IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe CC-36 Security Comments |
| Date: 2021-08-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | montemurro.michael@gmail.com  |

Background

This contribution proposes comment resolutions to comments received in CC36 on Clause 12 of P802.11be D1.0. The resolutions will be shown relative to D1.0 and when indicated D1.1

CIDs 6305, 6712, 7442, 6040, 7445, 7446, 6044, 6717, 6172, 6046, 6173, 6719, 7451, 6047, 6048, 6049, 5183, 6583, 6584, 6595, 6596, 5900, 5659, 6050, 6052, 6051, 6053, 6594, 6597, 6598, 6721, 6722, 6600, 5649, 7486, 7458, 5981, 6204, 6727, 4011

Straw\_poll: Adopt the resolutions in document 11-21/1285r2 for CIDs 6305, 6712, 7442, 6040, 7445, 7446, 6044, 6717, 6172, 6046, 6173, 6719, 7451, 6047, 6048, 6049, 5183, 6583, 6584, 6595, 6596, 5900, 5659, 6051, 6053, 6594, 6597, 6598, 6721, 6722, 6600, 5649, 7486, 7458, 5981, 6204, 6727, 4011, and incorporate the changes into the TGbe draft.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6305 | 11.2.3.16.3 | 185.62 | is this WNM Sleep Mode Response frame protected or not? Please make it clear | as in the comment |
| 6712 | 11.2.3.16.3 | 185.60 | "If a GTK/IGTK/BIGTK update is in progress for one or more links, the pending GTK(s), IGTK(s), and BIGTK(s) for the affected link(s) shall be included in the WNM Sleep Mode Response frame." The baseline text was fine but after breaking out as a separate bullet, it should be clarified that this should be done only if RSN is used and management frame protection is applied. | Change as "If RSN is used with management frame protection and a valid PTK is configured between the MLDs, and if a GTK/IGTK/BIGTK update is in progress for one or more links, the pending GTK(s), IGTK(s), and BIGTK(s) for the affected link(s) shall be included in the WNM Sleep Mode Response frame." Alternatively, combine this bullet with the one before it. |

### Discussion:

Clause 11.2.3.16.2 describes WNM Sleep Mode requirements for a STA/non-AP MLD. The 11be D.1.0 adds the following text with the text in the preceding paragraph:

“WNM sleep mode enables an extended power save mode for non-AP STAs in which a non-AP STA need not listen for every DTIM Beacon frame, and need not perform GTK/IGTK/BIGTK updates. A non-AP STA can sleep for extended periods as indicated by the WNM Sleep Interval field of the WNM Sleep Mode element, which is present in WNM Sleep Mode Request frames transmitted by the non-AP STA.

A non-AP MLD identifies the link to which the GTK/IGTK/BIGTK belongs based on the Link ID subfield carried in the corresponding subelement of the Key Data field.”

Clause 11.2.3.16.3 describes WNM Sleep Mode requirements for the AP/AP MLD. The last paragraph in the baseline is:

“If RSN is used with management frame protection and a valid PTK is configured for the STA, the current GTK, IGTK, and BIGTK shall be included in the WNM Sleep Mode Response frame. If a GTK/IGTK/BIGTK update is in progress, the pending GTK, IGTK, and BIGTK shall be included in the WNM Sleep Mode Response frame. If RSN is used without management frame protection and a valid PTK is configured for the STA, the current GTK shall be sent to the STA using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame.

The 11be D1.0 changes that text to:

“

When the association is not a multi-link setup:

—If RSN is used with management frame protection and a valid PTK is configured for the STA, the current GTK, IGTK, and BIGTK shall be included in the WNM Sleep Mode Response frame.

—If a GTK/IGTK/BIGTK update is in progress, the pending GTK, IGTK, and BIGTK shall be included in the WNM Sleep Mode Response frame.

—If RSN is used without management frame protection and a valid PTK is configured for the STA, the current GTK shall be sent to the STA using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame.

When the association is a multi-link setup:

—If RSN is used with management frame protection and a valid PTK is configured between the MLDs, the current GTK, IGTK, and BIGTK for each the links shall be included in the WNM Sleep Mode Response frame.

—If a GTK/IGTK/BIGTK update is in progress for one or more links, the pending GTK(s), IGTK(s), and BIGTK(s) for the affected link(s) shall be included in the WNM Sleep Mode Response frame.

—If RSN is used without management frame protection and a valid PTK is configured for the STA, the current GTK for all the links shall be sent to the STA using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame.”

With respect to the first comment and relative to the baseline, there is no requirement for the STA and AP to establish RSNA in order to use WNM Sleep mode. However it’s not clear that the requirements for STA and AP for WNM Sleep apply to non-AP MLD and AP MLD respectively. It would be useful to add a statement in the introductory clause of 11.2.3.16.1 to state this requirement.

### Proposed Resolution: (6035, 6712)

Revised. WNM sleep mode does not require an RSNA or MFP. The Clause has been updated to articulate the requirements more clearly for AP MLD and non-AP MLD and the cited text has been updated to indicate that the requirements are applicable when an RSNA has been established. Incorporate the text changes given in <https://mentor.ieee.org/802.11/dcn/21/11-21-1285-01-00be-cc36-security-comment-resolutions.docx> for “Proposed Resolution: (6035, 6712)”

***Add a general statement for WNM Sleep with respect to MLO. Modify the last paragraph at the end of clause 11.2.3.16.1 as follows***

### WNM sleep mode enables an extended power save mode for non-AP STAs in which a non-AP STA need not listen for every DTIM Beacon frame, and need not perform GTK/IGTK/BIGTK updates. A non-AP STA can sleep for extended periods as indicated by the WNM Sleep Interval field of the WNM Sleep Mode element, which is present in WNM Sleep Mode Request frames transmitted by the non-AP STA.

For MLO, WNM sleep mode enables extended power save mode between an AP MLD and a non -AP MLD. The WNM Sleep Mode Request and Response frames are exchanged between the non-AP MLD and AP MLD through an affiliated STA and affiliated AP over a setup link.

NOTE – Each STA affiliated with a non-AP MLD maintains its own power-save state and power-save mode (see Clause 35.3.11)

***In 11.2.3.16.3, modify the cited text as follows:***

For non-MLO, if RSN is used and a valid PTK is configured for the STA:

—If management frame protection is negotiated for the STA, the current GTK, IGTK, and BIGTK shall be included in the WNM Sleep Mode Response frame.

—If a GTK/IGTK/BIGTK update is in progress, the pending GTK, IGTK, and BIGTK shall be included in the WNM Sleep Mode Response frame.

—If management frame protection is not negotiated for the STA, the current GTK shall be sent to the STA using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame.

For MLO, if RSN is used and a valid PTK is configured for the non-AP MLD:

—If management frame protection is negotiated for the non-AP MLDs, the current GTK, IGTK, and BIGTK for each setup link shall be included in the WNM Sleep Mode Response frame.

—If a GTK/IGTK/BIGTK update is in progress for one or more links, the pending GTK, IGTK, and BIGTK for each of the affected link(s) shall be included in the WNM Sleep Mode Response frame. A non-AP MLD identifies the corresponding link to which the GTK/IGTK/BIGTK belongs based on the value of the Link ID subfield included in the subelement of the Key Data field.

—If management frame protection is not negotiated for the non-AP MLD, the current GTK for each setup link shall be sent to the STA using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 7442 | 12.2.4 | 0.00 | "shall be included" - where? Means the TA shall be set to that value? | Clarify |

### Discussion:

The cited text is:

“When an RSNA is established between peer MLD SMEs, the MLD MAC address of the MLD transmitting the frame in an Authentication, Association, or EAPOL-key frames shall be included in that frame.”

It wording of the requirement could be improved. The frame is transmitted by an affiliated STA while the MLD MAC Address is carried in the frame body.

### Proposed Resolution: (7442)

Revised. The MLD MAC Address is included in the frame body and is transmitted by a STA affiliated with the MLD. In 12.2.4, replace

“When an RSNA is established between peer MLD SMEs, the MLD MAC address of the MLD transmitting the frame in an Authentication, Association, or EAPoL-key frames shall be included in that frame.”

With

“When an RSNA is established between peer MLD SMEs, the MLD MAC address shall be included in the frame body of Authentication, Association (see 9.4.2.295b) and EAPOL-key frames (see 12.7.2).

NOTE—These frames are transmitted by a STA affiliated with the MLD.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6040 | 12.3.3.1 | 209.39 | The authentication frames are exhcnaged between MLDs through affiliated STAs. | update the text accordingly |

### Discussion:

The cited text is

“For MLO a non-AP MLD and AP MLD shall complete an IEEE 802.11 authentication prior to association through the exchange of Authentication frames between an affiliated STA and affiliated AP, respectively.”

The text could be improved to state that the frames are transmitted by the affiliated STA and AP, respectively.

### Proposed Resolution: (6040)

Revised. The text has been clarified in the direction proposed by the commenter. Replace

“For MLO a non-AP MLD and AP MLD shall complete an IEEE 802.11 authentication prior to association through the exchange of Authentication frames between an affiliated STA and affiliated AP, respectively.”

With

“For MLO, a non-AP MLD and AP MLD shall complete IEEE 802.11 authentication exchange prior to association. The Authentication frames for MLO are transmitted between the non-AP MLD and AP MLD through an affiliated STA and affiliated AP, respectively.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 7445 | 12.4.1 | 0.00 | what is a "STA entity" (ies)? | Use existing terminology, or clearly define this new terminology |
| 7446 | 12.4.3 | 0.00 | what is an "SAE entity" (different to STA entity?) Note that this change deprecates references to "peer" in the text which is well understood | Use existing terminology, or clearly define this new terminology |

### Discussion:

The term “SAE entity” is used throughout clause 12.4 and is defined in clause 3.1 (see 37.36)

The definition is:

“**simultaneous authentication of equals (SAE) entity:** an entity that is a station (STA) or an multi-link device (MLD) that participates in SAE authentication (see 12.4 (Authentication using a password)).”

So, the new terminology seems to be clearly defined.

### Proposed Resolution: (7445, 7446)

Rejected. The term “SAE Entity” is clearly defined in 3.1 (see D1.1 page 37, line 36) and is used throughout clause 12.4 to describe peer behavior in the SAE protocol.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6044 | 12.5.3.3.7 | 217.48 | The first sentence of the paragraph mentioned that a MLD maintains a GTK. The following sentence mentioend that each STA of MLD maintains a PN for GTK. They contradcit with each other. | Fix the issue. |
| 6717 | 12.5.3.3.7 | 217.49 | "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" Since an MLD only maintains a single GTKSA, this gives the impression that a single PN is maintained by an MLD for the GTKSA but 11be has passed motion (Motion 71) explicitly stating that different GTKs and corresponding PN spaces are maintained for different links. | For better clarity, split the sentences for non-MLD and MLD cases as: "Each transmitter STA that is not affiliated with an MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each transmitting MLD shall maintain a single PN (48-bit counter) for each PTKSA and each STA affiliated with a transmitter MLD shall maintain a single PN (48-bit counter) for each GTKSA. |
| 6172 | 12.5.3.3.7 | 217.48 | Clarify that the MLD maintains the PN for PTKSA and the affiliated STA maintains the PN for GTKSA. | At the cited location in 12.5.3.3.7:At 217.49, change "Each transmitter STA that is not affiliated with an MLD and each MLD"to"Each STA"At 217.50, change "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."To"Each MLD shall maintain a single PN for each PTKSA. Each STA that is affiliated with an MLD shall maintain a single PN for the GTKSA." |

### Discussion:

The cited text for these comments is:

“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 affiliated with the AP MLD for the GTKSA.”

It would be clearer to separate transmitter STA and MLD in the first cited sentence into two requirements.

### Proposed Resolution: (6044, 6172, 6717)

Revised. The text has been updated to clarify the requirements for a STA, an MLD, and an affiliated STA.

Change

“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 affiliated with the AP MLD for the GTKSA.”

To

“Each transmitter STA that is not affiliated with an MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each MLD shall maintain a single PN (48-bit counter) for each PTKSA. Each AP affiliated with an AP MLD shall maintain a single PN (48-bit counter) for each GTKSA. Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6046 | 12.5.5.3.6 | 220.06 | The first sentence of the paragraph mentioned that a MLD maintains a GTK. The following sentence mentioend that each STA of MLD maintains a PN for GTK. They contradcit with each other. | Fix the issue. |
| 6173 | 12.5.5.3.6 | 220.06 | This should just be MLD AP | At 220.6, change "Each transmitter STA that is not affiliated with an MLD and each MLD"To"Each STA"At 220.8, change "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."To"Each MLD shall maintain a single PN for each PTKSA. Each STA that is affiliated with an MLD shall maintain a single PN for the GTKSA." |
| 6719 | 12.5.5.3.6 | 217.06 | "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." Since an MLD only maintains a single GTKSA, this gives the impression that a single PN is maintained by an MLD for the GTKSA but 11be has passed motion (Motion 71) explicitly stating that different GTKs and corresponding PN spaces are maintained for different links. | For better clarity, split the sentences for non-MLD and MLD cases as: "Each transmitter STA that is not affiliated with an MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each transmitting MLD shall maintain a single PN (48-bit counter) for each PTKSA and each STA affiliated with a transmitter MLD shall maintain a single PN (48-bit counter) for each GTKSA. |

### Discussion:

The cited text for these comments is:

“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 affiliated with the AP MLD for the GTKSA.”

It would be clearer to separate transmitter STA and MLD in the first cited sentence into two requirements in separate sentences.

### Proposed Resolution: (6046, 6173, 6719)

Revised. The text has been updated to clarify the requirements for a STA, an MLD, and an affiliated STA.

Change

“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 affiliated with the AP MLD for the GTKSA.”

To

“Each transmitter STA that is not affiliated with an MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each MLD shall maintain a single PN (48-bit counter) for each PTKSA. Each AP affiliated with an AP MLD shall maintain a single PN (48-bit counter) for each GTKSA. Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 7451 | 12.6.1.1.2 | 0.00 | "... and the peer's (Supplicant's) MAC address..." - this seems to be irrelevant since the baseline text only binds a PMKSA to the Authenticator's MAC address (or the peer device for mesh), not to the Supplicant's MAC address (same comment in 12.6.1.1.6) | Remove references to supplicant's MAC in these definitions |

### Discussion:

The cited text is:

“Authenticator’s or peer’s MAC address. For multi-band RSNA, the MAC address is associated with the operating band in use when the PMKSA is established. For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD and the peer’s (Supplicant’s) MAC address is the MLD MAC address of the non-AP MLD.”

After reviewing the content and evolution of the referenced text in IEEE 802.11-2007, 802.11-2012, 802.11-2016, and 802.11-2020, the cited text does not refer to the supplicant.

### Proposed Resolution: (7451)

Revised. The cited text in the base standard only refers to the Authenticator MAC address and a statement about the Supplicant’s MLD MAC address is not required.

Change “For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD and the peer’s (Supplicant’s) MAC address is the MLD MAC address of the non-AP MLD.”

To

“For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6047 | 12.6.1.1.6 | 221.51 | update the bullet so that this bullet is applied when at least one peer is non-MLD | As in comment |
| 6048 | 12.6.1.1.6 | 221.52 | update the bullet so that this bullet is applied when at least one peer is non-MLD | AS in comment |
| 6049 | 12.6.1.1.6 | 221.53 | update the bullet so that this bullet is applied when the peers are both MLDs | AS in comment |

### Discussion:

The cited text is:

“—Supplicant MAC address or STA’s MAC address

—Authenticator MAC address or BSSID

—For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD and the Supplicant’s MAC address is the MLD MAC address of the non-AP MLD.”

Multi-link operation (MLO) only occurs between MLDs. Any security association involving a legacy STA or legacy AP does not involve MLO. A non-MLD cannot establish a security association with an MLD.

### Proposed Resolution: (6047, 6048, 6049)

Rejected. Multi-link operation is only specified between an AP MLD and a non-AP MLD. If a security association is established between an MLD and a legacy STA, the MLD would authenticate and associate with the legacy STA as a legacy STA. Therefore, further clarification for the PTKSA is not required.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 5183 | 12.6.10.2 | 223.01 | Any update to preauthentication? For example, allow to do the preauthentication via the air. Or clarify why only the preauthentication via the DS is allowed | As in comment. |

### Discussion:

Pre-authentication is defined in 12.6.10.2. The pre-authentication behavior described for a STA and AP are summarized in the following text:

“A Supplicant may initiate preauthentication when it has completed the 4-way handshake and configured the required temporal key(s). To effect preauthentication, the Supplicant sends an EAPOL-Start frame with the DA being the BSSID of a targeted AP’s BSS and the RA being the BSSID of the BSS of which it is a member. The target AP shall use a BSSID equal to the MAC address of its Authenticator. As preauthentication frames do not use the IEEE 802.1X EAPOL Ethertype field, the AP with which the STA is currently associated need not apply any special handling. The AP and the MAC in the STA shall handle these frames in the same way as other frames with arbitrary Ethertype field values that require distribution via the DS.

An AP’s Authenticator that receives an EAPOL-Start frame via the DS may initiate IEEE 802.1X authentication to the STA via the DS. The DS forwards this message to the AP with which the STA is associated.”

For MLO, the non-AP MLD would need to set the DA to the address of the AP MLD. The SA address is the address of the non-AP MLD. The AP MLD Authenticator would still receive an EAPOL-Start frame via the DS and initiate IEEE 802.1X authentication with the non-AP MLD via the DS. The DS would forward the messages between the non-AP MLD and AP MLD.

### Proposed Resolution: (5183)

Revised. Pre-authentication is possible between a non-AP MLD and AP MLD. Incorporate the changes under “Proposed Resolution: (5183) in <this> document.

***Make the following modifications to clause 12.6.10.2:***

A Supplicant may initiate preauthentication when it has completed the 4-way handshake and configured the required temporal key(s). To effect preauthentication, the Supplicant sends an EAPOL-Start frame with the DA being the BSSID of a targeted AP’s BSS and the RA being the BSSID of the BSS of which it is a member. The target AP shall use a BSSID equal to the MAC address of its Authenticator. As preauthentication frames do not use the IEEE 802.1X EAPOL Ethertype field, the AP with which the STA is currently associated need not apply any special handling. The AP and the MAC in the STA shall handle these frames in the same way as other frames with arbitrary Ethertype field values that require distribution via the DS.

An AP’s Authenticator that receives an EAPOL-Start frame via the DS may initiate IEEE 802.1X authentication to the STA via the DS. The DS forwards this message to the AP with which the STA is associated.

For MLO, the non-AP MLD may initiate pre-authentication by sending an EAPOL-Start frame with the DA being the address of the AP MLD. The AP MLD Authenticator would receive an EAPOL-Start frame via the DS and initiate IEEE 802.1X authentication with the non-AP MLD via the DS. The DS would forward the messages between the non-AP MLD and AP MLD.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6595 | 12.6.2 | 222.12 | "at last one common AKM" needs to be changed to "at least one common AKM" | change "at last" to "at least" |

### Discussion:

Trivial typo fix

### Proposed Resolution: (6595)

Accepted.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6583 | 12.6.2 | 222.03 | Define RSNA rekeying requirements and MLME-PN-WARNING operation with MLO, also considering common PTK and per-link GTK |   |
| 6584 | 12.6.2 | 222.03 | If dot11RSNAConfigGroupRekeyTime and time-based refresh is still relevant, and if GTK is going to be per-link it seems GTK refresh periods need to be the same for any security-based reasonNote: (1) No issue if GTK is common to all links, (2) time-based refresh seems to be only in Annex C in baseline now. |   |

### Discussion:

The cited clause, 12.6.2, covers RSN Selection. This comment seems to refer to 12.6.21 (RSNA rekeying), and in particular, the following paragraph:

“The IEEE 802.11 MAC shall issue an MLME-PN-WARNING.indication primitive when the packet number assignment for a particular PTKSA, IGTKSA, GTKSA or BIGTKSA reaches or exceeds the threshold that is defined in dot11PNWarningThresholdLow and dot11PNWarningThresholdHigh for the first time. The indication shall be issued only once for a given PTKSA, IGTKSA, GTKSA or BIGTKSA. The SME may use the indication as a trigger to establish a new PTKSA, IGTKSA, GTKSA or BIGTKSA before the Packet Number space is exhausted.”

In the baseline, the last paragraph of 12.6.14 (RSNA key management in an infrastructure BSS) describes the group key exchange:

“A second key exchange, the group key handshake, is also defined. It distributes a subsequent GTK. The AP’s Authenticator can use the group key handshake to update the GTK at the Supplicant. The group key handshake uses the EAPOL-Key frames for this exchange. When it completes, the Supplicant can use the MLMESETKEYS.request primitive to configure the GTK into the IEEE 802.11 MAC.”

This clause has not been modified by P802.11be. It mentions the Authenticator and Supplicant behavior for managing the PMK, the 4-way handshake and the group key handshake but at this point does not mention that for MLO, the pairwise keys are managed by the AP MLD while the group keys are managed by the Affiliated AP. This clause could be updated to address the above comments. It would also be good to make a clarification in both clause 12.6.14 to address GTK distribution with MLO and 12.6.21, to clarify that with MLO, the affiliated AP manages the group key updates.

With respect to the security issue, APs that operate in an ESS do not synchronize GTK updates and this does not compromise security. The process would be similar for MLO.

### Proposed Resolution: (6583, 6584)

Revised. The draft has been updated to clarify that the affiliated APs manage group key updates and the group key exchange between the AP MLD and non-AP MLD is triggered by the affiliated AP. Incorporate the changes under “Proposed Resolution: (6583, 6584)” in <this> document.

***In clause 12.6.14, add the following paragraph at the end of the clause:***

“For MLO, the AP MLD Authenticator and non-AP MLD Supplicant manage the PMK and pairwise key derivation. Both the 4-way handshake and group key handshake take place between the AP MLD Authenticator and the non-AP MLD Supplicant. The affiliated APs manage the group keys for their respective links. When group key update is triggered, the affiliated AP distributes the group key to STAs affiliated with a non-AP MLD through a group key handshake between the AP MLD and the non-AP MLD.”

***In clause 12.6.21, add the following paragraph after the 3rd paragraph:***

“For MLO, the AP MLD authenticator manages packet number assignment for the PTKSA with a non-AP MLD. For a given link, the affiliated AP authenticator manages packet number assignment for the IGTKSA, GTKSA or BIGTKSA. If an IGTKSA, GTKSA or BIGTKSA update is triggered, the affiliated AP updates group keys for the given link through a group key handshake between the AP MLD and non-AP MLD.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6596 | 12.6.3.2 | 222.63 | "APs affiliated with the AP MLD shall use the group cipher suite indicated by the non-AP MLD in the (Re)Association Request frame" This sentence is unnecessary becaues AP affiliated with AP MLD does not need to change group cipher suite after each individual association. | Delete "APs affiliated with the AP MLD shall use the group cipher suite indicated by the non-AP MLD in the (Re)Association Request frame" |

### Discussion:

The cited text in D1.0 is as follows:

“If an AP MLD Authenticator receives a (Re)Association Request frame that includes an RSNE and if it chooses to accept the association as a secure association, then it shall use the AKM suite and pairwise cipher suite in the (Re)Association Request frame to establish an RSNA with a non-AP MLD. APs affiliated with the AP MLD shall use the group cipher suite indicated by the non-AP MLD in the (Re)Association Request frame.”

The group cipher is the same for all links. The Supplicant needs to provide both the pairwise cipher and group cipher in the RSNE included in the (re-)association request and the AP MLD maintains the PTKSA while the affiliated APs maintain the GTKSA. The sentence can be deleted but the behavior needs to be captured.

### Proposed Resolution: (6596)

Revised. The cited sentence needs to be deleted but the behavior for negotiating the group cipher needs to be clarified.

At 244.59 relative to D1.1. replace:

“If an AP MLD Authenticator receives a (Re)Association Request frame that includes an RSNE and if it chooses to accept the association as a secure association, then it shall use the AKM suite and pairwise cipher suite in the (Re)Association Request frame to establish an RSNA with a non-AP MLD. APs affiliated with the AP MLD shall use the group cipher suite indicated by the non-AP MLD in the (Re)Association Request frame.”

With

“If an AP MLD Authenticator receives a (Re)Association Request frame that includes an RSNE and if it chooses to accept the association as a secure association, then it shall use the AKM suite and pairwise cipher suite in the (Re)Association Request frame to establish an RSNA with a non-AP MLD. The AP MLD manages the PTKSA while the affiliated APs manage the GTKSA.”

Also clarify the non-AP MLD behavior, at 244.30, replace

“For MLO, the initiating non-AP MLD’s RSNE shall include one AKM suite selector and one pairwise cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD in its MLD Probe Response frame. It shall also specify the group cipher suite specified by the targeted AP.”

With

“It shall also specify the group cipher suite specified by the targeted AP. For MLO, the initiating non-AP MLD’s RSNE shall include one AKM suite selector, one pairwise cipher suite selector, and one group cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD. A non-AP MLD would determine the appropriate AKM suite selector and pairwise cipher suite selector during MLO discovery by monitoring Beacon frames transmitted by APs affiliated with the AP MLD or performing basic probing with each AP affiliated with the AP MLD or by performing ML probing with one or more APs affiliated with the AP MLD.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 5900 | 12.7.1.3 | 233.38 | "For the rest of this clause and within the context of protecting individually addressed communications between the two MLDs, AA shall be set to the AP MLD MAC address and SPA shall be set to the non-AP MLD MAC address."This statement does not seem to cover baseline 12.7.1.6 FT, and 12.7.8 TPK | add statements to say S/R1KH-D in 12.7.1.6.4, BSSID, STA-ADDR in 12.7.1.6.5, MAC\_I/R in 12.7.8.2 are also MLD addresses when applicable |

### Discussion:

In D1.1, Clause 12.7.1.1, the general clause, there is the following statement:

“Between an AP MLD and a non-AP MLD, the IEEE 802.1X Authenticator MAC address (AA) and the MLD MAC address of the AP MLD are the same, and the Supplicant’s MAC address (SPA) and the MLD MAC address of the non-AP MLD are equal”

This could be worded more like a requirement but it seems to be a better place to specify this requirement and would cover 12.7.1.6.4, 12.7.1.6.5, and 12.7.8.2. the cited text could then be deleted.

### Proposed Resolution: (5900)

Revised. There is a statement in 12.7.1.1 regarding the AA and SPA addresses but it is not worded as a requirement. The cited text has been deleted and moved to 12.7.1.1.

Relative to D1.1, at 245.12, change:

“Between an AP MLD and a non-AP MLD, the IEEE 802.1X Authenticator MAC address (AA) and the MLD MAC address of the AP MLD are the same, and the Supplicant’s MAC address (SPA) and the MLD MAC address of the non-AP MLD are equal.”

To

“Between an AP MLD and a non-AP MLD, the IEEE 802.1X Authenticator’s MAC address (AA) shall be set to the MLD MAC address of the AP MLD, and the Supplicant’s MAC address (SPA) shall be set to the MLD MAC address of the non-AP MLD.”

At 245.36, delete “For a non-AP MLD associated with an AP MLD, the Supplicant is the non-AP MLD and the Authenticator is the AP MLD. For the rest of this clause and within the context of protecting individually addressed communications between the two MLDs, AA shall be set to the AP MLD MAC address and SPA shall be set to the non-AP MLD MAC address.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 5659 | 12.7.2 | 225.54 | 4-way handshake message 3 validation step for A2 is described for Authenticator while message 3 is sent to Supplicant. This does not make sense and is likely a copy-paste error. | Replace "For MLO, the Authenticator's SME validates" with "For MLO, the Supplicant's SME validates" |

### Discussion:

After review, it is the supplicant, not the authenticator that validates 4-way handshake message 3 on receipt.

### Proposed Resolution: (5659)

Accepted.

Note to Editor: Relative to D1.1, the cited location is at 247.59.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6050 | 12.7.2 | 225.13 | the link Id + related address in Association Request that is not accepted need not be in EAPOL-Key 2. | As in comment |
| 6052 | 12.7.2 | 225.13 | the link Id + related address in Association Request that is not accepted need not be verified. | As in comment |

### Discussion:

In the 4-way handshake for legacy devices, the Supplicant includes the RSNE and RSNXE in message 2 so that Authenticator can verify that information (RSNE and RSNXE) supplied by the Supplicant in the Reassociation Request. In the case of MLO, the Authenticator also needs to verify that the link information provided by the non-AP MLD Supplicant in the Reassociation Request (Affiliated STA MAC Address, RSNE and RSNXE). This helps prevent against man-in-the-middle attacks (see 12.7.6.8) in the base standard.

At the time that the non-AP MLD Supplicant provides the link ID, related MAC address, RSNE, and RSNXE in the Reassociation Request, there is no indication that a link is not accepted by the AP MLD. The information supplied in message 2 must be the same as supplied in the Reassociation Request to be verified. Note that the Reassociation request is not protected.

### Proposed Resolution: (6050, 6052)

Rejected. The non-AP MLD supplicant needs to provide the link ID and related address in Message 2 of the 4-way handshake so that the Authenticator can validate the information and to guard against man-in-the-middle attacks.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6051 | 12.7.2 | 225.21 | The validation of Address 2 should not be the matching of an affiliated STA MAC address included in one of the MLO Link KDEs. The accurate matching (the link where the frame is transmitted) is needed. | As in comment |

### Discussion:

The cited paragraph requires the Authenticator to verify that Address 2 (the TA) matches one of the links included in the MLO Link KDEs (since the contents of the EAPOL-Key are MIC’d). This allows the Authenticator to ensure that the frame from the Supplicant was received on one of the non-AP MLD affiliated STA links.

### Proposed Resolution: (6051)

Rejected. The comparison ensures that the frame was received by a STA affiliated with the non-AP MLD. There is no link information provided in the frame body other than the MLO Link KDEs.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6053 | 12.7.2 | 225.54 | supplicant may not know the Beacons of each link. | Change the text according to the comment. |

### Discussion:

The cited sentence is: “For MLO, the Supplicant’s SME shall validate the security configuration for each LinkID field, affiliated AP MAC address, RSNE, and RSNXE for each affiliated AP link included in message 3 against the affiliated AP MAC address, RSNE, and RSNXE received for each link in Beacons, Probe Response, and ML Probe Response frames.”

For message 3, the non-AP MLD Supplicant is validating the MAC Address, RSNE, and RSNXE supplied by the AP MLD during network discovery. The information can be obtained from Beacons, Probe Responses, or ML Probe Responses. The “and” in the cited sentence should be an “or”

### Proposed Resolution: (6053)

Revised. The information supplied by the Supplicant in message 3 could be obtained through the receipt of Beacon, Probe Response, or ML Probe Response frames

At 247.52 relative to D1.1, change “for each link in Beacons, Probe Response, and ML Probe Response frames” to “for each link in Beacon, Probe Response that is not an ML probe response, or Probe Response frame that is an ML probe response frame.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6594 | 12.7.2 | 226.53 | We need to have RSNEInfo bit in Link information field of MLO Link KDE because RSNE is not needed when sent by supplicant since RSNE is the same in all the links for supplicant and is already covered by RSNE in message 2. | Add RSNEInfo bit in Link information field of MLO Link KDE. |

### Discussion:

After review, the MLO Link KDE should include a bit to signal the presence of the RSNE in the KDE.

### Proposed Resolution: (6594)

Revised. Add an RSNE Info bit to signal the presence of the RSNE in the MLO Link KDE. Incorporate the changes under “Proposed Resolution: (6594)” in <this> document.

***Relative to D1.1 at 248.56, replace Figure 12-47d with:***

“

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | LinkID | RSNEInfo | RSNXEInfo | Reserved |
| bits: | 4 | 1 | 1 | 2 |

“

 ***At 248.65, inset the following sentence as a new paragraph:***

“The RSNEInfo field indicates that the RSNE is present in the MLO Link KDE when its value is equal to 1, otherwise the RSNE is not present.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6597 | 12.7.6.1 | 229.13 | "For MLO, the RSNE is present in the MLO LinkKDE." This sentence is not true for supplicant because supplicant has the same RSNE in all links.. | Revise as "For AP MLD, the RSNE is present in the MLO Link KDE." |
| 6598 | 12.7.6.1 | 229.29 | "For MLO, the RSNXE is present in the MLO Link KDE." This sentence is not true for the supplicant because supplicant has the same RSNXE in all links. | Revise as "For AP MLD, the RSNXE is present in the MLO Link KDE." |

### Discussion:

The cited text for these comments is the following:

229.13: “RSNE represents the appropriate RSNEs. For MLO, the RSNE is present in the MLO Link KDE.”

229.29: “For MLO, the RSNXE is present in the MLO Link KDE.”

With both cases for the AP MLD, the RSNE is contained within the MLO Link KDE. Therefore the suggested text is more accurate.

### Proposed Resolution: (6859, 6860)

Accepted.

Note to Editor: Relative to D1.1, the locations are 251.21 and 251.36.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6721 | 12.7.4 | 228.09 | Since an STA can maintain multiple GTKs, IGTKs and BIGTKs with different Key IDs, the MLO GTK/IGTK/BIGTK should also identify the associated Key ID as is done for GTK/IGTK/BIGTK. | Change the notations as MLO GTK[N], MLO IGTK[M] and MLO BIGTK[Q] and modify the descriptions accordingly by adding ", with the key identifier set to N/M/Q" |

### Discussion:

In clause 12.7.4 of the base standard, the GTK, IGTK, and BIGTK notation definitions included the key ID as part of the notation. In the base 4-way handshake message 3, the PN for the GTK is carried in the KeyRSC field so it may have made more sense to include the KeyID as an argument to the GTK KDE. For the MLO KDEs, the key ID and PN are contained within the KDE definitions, so the notation does not require an argument as part of the notation. This is probably true for the IGTK and BIGTK.

Furthermore, since there is an MLO KDE per link, the N/M/Q parameters would likely be different for different links, making the notation even more complex.

### Proposed Resolution: (6721)

Rejected. The Key ID and PN in the MLO KDE for each GTK, IGTK, and BIGTK is contained within the definition of the KDE itself, therefore there is no reason to include the KDE as an argument in the EAPOL-key notation.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6722 | 12.7.5 | 228.20 | Definition of a\_n is not clear enough; can the same MLO KDE (e.g. MLO GTK) occur multiple times for the same link, e.g. for different Key IDs. | Allow the same MLO KDE (e.g. MLO GTK) to occur multiple times for the same link (and not just for different links), e.g. for different Key IDs. |

### Discussion:

The cited definition of “an” in the EAPOL-key notation can be found at 250.26 in D1.1 and is:

“ “an” means that the KDE could occur multiple times in the field for n links.”

There can only be a single MLO GTK per link and there is only one Key ID passed from the Authenticator to the Supplicant in the 4-way handshake or group key handshake. Therefore the MLO GTK KDE can only occur once per link (similar to the GTK)

### Proposed Resolution: (6722)

Rejected. There is only one MLO GTK per link passed from the Authenticator to the Supplicant in the 4-way handshake or the group key handshake. The “n” notation is defined clearly to indicate that there can be an MLO GTK per link.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6600 | 12.7.6.1 | 228.43 | Based on my search in the spec, MAC address KDE is only used to carried MLD MAC address. Change the name of MAC address KDE to MLD MAC address KDE. | Change the name of MAC address KDE to MLD MAC address KDE. Update the description in the table of KDE. |

### Discussion:

The MAC Address KDE is defined in the base standard and carries a MAC address. See Table 12-9 and Figure 12-37 of IEEE 802.11-2020

Since the MLD MAC address is a MAC address and there is no ambiguity in the 4-way handshake introduced in re-using the MAC Address KDE, there is no need to create a new KDE. Furthermore, the MAC Address KDE may be used in future amendments (e.g. P802.11bi, for different purposes).

### Proposed Resolution: (6600)

Rejected. The MAC Address KDE is already defined in the base standard and is suitable for use in carrying the MLD MAC Address. It is not used for any other purpose in the 4-way handshake. Also, the description for the use of this KDE in the 4-way handshake to carry the MLD MAC address is clearly described in Clause 12.7.4 (see 249.58 of D1.1).

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 5649 | 3.1 | 37.31 | The definition of simultaneous authentication of equals (SAE) entity is an 802.11 specific definition and does not belong in clause 3.1. The introduction of SAE entity does improve the readability of clause 12. But, note that if an MLD is defined to be a STA (as suggested in other comments), there is no need to introduce the concept of the SAE entity or change the text in clause 12. | Either move the definition of SAE entity to clause 3.2 or if an MLD is defined to be a STA (as suggested in other comments), delete the definition and remove SAE entity from the amendment. |
| 7486 | 3.1 | 37.32 | The definition of SAE entity seems to be better described in 12.4, as SAE itself is not defined in 3.1. | As in comment. |

### Discussion:

The cited definition can be found in Clause 3.1 (D1.1 37.36) and is:

“**simultaneous authentication of equals (SAE) entity:** an entity that is a station (STA) or an multi-link device (MLD) that participates in SAE authentication (see 12.4 (Authentication using a password)).”

Currently in P802.11be, an MLD is defined as an entity that is distinct from a STA and the definition of SAE entity is an 802.11 specific definition, so it should be moved to Clause 3.2. Clause 3.2, not Clause 12, is the appropriate clause to define such a term.

### Proposed Resolution: (5649, 7486)

Revised. An SAE entity is a definition that is specific to 802.11 and should be moved from Clause 3.1 to Clause 3.2. The definition has a reference to Clause 12.4, where the term is used.

Move the cited definition to Clause 3.2 in the appropriate position.

Note to Editor: In the cited definition, change “an multi-link” to “a multi-link”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 7458 | 35.3.5.2 | 0.00 | "derive the PMK under the SAE method and PTK" - sentence has grammar issues, and it is unclear why it is specific to SAE | Fix, generalize, clarify or delete |
| 5981 | 35.3.5.2 | 256.09 | PTK derivation will use link addres also. | AS35.3.5.2 |
| 6204 | 35.3.5.2 | 256.04 | The first paragraph of this clause is redundant with the details described in Clause 12 and should be modified to describe the security association. | Make the changes described in https://mentor.ieee.org/802.11/dcn/21/11-21-0788-00-00be-tgbe-cc34-cids-2476-3133.docx |

### Discussion:

In D1.1, the cited text is:

“After a successful multi-link (re)setup between a non-AP MLD and an AP MLD, a PMKSA and PTKSA are established between the non-AP MLD and the AP MLD (see Clause 12 (Security)). The PTKSA is used for cryptographic encapsulation across all setup links as described in 12.5.3.3 (CCMP cryptographic encapsulation) and 12.5.5.3 (GCMP cryptographic encapsulation).”

The text was updated after D1.0 was made available and incorporates the text suggested in document 11-21/788. It makes no mention of SAE or PTK derivation.

### Proposed Resolution: (7458, 5981, 6204)

Revised. The text has already been updated in D1.1 through the acceptance of <https://mentor.ieee.org/802.11/dcn/21/11-21-0788-01-00be-tgbe-cc34-cids-2476-3133.docx>. There are cross-references to Clause 12 and no mention of SAE.

Note to Editor: No updates to the draft are required.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6727 | 35.3.5.2 | 256.11 | Clause 12.7.7 (Group key handshake) should also be expanded to allow delivery of the GTK/IGTK/BIGTK of other setup links using a single group key handshake. | Expand Clause 12.7.7 (Group key handshake) to allow delivery of the GTK/IGTK/BIGTK of other setup links using a single group key handshake. |

### Discussion:

The cited text in D1.1 is the following:

“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). *When a GTK/IGTK/BIGTK update is triggered for an AP affiliated with the AP MLD, the updated GTK/IGTK/BIGTK may be delivered to the non-AP MLD using the Group key handshake over any enabled link as defined in 12.7.7 (Group key handshake)*.

The italized text above was added through the acceptance of <https://mentor.ieee.org/802.11/dcn/21/11-21-0300-03-00be-crs-for-d0-3-group-key-handshake-cids.docx>. Clause 12.7.7 allows for the delivery of group keys for multiple links using a single group key handshake.

### Proposed Resolution: (6727)

Revised. The text has already been updated in D1.1 through the acceptance of <https://mentor.ieee.org/802.11/dcn/21/11-21-0300-03-00be-crs-for-d0-3-group-key-handshake-cids.docx>. The updated text makes reference to Clause 12.7.7 which allows a single group key handshake to be used to update group keys for multiple links.

Note to Editor: No updates to the draft are required.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 4011 | 9.4.2.47 | 121.55 | Clause 9.4.2.47 needs to be updated to include the GTK/IGTK/BIGTK for other link(s). | As in comment |

### Discussion:

Clause 9.4.2.47 defines the FT element. This element needs to be updated for MLO so that it can carry the KDEs defined for the 4-way handshake in the FT Protocol.

A contribution was recently accepted that updated this clause: <https://mentor.ieee.org/802.11/dcn/21/11-21-0971-03-00be-pdt-for-fast-ml-transition.docx>. (See motion 224)

### Proposed Resolution: (4011)

Revised. The additional elements for MLO update clause 9.4.2.47 for the FT element as described in Part 1 of <https://mentor.ieee.org/802.11/dcn/21/11-21-0971-03-00be-pdt-for-fast-ml-transition.docx>.

Note to Editor: This contribution has been approved in Motion 224 so no further changes required for the draft.