IEEE P802.11Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed resolution to 11be cc34 CIDs on GTK for MLO | | | | |
| Date: 2021-03-19 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Qi Wang | Apple |  |  | qi\_wang2@apple.com |
| Jarkko Kneckt |  |  | jkneckt@apple.com |
| Yong Liu |  |  | yongliu@apple.com |
| Jinjing Jiang |  |  | jinjing@apple.com |

**Introduction**

This submission proposes the resolution to 11be CC34 CIDs on the GTK and PN check for group addressed data frames delivery for MLO.

Comments:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Page/Line | Clause | Comment | Proposed change | Resolution |
| 1874 | Jarkko Kneckt | 132/1 | 35.3.5.2 | MLD STAs should have GTK and PN at the ML level, not on the link level. This simplifies group addressed frames reception at non-AP MLD. | Please define GTK and PNs to the ML level, not on the link level. | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of MLD and a single corresponding PN check is performed at the MLD level.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2287 | Michael Montemurro | 116/49 | 12.5.3.3.7 | This should just be MLD AP | Change "STA" to "STA or MLD" | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of a MLD.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2288 | Michael Montemurro | 116/52 | 12.5.3.3.7 | This should just be MLD AP | Change "STA" to "STA or MLD" | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of a MLD.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2314 | Ming Gan | 132/01 | 35.3.5.2 | It is not clear that for what each link has its own PN Space. It is for group addressed frame? | As in comment | Revised.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of MLD and a single corresponding PN check is performed at the MLD level.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-02-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-02-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2476 | Payam Torab Jahromi | 131/59 | 35.3.5.2 | Change "The PMK, PTK, and the same PN space are used for all the setup links between the ﾠnon-AP MLD and the AP MLD for the PTKSA." to "The PMK, PTK, and PN space are common to all the links set up between the non-AP MLD and the AP MLD for the PTKSA." | As in the comment | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of MLD and a single corresponding PN check is performed at the MLD level.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2533 | Qi Wang | 116/51 | 12.5.3.3.7 | "Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD for the PTKSA and the PN that is maintained by the AP affiliated with the AP MLD for the GTKSA. " It's unclear why PN check for group addressed frames should be at the individual AP level instead of at the MLD level associated with a common GTK used by all links. | Unify the design for unicast and groupcast frame delivery. Specify that a common GTK and PN check applied to group addressed frames delivery over all links. | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of MLD and a single corresponding PN check is performed at the MLD level.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2534 | Qi Wang | 117/14 | 12.6.1.1.2 | "Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD for the PTKSA and the PN that is maintained by the AP affiliated with the AP MLD for the GTKSA. " It's unclear why PN check for group addressed frames should be at the individual AP level instead of at the MLD level associated with a common GTK used by all links. | Unify the design for unicast and groupcast frame delivery. Specify that a common GTK and PN check applied to group addressed frames delivery over all links. | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of MLD and a single corresponding PN check is performed at the MLD level.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2535 | Qi Wang | 132/1 | 35.3.5.2 | "Different links use different GTK/IGTK/BIGTK and each link has its own PN space. The GTK/IGTK/BIGTK of each setup links are delivered to the non-AP MLD using a single 4-way handshake as defined in 12.7.6 (4-way handshake.)" It's unclear why PN check for group addressed frames should be at the individual AP level instead of at the MLD level associated with a common GTK used by all links. | Unify the design for unicast and groupcast frame delivery. Specify that a common GTK and PN check applied to group addressed frames delivery over all links. | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of MLD and a single corresponding PN check is performed at the MLD level.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |
| 2577 | Rojan Chitrakar | 116/53 | 12.5.3.3.7 | "The PN shall be implemented as a 48-bit strictly increasing integer,..." Presumably the PN would not be incremented when a frame is re-transmitted by an MLD on the same link (baseline rule). The PN should not be incremented when the frame is re-transmitted by the MLD on another link to prevent the frame being dropped as replayed frame by the receiving MLD. | Clarify that the PN shall not be incremented when a frame is re-transmitted by the MLD on another link. | Revised. Agreed in principle.  Specify that a single GTK is used by the transmission of group addressed data frames over all links of MLD and a single corresponding PN check is performed at the MLD level.  11be editor: please incorporate the text changes in:  [https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed -resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0411-03-00be-proposed%20-resolution-to-11be-CID34-CIDs-on-GTK-for-MLO.docx) |

**Discussion:**

Per 11be D0.4 [1], each link of an MLD uses an independent GTK and PN check for the group addressed data frames delivery. In this submission, we propose to unify the multi-link delivery approach for both individually addressed data frames and group addressed data frames. Specifically, we propose to establish a single GTK per security domain at the MLD level, use such a single GTK on all links for the group addressed data frame delivery, and perform the corresponding PN check at the MLD level.

Our rationale are as follows:

**1. Using a single GTK for all links per security domain introduces no new security risk.**

In Fig. 1, we illustrate an example where an AP MLD hosts two SSIDs and uses a single GTK for all 3 links per security domain (e.g., SSID 2 = Guest). Because guest #1 and guest #2 are equally trusted by the host of SSID2, guest #1’s possession of the GTK on link 2 and link 3 of the MLD poses no greater risk than guest #2’s possession of the GTK on link 2 and link 3 of the MLD.

****

Fig. 1: Illustration of single GTK vs. multiple GTKs per security

**2. Using a single GTK on all links and a corresponding single PN check at the MLD level unifies the design for unicast and groupcast data frames delivery for MLO.**

The following methods are adopted by 11be for the delivery of individually addressed data frame for MLD.

* A single PTK and PN check at the MLD level for all links.
* Duplicate detection occurs before decryption/replay detection, as in the single-link case.
* Replacement of relevant and required link level address with relevant MLD MAC address during AAD construction. Use of relevant MLD MAC address as A2 for Nonce construction. (See [3])
* Block Ack agreement is established at the MLD level.
  + MLD level Block Ack agreement should be applied to GCR-BA for MLO as well.

Additionally, for reception over a single link, duplicate detection for unicast frames occurs before decryption/replay detection (note: no duplicate issue for groupcast frames), as depicted in Fig. 2. For reception over multiple links, duplicated group addressed data frames received over multiple links need to be detected, and it is desirable to maintain the same processing order (i.e., duplicate detection occurs before decryption/replay detection) for group addressed data frames. Given duplicate detection for MLO needs to occur at the MLD level, the PN check should occur at the MLD level as well, after duplicate detection, as depicted in Fig. 3.



Fig. 2: Receiver processing order for duplicate detection and Replay detection for SLO



Fig. 3: Desired receiver processing order for duplicate detection and Replay detection for MLO

As a result, using a single GTK on all links and a corresponding single PN check at the MLD level unifies the design for unicast and groupcast data frames delivery for MLO. See [2] for more details.

**Proposed resolution for CID 1874, 2287, 2288, 2314, 2476, 2533, 2534, 2536, 2577:**

***Editor’s note: Please modify the 11be spec as shown below. The proposed changes are with respect to 11be\_D0.4 [1].***

**12.5.3.3.7 CCM originator processing**

***Change the fifth paragraph as follows***

***Change the fifth paragraph as follows:***

The PN values sequentially number each MPDU. Each transmitter STA that is not affiliated with an MLD and each MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD for the PTKSA and the PN that is maintained by the AP MLD for the GTKSA. The PN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding temporal key is initialized or refreshed.

**12.5.5.3 GCMP cryptographic encapsulation**

**12.5.5.3.6 GCM originator processing**

***Change the sixth paragraph as follows:***

The PN values sequentially number each MPDU. Each transmitter STA that is not affiliated with an MLD and each MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD for the PTKSA and the PN that is maintained by the AP MLD for the GTKSA. The PN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding temporal key is initialized or refreshed.

**35.3.5.2 Multi-link security**

After successful multi-link (re)setup between a non-AP MLD and an AP MLD, a PMK is established and a PTK is derived through a 4-way handshake between the non-AP MLD and the AP MLD (see 12.7.6 (4-way handshake)). The PMK, PTK, and the same PN space are used for all the setup links between the non-AP MLD and the AP MLD for the PTKSA. The non-AP MLD and the AP MLD use their respective MLD address to derive the PMK under the SAE method and PTK.

All the setup links use a common GTK and a single PN space between the non-AP MLD and the AP MLD for the GTKSA. See 12.5.3.3.7 and 12.5.5.3.6. (CID-1874, 2287, 2288, 2314, 2476, 2533, 2534, 2536, 2577).

Different links use different IGTK/BIGTK and each link has its own corresponding PN space. The common GTK used by all setup links and the IGTK/BIGTK of each setup link with a given peer MLD are delivered to the non-AP MLD using a single 4-way handshake as defined in 12.7.6 (4-way handshake). (CID-1874, 2287, 2288, 2314, 2476, 2533, 2534, 2536, 2577).

**References**

[1] IEEE P802.11be™/D0.4, Draft standard for information technology – Telecommunications and information exchange between systems local and metropolitan area networks – Specific requirements Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, Amendment 9: Enhancements for extremely high throughput (EHT)

[2] IEEE 802.11-21/0041r3, “Group addressed data frame delivery methods for MLO”, Q. Wang, et al.

[3] IEEE 802.11-20/1545r1, “MLD security considerations”, G. Patwardhan, et al.