IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11bc LB 252 resolution for CIDs assigned to Abhi (part 3) |
| Date: April 8, 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Abhishek Patil | Qualcomm Inc. |  |  | appatil@qti.qualcomm.com |
| George Cherian |  |  |  |
| Jouni Malinen |  |  |  |
| Mark Rison | Samsung |  |  |  |
| Stephen McCann | Huawei |  |  |  |
| Bahar Sadeghi | Intel |  |  |  |
| Tomo Adachi | Toshiba |  |  |  |

 Abstract

This submission proposes resolutions for the following 43 comments submitted during LB 252 for 11bc D1.0:

1087, 1088, 1044, 1554, 1268, 1441, 1601, 1323, 1408, 1260, 1081, 1630, 1318, 1324, 1322, 1321, 1320, 1319, 1583, 1326, 1328, 1329, 1631, 1330, 1331, 1334, 1165, 1336, 1335, 1338, 1356, 1337, 1418, 1584, 1354, 1350, 1034, 1352, 1357, 1386, 1348, 1349, 1037

Revisions:

* Rev 0: Initial version of the document.
* Rev 1:
	+ Revised based on feedback from Mark Rison and Stephen McCann. Added as co­-authors
	+ Added several CIDs from clause 11 which were getting resolved anyways!
* Rev 2:
	+ Several updates to the replay protection logic based on offline and on-call discussions
	+ Deleted Replay Protection field and updated text to separately signal Frame Tx Time and Frame Count subfields in EBCS UL frame
		- Added corresponding ‘presence’ indicators to the Control field in the frame
	+ Size of Frame Count subfield increased to 48-bits
	+ Frame Count subfield is checked for replay protection only if the frame includes Frame Signature field and the verification of Frame Signature is ‘pass’
		- Frame Count is compared against last known (if any) Frame Count value
	+ Additional CIDs related to clause 11 are resolved
	+ Spec text to clarify that the EBCS UL frame is transmitted by a non-AP STA that is not associated with any AP
		- Addition based on offline discussion with Tomo and Bahar
		- Helps resolve CIDs 1630 & 1631
* Rev 3:
	+ Updated based on offline feedback from Mark Rison
* Rev 4:
	+ Live updates made when the doc was discussed during TGbc telco 5/11/21 and 5/12/21
	+ Removed the comments table from this document since doc 11-21/306 is tracking it.
		- It was getting cumbersome to keep the two version up to date.
		- Live updates were made to doc 11-21/306 during the telco

***TGbc Editor: The baseline for the proposed changes is 802.11bc D1.02***

**9.4.2.296 EBCS Parameters element**

***TGbc Editor: please make changes to this clause as shown below:***

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]An EBCS AP advertises its EBCS operational parameters in the EBCS Parameters element.

788ee

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension |  | EBCS Info Frame Tx Countdown |
| Octets: | 1 | 1 | 1 |  | 2 |

**Figure 9-788ee - EBCS Parameters element format**[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

[CID 1087][CID 1087]

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

[CID 1088, 1044, 1554][CID 1088, 1044, 1554][CID 1268, 1601, 1441][CID 1087]The EBCS Info Frame Tx Countdown field indicates the number of TBTTs until the transmission of the next EBCS Info frame. The value 1 indicates that the frame is transmitted following the next TBTT. The value 0 is reserved.

**9.3.3.2 Beacon frame format**

***TGbc Editor: please make changes to the following row in Table 9-32 as shown below:***

**Table 9-32**—**Beacon frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 93 | EBCS Parameters element | [CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]This element is optionally present if dot11EBCSSupportActivated is true. |

**9.3.3.10 Probe Response frame format**

***TGbc Editor: please make changes to the following row in Table 9-41 as shown below:***

**Table 9-41**—**Probe Response frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 113 | EBCS Parameters element | [CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]This element is optionally present if dot11EBCSSupportActivated is true. |

**9.4.2.26 Extended Capabilities element**

***TGbc Editor: please insert a new row to Table 9-153 as shown below:***

**Table 9-153—Extended Capabilities field**[CID 1087]

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | EBCS Relaying Supported | An AP that has dot11EBCSRelayingServiceSupported equal to true sets the EBCS Relaying Supported field to 1. Otherwise an AP sets the field to 0. A non-AP STA sets the field to 0. |

**9.6.7.100 EBCS UL frame format**

The EBCS UL frame is transmitted by an EBCS non-AP STA and carries higher layer payload intended for a destination specified within the frame.

The format of the EBCS UL frame Action field is defined in Figure 9-909b (EBCS UL frame Action field format).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Category | Public Action | Control | Destination URI | HLP Container | STA Certificate Container (optional) | Frame Tx Time (optional) | Frame Count(optional) | Frame Signature (optional) |
| Octets: | 1 | 1 | 1 | variable | variable | variable | 0 or 4 | 0 or 6 | variable |

 **Figure 9-909b - EBCS UL frame Action field format**

The Category field is defined in 9.4.1.11 (Action field).

The Public Action field is defined in 9.6.7.1 (Public Action frames).

the

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | B0 | B1 | B2 | B3 B5 | B6 B7 |
|  |  |  | STACertificate Present | Frame Tx Time Present | Frame Count Present | Frame Signature Type  | Reserved |
| Bits: |  |  | 1 | 1 | 1 | 3 | 3 |

 **Figure 9-909c - Control field format**[CID 1268, 1601, 1441, 1354, 1350]

[CID 1268, 1601, 1441][CID 1268, 1601, 1441]The STA Certificate Present subfield is set to 1 when the STA Certificate Container field is carried in the frame. Otherwise, the subfield is set to 0.

[CID 1354, 1350]The Frame Tx Time Present subfield is set to 1 when the Frame Tx Time field is carried in the frame. Otherwise, the subfield is set to 0.

[CID 1354, 1350]The Frame Count Present subfield is set to 1 when the Frame Count field is carried in the frame. Otherwise, the subfield is set to 0.

The encoding of the Frame Signature Type subfield is shown in Table 9-397a (Encoding of Frame Signature Type subfield).

 **Table 9-397a - Encoding of Frame Signature Type subfield**

|  |  |  |
| --- | --- | --- |
| **Subfield value** | **Algorithm** | **Encoding** |
| 0 | HLSA | The authentication of the HLP payload is provided by a higher layer and is included in the HLP Payload field |
| 1 | RSA-2048 | See 12.100.2.5 (Signature of the EBCS UL frame)[CID 1087] |
| 2 | ECDSA-P256 |
| 3 | Ed25519 |
| 4-7 | Reserved |  |

The Destination URI field contains a Destination URI element as defined in 9.4.2.89 (Destination URI element) that specifies the destination to which the HLP payload needs to be relayed.

The format of the HLP Container field is shown in Figure 9-909d (HLP Container field format).

|  |  |  |
| --- | --- | --- |
|  | HLP Payload Length | HLP Payload |
| Octets: | 2 | variable |

**Figure 9-909d – HLP Container field format**

The HLP Payload Length subfield indicates the length of the HLP Payload subfield in octets.

The HLP Payload subfield carries the HLP payload.

The format of the STA Certificate Container field is shown in Figure 9-909e (STA Certificate Container field format).

|  |  |  |
| --- | --- | --- |
|  | STA Certificate Length | STA Certificate |
| Octets: | 2 | variable |

**Figure 9-909e – STA Certificate Container field format**

The STA Certificate Length subfield carries a nonzero value that indicates the length of the STA Certificate subfield in octets.

The STA Certificate subfield carries the X.509v3 certificate of the STA encoded according to IETF RFC 5280.

[CID 1354, 1350]

|  |  |  |
| --- | --- | --- |
|  |  |  |

[CID 1354, 1350]The Frame Tx Time field, if present, carries the time, expressed as number of seconds since 2020-01-01 00:00:00 UTC, when the frame is queued for transmission.

[CID 1354, 1350]The Frame Count field, if present, carries a numeric value that is incremented for each EBCS UL frame transmission.

[CID 1087]The Frame Signature field is not present if the Frame Signature Type subfield indicates HLSA. Otherwise, the field is present and carries a signature of the EBCS UL frame (see 12.100.2.5 (Signature of the EBCS UL frame)).

##### 11.100.3.1 General

***TGbc Editor: please make changes to this clause as shown below:***

[CID 1087]The EBCS UL Service procedure allows a non-AP STA to transmit an EBCS UL frame with the expectation that one or more EBCS proxies that are affiliated with one or more EBCS APs in the neighborhood would relay the HLP payload carried in the frame to a destination specified in the frame. [CID 1268, 1601, 1441, 1323]

[CID 1321]NOTE – The relaying service is best effort with no guarantee that the HLP payload will be delivered to the [CID 1319]specified destination.[CID 1268, 1601, 1441]

##### 11.100.3.2 EBCS UL operation at an EBCS AP

***TGbc Editor: please make changes to this clause as shown below:***

[CID 1087, 1088, 1044, 1544, 1268, 1601, 1441]An EBCS AP that is affiliated with an EBCS proxy (see 4.5.xx (EBCS relaying service)) provides access to a relaying service in which the HLP payload carried in an EBCS UL frame received from an EBCS non-AP STA is relayed to a destination specified in the frame. Among all APs in a multiple BSSID set, only the AP corresponding to the transmitted BSSID shall be affiliated with an EBCS proxy. Among all APs in a co-hosted BSSID set, only one AP shall be affiliated with an EBCS proxy.

[CID 1087, 1326]An EBCS AP that provides access to a relaying service shall have dot11EBCSRelayingServiceSupported equal to true. Otherwise dot11EBCSRelayingServiceSupported shall not be true. [CID 1268, 1601, 1441][CID 1268, 1601, 1441][CID 1329, 1330]

[CID 1268, 1601, 1441]An EBCS proxy evaluates various criteria such as the ones described in 12.100.2.6 (Authentication of an EBCS UL frame) to decide whether to relay the HLP payload to the specified destination. An EBCS proxy may limit the amount or frequency of HLP payloads that are relayed to the specified destination. An EBCS proxy may append additional information before relaying the HLP payload to the specified destination. The evaluation of criteria, the decision to limit the amount or frequency of relaying, and the decision to append addition information can be based on local policies or based on a relationship established with the specified destination.

NOTE 1 – The establishment of such a relationship is out of scope of this standard.

NOTE 2 – An EBCS proxy can decide to not relay the HLP payload for any reason such as not having a relationship with the specified destination, the implemented criteria for relaying not being satisfied or for any other reason.

[CID 1329, 1330]NOTE 3 – An EBCS proxy generates an IP packet carrying the HLP payload and addressed to the specified destination when the criteria for relaying are met.

[CID 1087, 1334]

[CID 1087][CID 1088, 1044, 1554][CID 1087]

* + - 1. **EBCS UL operation at an EBCS non-AP STA**

***TGbc Editor: please make changes to this clause as shown below:***

An EBCS non-AP STA may request relaying of an HLP payload to a specific destination by transmitting an EBCS UL frame. The frame carries the URI of the intended destination.[CID 1087, 1268, 1601, 1441] The Address 1 and Address 3 fields of the frame shall be set to the broadcast address.

[CID 1087]An EBCS non-AP STA should include a STA certificate in an EBCS UL frame to help authenticate it (see 12.100.2.6 (Authentication of an EBCS UL frame)).

[CID 1352, 1354, 1350]An EBCS non-AP STA should include the Frame Count field in an EBCS UL frame that it transmits to reduce the possibility of a successful replay attack. Frame Tx Time Present subfield in the Control field shall be set to 1 and the Frame Tx Frame Tx Time Present of the Control field and the Frame Tx Time field is not present in the frame When the STA provides a frame count, the Frame Count Present subfield of the Control field shall be set to 1 and tshall beset to 1 in the first EBCS UL frame that the STA transmits and shall be subsequent of an EBCS UL frame; otherwise the Frame Count Present subfield of the Control field shall be set to 0 and the Frame Count field is not present in the frame[CID 1260, 1357]

NOTE—How a STA obtains time information is out of scope of this standard.

[CID 1268, 1601, 1441][CID 1087, 1348]The Frame Signature field, if present in the EBCS UL frame, shall be computed as defined in 12.100.2.5 (Signature of the EBCS UL frame).

[CID 1087, 1386]An EBCS non-AP STA is not required to monitor the WM and may transmit an EBCS UL frame without discovering nearby EBCS APs that provide access to the relaying service.

**12.100.2.6 Authentication of an EBCS UL frame**[CID 1334, 1034, 1037, 1354, 1350]

***TGbc Editor: please make changes to this clause as shown below:***

An EBCS proxy shall discard an EBCS UL frame if any of the following conditions are met:

1. The STA Certificate subfield is present and any of the following conditions are met:
	1. The certificate of the authority (i.e., specified destination or the CA that signed the STA’s certificate) is not installed.
	2. The verification of the STA’s certificate using the installed certificate fails.
	3. The Frame Signature Type subfield does not indicate HLSA and the verification of the signature of the frame using the STA’s certificate fails.
	4. The Frame Signature Type subfield does not indicate HLSA and the verification of the signature of the frame using the STA’s certificate has passed and the Frame Count field is present, and the value is less than or equal to the *last seen Frame Count* (if any) from the EBCS non-AP STA.
2. The Frame Tx Time field is present and the difference between the value carried in the field and the time when the EBCS UL frame is received is greater than an acceptable value.

NOTE 1 – The acceptable time difference at an EBCS proxy can be selected based on local policies or based on the relationship with the specified destination. The selection of an acceptable time difference is out of scope of this standard.

NOTE 2 – When the Frame Signature Type subfield indicates HLSA, replay protection is performed by a higher layer and is out of scope of this standard.

An EBCS proxy shall save the value in the most recently received Frame Count field of an EBCS UL frame, as *last seen Frame Count*, for a certain transmitter only if the EBCS UL frame was not discarded based on the conditions above. In addition, an EBCS proxy may have an expiration time after which the *last seen Frame Count* value for a certain transmitter is discarded.

**6.3.201.2.2 Semantics of the service primitive**[CID 1268, 1601, 1441, 1334, 1034, 1037, 1354, 1350]

***TGbc Editor: please make changes to this clause as shown below:***

The primitive parameters are as follows:

 MLME-EBCSUL.request(

DestinationURI,

HLPPayload,

STACertificate,

FrameTxTime,

FrameCount,

PrivateKey

 )

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
|  |  |  |  |
|  |  |  |  |
| DestinationURI | Destination URI element | As defined in 9.4.2.89(Destination URI element). | Specifies the destination to which the HLP payload is to be relayed. |
| HLPPayload | Sequence of octets | N/A | Specifies the HLP payload to be relayed to the specified destination. |
| STACertificate | Sequence of octets | N/A | When present, specifies the certificate for the STA. |
| FrameTxTime | Frame Tx Time field as defined in 9.6.7.100 | As defined in 9.6.7.100 | When present, specifies the time when an EBCS UL frame is queued for transmission |
| FrameCount | Frame Count field as defined in 9.6.7.100 | As defined in 9.6.7.100 | When present, specifies a count of the number of EBCS UL frame transmissions. |
| PrivateKey | Sequence of octets | N/A | When present, specifies the private key for signature generation. |

**6.3.201.3.2 Semantics of the service primitive**[CID 1268, 1601, 1441, 1334, 1034, 1037, 1354, 1350]

***TGbc Editor: please make changes to this clause as shown below:***

The primitive parameters are as follows:

 MLME-EBCSUL.indication(

DestinationURI,

HLPPayload,

FrameTxTime,

FrameCount

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
|  |  |  |  |
|  |  |  |  |
| DestinationURI | Destination URI element | As defined in9.4.2.89 (Destination URI element). | Specifies the destination to which the HLP payload is to be relayed. |
| HLPPayload | Sequence of octets | N/A | Specifies the HLP payload to be relayed to the specified destination. |
| FrameTxTime | Frame Tx Time field as defined in 9.6.7.100 | As defined in 9.6.7.100 | When present, specifies the time when an EBCS UL frame is queued for transmission |
| FrameCount | Frame Count field as defined in 9.6.7.100 | As defined in 9.6.7.100 | When present, specifies a count of the number of EBCS UL frame transmissions. |

***TGbc Editor: please insert the following subclause at the end of clause 4.5 [text based on doc 11-21/0568r4]:***

[CID 1087, 1088, 1044, 1554, 1268, 1601, 1441, 1081]

**4.5.xx EBCS relaying service**

**4.5.xx.1 General**

The EBCS relaying service provides a mechanism for an EBCS non-AP STA to send an HLP payload to a specified destination.

**4.5.xx.2 EBCS proxy operation**

An EBCS proxy is a logical component affiliated with an EBCS AP, and which might be collocated with the EBCS AP, that can relay an HLP payload carried in an EBCS UL frame received by an EBCS AP to a destination specified in the frame, typically within an external network.

An EBCS proxy that provides the relaying service evaluates certain criteria before relaying the HLP payload carried in an EBCS UL frame to the destination specified in the frame. Such criteria can include, but are not limited to, verifying the STA certificate, if present, to determine whether the STA transmitting the frame is authorized to send an HLP payload to the specified destination, performing replay checking, and limiting the amount or frequency of HLP payload that is relayed to the specified destination. The evaluation of the criteria can be based on local policies installed at the EBCS proxy and/or based on a relationship established with the specified destination. The establishment of such a relationship is out of scope of this standard.

An EBCS proxy can establish more than one relationship, each with a different destination and potentially different criteria. An EBCS proxy can also append additional information before it relays the HLP payload. The format and content of the information appended are based on the agreement with the specified destination. The relaying service is best effort and the EBCS proxy can decide not to relay the HLP payload if any of the implemented criteria for relaying are not satisfied or for any other reason.

NOTE 1 – The communication between an EBCS AP and an EBCS proxy and the communication between an EBCS proxy and a specified destination are out of scope of this standard.

NOTE 2 – An EBCS proxy evaluating various criteria before it relays an HLP payload helps reduce the likelihood of a DoS attack on the specified destination.

**4.5.xx.3 Example configurations for EBCS proxy**

Figure 4-20a (Illustration of relaying operation at an EBCS AP with collocated EBCS proxy) provides an example of the relaying service based on a relationship with a specified destination. In the figure, EBCS proxy P1 and EBCS proxy P3 have established a relationship with a destination (D). An EBCS non-AP STA (S) transmits an EBCS UL frame that is received by EBCS APs in the neighborhood (i.e., AP1, AP2 and AP3). The EBCS UL frame carries the HLP payload, a field carrying the address of D and other fields for security. P1 and P3 verify the certificate of S based on their agreement with D and perform a replay check, to determine whether the criteria for relaying the HLP payload to D are met. If the local policy or the agreement with D requires limiting the amount or frequency of HLP payloads being sent to D, then each of P1 and P3 does not send an HLP payload to D, if it determines that a limit was reached. If the agreement with D requires the inclusion of additional information, P1 and P3 append appropriate information, before relaying the HLP payload. In the figure, EBCS AP2 discards the EBCS UL frame. This could be for any number of reasons such as it not providing a relaying service, its collocated proxy not having established a relationship with D, or one or more criteria for relaying not having been satisfied.

**Figure 4-20a: Illustration of relaying operation at an EBCS AP with collocated EBCS proxy**

In another example, depicted in Figure 4-20b (Illustration of relaying when EBCS proxy is not collocated within an EBCS AP), the EBCS proxy (P) is not collocated with either EBCS AP1 or EBCS AP3, but resides on an entity in the LAN that AP1 and AP3 belong to. EBCS AP1 and EBCS AP3 send the contents of the EBCS UL frame to P, which evaluates whether the criteria for relaying are met before it relays the HLP payload to the specified destination.

**Figure 4-20b: Illustration of relaying when EBCS proxy is not collocated within an EBCS AP**

The configuration shown in Figure 4-20b (Illustration of relaying when EBCS proxy is not collocated within an EBCS AP) could be prevalent in commercial deployments, such as airports, train stations, malls, or a warehouse, where multiple EBCS APs are likely to be connected to a single entity on a common LAN (such as a network controller) which provides access to destinations outside the LAN. In such a configuration, the EBCS proxy resides on an entity in the LAN. On the other hand, the configuration shown in Figure 4-20a (Illustration of relaying operation at an EBCS AP with collocated EBCS proxy) could be prevalent in residential deployments where an EBCS AP has direct connectivity to destinations outside the LAN.

NOTE – Where a destination has relationships with multiple EBCS proxies, it might, as part of the relationship with each proxy, set a relaying limit (e.g., amount or frequency of relaying per proxy) so that the aggregate from all the proxies is below a certain threshold. In addition, EBCS proxies might collaborate to limit the aggregate payload being relayed to the specified destination. Such mechanisms are out of scope of this standard.[CID 1337]

**C.3 MIB Detail**

***TGbc Editor: please insert a new entry to the following paragraph:***

***Change the end of the “Dot11StationConfigEntry” of the “dot11StationConfig TABLE” as follows:***

 …

 dot11EBCSTerminationNoticeMaximumInterval, Unsigned32,

 dot11EBCSRelayingServiceSupported TruthValue[CID 1087]

 }

***TGbc Editor: please insert a new entry to the following paragraph:***

***Insert the following elements at the end of the dot11StationConfigTable element definitions:*** [CID 1087]

dot11EBCSRelayingServiceSupported OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities. This attribute when true, indicates that the EBCS AP is affiliated with an EBCS proxy that provides relaying service. The capability is disabled otherwise."

::= { dot11StationConfigEntry <ANA> }

***TGbc Editor: please insert a new entry to the following paragraph:***

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* Compliance Statements - EBCS

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

dot11EBCSComplianceGroup OBJECT-GROUP

OBJECTS {

 …

 dot11EBCSTerminationNoticeMaximumInterval,

 dot11EBCSRelayingServiceSupported[CID 1087]

 }

 STATUS current