchange

Description automatically generated

*Create Annex AX and put the following text and figures as follows:*

Annex AX.1 – Examples of device ID usage

Figure AX-1 shows an example of a device ID exchange in non-FILS or non-PASN authentication (e.g., SAE). AP advertises its support of device ID in RSNXE in Beacon or Probe Response. The non-AP STA with a MAC address of MAC1 initiates the first connection with AP (i.e., no initial device ID). After authentication frame exchange, non-AP STA indicates its activation of device ID via Device ID Active field in the RSNXE set to 1 in Association Request. Similarly, AP indicates its activation of device ID via Device ID Active field in the RSNXE set to 1 in Association Response. In 4-way Handshake Message 3, AP assigns a device ID (devID1) to non-AP STA in device ID KDE. Both non-AP STA and AP store devID1. When non-AP STA terminates connection with AP and returns to the same ESS with another MAC (MAC2), after device ID activation from non-AP STA and AP via Association Request/Response frame exchange, non-AP STA provides previously assigned device ID (devID1) to AP in device ID KDE in 4-way Handshake Message 2. Because of devID1, AP identifies the non-AP STA despite non-AP STA’s randomized MAC (MAC2). Additionally, AP may respond positive recognition of devID1 and assign another device ID (devID2) in device ID KDE in 4-way Handshake Message 3.

A black background with a white text

Description automatically generated

Figure AX-1 – Example of device ID exchange in non-FILS or non-PASN

Figure AX-2 shows an example of a device ID exchange in FILS. AP advertises its support of device ID in RSNXE in Beacon or Probe Response. The non-AP STA with a MAC address of MAC1 initiates the first connection with AP (i.e., no initial device ID). After authentication frame exchange, non-AP STA indicates its activation of device ID via Device ID Active field in the RSNXE set to 1 in Association Request. Similarly, AP indicates its activation of device ID via Device ID Active field in the RSNXE set to 1 in Association Response. In Association Response, AP assigns a device ID (devID1) to non-AP STA in Device ID element. Both non-AP STA and AP store devID1. When non-AP STA terminates connection with AP and returns to the same ESS with another MAC (MAC2), non-AP STA indicates its activation of deviceID in RSNXE in Association Request and provides previously assigned device ID (devID1) to AP in Device ID element in Association Request. Because of devID1, AP identifies the non-AP STA despite non-AP STA’s randomized MAC (MAC2). Additonally, AP may respond positive recognition of devID1 and assign another device ID (devID2) in device ID element in Association Response. (Notice the device ID activation from AP via Association Response frame as well).

A black background with white text

Description automatically generated

Figure AX-2 – Example of device ID exchange in FILS

Figure AX-3 shows an example of a device ID exchange in PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS containing AP1 and AP2. AP1 and AP2 advertise their support of device ID in RSNXE in Beacon or Probe Response. The non-AP STA with a MAC address of MAC1 first initiates the connection with AP1 by sending the first PASN frame with the Device ID Active field in the RSNXE set to 1 and with the KEK in PASN Active field in the RSNXE set to 1. Upon receiving the first PASN frame, AP1 indicates its activation of device ID via Device ID Active field in the RSNXE set to 1 and its activation of KEK via KEK in PASN Active field in the RSNXE set to 1, and then assigns a device ID (devID1) and sends it to the non-AP STA in Device ID in Device ID subelement in PASN Ecrypted Data element in the second PASN frame. Both non-AP STA and AP store devID1. The non-AP STA then continues to establish an FTM session with AP1. When the non-AP STA with a MAC address of MAC2 (non-AP STA changing its MAC from MAC1 to MAC2) performs PASN with AP2 to establish another FTM session, the non-AP STA sends previously assigned device ID (devID1) to AP2 in Device ID in Device ID element in the first PASN frame. Because of devID1, AP2 identifies the non-AP STA despite non-AP STA’s randomized MAC (MAC2). Upon receiving the device ID (devID1) in first PASN frame, AP2 may respond positive recognition of devID1 in Device ID status in Device ID subelement in PASN Ecrypted Data element in second PASN frame and AP2 may assign another device ID (devID2) and send it to the non-AP STA in Device ID in Device ID subelement in PASN Ecrypted Data element in the second PASN frame. (Notice the device ID activation and KEK activation from non-AP STA and AP via first and second PASN frames as well). The non-AP STA then proceeds to establish the FTM session. Similarly, when the non-AP STA with a MAC address of MAC3 returns to AP1, it sends the previously assigned device ID (devID2) and is assigned another device ID (devID3) that will be used in the subsequent PASN for another FTM session.

A black background with white circles

Description automatically generated

Figure AX-3 – Example of device ID exchange in PASN

Annex AX.2 – Examples of IRM usage

Figure AX-4 shows an example of a IRM exchange in non-FILS or non-PASN authentication (e.g., SAE). AP advertises its support of IRM in RSNXE in Beacon or Probe Response. The non-AP STA with a MAC address of MAC1 initiates the first connection with AP (i.e., no initial IRM). After authentication frame exchange, non-AP STA indicates its activation of IRM via IRM Active field in the RSNXE set to 1 in Association Request. Similarly, AP indicates its activation of IRM via IRM Active field in the RSNXE set to 1 in Association Response. In 4-way Handshake Message 4, non-AP STA assigns an IRM (IRM1) to itself in IRM KDE. Both non-AP STA and AP store IRM1. When non-AP STA terminates connection with AP and returns to the same ESS, non-AP STA uses previously assigned IRM (IRM1) as its MAC address. (Notice that the IRM activation from non-AP STA and AP via Association Request/Response frame exchange as well). Because of IRM1, AP identifies the non-AP STA. Additionally, AP may respond positive recognition of IRM1 in IRM KDE in 4-way Handshake Message 3 and non-AP STA may assign another IRM (IRM2) to itself in IRM KDE in 4-way Handshake Message 4.

A black background with white text

Description automatically generated

Figure AX-4 – Example of IRM exchange in non-FILS or non-PASN

Figure AX-5 shows an example of a IRM exchange in FILS. AP advertises its support of IRM in RSNXE in Beacon or Probe Response. The non-AP STA with a MAC address of MAC1 initiates the first connection with AP (i.e., no initial IRM). After authentication frame exchange, non-AP STA indicates its activation of IRM via IRM Active field in the RSNXE set to 1 in Association Request. In Association Request, non-AP STA assigns an IRM (IRM1) to itself in IRM element. AP also indicates its activation of IRM via IRM Active field in the RSNXE set to 1 in Association Response. Both non-AP STA and AP store IRM1. When non-AP STA terminates connection with AP and returns to the same ESS, non-AP STA uses previously assigned IRM (IRM1) as its MAC address. (Notice that the IRM activation from non-AP STA and AP via Association Request/Response frame exchange as well). Because of IRM1, AP identifies the non-AP STA. Additionally, AP may respond positive recognition of IRM1 in IRM element in Association Response and non-AP STA may assign another IRM (IRM2) to itself in IRM element in Association Request.

A black background with white text

Description automatically generated

Figure AX-5 – Example of IRM exchange in FILS

Figure AX-6 shows an example of a IRM exchange in PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS containing AP1 and AP2. AP1 and AP2 advertise their support of IRM in RSNXE in Beacon or Probe Response. The non-AP STA with a MAC address of MAC1 first initiates the connection with AP1 by sending the first PASN frame with the IRM Active field in the RSNXE set to 1 and with the KEK in PASN Active field in the RSNXE set to 1. Upon receiving the first PASN frame, AP1 indicates its activation of IRM via IRM Active field in the RSNXE set to 1 and its activation of KEK via KEK in PASN Active field in the RSNXE set to 1. In the third PASN frame, non-AP STA assigns an IRM (IRM1) to itself and sends it to the AP1 in IRM in IRM subelement in PASN Ecrypted Data element. Both non-AP STA and AP1 store IRM1.The non-AP STA then continues to establish an FTM session with AP1. When the non-AP STA performs PASN with AP2 to establish another FTM session, the non-AP STA uses previously assigned IRM (IRM1) as its MAC address. Because of IRM1, AP2 identifies the non-AP STA. Upon receiving the IRM (IRM1) in first PASN frame, AP2 may respond positive recognition of IRM1 in IRM Status in IRM subelement in PASN Ecrypted Data element in second PASN frame. Additionally, non-AP STA may assign another IRM (IRM2) to itself in IRM in IRM subelement in PASN Ecrypted Data element in third PASN frame. (Notice the IRM activation and KEK activation from non-AP STA and AP via first and second PASN frames as well). Similarly, when the non-AP STA returns to AP1, it uses the previously assigned IRM (IRM2) as its MAC address and is assigned another IRM (IRM3) that will be used in the subsequent PASN for another FTM session.

A black background with white circles

Description automatically generated

Figure AX-6 – Example of IRM exchange in PASN