IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbi Requirements and Issues Tracking |
| Date: 2023-07-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Carol Ansley | Cox Communications |  | +1-404-229-1672 | carol@ansley.com |

### Overview

This document maps Requirements to topics and can track proposals. This document also has a table to track issues wider than specific requirements.

|  |  |
| --- | --- |
| R0 | Initial Draft for Discussion |
| R1 | Added table to track text submissions |
| R2 | Updates from discussions – July Plenary |

# Requirements

The following table summarizes the requirements for TGbi.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Requirement** | **Issue**  | **Status** | **Information** |
| 5 | 11bi shall define a mechanism for a CPE Client and CPE AP **to** **protect the (Re)Association Request/Response**.  | (re)association |  |   |
| 21 | 11bi shall define a mechanism to protect the Frame Body field of the (Re)Association Request frame | (re)association |  |   |
| 22 | 11bi shall define a mechanism to protect the Frame Body field of the (Re)Association Response frame  | (re)association |  |   |
| 6 | 11bi shall define a mechanism for a CPE Client **to change its own OTA MAC Address** when reassociating from a CPE AP to another CPE AP.12 May 2022 – May consider APs outside of ESS in other discussions. | (re)association and MAC address |  |   |
| 24 | 11bi shall define a mechanism to carry the DS MAC address of a 11bi non-AP STA or an 11bi non-AP MLD in a protected (Re)association Request frame (and any other TBD protected management frames) from the 11bi non-AP STA to a 11bi AP or from the 11bi non-AP MLD to a 11bi AP MLD. | (re)association and MAC address |  |   |
| 49 | 11bi shall define a mechanism for a CPE non-AP STA to request capabilities and operation parameters of the associated CPE AP or a CPE non-AP MLD to request capabilities and operation parameters of APs affiliated with the associated CPE AP MLD using an individually addressed protected request/response action frame. | AP and MLD AP parameters |  |   |
| 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). | AP verification |  |   |
| 1 | 11bi shall define a mechanism to prevent an eavesdropper distinguishing whether authentication exchanges between CPE Clients and CPE AP use identical **SAE credentials** or distinct SAE credentials (where a CPE AP supports multiple SAE credentials). | authentication |  |   |
| 4 | 11bi shall define a mechanism for a CPE Client and CPE AP **to establish keys from an Authentication exchange** which can then be used to protect the (Re)Association Request/Response.  | authentication |  |   |
| 48 | 11bi shall define a mechanism for a CPE Client and CPE AP to carry 802.1X EAPOL PDUs in Authentication frames to perform IEEE 802.1X authentication. | authentication |  |   |
| 16 | 11bi shall define a mechanism such that the BPE AP may exclude certain TBD elements when transmitting Beacon frames. | BPE AP |  |   |
| 18 | 11bi shall define a mechanism for a BPE AP to facilitate changing its AP identification information while there are Clients associated, without disrupting the connectivity from the Clients, and/or clients in the process of associating. | BPE AP |  |   |
| 19 | *New proposed text:* 11bi shall define a mechanism for a BPE Client and BPE AP to establish a BPE AP’s identifier (TBD), (48 bit-value) without the identifier being transmitted in the clear.*This will likely be the same mechanism as used in Req 12.* | BPE AP |  |   |
| 35 | 11bi requires that a BPE AP shall change its Beacon TBTT when the BPE AP identification information changes in the Beacon.  | BPE AP |  |   |
| 40 | 11bi shall define a mechanism for a BPE AP to obfuscate the RA, SN and PN of the group frames to avoid BPE AP tracking. | BPE AP |  |   |
| 38 | 11bi shall define a mechanism to obfuscate affiliated BPE APs parameters so that eavesdropping STAs cannot determine that they belong to the same AP MLD. | BPE AP MLD |  |   |
| 40a | 11bi shall define a mechanism for a BPE AP to change the OTA TSF (e.g., the TSF that is transmitted in the beacon) by a random value. | BPE AP TSF |  |   |
| 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. |  BPE Beacon frame |  |   |
| 51 | 11bi shall define a mechanism for the BPE Client to solicit an BPE Beacon frame from a BPE AP.  | BPE Beacon frame |  |   |
| 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. | BPE client |  |   |
| 46 | 11bi shall define a mechanism for BPE Clients and BPE APs to encrypt the +HTC field and the HT Control field. | BPE HTC+ and HTC note that the analogous CPE requirement was not approved |  |   |
| 39 | 11bi shall define a mechanism for a BPE AP and a BPE Client to change the OTA MAC addresses, SN and PN they use for unicast transmissions. | BPE MAC address while associated |  |   |
| 41 | BPE Clients and BPE APs shall reset the Scrambler Seed on individual and group addressed frames when a TA MAC address is changed. | BPE MAC address while associated |  |   |
| 45 | 11bi shall define a mechanism for BPE Clients and BPE APs to encrypt or obfuscate (TBD) a subset of MAC Header fields (specific fields TBD). | BPE MAC Header fields |  |   |
| 44 | 11bi shall define a mechanism for a BPE Client and BPE AP to obfuscate the transmitted TID to an uncorrelated new value on downlink and uplink to new values in Associate STA State 4, without any loss of connection. | BPE TID |  |   |
| 12 | 11bi shall define a mechanism for a CPE Client and CPE AP to establish the CPE Client’s DS MAC Address without the CPE Client’s DS MAC Address being transmitted in the clear.12 Sept 2022 – DS MAC address term may need to be changed | MAC address |  |   |
| 25 | 11bi shall define a mechanism to randomize over the air MAC address of the 11bi non-AP STA or 11bi non-AP MLD (carried in Address 1 field or Address 2 field of the MAC header) during BSS transition.(related to R6) | MAC address |  |   |
| 7 | 11bi shall define a mechanism for a CPE Client to initiate **changing** **its own OTA MAC Address** used with a CPE AP in Associate STA State 4 without any loss of connection. | MAC address change while associated |  |   |
| 8 | ~~11bi shall define a mechanism for a CPE AP to initiate~~ **~~changing the OTA MAC Addresses of all associated CPE Client’s~~** ~~in the BSS (those CPE Clients in Associate STA State 4) simultaneously without any loss of connection~~Edited to: 11bi shall define a mechanism for a CPE AP to initiate **changing the OTA MAC Addresses of a set of associated CPE Client’s** in the BSS (those CPE Clients in Associate STA State 4) without any loss of connection. | MAC address change while associated |  |   |
| 9 | ~~11bi shall define a mechanism for a CPE Client and CPE AP~~ **~~to change the transmitted SN~~** ~~to an uncorrelated new value on downlink and uplink to new values in Associate STA State 4, without any loss of connection.~~Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP **to change the transmitted SN and the scrambler seed** on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated |  |   |
| 10 | ~~11bi shall define a mechanism for a CPE Client and CPE AP~~ **~~to change the transmitted PN~~** ~~to an uncorrelated new value on downlink and uplink to new values in Associate STA State 4, without any loss of connection.~~Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP **to change the transmitted PN** on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated |  |   |
| 11 | ~~11bi shall define a mechanism for a CPE Client and CPE AP~~ **~~to change the CPE Client’s AID~~** ~~to an uncorrelated new value in Associate STA State 4, without any loss of connection.~~Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP **to change the CPE Client’s AID** to an uncorrelated new value in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated |  |   |
| 31 | 11bi shall define a mechanism for CPE Clients and CPE APs to encrypt or obfuscate (TBD) a subset of MAC Header fields (specific fields TBD) | MAC Header fields |  |   |
| 52 | 11bi shall define a mechanism for an 11bi non-AP MLD to request capabilities and operation parameters of APs affiliated with the associated 11bi AP MLD using a protected request/response action frame. | MLD parameters |  |   |
| 3 | 11bi shall define a minimal set of Elements for transmission by a CPE Client in **a probe request** prior to authentication. | Probe request |  |   |
| 20 | 11bi shall define a mechanism for the 11bi non-AP STA to refrain from transmitting Probe Request frames containing elements except TBD element(s) |  Probe request |  |   |
| 26 | 11bi shall define an optional protected version of the following unicast management frames between a CPE AP and an associated CPE Client:* Notify Channel Width frame
* SM Power save frame
* CSI frame
* Noncompressed Beamforming frame
* Compressed Beamforming frame
* VHT Compressed Beamforming frame
* Group ID Management frame
* Operating Mode Notification frame
* HE Compressed Beamforming/CQI frame
* Quiet Time Period Action frame
* EHT Compressed Beamforming/CQI frame
 | Protected management frames |  |   |
| 2 | 11bi shall define a mechanism to prevent an eavesdropper distinguishing whether reassociation exchanges between CPE Clients and CPE APs use identical **PMK** or distinct PMK | reassociation |  |   |
| 13 | ~~11bi shall define a mechanism for CPE Clients and CPE APs to transmit and receive the CPE Client’s DS MAC Address in SA and DA in protected form on both the downlink and uplink.~~Edited to: 11bi shall define or reuse a mechanism for CPE Clients and CPE APs to protect the SA/DA values from exposure OTA to 3rd parties. | SA/DA |  |   |
| 30 | 11bi shall define a mechanism for a CPE Client and CPE AP to obfuscate the transmitted TID to an uncorrelated new value on downlink and uplink to new values in Associate STA State 4, without any loss of connection. | TID |  |   |

# Issues:

The following table contains issues identified for more in depth discussion, potentially affecting multiple requirements.

|  |  |  |
| --- | --- | --- |
|  | **Issue** | **Summary** |
| 1 | Amendment scope – non-MLD STAs and APs as well as MLDs or only MLDsEHT baseline, or VHT or ? | Discussed May 2023 interim, affects scope of amendment, current requirements include non-MLD STAs explicitlyJuly Plenary – still open  |
| 2 | AID handling  | Discussed May 2023 interim, used in many contextsDifferent than other requirements in that the AIDs are a small block of numbers shared across the associated STAs, including any legacy STAsJuly Plenary – discussed whether to AP assign or randomized - still open |
| 3 | Removal or rejection of requirements?Also, may identify new requirements | If group agrees that a requirement is not feasible, how to remove it? Motion?July Plenary – Requirement 30 may need to be broadened |
| 4 | TID obfuscation may need to extend beyond only the MAC Header mentioned in R30 | Discussed July Plenary, similar to AID used in many placesMuch concern about the use of TID tracking for the implications on privacy from the standpoint of application usage |
| 5 | Should CPE and BPE devices be MLD-compliant? | Discussed July Plenary – should this be a new requirement? Strong views both ways.Are there any restrictions in the PAR? |

# Text Submissions: (Proposed)

The following table contains issues identified for more in depth discussion, potentially affecting multiple requirements.

|  |  |  |  |
| --- | --- | --- | --- |
| Section | **Document Source** | **Status** | **Information** |
| 4.5.4.10 | 23/1214r1 | TBD | Introduction, all reqs. (informative) |
|  |  |  |  |