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 |

Abstract

This submission solves the CIDs 1521 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **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. Please this on BSS Privacy Beaconing and submission 11-24-1576r0 on BSS Protection parameters anonymization to the 802.11bi draft. |

### 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.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 the preconfigured discovery 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 may not contain payload, if a BPE AP has no associated non-AP MLDs. A Privacy Beacon frame shall contain payload, if an BPE AP MLD has one or more associated non-AP MLD.

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

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 Privacy Beacon frame, except the Timestamp field, is encrypted by the GTK. The Timestamp field is masked out from the encryption, and the field is anonymized as described in 10.71.4.5 (Timestamp anonymization). A receiver decrypts the Privacy Beacon frame and 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 with which 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 value for the BPE AP, then the affiliated non-AP MLD shall obtain the updated BSS parameter values of the BPE AP before sending data to the AP. A STA of an non-AP MLD may send a Capabilities And Operation Parameters Request frame to request parameters of the APs affiliated with the receiving BPE AP MLD. A BPE AP MLD that receives a Capabilities And Operation Parameters Request frame from an associated BPE non-AP MLD shall respond with a Capabilities And Operation Parameters Response frame containing the parameters of the APs affiliated with the AP MLD. A BPE AP may send an 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 MLD shall indicate the status of buffered frames in TIM element as specified in 35.3.12.4(Traffic indications).

The BPE MLDs follow the power management rules as specified in 35.3.12(ML power management).

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 actively scan for BPE AP MLDs by transmitting Privacy Beacon Solicit Request frames, 9.6.38.X(Privacy Beacon Solicit Request frame format). A BPE AP should transmit a Privacy Beacon frame within a *dot11PrivacyBeaconResponseTime*, if it has received a Privacy Beacon Solicit Request frame.

A BPE non-AP MLD may discover an AP MLD from a received Privacy Beacon frame by using the BPE AP MLD specific discovery key. The discovery key is preconfigured to the BPE non-AP MLD. The discovery key preconfiguration, 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 AP identity key for the BPE AP MLD transmitter of the received Privacy Beacon frame. A BPE AP MLD matching the preconfigured information is discovered if the Address1 of the Privacy Beacon frame matches with a secure hash calculated with the Address3 of the Privacy Beacon frame and the preconfigured AP Identity Key.

Address 1 == Truncate-48(HMAC-SHA-256(“BPE AP MLD address resolution”, AP Identity Key, Address 3)).         (9–XX)

, where:

- Address 1 is the A1 field of the Privacy Beacon.

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

- Address 3 is the A3 field of the Privacy Beacon.

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

The BPE AP shall select a new pseudorandom Address 3 value when Address 2 of the Privacy Beacon frame changes.

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

The frame body, except the Timestamp field, is encrypted. The Timestamp field is masked out from the encryption. The Timestamp field is anonymized as described in 10.71.4.5(timestamp anonymization).

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

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 1 | Timestamp | See 9.4.1.10 (Timestamp field) for Timestamp field format. The timestamp is present if AP MLD has one or more associated non-AP MLDs.  |
| 2 | BSS Parameter Change Count (BPCC) | The BPCC element is present if AP MLD has one or more associated non-AP MLDs. |
| 3 | TIM | The TIM element is present if AP MLD has one or more associated non-AP MLDs. |
| Last | Reduced Neighbor Report | The RNR element is present if AP MLD has one or more associated non-AP MLDs. |

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

**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 accordingly.*

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

The Privacy Beacon Solicit Request frame is transmitted as a non-protected management frame to the broadcast address. The frame allows Privacy Beacon frame transmissions as a response to the frame.

**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).

*TGbi editor: Add the new MIB variable to the end of the "Dot11StationConfigEntry"*

**C.3 MIB detail**

Dot11StationConfigEntry ::= SEQUENCE

{

...

dot11PrivacyBeaconResponseTime Unsigned32

}

*TGbi editor: Add the new dot11StationConfigEntry to the end of the dot11StationConfigEntry TABLE.*

dot11PrivacyBeaconResponseTime OBJECT-TYPE

 SYNTAX Unsigned32 (0. .8)

 UNITS "TUs"

 MAX-ACCESS read-create

 STATUS current

 DESCRIPTION

"This is a control variable.
It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This attribute indicates the duration in which the BPE AP transmits a Privacy Beacon as a response to a received Privacy Beacon Solicit Request frame."

 DEFVAL { 5 }

 ::= { dot11StationConfigEntry <ANA> }

**References:**

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