IEEE P802.11
Wireless LANs

|  |
| --- |
| BSS Privacy – Beaconing  |
| Date: 2024-09-10 |
| 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 |
| Jarkko Kneckt | Apple Inc. |  |  | jkneckt@apple.com |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission solves the CIDs 1521, 1122, 1157, and 1376 of the 802.11bi internal comment collection.

The submission defines BSS Privacy (BP) operations to meet the 802.11bi requirements 15, 16, 19, 50, 51 and 53.

This submission builds on top of the 802.11bi Draft 0.4.

R3 clarifies the Privacy Beacon frame format.

R4 removes RSNE/RSNXE provision

R5 adds to the addressed CID list

R6 streamlines the discovery phase and clarifies the identity key

R7 adds details for the Privacy Beacon payload (DFS support) and encryption (AAD). The solicit frame is deleted.

R8 addresses comment received from 802.11bi THU AM1. The comment resolution text is corrected, the privacy beacon payload is clarified and AAD comments are addressed.

|  |  |  |  |
| --- | --- | --- | --- |
| **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 peocedures 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. |
| 1122 | BPE AP mechanism to change its MAC address is not defined in this document. | remove the sentence "A BPE EDP AP MLD and its associated non-AP MLDs may change their OTA MAC addressestogether with associated values for both unicast and group transmissions." | Revised. Agree in principle. The submission 11-24-1579r9 and 11-24-1576r8 introduce a mechanism for the BPE AP to change its MAC address, thus removing the need to delete the sentence. |
| 1157 | Change of OTA MAC address is not defined for the BPE AP/non-AP. Is the same mechanism as for the change of the CPE MAC address ? | please clarify the mechanism for the change of the BPE MAC address. | Revised. Agree in principle. The submission 11-24-1576r8 introduces a mechanismfor the BPE AP to change its MAC address. |
| 1376 | "For encrypted frames, the transmitter shall compute an over-the-air PN (OPN) value from the PN value in the CCMP header or GCMP header of the frame as follows:" -- don't we also need to anonymise the PN in the MME etc.? | As it says in the comment | Reject. CPE AP does not anonymize fields that are broadcasted to all STAs. The BPE AP transmits Privacy Beacons which do not include the MME. So in both cases, the privacy issue pointed out by the comment does not exist.  |

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

|  |  |  |
| --- | --- | --- |
| **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) |
| 16 | 11bi shall define a mechanism such that the BPE AP may exclude certain TBD elements when transmitting Beacon frames. | **Approved** (Motion #16, July 13, 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) |
| 50 | 11bi shall define a BPE Beacon frame that includes a secure mechanism to identify a BPE AP and/or a network that includes that BPE AP. 11bi shall extend the BPE Beacon frame with a subset of encrypted or obfuscated, TBD, fields and define a mechanism for the BPE AP to transmit the new type of Beacon frame.The BPE Beacon frame shall contain fields and have a structure that allows associated BPE clients to minimise the power consumption for BPE Beacon frame reception. | **Approved** (Motion #20, 14 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) |

**Normative text:**

*TGbi editor: Add the following text in the begin of the clause 10.71.8*

10.71.8 BSS Privacy operations

BSS Privacy Enhancement (BPE) operations protect privacy of BPE AP MLDs and associated non-AP BPE 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.X (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).

*TGbi editor: Add the new clause 10.71.8.1*

**10.71.8.1 BPE AP MLD discovery**

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

A Privacy Beacon frame shall not contain a Multiple BSSID element.

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

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).

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.

A 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.

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 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.

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.

Identity Hash == Truncate-48(HMAC-SHA-256(“BPE AP MLD address resolution”, Identity Key, Address 2)).      (9–XX)

, 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.

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

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

* + - 1. Timestamp anonymization

For Privacy Beacon frames, the transmitter shall compute an over-the-air Timestamp (OTSF) value from the Timestamp value of the frame as follows:

 OTSF = (Timestamp + EDP\_Timestamp\_offset) mod 264,

where EDP\_Timestamp\_offset is the Timestamp offset value generated for the BPE AP MLD.

The BPE AP shall transmit Privacy Beacon frames over the air using the OTSF value in the Timestamp field (see (9.3.4.X Privacy Beacon frame format)).

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

* + - 1. Timestamp deanonymization

For Privacy Beacon frames, the receiver shall recover the original Timestamp value (assigned by the transmitter) from the OTSF value encoded in the Timestamp fields as follows:

 Timestamp = (OTSF − EDP\_Timestamp\_offset) mod 264,

where EDP\_Timestamp\_offset is the Timestamp offset value generated for the BPE AP MLD.

The recovered original Timestamp value shall replace the OTSF value in subsequent processing of the Privacy Beacon frame in the receiving MLD.

*TGbi editor: Add the Type and Subtype combination in the Table 9-1.*

**9.2.4.1.3 Type and Subtype subfields**

**Table 9-1 Valid type and subtype combinations**

|  |  |  |  |
| --- | --- | --- | --- |
| **Type value** **B3 B2** | **Type description** | **Subtype value** **B7 B6 B5 B4** | **Subtype description** |
| 11 | Extension | 0010 | Privacy Beacon |

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

**9.3.4.X Privacy Beacon frame format**

The format of the of the Privacy Beacon frame is shown in Figure 9-A (Privacy Beacon frame format)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Frame Control  | Duration | Address 1 | Address 2 | Identity Hash | Timestamp | Frame Body | FCS |
| Octets: | 2 | 2 | 6 | 6 | 6 | 8 | Variable | 4 |

**Figure 9-A Privacy Beacon frame format**

The Address 1 field is set to the broadcast address.

The Address 2 field is set to the anonymized BSSID.

The Identity Hash field is set to a value, as described in 10.71.8.1 (BPE AP MLD discovery).

The Timestamp field format is described in 9.4.1.10 (Timestamp field). The Timestamp field is anonymized as described in 10.71.4.5(timestamp anonymization).

The frame body of the Privacy Beacon frame contains the information shown in Table 9–B (Privacy Beacon frame body).

**Table 9-B Privacy Beacon frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 1 | BSS Parameter Change Count (BPCC) | The BPCC element is present if AP MLD has associated non-AP MLDs, otherwise not present. |
| 2 | TIM | The TIM element element is present if AP MLD has associated non-AP MLDs, otherwise not present. |
| 3 | Reduced Neighbor Report | The RNR element element is present if AP MLD has associated non-AP MLDs, otherwise not present. |
| 4 | Extended Channel Switch Announcement | The Extended Channel Switch Announcement element is optionally present if AP MLD has associated non-AP MLDs, and dot11SpectrumManagementRequired is true or dot11ExtendedChannelSwitchActivated is true. |

*TGbi editor: Modify the clause 12.5.4.3.3 as shown below.*

**12.5.4.3.3 Construct AAD**

The AAD construction is defined in 12.5.2.3.3 (Construct AAD), except the AAD construction of the Privacy Beacon frame is performed as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | FC  | A1 | A2 | IH |
| Octets: | 2 | 6 | 6 | 6 |

Figure 12-XX—AAD construction for Privacy Beacon frame

Figure 12-XX (AAD construction for Privacy Beacon frame) depicts the format of the AAD.

a) FC—MPDU Frame Control field

b) A1—MPDU Address 1 field.

c) A2—MPDU Address 2 field.

d) IH—MPDU Identity Hash field.

**References:**

[1] 11-21-1848-16-00bi-requirements-document