IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11bc CC31 – Resolution for CIDs assigned to Abhi – Part 3 |
| Date: September 7, 2020 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Abhishek Patil | Qualcomm Inc. |  |  | appatil@qti.qualcomm.com |

 Abstract

This submission proposes resolutions for the following CIDs submitted during CC31 for 11bc D0.1 (7 CIDs):

244, 257, 254, 246, 49, 183, 362

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Updates based on feedback from Bahar
* Rev 2: Updated based on feedback received when the doc was presented on AM2 telco on 9/15/20

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbc Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbc Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbc Editor: Editing instructions preceded by “TGbc Editor” are instructions to the TGbc editor to modify existing material in the TGbc draft. As a result of adopting the changes, the TGbc editor will execute the instructions rather than copy them to the TGbc Draft.***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Type** | **Pg/Ln** | **Section** | **Comment** | **Proposed Change** | **Resolution** |
| 49 | Bahareh Sadeghi | T | 29.13 | 9.6.7.bc | In the eBCS UL frame format, the signature length can be variable and hence the AP needs to parse every packet to learn the length of the signature at the end of the frame. This adds complexity. It would be better to fix the signature length. | if there would be a way to fix the signature length or make it known it would reduce solution complexity. | **Revised**The text is revised to describe four schemes for providing source authentication (as defined in clause 12).**TGbc editor please make changes as shown in doc 11-20/1385r2 tagged as 49** |
| 257 | Mark RISON | T | 47.21 | 11.bc.3.3 | "The Frame Signature field when present in the frame shall carry the signature for the contents of the eBCS 21UL frame Action field except for the field itself." is not clear. Need a reference as to how the signature is calculated, exactly | As it says in the comment | **Revised**The text is revised to describe four schemes for providing source authentication (as defined in clause 12).**TGbc editor please make changes as shown in doc 11-20/1385r2 tagged as 257** |

[49, 257]

**9.6.7.bc eBCS UL frame format**

***TGbc editor: Please make changes to Figure 9-bc15 in this subclause as shown below:***

***NOTE: The baseline text in the paragraph below includes the changes proposed in doc 11-20/1298r1 for CID 318:***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | eBCS ULControl | Destination URI | HLPPayload Length | HLPPayload | STACertificate Length | STACertificate |
| Octets: | 1 | 1 | 1 | variable | 2 | variable | 0 or 2 | 0 orvariable |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Timestamp | eBCS ULCapabilities |  | Frame Signature |
| Octets: | 0 or 8 | 0 or 4 |  | 1. or variable
 |

 **Figure 9-bc15 - eBCS UL frame Action field format**

***TGbc editor: Please make changes to Figure 9-bc16 in this subclause as shown below:***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 – B5 | B6 – B7 |
|  | STACertificate Present | PacketNumber Present | eBCS ULCapabilities Present | Timestamp Present | Reserved | FrameSignature Type |
| Bits: | 1 | 1 | 1 | 1 | 2 | 2 |

**Figure 9-bc16 - eBCS UL Control field format**

***TGbc editor: Please modify the following paragraph and add a new Table in this subclause as shown below:***

The encoding of Frame Signature Type subfield is shown in Table 9-bcxx (Encoding of Frame Signature Type subfield).

**Table 9-bcxx - Encoding of Frame Signature Type subfield**

|  |  |  |
| --- | --- | --- |
| Subfield value | Definition | Encoding |
| 0 | HLSA | The authentication of uplink data is provided by higher layer and is included in the HLP Payload field and the Frame Signature field is not present |
| 1 | RSA-2048 | See 12.bc.2.5 (Signature of the eBCS UL frame) and 12.bc.2.2 (Authentication of an eBCS UL frame) |
| 2 | ECDSA-P256 |
| 3 | Ed25519 |

***TGbc editor: Please modify the following paragraphs in this subclause as shown below:***

The Frame Signature field when present carries signature for the contents of the eBCS UL frame Action field except the Frame Signature field.

**11.bc.3.3 eBCS UL operation at an eBCS non-AP STA**

***TGbc editor: Please modify the following paragraph in this subclause as shown below:***

The Frame Signature field when present in the frame shall carry the signature for the contents of the eBCS UL frame Action field except for the field itself. The contents of this field provides protection against any attack that attempts to tamper the content of the frame. Also see 12.bc.2.5 (Signature of the eBCS UL frame) and 12.bc.2.2 (Authentication of an eBCS UL frame).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 183 | Mark RISON | E | 30.35 | 9.6.7.bc | "The Frame Signature Length field indicated the length of the Frame Signature field. The presence of this 35field indicated by the Frame Signature Present subfield in the eBCS UL Control field being equal to 1. " duplicates "The Frame Signature Present subfield is set to 1 when the Frame Signature Length and Frame Signature 37fields are carried in the element. Otherwise the subfield is set to 0. " above | As it says in the comment | **Revised**Agree with the comment. Removed duplicate and redundant text with respect to the ‘Presence’ bit.**TGbc editor please make changes as shown in doc 11-20/1385r2 tagged as 183** |

[183]

**9.6.7.bc eBCS UL frame format**

***TGbc editor: Please modify the following paragraphs in this subclause as shown below:***

The STA Certificate Length field indicates the length of the STA Certificate field.

The STA Certificate field carries the certificate of the transmitting STA.

The Timestamp field provides protection against replay attack. The format of the Timestamp field is shown in Figure 9-bc17 - Timestamp field format.

***TGbc editor: Please modify the following paragraph in this subclause as shown below:***

The eBCS UL Capabilities element when present carries a request directed towards an eBCS AP, that provides forwarding service, to embed metadata (such as location, data or IP address) before forwarding the HLP contents to the remote destination.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 362 | Antonio DeLaOlivaDelgado  | T | 46.00 | 11.bc.3.2 | The UL operation should always consider rate limitation for the uplink frames sent by an STA, at least for unassociated ones. | Modify paragrpah: "In order to prevent DoS or injection attacks directed towards the remote destination, it is strongly recommended that eBCS APs that support forwarding service perform source authentication and validate the frame signature. For data recieved from un associated STAs, rate limiting is strongly recommended" | **Revised**Agree with the comment. Added text which recommends an eBCS AP to perform throttling to control the amount of content being forwarded to the remote server.**TGbc editor please make changes as shown in doc 11-20/1385r2 tagged as 362** |
| 244 | Mark RISON | T | 46.01 | 11.bc.3.1 | The description seems to suggest a non-AP STA might do an eBCS UL transmission to multiple APs, all of which might rebroadcast the data. Isn't this a recipe for network storms? Surely it should be restricted to the AP the STA is associated with? | As it says in the comment | **Reject**eBCS APs are not required to or suppose to rebroadcast data. Therefore, the concern raised by the comment does not apply. Further, it is recommended that an eBCS AP performs source authentication and apply throttling to regulate the amount of data it forwards the remote destination. |

[362]

**11.bc.3.2 eBCS UL operation at an eBCS AP**

***TGbc editor: Please make changes to the following paragraph in this subclause as shown below:***

***NOTE: The baseline text in the paragraph below includes the changes proposed in doc 11-20/1298r1 for CID 247:***

denial-of-service attack Furthermore, eBCS APs should throttle the amount or frequency of uplink it forwards to a remote server.

An eBCS AP that authenticates the transmitter of the packet before forwarding it to a remote destination shall provide an indication of the authentication scheme in the eBCS Capabilities element that it transmits. An eBCS AP that does not perform authentication of the transmitter shall forward the frame to the remote destination indicated in the frame irrespective of whether the frame carries the STA Certificate field or the Timestamp field or the Frame Signature field.

An eBCS AP may limit the amount or frequency of uplink data it forwards to a remote destination and shall provide an indication of the throttling scheme in the eBCS UL Capabilities element that it transmits.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 254 | Mark RISON | T | 47.00 | 11.bc.3.3 | A lot of this seems to duplicate Clause 9. Clause 9 is format and encoding and interpretation. Here we should only have behaviour. | As it says in the comment | **Revised**Agree with the comment. Revised text to remove duplications from clause 9. Also renamed the frame name so that the first character is not lower case. **TGbc editor please make changes as shown in doc 11-20/1385r1 tagged as 254** |

[254]

***TGbc editor: Please rename all instances of ‘eBCS UL frame’ to ‘UL eBCS frame’:***

**11.bc.3.3 eBCS UL operation at an eBCS non-AP STA**

***TGbc editor: Please make changes to the following paragraphs in this subclause as shown below:***

***NOTE: The baseline text in the paragraphs below includes the changes proposed in doc 11-20/1298r1 for CID 251, 252:***

An eBCS non-AP STA that intends to send data to a remote destination shall transmit an eBCS UL frame to the broadcast destination address (i.e., Address 1 and Address 3 fields are set to broadcast address) carrying data intended for a remote destination. The URI to the remote destination shall be carried in the frame. The frame may also carry additional request from the transmitting STA to the forwarding AP and fields for source authentication, preventing replay attack and protecting the contents of the frame.

The format of the eBCS UL frame is described in 9.6.7.bc (eBCS UL Frame Format).

***TGbc editor: Please make changes to the following paragraph in this subclause as shown below:***

***NOTE: The baseline text in the paragraphs below includes the changes proposed in doc 11-20/1298r1 for CID 256:***

An eBCS non-AP STA may request an eBCS AP, that provides forwarding service, to embed metadata (such as location, data or IP address) by including the eBCS UL Capability element in the eBCS UL frame.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 246 | Mark RISON | T | 46.00 | 11.bc.3.2 | The eBCS Non-AP UL Capabilities element is weird, because it is apparently also used in eBCS UL frames, in which case it's not capabilities, it's some kind of request | Make the Capabilities element be used only to signal capabilities. Create a new element (or a new field) for the optional eBCS UL frame request info | **Revised**Agree with the commenter. The element carries AP’s capabilities when included in a Beacon or Probe frame. While it carries request from a non-AP STA in an eBCS UL frame.In addition, this element need not be limited to providing uplink capabilities, instead can be used to carry DL capabilities of the AP (or non-AP).Further, the name of an element should not start with a lower case letter.Therefore, propose to rename the element to E-BCS Parameters element.Furthermore, the subclause describing AP and non-AP’s usage of the element is renamed to E-BCS AP Parameters and E-BCS Non-AP Parameters.**TGbc editor: Throughout the 802.11bc spec:****Please rename all instances of ‘eBCS UL Capabilities’ element to ‘E-BCS Parameters’ element.****Please rename all instances of ‘eBCS AP UL Capabilities’ element to ‘E-BCS AP Parameters’.****Please rename all instances of ‘eBCS Non-AP UL Capabilities’ element to ‘E-BCS Non-AP Parameters’.** |