IEEE P802.11
Wireless LANs

|  |
| --- |
| BPE AP Discovery |
| Date: 2025-01-14 |
| 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 available BPE AP MLDs through their Privacy Beacons. Passive scanning keeps the non-AP STA radio busy for ~ 100ms for each scanned channel. Long scanning time consumes non-AP STA power and complicates low latency data transmissions.

This submission allows a BPE STA to send an unprotected broadcast frame to solicit Privacy Beacons from the BPE APs in proximity. The BPE STA may receive Privacy Beacons in a shorter time which speeds up the BPE AP detection.

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

|  |  |  |
| --- | --- | --- |
| **Requirement ID** | **Requirement**  | **Status** |
| 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 and the text modifications (additions and deletions) are shown.*

**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)~~

Identity Hash = Truncate-48(HMAC-SHA-256(Identity Key, “BPE AP MLD address resolution” || 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.

~~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 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).

*Instructions to the 11bi Editor: Add the new entry to***"***Dot11StationConfigEntry" as follows (not all lines shown):*

Dot11StationConfigEntry ::= SEQUENCE

{

…

dot11PrivacyBeaconResponseTime Unsigned32,

…

dot11PrivacyBeaconResponseTime OBJECT-TYPE

SYNTAX Unsigned32 (0…100)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable. It is written by an external management entity or the SME. Changes take effect as soon as practical in the implementation.

This attribute, defines the maximum time in which a BPE AP transmits a Privacy Beacon as a response to a received Privacy Beacon Solicit Request frame."

DEFVAL { 5 }

::= { dot11StationConfigEntry <ANA> }

**References:**

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

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