IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 CRs for 10.71.8 |
| Date: 2025-07-04 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry | Cisco Systems |  |  | jerhenry@cisco.com |
| Domenico Ficara | Cisco Systems |  |  | dficara@cisco.com |
| Ugo Campiglio | Cisco Systems |  |  | ucampigl@cisco.com |
| Javier Contreras | Cisco Systems |  |  | jacontre@cisco.com |

Abstract

This submission proposes resolutions for the following CIDs:

615, 632, 612, 319, 98, 105, 829, 361, 611, 363, 613, 614, 362, 640, 641, 839, 135, 136, 137, 259.

Revisions:

* Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D1.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D1.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 615 | 10.71.8 | 0.00 | "Privacy Beacons" should be "Privacy Beacon frames" (4x). Also "Privacy Beacon" when not followed by "frame" | As it says in the comment | Revised TGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 615 |
| 632 | 10.71.8 | 0.00 | There are references to "identity key" or "Identity Key" but it is not clear what this is. Is it an alias for the PGTK, perhaps? | As it says in the comment | RejectedThere is no line associated with this CID, so it is unclear if it points to a specific iteration of Identity Key. The term is explained at pp 105-6 and 106-24 (in d1.2) |
| 612 | 10.71.8 | 94.01 | "named as a BPE group" is weird | Change to "called a BPE group" with "BPE group" italicised | AcceptedThis is not 94.01, but 94.18.TGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 612 |
| 319 | 10.71.8 | 94.04 | Title "BSS Privacy Operations" is missing the word "Enhancements" | change title to "BSS Privacy Enhancements Operations" | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 319 |
| 98 | 10.71.8 | 94.07 | "...protect privacy...", Should be "protect the privacy | At cited location "protect the privacy" | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 98 |
| 105 | 10.71.8 | 94.07 | As dicussed in the requirement, mobile AP MLD may support BPE EDP features, non-mobile AP MLD does not have the stated privacy issue, so BPE EDP features should apply only to mobile MP MLD. Otherwise some of the current design decisions do not make sense, e.g., "A Privacy Beacon frame shall not contain a Multiple BSSID element". | Add "A BPE AP MLD shall be a mobile AP MLD". | RejectedThe requirements do not forbid a non-mobile AP from supporting this feature. The case of of home or small shop APs was discussed as well. The contributions describing roaming for BPE APs does not macth well thenmobile AP case. Multiple BSSID in the Privacy beacon fram might inform an eavesdropper and defeat the BPE purpose. |
| 829 | 10.71.8 | 94.09 | Phrasing "clear over the air" does not seem clear. | Change to "over the air in the clear." | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 829 |
| 361 | 10.71.8 | 94.14 | Missing article: "MLDs that have preshared identity key" | Change to: "MLDs that have the preshared identity key" | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/XXX under all headings that include CID 361 |
| 611 | 10.71.8 | 94.14 | "have preshared identity key of the BPE AP MLD" -- grammar unclear. Is "preshared" a verb or an adjective here? Also article missing | As it says in the comment | Revised Added ‘the’. TGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 611 |
| 363 | 10.71.8 | 94.18 | Add mention of AP AID assignment | Add mention such as "The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLd as described in 10.71.7." | RevisedThis is 94.24.TGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 363 |
| 613 | 10.71.8 | 94.19 | "the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization," -- it's confusing that BPE uses CPE techniques | As it says in the comment | Rejected11-25/1008 clarifies that BPE is EDP that uses a subset of CPE features. |
| 614 | 10.71.8 | 94.21 | "see10.71.3" missing space | As it says in the comment | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 614 |
| 362 | 10.71.8 | 94.22 | Missing space: "see10.71.3" | add space "see 10.71.3" | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 362 |
| 640 | 10.71.8.2 | 95.48 | "by using the offsets" should be "by using offsets". Also 95.62 | As it says in the comment | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 640 |
| 641 | 10.71.8.2 | 95.58 | "PN Group offset" should be lowercase "group". Also 96.2 | As it says in the comment | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 641 |
| 839 | 10.71.8.3 | 95.48 | What is a "BPE affiliated AP"? Is that an AP affiliated with a BPE AP MLD? The term does not appear anywhere else in the document | Revise wording to make clear what type of entity is being referred to. | RevisedThe rest of the clause uses BPE AP (and BPE AP MLD), but not ‘affiliated’.TGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 839 |
| 135 | 10.71.8.3 | 95.54 | Change "OTA group address" to "receiver address" | As in comment | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 135 |
| 136 | 10.71.8.3 | 96.01 | Change "group address" to "receiver address" | As in comment | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 136 |
| 137 | 10.71.8.3 | 96.09 | Change "group management frames" to "group addressed management frames" | As in comment | AcceptedAlso solved with CID #508, as shown in 11-25/1110 with resolution for CID 137. |
| 259 | 10.71.8.3 | 98.52 | The integrity protection of group data frames is important and should be emphasized. | Please change the sentence:" ... GTK to encrypt and integrity protected the ...". | Revised98.52 is not in this clause, there is no clause 10.71.8.3 on p 98, and no identifiable line 52 that can have the referenced meaning in clause 10.71.8.3. 96.9 is identified as the most likely location.TGbi editor to make the changes shown in the latest version of 11-25/1110 under all headings that include CID 259 |

**Discussion**

Clause 10.71.8 (draft 1.2) before the CIDs:

**10.71.8 BSS Privacy Operations**

BSS Privacy Enhancement (BPE) operations protect privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is protected by not sending BPE AP MLD discovery information, e.g., SSID, capability or operation elements, clear over the air.

APs affiliated with a BPE AP MLD transmit Privacy Beacon frames 9.3.4.4 (Privacy Beacon frame format) instead of Beacon frames 9.3.3.2 (Beacon frame format). A BPE AP MLD is discoverable only by non-AP MLDs that have preshared identity key of the BPE AP MLD as described in 10.71.8.1 (BPE AP MLD Discovery).

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group named as a BPE group. The BPE group has a single schedule. At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see10.71.3 (Establishing frame anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE frame anonymization parameter sets).

**10.71.8.1 BPE AP MLD Discovery**

Each BPE AP affiliated with the BPE AP MLD transmits Privacy Beacon frames.(#616) A BPE STA may discover a BPE AP through received Privacy Beacons as described in 10.71.8.2 (BPE AP MLD beaconing).

A BPE AP shall not respond to Probe Request frames and a BPE AP shall not transmit Probe Response frames. A BPE MLD shall not transmit unprotected GAS frames.

A BPE non-AP MLD may transmit unprotected Privacy Beacon Solicit Request frames (see (The OTA MAC Collision Warning element is defined in 9.4.2.350 (OTA MAC Collision Warning element).))(#617) to solicit unprotected Privacy Beacons from BPE APs. A BPE non-AP STA may detect from a(#830) received Privacy Beacon frames whether the transmitting AP MLD identity key(#618) is configured(#633) to the STA, as defined in 10.71.8.2 (BPE AP MLD beaconing). If the BPE STA has the configured identity key, it(#830) may associate with the BPE AP. On reception of a Privacy Beacon Solicit Request frame, a BPE AP should schedule an unprotected Privacy Beacon frame for transmission at least within a dot11PrivacyBeaconResponseTime.(#99)

NOTE 1—An unprotected Privacy Beacon frame is used only by unassociated STAs affiliated with a BPE non-AP MLD to check whether they have AP identity key and can associate with the AP, i.e., an unprotected Privacy Beacon frame has no frame body as described in 9-76a (Privacy Beacon frame body).(#620)

NOTE 2—If the medium is congested, the transmission of a Privacy Beacon frame might take longer than the dot11PrivacyBeaconResponseTime.

A BPE STA may initiate authentication and association with a BPE AP by sending frames with receiver address set to the Address 2 of the Privacy Beacon frame.

**10.71.8.2 BPE AP MLD beaconing**

A BPE AP MLD shall indicate the status of buffered frames in the(#623) TIM element of a Privacy Beacon frame as specified in 35.3.12.4 (Traffic indications). The BPE non-AP MLD power management rules are specified in 35.3.12 (ML power management).

The frame body(#100, #628) of a Privacy Beacon frame is encrypted by the GTK, and it(#751) can be decrypted only by the BPE non-AP MLDs associated with the BPE AP MLD of the transmitting BPE AP. (#626)If the BPE AP has no associated STAs, then the BPE AP may transmit unprotected Privacy Beacon frames that have no frame body; otherwise the BPE AP transmits protected Privacy Beacon frames.(#417)

The MAC header(#629) of the Privacy Beacon frame contains a Timestamp field that is anonymized as described in 10.71.5.5 (Timestamp anonymization). A receiver deanonymizes the Timestamp field as described in 10.71.6.5 (Timestamp deanonymization).

A BPE non-AP MLD may discover an AP MLD by using the configured shared identity key. The identity key presharing, maintenance and update procedures are out of the scope of this standard.(#631, #633)

A BPE non-AP MLD shall use Equation (10-28)(#101) to determine whether the AP MLD has configured identity key of the transmitter of the received Privacy Beacon frame. A configured BPE AP MLD is discovered if the Identity Hash field of the Privacy Beacon frame matches with a secure hash calculated with the Address 2 of the Privacy Beacon frame and the configured identity key.(#631, #Ed)

Identity Hash = Truncate-48(HMAC-SHA-256(Identity Key, "BPE AP MLD address resolution" || Address 2))

where

 Identity Hash is the value of the Identity Hash field of the Privacy Beacon.

 Identity Key is a 128-bit identifier of the BPE AP MLD.

 Address 2 is the Address(#634) 2 field of the Privacy Beacon.

A BPE AP may include an(#102) Extended Channel Switch Announcement element in the Privacy Beacons as described in 11.8.8.2(Selecting and advertising a new channel in a non-DMG infrastructure BSS).

A BPE AP MLD shall not be part of a Multiple BSSID set.(#834)

NOTE—The BPE AP identity key is AP MLD and single ESS specific. Sharing the key to two or more ESSs might cause privacy violations within ESSs that share the same identity key.(#1)

An associated non-AP MLD maintains a BSS Parameter Change Count (BPCC)(#636) value for each BPE AP with which(#103) it has a link. If an associated non-AP MLD detects that a BPCC value of a BPE AP in a received Privacy Beacon frame is larger than the stored BPCC value of the AP, then the non-AP MLD shall obtain the updated BSS parameter values of the AP before it sends(#637) data to the AP.

An associated BPE non-AP MLD may use the procedure defined in 12.16.4 (Capabilities and operation parameters request and response procedure(#159)) to obtain the capabilities and operation parameters of BPE AP MLD.(#638)

A BPE AP may broadcast unsolicited encrypted Capabilities And Operation Parameters Response frames to signal updated BSS parameter values to STAs affiliated with associated BPE non-AP MLDs. (#639, #366, #838)

**10.71.8.3 Group addressed frames anonymization**

A BPE affiliated AP shall anonymize group addressed frames by using the offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The OTA group address is anonymized as described in 10.71.5.4 (Addressing).

The SN is anonymized with the SNS1 DL offset as described in 10.71.5.2 (Sequence number anonymization).

The PN is anonymized with the PN Group offset as described in 10.71.5.3 (Packet number anonymization).

A BPE affiliated STA shall deanonymize the received group frames by using the offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The transmitter address is filtered as descried in 10.71.6.1 (Address filtering).

The group address is deanonymized as described in 10.71.5.4 (Addressing).

The PN is deanonymized with the PN Group offset as described in 10.71.6.3 (Packet number deanonymization).

The SN is deanonymized with the SNS1 DL offset as described in 10.71.6.4 (Sequence number deanonymization).

To improve the BPE AP privacy, the BPE AP shall use GTK to encrypt the payload of the group addressed Management frames.(#508)

**Discussion**

CID 615:

Revised

The baseline does not use “a Beacon” as a noun, but rather Beacon frame, Beacon interval etc.

**10.71.8 BSS Privacy Operations**

BSS Privacy Enhancement (BPE) operations protect privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is protected by not sending BPE AP MLD discovery information, e.g., SSID, capability or operation elements, clear over the air.

APs affiliated with a BPE AP MLD transmit Privacy Beacon frames 9.3.4.4 (Privacy Beacon frame format) instead of Beacon frames 9.3.3.2 (Beacon frame format). A BPE AP MLD is discoverable only by non-AP MLDs that have preshared identity key of the BPE AP MLD as described in 10.71.8.1 (BPE AP MLD Discovery).

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group named as a BPE group. The BPE group has a single schedule. At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see10.71.3 (Establishing frame anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacon frames and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE frame anonymization parameter sets).

**10.71.8.1 BPE AP MLD Discovery**

Each BPE AP affiliated with the BPE AP MLD transmits Privacy Beacon frames.(#616) A BPE STA may discover a BPE AP through received Privacy Beacon frames as described in 10.71.8.2 (BPE AP MLD beaconing).

A BPE AP shall not respond to Probe Request frames and a BPE AP shall not transmit Probe Response frames. A BPE MLD shall not transmit unprotected GAS frames.

A BPE non-AP MLD may transmit unprotected Privacy Beacon Solicit Request frames (see (The OTA MAC Collision Warning element is defined in 9.4.2.350 (OTA MAC Collision Warning element).))(#617) to solicit unprotected Privacy Beacon frames from BPE APs. A BPE non-AP STA may detect from a(#830) received frames whether the transmitting AP MLD identity key(#618) is configured(#633) to the STA, as defined in 10.71.8.2 (BPE AP MLD beaconing). If the BPE STA has the configured identity key, it(#830) may associate with the BPE AP. On reception of a Privacy Beacon Solicit Request frame, a BPE AP should schedule an unprotected Privacy Beacon frame for transmission at least within a dot11PrivacyBeaconResponseTime.(#99)

NOTE 1—An unprotected Privacy Beacon frame is used only by unassociated STAs affiliated with a BPE non-AP MLD to check whether they have AP identity key and can associate with the AP, i.e., an unprotected Privacy Beacon frame has no frame body as described in 9-76a (Privacy Beacon frame body).(#620)

NOTE 2—If the medium is congested, the transmission of a Privacy Beacon frame might take longer than the dot11PrivacyBeaconResponseTime.

A BPE STA may initiate authentication and association with a BPE AP by sending frames with receiver address set to the Address 2 of the Privacy Beacon frame.

**10.71.8.2 BPE AP MLD beaconing**

A BPE AP MLD shall indicate the status of buffered frames in the(#623) TIM element of a Privacy Beacon frame as specified in 35.3.12.4 (Traffic indications). The BPE non-AP MLD power management rules are specified in 35.3.12 (ML power management).

The frame body(#100, #628) of a Privacy Beacon frame is encrypted by the GTK, and it(#751) can be decrypted only by the BPE non-AP MLDs associated with the BPE AP MLD of the transmitting BPE AP. (#626)If the BPE AP has no associated STAs, then the BPE AP may transmit unprotected Privacy Beacon frames that have no frame body; otherwise the BPE AP transmits protected Privacy Beacon frames.(#417)

The MAC header(#629) of the Privacy Beacon frame contains a Timestamp field that is anonymized as described in 10.71.5.5 (Timestamp anonymization). A receiver deanonymizes the Timestamp field as described in 10.71.6.5 (Timestamp deanonymization).

A BPE non-AP MLD may discover an AP MLD by using the configured shared identity key. The identity key presharing, maintenance and update procedures are out of the scope of this standard.(#631, #633)

A BPE non-AP MLD shall use Equation (10-28)(#101) to determine whether the AP MLD has configured identity key of the transmitter of the received Privacy Beacon frame. A configured BPE AP MLD is discovered if the Identity Hash field of the Privacy Beacon frame matches with a secure hash calculated with the Address 2 of the Privacy Beacon frame and the configured identity key.(#631, #Ed)

Identity Hash = Truncate-48(HMAC-SHA-256(Identity Key, "BPE AP MLD address resolution" || Address 2))

where

 Identity Hash is the value of the Identity Hash field of the Privacy Beacon frame.

 Identity Key is a 128-bit identifier of the BPE AP MLD.

 Address 2 is the Address(#634) 2 field of the Privacy Beacon frame.

A BPE AP may include an(#102) Extended Channel Switch Announcement element in the Privacy Beacon frames as described in 11.8.8.2(Selecting and advertising a new channel in a non-DMG infrastructure BSS).

A BPE AP MLD shall not be part of a Multiple BSSID set.(#834)

NOTE—The BPE AP identity key is AP MLD and single ESS specific. Sharing the key to two or more ESSs might cause privacy violations within ESSs that share the same identity key.(#1)

An associated non-AP MLD maintains a BSS Parameter Change Count (BPCC)(#636) value for each BPE AP with which(#103) it has a link. If an associated non-AP MLD detects that a BPCC value of a BPE AP in a received Privacy Beacon frame is larger than the stored BPCC value of the AP, then the non-AP MLD shall obtain the updated BSS parameter values of the AP before it sends(#637) data to the AP.

An associated BPE non-AP MLD may use the procedure defined in 12.16.4 (Capabilities and operation parameters request and response procedure(#159)) to obtain the capabilities and operation parameters of BPE AP MLD.(#638)

A BPE AP may broadcast unsolicited encrypted Capabilities And Operation Parameters Response frames to signal updated BSS parameter values to STAs affiliated with associated BPE non-AP MLDs. (#639, #366, #838)

**10.71.8.3 Group addressed frames anonymization**

A BPE affiliated AP shall anonymize group addressed frames by using the offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The OTA group address is anonymized as described in 10.71.5.4 (Addressing).

The SN is anonymized with the SNS1 DL offset as described in 10.71.5.2 (Sequence number anonymization).

The PN is anonymized with the PN Group offset as described in 10.71.5.3 (Packet number anonymization).

A BPE affiliated STA shall deanonymize the received group frames by using the offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The transmitter address is filtered as descried in 10.71.6.1 (Address filtering).

The group address is deanonymized as described in 10.71.5.4 (Addressing).

The PN is deanonymized with the PN Group offset as described in 10.71.6.3 (Packet number deanonymization).

The SN is deanonymized with the SNS1 DL offset as described in 10.71.6.4 (Sequence number deanonymization).

To improve the BPE AP privacy, the BPE AP shall use GTK to encrypt the payload of the group addressed Management frames.(#508)

CID 612

Accepted

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group ~~named as~~ called a *BPE group*. The BPE group has a single schedule. At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see10.71.3 (Establishing frame anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacon frames and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE frame anonymization parameter sets).

CID 319

Accepted

**10.71.8 BSS Privacy Enhancements Operations**

CID 98

Accepted

BSS Privacy Enhancement (BPE) operations protect the privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is protected by not sending BPE AP MLD discovery information, e.g., SSID, capability or operation elements, clear over the air.

CID 829

Accepted

BSS Privacy Enhancement (BPE) operations protect the privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is protected by not sending BPE AP MLD discovery information, e.g., SSID, capability or operation elements, ~~clear~~ over the air in the clear.

CID 361, 611

Accepted, Revised

APs affiliated with a BPE AP MLD transmit Privacy Beacon frames 9.3.4.4 (Privacy Beacon frame format) instead of Beacon frames 9.3.3.2 (Beacon frame format). A BPE AP MLD is discoverable only by non-AP MLDs that have the preshared identity key of the BPE AP MLD as described in 10.71.8.1 (BPE AP MLD Discovery).

CID 363

Revised

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group called a *BPE group*. The BPE group has a single schedule. At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see10.71.3 (Establishing frame anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacon frames and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE frame anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID).

CID 614, 362

Accepted

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group called a *BPE group*. The BPE group has a single schedule. At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see 10.71.3 (Establishing frame anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacon frames and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE frame anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID).

CID 640

Accepted

A BPE affiliated AP shall anonymize group addressed frames by using ~~the~~ offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

CID 641

Accepted

The PN is anonymized with the PN ~~G~~group offset as described in 10.71.5.3 (Packet number anonymization).

…/…

The PN is deanonymized with the PN ~~G~~group offset as described in 10.71.6.3 (Packet number deanonymization).

CID 839

Revised

A BPE ~~affiliated~~ AP shall anonymize group addressed frames by using offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

CID 135

Accepted

A BPE AP shall anonymize group addressed frames by using offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The ~~OTA group~~ receiver address is anonymized as described in 10.71.5.4 (Addressing).

CID 136

Accepted

A BPE affiliated STA shall deanonymize the received group frames by using offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The transmitter address is filtered as descried in 10.71.6.1 (Address filtering).

The ~~group~~ receiver address is deanonymized as described in 10.71.5.4 (Addressing).

CID 137

Accepted (no change visible, as this is already solved with CID 508)

To improve the BPE AP privacy, the BPE AP shall use GTK to encrypt the payload of the group addressed Management frames.(#508)

CID 259

Revised

To improve the BPE AP privacy, the BPE AP shall use GTK to encrypt and protect the integrity of the payload of the group addressed Management frames.

*TGbi editor: Modify clause 10.71.8 as follows (track change on):*

**10.71.8 BSS Privacy Enhancements (#319) Operations**

BSS Privacy Enhancement (BPE) operations protect the (#98) privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is protected by not sending BPE AP MLD discovery information, e.g., SSID, capability or operation elements, over the air in the clear (#829).

APs affiliated with a BPE AP MLD transmit Privacy Beacon frames 9.3.4.4 (Privacy Beacon frame format) instead of Beacon frames 9.3.3.2 (Beacon frame format). A BPE AP MLD is discoverable only by non-AP MLDs that have the (#361,611) preshared identity key of the BPE AP MLD as described in 10.71.8.1 (BPE AP MLD Discovery).

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group called (#612) a *BPE group* (#612). The BPE group has a single schedule. At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see (#614,362) 10.71.3 (Establishing frame anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE frame anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID). (#363)

**10.71.8.1 BPE AP MLD Discovery**

Each BPE AP affiliated with the BPE AP MLD transmits Privacy Beacon frames.(#616) A BPE STA may discover a BPE AP through received Privacy Beacon frames (#615) as described in 10.71.8.2 (BPE AP MLD beaconing).

A BPE AP shall not respond to Probe Request frames and a BPE AP shall not transmit Probe Response frames. A BPE MLD shall not transmit unprotected GAS frames.

A BPE non-AP MLD may transmit unprotected Privacy Beacon Solicit Request frames (see (The OTA MAC Collision Warning element is defined in 9.4.2.350 (OTA MAC Collision Warning element).))(#617) to solicit unprotected Privacy Beacon frames (#615) from BPE APs. A BPE non-AP STA may detect from a(#830) received Privacy Beacon frames whether the transmitting AP MLD identity key(#618) is configured(#633) to the STA, as defined in 10.71.8.2 (BPE AP MLD beaconing). If the BPE STA has the configured identity key, it(#830) may associate with the BPE AP. On reception of a Privacy Beacon Solicit Request frame, a BPE AP should schedule an unprotected Privacy Beacon frame for transmission at least within a dot11PrivacyBeaconResponseTime.(#99)

NOTE 1—An unprotected Privacy Beacon frame is used only by unassociated STAs affiliated with a BPE non-AP MLD to check whether they have AP identity key and can associate with the AP, i.e., an unprotected Privacy Beacon frame has no frame body as described in 9-76a (Privacy Beacon frame body).(#620)

NOTE 2—If the medium is congested, the transmission of a Privacy Beacon frame might take longer than the dot11PrivacyBeaconResponseTime.

A BPE STA may initiate authentication and association with a BPE AP by sending frames with receiver address set to the Address 2 of the Privacy Beacon frame.

**10.71.8.2 BPE AP MLD beaconing**

A BPE AP MLD shall indicate the status of buffered frames in the(#623) TIM element of a Privacy Beacon frame as specified in 35.3.12.4 (Traffic indications). The BPE non-AP MLD power management rules are specified in 35.3.12 (ML power management).

The frame body(#100, #628) of a Privacy Beacon frame is encrypted by the GTK, and it(#751) can be decrypted only by the BPE non-AP MLDs associated with the BPE AP MLD of the transmitting BPE AP. (#626)If the BPE AP has no associated STAs, then the BPE AP may transmit unprotected Privacy Beacon frames that have no frame body; otherwise the BPE AP transmits protected Privacy Beacon frames.(#417)

The MAC header(#629) of the Privacy Beacon frame contains a Timestamp field that is anonymized as described in 10.71.5.5 (Timestamp anonymization). A receiver deanonymizes the Timestamp field as described in 10.71.6.5 (Timestamp deanonymization).

A BPE non-AP MLD may discover an AP MLD by using the configured shared identity key. The identity key presharing, maintenance and update procedures are out of the scope of this standard.(#631, #633)

A BPE non-AP MLD shall use Equation (10-28)(#101) to determine whether the AP MLD has configured identity key of the transmitter of the received Privacy Beacon frame. A configured BPE AP MLD is discovered if the Identity Hash field of the Privacy Beacon frame matches with a secure hash calculated with the Address 2 of the Privacy Beacon frame and the configured identity key.(#631, #Ed)

Identity Hash = Truncate-48(HMAC-SHA-256(Identity Key, "BPE AP MLD address resolution" || Address 2))

where

 Identity Hash is the value of the Identity Hash field of the Privacy Beacon frame (#615).

 Identity Key is a 128-bit identifier of the BPE AP MLD.

 Address 2 is the Address(#634) 2 field of the Privacy Beacon frame (#615).

A BPE AP may include an(#102) Extended Channel Switch Announcement element in the Privacy Beacon frames (#615) as described in 11.8.8.2(Selecting and advertising a new channel in a non-DMG infrastructure BSS).

A BPE AP MLD shall not be part of a Multiple BSSID set.(#834)

NOTE—The BPE AP identity key is AP MLD and single ESS specific. Sharing the key to two or more ESSs might cause privacy violations within ESSs that share the same identity key.(#1)

An associated non-AP MLD maintains a BSS Parameter Change Count (BPCC)(#636) value for each BPE AP with which(#103) it has a link. If an associated non-AP MLD detects that a BPCC value of a BPE AP in a received Privacy Beacon frame is larger than the stored BPCC value of the AP, then the non-AP MLD shall obtain the updated BSS parameter values of the AP before it sends(#637) data to the AP.

An associated BPE non-AP MLD may use the procedure defined in 12.16.4 (Capabilities and operation parameters request and response procedure(#159)) to obtain the capabilities and operation parameters of BPE AP MLD.(#638)

A BPE AP may broadcast unsolicited encrypted Capabilities And Operation Parameters Response frames to signal updated BSS parameter values to STAs affiliated with associated BPE non-AP MLDs. (#639, #366, #838)

**10.71.8.3 Group addressed frames anonymization**

A BPE (#839) AP shall anonymize group addressed frames by using (#640) offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The receiver (#135) address is anonymized as described in 10.71.5.4 (Addressing).

The SN is anonymized with the SNS1 DL offset as described in 10.71.5.2 (Sequence number anonymization).

The PN is anonymized with the PN group (#641) offset as described in 10.71.5.3 (Packet number anonymization).

A BPE affiliated STA shall deanonymize the received group frames by using the offsets as described in 10.71.4 (Establishing BPE frame anonymization parameter sets):

The transmitter address is filtered as descried in 10.71.6.1 (Address filtering).

The receiver (#136) address is deanonymized as described in 10.71.5.4 (Addressing).

The PN is deanonymized with the PN group (#641) offset as described in 10.71.6.3 (Packet number deanonymization).

The SN is deanonymized with the SNS1 DL offset as described in 10.71.6.4 (Sequence number deanonymization).

To improve the BPE AP privacy, the BPE AP shall use GTK to encrypt and protect the integrity of (#259) the payload of the group addressed Management frames.(#508)