IEEE P802.11
Wireless LANs

|  |
| --- |
| Steering to BPE AP MLD Comment Resolution  |
| Date: 2025-04-24 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jarkko Kneckt | Apple Inc. | Cupertino, CA |  | jkneckt@apple.com |
|  |  |  |  |  |

This submission is a comment resolution to the CIDs 760 and 761.

This submission is related to a presentation 11-25-708r0, which discusses on making the BPE AP MLD as part of the larger ESS.

# **Solved comments:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 760 | 96.56 | 10.71.8.1 | The discovery aspect described in this clause is about a STA already knowing an AP and finding it. It does not address the case of a new STA, in a new location, finding a BPE AP it had no relationship with in the past. | Design a mechanism so that a new STA can learn about a BPE AP it did not know about before, for example for BPE-enabled public venues. | REVISED. Agree in principle with the comment. TGBi Editor, please make the changes to 802.11bi draft 1.0 as presented in the submission 11-25-709-r0.  |
| 761 | 96.56 | 10.71.8.1 | The discovery mechanism supposes a single AP. But if neighboring APs are changing their OTA MAC, roaming becomes complicated. | Design a mechanism for a STA associated to a BPE AP to find neighboring APs' MAC (and validity duration) | REVISED. Agree in principle with the comment. TGBi Editor, please make the changes to 802.11bi draft 1.0 as presented in the submission 11-25-709-r0.  |

**Normative Text**

**3.2 Definitions specific to IEEE 802.11**

*Instructions to the Editor: Please add the following new definition in the correct alphabetical order*

**Identity key:** A random value, assigned by the BPE access point (AP) multi-link device (MLD), that is used to detect the identity of the BPE AP.

**9.4.2.25 Extended Capabilities element**

*Instructions to the Editor: Please add the following row before the reserved fields to Table 9-192.*

**Table 9-192—Extended Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| 111 | BPE Available | In an AP, set to 1 to indicate that the AP belongs to an ESS that has one or more BPE APs available. In a non-AP MLD, set to 1 to indicate that the non-AP MLD is BPE capable. |

**9.4.2.35 Neighbor Report element**

*Instructions to the Editor: Please make the following changes to the Table 9-212.*

**Table 9-212—Optional subelement IDs for Neighbor Report**

|  |  |  |
| --- | --- | --- |
| **Subelement ID** | **Name** | **Extensible** |
| … | … | … |
| 202 | RSN (see 9.4.2.23 (RSNE)) | NO |
| 203 | RSNXE (see 9.4.2.240 (RSNXE)) | YES |
| 204 | BSSID Of the Next Epoch | YES |
| ~~202~~ 205 -220  | Reserved |  |

**9.4.2.66.2 Transition event report**

*Instructions to the Editor: Please make the following changes to the Table 9-238.*

**Table 9-238—Transition and Transition Query reasons**

|  |  |
| --- | --- |
| **Transition Reason code** | **Description** |
| 21 | BPE AP MLD Discovery  |
| ~~21~~ 22 - 255 | Reserved |

**10.71.8.1 BPE AP MLD Discovery**

*Instructions to the Editor: Please append the following text to the end of the clause*

An ESS may contain non-EDP APs, non-EDP AP MLDs, CPE AP MLDs and BPE AP MLDs. An AP MLD may recommend an associated non-AP MLD to operate with BPE AP MLD as described in 10.71.8.3(Steering to BPE AP MLD).

**10.71.8.3 Steering to BPE AP MLD**

*Instructions to the Editor: Please add the new clause as shown below*

An AP sets the BPE Available field of the Extended Capabilities element of the Beacon, Probe Response and (Re)Association Response frames to indicate that the ESS in which the AP operates contains one or more BPE AP MLDs.

A BPE capable non-AP MLD sets the BPE Available field in the Extended Capabilities element of the (Re)Association Request frame to indicate that it is capable to receive encrypted individually addressed BTM Request frames that include BPE AP MLDs as BSS transition candidate AP MLDs.

A non-AP STA that has received a frame with set BPE Available field in the Extended Capabilities element from its associated AP may query information of available BPE AP MLDs by sending an encrypted BTM Query frame to its associated AP. The BTM Query frame with the BSS Transition Query Reason field set to a BPE AP MLD indicates that the non-AP MLD is interested to only receive information of the available BPE AP MLDs.

An AP may send an encrypted solicited or unsolicited BTM Request frame that contains information of BPE AP MLDs to an associated non-AP STA that has set the BPE Available field of the Extended Capabilities element on its (Re)Association Response frame.

Each AP affiliated with the BPE AP MLD should be reported in a separate Neighbor Report element. Such a Neighbor Report shall include at least the following subelements: BSSID of the current and next epochs, RSNE, RSNXE, BSS Load, HT Capabilities, HT Operation, VHT Capabilities, VHT Operation, HE Capabilities EHT Capabilities, EHT Operation and Basic Multi-link element.

A STA that has received a BTM Request frame with BPE AP may detect the presence of a reported AP affiliated with BPE AP MLD by receiving a frame which address of a MAC header matches with the BSSID reported in the Neighbor Report.

*The remainder of the submission describes how the Identity Key is received and taken into use at association and Fast Transition.*

**6.5.14.1 MLME-SETKEYS.request**

**6.5.14.1.2 Semantics of the service primitive**

*Instructions to the Editor: Please modify the Key Type as shown below.*

|  |  |  |  |
| --- | --- | --- | --- |
| Name  | Type  | Valid range  | Description |
| Key Type  | Enumeration  | Group, Pairwise,PeerKey, IGTK,BIGTK, WIGTK,PGTK, Identity Key  | Defines whether this key is a GTK, TK, TPK-TK, IGTK, BIGTK, or WIGTK, PGTK, or Identity Key respectively. |

**6.5.14.1.4 Effect of receipt**

When the Key Type is Group, IGTK, BIGTK, or WIGTK, or PGTK and the key matches the GTK, IGTK,BIGTK, or WIGTK, ~~or~~ PGTK, or Identity Key if any, installed as a result of EAPOL-Key PDUs (see 12.7.7.4 (Group key handshake implementation considerations)) or exiting WNM sleep mode (see 11.2.3.15.1 (WNM sleep mode capability)) receipt of this primitive shall have no effect except updating the RSC(s) when they are greater than those currently stored. Otherwise, irrespective of the Key Type parameter, when the Key parameter is the same as a key installed as a result of EAPOL-Key PDUs or exiting WNM sleep mode, receipt of this primitive shall have no effect. Otherwise, receipt of this primitive causes the MAC to apply the keys as follows, subject to the MLME-SETPROTECTION.request primitive:

— The MAC uses the key and key ID for the transmission of subsequent frames to which the key and

key ID apply (as defined by the Key Type and Address parameters).

— When the Key Type parameter is not PGTK or Identity Key, t~~T~~he MAC installs the key with the associated key ID

such that received frames for that cipher, of the appropriate type, and containing the matching key

ID are processed using that key and its associated state information. When the Key Type parameter

is PGTK, the MAC installs the key such that the successive start times of the EDP Epochs are processed using that key. When the Key Type parameters is Identity Key, the MAC installs the key such that the transmitted or received Privacy Beacon frames are processed using that key.

— When the Key Type parameter is Pairwise or PeerKey, and the Key, Key ID, and Address (where

valid) parameters identify a new key to be set, the MAC shall initialize the transmitter TSC/PN

counter and the receiver replay counter(s) to 0. When the Key Type parameter is not Pairwise, Peer-

Key, or BIGTK, ~~or~~ PGTK, or Identity Key and the Key, Key ID, and Address (where valid) parameters identify a new key to be set, the MAC shall initialize, depending on the direction of the traffic, the transmitter TSC/PN/IPN/WIPN counter to 0 or 1 (see Clause 12 (Security) and Clause 29 (Wake-Up Radio (WUR) MAC specification(11ba))) or the receiver replay counter(s) to the value in the Receive

Sequence Count parameter. When the Key Type parameter is BIGTK, and the Key and Key ID

parameters identify a new key to be set, the MAC shall initialize, depending on the direction of the

traffic, the transmitter BIPN counter as specified in 12.5.3.4 (BIP replay counters and packet numbers) or the receiver replay counter to the value in the Receive Sequence Count parameter. When the

Key Type, Key, Key ID, and Address (where valid) parameters identify an existing key, the MAC

shall not change the transmitter TSC/PN/IPN/BIPN/WIPN counter or the receiver replay counter(s)

associated with that key.

**9.4.2.46 FTE**

*Instructions to the Editor: Please add the new subelement to the end of the list and number correctly.*

**Table 9-221—Subelement IDs**

|  |  |
| --- | --- |
| **Value**  | **Subelement Name** |
| <ANA> | Identity Key |

The Identity Key subelement contains the Identity Key, used to encrypt the identity of the AP MLD in the Privacy Beacons. The Identity Key subelement format is shown in Figure 9–XX (Identity Key subelement format).

|  |  |  |
| --- | --- | --- |
| Subelement ID | Length | Wrapped Key |
| 1 | 1 | 16 |

**Figure 9-442d—Identity Key subelement format**

The Wrapped Key field contains the wrapped Identity Key being distributed.

**12.6.1.1.1 General**

*Instructions to the Editor: Please Change the second paragraph by adding a new subbullet at the end of the list as shown below*

* Identity Key Security Association: A result of a successful group key handshake with a BPE AP MLD, the Reassociation Response frame of the fast BSS transition protocol, the encrypted Reassociation Response frame specified in 12.16.6.2(MLO), or successful FILS authentication.

**12.6.1.1.15 Identity Key Security Association**

*Instructions to the Editor: Please add the new clause as shown below*

An Authenticator's SME creates an Identity Key Security Association for BPE AP MLD. An Identity Key has the lifetime of the BPE AP MLD.

A Supplicant's SME creates an Identity Key Security Association when the SME receives an Identity Key from its Authenticator.

An Identity Key Security Association consists of the following:

— Identity Key

**12.7.4 EAPOL-Key PDU notation**

*Instructions to the Editor: Please add the last sentence in blue font as shown.*

**change the first paragraph as follows (not all lines shown):**

The following notation is used throughout the remainder of 12.7 (Keys and key distribution) and 13.4 (FT

initial mobility domain association) to represent EAPOL-Key PDUs:

EAPOL-Key(S, M, A, I, K, Reserved, RSC, ANonce/SNonce, MIC, {Key Data})

where

.... .....

WIPN is the last WIPN, as provided by the WIGTK KDE

PGTK is the PGTK KDE

Identity Key is the Identity Key KDE

**12.7.7.2 Group key handshake message 1**(#1001)

*Instructions to the Editor: Please add the last sentence in blue font as shown.*

**Change the first paragraph by inserting a sub-bullet at the end of Key Data as follows (not all lines shown):**

Message 1 uses the following values for each of the EAPOL-Key PDU fields:

Key Data =

— For MLO, when present, PGTK, PGTK Switch Time Indication (see 12.7.2 (EAPOL-Key

frames(#1001)))

— For BPE MLO, when present, Identity Key (see 12.7.2 (EAPOL-Key

frames(#1001)))

**12.11.2.6.3 (Re)Association Response for FILS key confirmation**

*Instructions to the Editor: Please modify as shown.*

Change the second paragraph as follows:

The FILSR constructs a Key Delivery element indicating the current GTK and GTK PN, and the current IGTK and IPN if management frame protection is enabled, and the current BIGTK and BIPN if beacon protection is enabled, and the current WIGTK and WIPN if WUR frame protection is enabled, ~~and~~ the current PGTK if EDP epoch operation is supported by both the AP MLD and the non-AP MLD, and the Identity Key if the AP MLD is BPE AP MLD.(#Ed) For non-MLO, the GTK is carried in a GTK KDE. The IGTK and IPN are carried in an IGTK KDE, the BIGTK and BIPN are carried in a BIGTK KDE and the WIGTK and WIPN are carried in a WIGTK KDE. For MLO, the PGTK is carried in a PGTK KDE, Identity Key is carried in Identity Key KDE, GTKs for all setup links are carried in MLO GTK KDEs, the IGTKs in MLO IGTK KDEs, and the BIGTKs in MLO BIGTK KDEs.

Change the last paragraph as follows

Upon successful completion of the FILS authentication procedure, the FILSO shall process the Key Delivery element in the (Re)Association Response frame. The FILSO installs the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and WIGTK and WIGTK RSC if present in the Key Delivery element and dot11RSNAWURFrameProtectionActivated is true and PGTK if present in the Key Delivery element and EDP epoch operation is supported by both the AP MLD and the non-AP MLD.(#Ed) For MLO, the FILSO installs the Identity Key and PGTK and installs GTKs, IGTKs and BIGTKs for each setup link.

**12.16.6.2 MLO**

*Instructions to the Editor: Please modify as shown.*

If a Key Delivery(#1447) element is included in the (Re)Association Response frame, the EDP AP MLD

shall construct the Key Delivery element with the RSC field set to 0, with the MLO GTK KDE for each setup link, with the MLO IGTK KDE for each setup link if management frame protection is negotiated, with the MLO BIGTK KDE for each setup link if beacon protection is enabled, with Identity Key KDE if the AP MLD is BPE and with the PGTK KDE if EDP epoch is supported by both AP MLD and non-AP MLD.(#1001)

…

On successful (re)association,

— The(#1450) EDP non-AP MLD shall process the Key Delivery element in the (Re)Association

Response frame if present. (#1127)

— The(#1450) EDP non-AP MLD shall install(#1452) the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and PGTK if EDP epoch is supported by both AP MLD and non-AP MLD, and Identity Key if AP MLD is BPE AP MLD. (#1127, #1001)

**13.2.2 Authenticator key holders**

*Instructions to the Editor: Please modify as shown.*

Change the seventh paragraph as follows

The R1KH shall meet the following requirements:

* For MLO, if EDP epoch is supported by both the AP MLD and the non-AP MLDs, the R1KH shall derive and distribute the PGTK to all connected non-AP MLDs
* For BPE MLO, the R1KH shall derive and distribute the Identity Key to all connected non-AP BPE MLDs.

**13.8.5 FT authentication sequence: contents of fourth message**(#1001)

Change the fifth paragraph as follows:

If present, the FTE shall be set as follows:

— When this message of the authentication sequence appears in a Reassociation Response frame, the

Optional Parameter(s) field in the FTE may include the GTK, IGTK, BIGTK, WIGTK subelements

or Identity Key, PGTK, MLO GTK, MLO IGTK and MLO BIGTK subelements. If a GTK, an IGTK, a BIGTK,WIGTK, a PGTK, an Identity Key, an MLO GTK, an MLO IGTK or an MLO BIGTK are included, the Key field of the subelement shall be wrapped using PTK-KEK or KEK2 and the appropriate key wrap algorithm, as specified in Table 12-11 (Integrity and key wrap algorithms) and 12.7.2 (EAPOL-Key frames).The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received message, the receiver shall ignore this trailing padding. Addition of padding does not change the value of the Key Length field. Note that the length of the encrypted Key field can be determined from the length of the GTK, IGTK, BIGTK, PGTK, Identity Key, WIGTK, MLO GTK, MLO IGTK, or MLO BIGTK subelement.