IEEE P802.11
Wireless LANs

|  |
| --- |
| BPE AP Discovery |
| Date: 2025-01-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jarkko Kneckt | Apple Inc | Cupertino, CA |  | jkneckt@apple.com |
| Yanjun Sun | Apple Inc |  |  |  |

Abstract

This submission is related to BSS Privacy Enhanced (BPE) APs discovery.

Currently, a BPE STA may only passively scan to detect available BPE AP MLDs through their Privacy Beacons. This submission allows STA to send a frame to solicit Privacy Beacons from the BPE APs in proximity to speed up the BPE AP detection.

Currently, all BPE AP parameters (RSNE and RSNXE) that are required to authenticate and associate with the BPE AP, are preshared to the BPE non-AP STA. This submission defines PASN based protected signaling to:

* Obtain BPE AP parameters securely
* Enable BPE AP to verify whether the requesting BPE STA is allowed to receive the AP information
* Reduce PASN signaling overheads and delays

The submission is related to the presentation 11-25-136r0 that provides high level introduction.

### This normative text meets the following 802.11bi comments [1]:

|  |  |  |  |
| --- | --- | --- | --- |
| **CID** | **Comment** | **Proposed Change**  | **Proposed Resolution** |
| 1521 | 802.11bi defines requirements for the BSS Privacy Enhancements (BPE). Please add procedures needed for BPE anonymizations. | Please define BPE procedures that use encrypted Beacon as in 22/1306, allow AP discovery only for preconfigured STAs, anonymize STA and AP addresses and anonymization of the multicast transmissions. | Revised. Agree in principle. The submission 11-24-1579r9 defines the BSS Privacy Beaconing. |

###

### This normative text meets the following 802.11bi requirements [2]:

|  |  |  |
| --- | --- | --- |
| **Requirement ID** | **Requirement**  | **Status** |
| 15 | 11bi shall define a mechanism for a BPE Client to determine which of the BPE Client’s configured networks a BPE AP belongs to (if any), while providing mitigation against an eavesdropper identifying the ESS of the BPE AP. | **Approved** (Motion #21, 14 Sept 2022) |
| 19 | 11bi shall define a mechanism for a BPE Client and BPE AP to establish a BPE AP’s identifier (TBD), without the identifier being transmitted in the clear. | **Approved** (Motion #24, 15 Sept 2022) |
| 51 | 11bi shall define a mechanism for the BPE Client to solicit an BPE Beacon frame from a BPE AP.  | **Approved** (Motion #20, 14 Sept 2022) |
| 53 | 11bi shall define a mechanism that will allow a non-AP STA to verify the identity of a known AP before association (without exposing its identity). | **Approved** (Motion #25, 15 Sept 2022) |

*TGbi editor: Add the new clause 10.71.8.1.*

*NOTE: The new clauses 10.71.8.1 and 10.71.8.2 have the same content as clause 10.71.8.1 of the submission 1549r9, except the text is reordered.*

**10.71.8.1 BPE AP MLD beaconing**

Each BPE AP affiliated with the BPE AP MLD transmits Privacy Beacon frames 9.3.X (Privacy Beacon frame format).

A BPE AP MLD shall indicate the status of buffered frames in a 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).

A payload of a Privacy Beacon frame is encrypted by the GTK, and it is receivable only for the BPE non-AP MLDs associated with the BPE AP MLD of the transmitting BPE AP. The AAD of the frame is constructed as defined in clause 12.5.4.3.3 (Construct AAD).

The MAC Header of the Privacy Beacon frame contains a Timestamp field that is anonymized as described in 10.71.4.5(Timestamp anonymization). A receiver deanonymizes the Timestamp field as described in 10.71.5.5 (Timestamp deanonymization).

A BPE non-AP MLD shall use the equation 9–XX to determine whether it is preconfigured with the transmitter of the received Privacy Beacon frame. A preconfigured 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 preconfigured Identity Key.

A BPE non-AP MLD may discover an AP MLD by using the preshared Identity Key. The Identity Key presharing, maintenance and update procedures are out of the scope of the specification.

Identity Hash == Truncate-48(HMAC-SHA-256(“BPE AP MLD address resolution”, Identity Key, Address 2)).      (10–X1)

, where:

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

– Identity Key is 128-bit identifier of the tested AP MLD.

– Address 2 is the A2 field of the Privacy Beacon.

A BPE AP may include 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 Privacy Beacon frame shall not contain a Multiple BSSID element.

An associated non-AP MLD maintains a BPCC value for each BPE AP 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 may send data to the AP.

An associated BPE non-AP MLD and a BPE AP MLD may use the procedure defined in 12.14.3 (EDP capabilities and operation parameters request and response procedure) to obtain capabilities and operation parameters of BPE AP MLD.

A BPE AP may send encrypted, unsolicited broadcast addressed Capabilities And Operation Parameters Response frames to signal updated BSS parameter values to STAs of associated BPE non-AP MLDs

*TGbi editor: Add the new clause 10.71.8.2.*

*NOTE: The new clauses 10.71.8.1 and 10.71.8.2 have the same content as clause 10.71.8.1 in submission 1549r9, except the text is reordered and the text modifications (additions and deletions) are shown.*

**10.71.8.2 BPE AP MLD discovery**

A BPE AP shall not respond to ~~the~~ 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 9.6.38.X(Privacy Beacon Solicit Request frame format), to solicit Privacy Beacons from BPE APs. A BPE non-AP STA may detect from received Privacy Beacons whether the transmitting AP MLD information is preshared to the STA, as defined in 10.71.8.1(BPE AP MLD beaconing). A BPE AP should transmit a Privacy Beacon frame within a *dot11PrivacyBeaconResponseTime*, if it has received a Privacy Beacon Solicit Request frame.

A BPE STA may use BPE active scanning optimized PASN, see 10.71.8.3(BPE active scanning optimized PASN), to setup a TK to protect a BPE AP capabilities and operation parameters obtaining as defined in 12.14.3(EDP capabilities and operation parameters request and response procedure).

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

*TGbi editor: Add the new clause 10.71.8.3*

**10.71.8.3 BPE active scanning optimized PASN**

This clause defines modifications to the PASN, 12.13(Preassociation Security Negotiation (PASN)), when a BPE non-AP STA setups a TK to protect management frames exchange, e.g., when a BPE non-AP MLD obtains AP capabilities and operation parameters.

A BPE non-AP STA shall include an RSNE to the PASN authentication frames with either of the following values:

* If the STA-ID subfield of PASN Parameters element is present, then the RSNE PMKID field is not present, the AKM Suite Count field is set to 0, and the Pairwise Cipher field is set to GCMP-256.
* If the STA-ID subfield of PASN Parameters element is not present, then the PMKID field is present, and the AKM field and Pairwise Cipher field are set to the values that were used to calculate the PMKID.

The STA-ID field of the PASN Parameters element of the first PASN authentication frame, when present, indicates whether the transmitter is allowed to setup a TK with the BPE AP. The STA-ID is calculated as shown in the equation 10–X2.

STA-ID = Truncate-48(HMAC-SHA-256(“BPE Non-AP MLD identification”, Identity Key, Address1|Address 2)) (10–X2)

, where

* Identity Key is 128-bit identifier of the AP MLD
* Address 1 is the A1 of the PASN authentication frame and it is set to the link address of the BPE AP
* Address 2 is the A2 of the PASN authentication frame and it is set to the link address of the transmitting STA. The STA shall randomize and use a different Address2 for each PASN setup.

If a BPE AP receives a PASN authentication frame with a STA-ID, then the BPE AP shall calculate a STA-ID from the Address1 and Address2 of the received PASN frame. If the calculated STA-ID value is equal to the value of the received STA-ID field of the PASN authentication frame, then the BPE AP shall respond with a PASN authentication frame.

A BPE non-AP STA may set the AP Information Requested subfield of the PASN Parameters element of the first PASN authentication frame to indicate that the STA desires to receive an AP Capabilities And Operation Parameters Response frame with a complete set of AP MLD parameters. If a BPE AP receives a PASN authentication frame with a set AP Information Requested subfield, then the BPE AP shall transmit the AP Capabilities And Operation Parameters Response frame immediately after a successful PASN authentication.

A BPE non-AP STA may include a TK Adoption Delay field to the PASN Parameters element of the first PASN Authentication frame. If the TK Adoption Delay field is present, the BPE AP may send TK encrypted frames a TK Adoption Delay after the second PASN Authentication frame, regardless of whether the STA has transmitted the third PASN authentication frame.

If a BPE AP receives a first PASN authentication frame with a TK Adoption Delay field and the responding AP needs a longer TK adoption delay, then the AP shall include to the second PASN authentication frame a TK Adoption Delay field set to the TK adoption delay value required by the AP. The AP may transmit TK protected frames to the STA after all TK adoption delays have expired.

If the STA desires to continue TK protected frames transmissions with the BPE AP, the STA may transmit a third PASN authentication frame or TK encrypted frames. The STA may transmit TK encrypted frames after all TK adoption delays have expired.

NOTE – A BPE non-AP STA might optimize BPE AP parameters obtaining by transmitting the first PASN authentication frame including a set AP Information Requested field and TK Adoption Delay field. The requested AP sends AP Capabilities And Operation Parameters Response frame immediately after the TK Adoption Delays have expired, and the non-AP STA needs no additional frame transmissions.

*TGbi editor: Modify the figure and add the new paragraph as shown.*

**9.4.2.306 PASN Parameters element**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Element ID  | Length | Element ID Extension | Control  | Wrapped Data | Comeback Info | Finite Cyclic Group ID | Ephemeral Public Key Length | Ephemeral Public Key | TK Adoption Delay | STA-ID |
| Octets: 1 | 1 | 1 | 1 | 1 | Variable | 0 or 2 | 0 or 1 | Variable | 0 or 1 | 0 or 6 |

**Figure 9-1055—PASN Parameters element format**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Comeback Delay Present | Group And Key Parameters Present | TK Adoption Delay Present | STA-ID Present | AP Information Requested | Reserved |
| Bits: | 1 | 1 | 1 | 1 | 1 | 3 |

**Figure 9-1056—PASN Parameters element Control Info field format**

The Comeback Info Present subfield indicates if the Comeback Info field is included in the PASN

Parameters element. The Group and Key Present subfield indicates if the PASN Parameters element includes the Finite Cyclic Group ID, the Ephemeral Public Key Length, and the Ephemeral Public Key fields. The TK Adoption Delay Present subfield indicates if the TK Adoption Delay field is included in the PASN Parameters element. The STA-ID Present subfield indicates if the STA-ID field is included in the PASN Parameters element. The AP Info Requested subfield indicates if the AP capabilities and operations information is requested as defined in 10.71.8.3(BPE active scanning optimized PASN).

*TGbi editor: Add the following two paragraphs to the end of the clause.*

The TK Adoption Delay field is the time in units of 64 microseconds after the second PASN authentication frame after which the TK protected frames can be transmitted.

The STA-ID field is an identifier of the BPE non-AP STA as defined in 10.71.8.3(BPE active scanning optimized PASN).

*TGbi editor: Add the Privacy Beacon Solicit frame to the Table 9-628s as shown.*

**9.6.38.1 EDP Action field**

**Table 9-628s – EDP Action field values**

|  |  |
| --- | --- |
| **Value** | **Meaning** |
| 1 | Capabilities and Operation Parameters Request  |
| 2 | Capabilities and Operation Parameters Response |
| 3 | Privacy Beacon Solicit Request  |
| 4 – 255 | Reserved |

*TGbi editor: Add the new clause and renumber the clause accordingly.*

**9.6.38.X Privacy Beacon Solicit Request frame format**

The Privacy Beacon Solicit Request frame is transmitted as non-protected management frame to the broadcast address. The frame solicits Privacy Beacon frame transmissions as a response to the frame as described in 10.71.8.2(BPE AP MLD discovery).

**Table 9-628XX – Privacy Beacon Solicit Request Action field format**

|  |  |
| --- | --- |
| **Order** | **Meaning** |
| 0 | Category  |
| 1 | EDP Action |

The Category field is defined in 9.4.1.11 (Action field).

The EDP Action field is defined in 9.6.38.1 (EDP Action field).

**References:**

[1] 11-24-1094-11-00bi-ieee-802-11bi-cc49-comments

[2] 11-21-1848-16-00bi-requirements-document