IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGme LB258 Miscellaneous MAC Comment Resolutions | | | | |
| Date: 2022-06-24 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | [montemurro.michael@gmail.com](mailto:montemurro.michael@gmail.com) |

Background

This contribution proposes comment resolutions to MAC adhoc comments received in LB258 on REVme D1.0. The resolutions will be shown relative to D1.0.

CIDs 1388, 1464, 1465, 1515, 1528, 1689, 1756, 1792, 1796, 1835, 1551, and 1552.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1388 | 2750.00 | 11.3.5.4 |  |  | "Except when the association is part of a fast BSS transition, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA and temporal keys held for communication with the AP or PCP by using the MLME- DELETEKEYS.request primitive (see 12.6.18 (RSNA security association termination)) before invoking an MLME-REASSOCIATE.request primitive." -- so for fast BSS transition, the SAs and keys are retained ... but the PNs are always reset (under c)4) | Change "Except when the association is part of a fast BSS transition, t" to "T" |

### Discussion:

* The cited text is:

A screenshot of a computer

Description automatically generated with medium confidence

* Updated based on comments from Mark Rison.
* The proposed change is to change:

“Except when the association is part of a fast BSS transition, the”

To

“The”

* In the case of a fast BSS Transition in the successful case, the old keys are not deleted until after the (re)association completes. See 3291.29.

### Proposed Resolution: (1388)

REJECTED. In the case of fast BSS transition, the keys are deleted after successful reassociation as per 3291.29.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1464 | 2684.00 | 11.1.4.6 |  |  | "The Supported Rates and BSS Membership Selectors element and Extended Supported Rates and BSS Membership Selectors element in Beacon and Probe Response frames is used by STAs in order to avoid associating with a BSS if they do not support all of the data rates in the BSSBasicRateSet parameter or all of the BSS membership requirements in the BSSMembershipSelectorSet parameter." -- it's more than just associating; it also applies to IBSS, MBSS and non-associating PBSS | Change "to avoid associating with" to "to avoid joining" |

### Discussion:

* The cited text in context is:

A screenshot of a computer

Description automatically generated with medium confidence

* The comment indicates that the cited element are used by a STA in order to select an IBSS, PBSS, or MBSS. Since not all of those cases use association, its probably better to use join rather than associate.

### Proposed Resolution: (1464)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1465 | 2685.00 | 11.1.5 |  |  | "Together, these parameters are used by the management entity in a STA to avoid associating with a BSS if the STA cannot receive and transmit all of the data rates in the BSSBasicRateSet" -- it's more than just associating; it also applies to IBSS, MBSS and non-associating PBSS | Change "to avoid associating with" to "to avoid joining" |

### Discussion:

* This CID is similar to CID 1464
* Cited text is the following

Text, letter

Description automatically generated

* The comment indicates that the cited element are used by a STA in order to select an IBSS, PBSS, or MBSS. Since not all of those cases use association, its probably better to use join rather than associate.

### Proposed Resolution: (1465)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1515 | 2082.00 | 10.2.7 |  |  | "MSDUs or MMPDUs carried in a group addressed MPDU shall not be fragmented" -- an MPDU cannot by definition be fragmented (though it can be a fragment) | Change to "A group addressed MPDU shall not be a fragment" |

### Discussion:

* Cited text is:

Text

Description automatically generated

* Updated based on comments from Mark Rison.
* The comment is correct that an MPDU cannot be a fragement. However it would be good to modify the sentence to reflect that the MPDU shall not carry a fragment of an MSDU or MMPDU since the latter part of the sentence refers to the length of the MSDU or MMPDU.
* An updated resolution could be:

Change

“MSDUs or MMPDUs carried in a group addressed MPDU shall not be fragemented”

To

“A group addressed MPDU shall not be a fragment of an MSDU or MMPDU”

### Proposed Resolution: (1515)

REVISED. Relative to D1.0 at 2082.11, change

“MSDUs or MMPDUs carried in a group addressed MPDU shall not be fragemented even if their length exceeds the dot11Fragmentation threshold.”

To

“A group addressed MPDU shall not carry a fragmented of an MSDU or MMPDU even if the length of the MSDU or MMPDU exceeds the dot11FragmentationThreshold.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1528 | 3082.00 | 11.52 |  |  | Given beacon protection, we also need broadcast probe response protection in FILS, or at least a statement that thou shalt not trust unprotected broadcast probe responses | At the end of the third para of the referenced subclause add "If dot11BeaconProtectionEnabled is true, a non-AP STA shall discard broadcast Probe Response frames." |

### Discussion:

* The cited text is: A screenshot of a computer

  Description automatically generated with medium confidence
* Beacon protection is enabled on the AP but only provides protection to associated STAs.
* A STA has no security association or is not associated with an AP has no way to trust any information it receives in Beacons, Probe Response, or FILS Discovery frames.
* A STA can make use of untrusted broadcast Probe Response and FILS Discovery frames to discover an AP. A STA could verify the information in Beacon frames after it has successfully associated.
* A STA that is associated to an AP could discover neighboring APs using FILS Discovery or broadcast Probe Response frames.
* *Comment from Mark Rison “There’s still a problem if an associated STA believes a broadcast probe response purportedly from its AP”* – In that case, any information in a broadcast Probe Response could be validated against information in a Beacon frame.

### Proposed Resolution: (1528)

REJECTED. Beacon protection only provides protection to associated STAs. It does not apply to unassociated STAs. Unassociated STAs can use broadcast Probe Response frames and FILS discovery frames to discover APs however, the information received in such frames cannot be trusted. The proposed change would limit the STAs ability to discover APs.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1689 | 2847.00 | 11.12 |  |  | "For all other group addressed Management frames, the group addressed frame protection service shall take the following actions: -- Management frame protection for multicast/broadcast shall be set using the MLME- SETPROTECTION.request primitive with the Protectlist including a Key Type value of IGTK. A non-AP STA shall also set the Protect Type value to Rx. In an IBSS, a STA shall set the ProtectType value to Rx\_Tx. An AP shall set the Protect Type value to Tx. -- The IGTK shall be installed using the MLME-SETKEYS.request primitive with the value IGTK for the Key Type parameter of the SetKeyDescriptor. -- The frames shall be encapsulated and protected using BIP (see 12.5.4 (Broadcast/multicast integrity protocol (BIP)))." -- should be clearer that there is also a protection service for Beacon frames, though it is not 100% clear what the scope of "the group addressed frame protection service" is | Change to ""For all other group addressed Management frames except for Beacon frames, the group addressed frame protection service shall take the following actions: -- Management frame protection for multicast/broadcast shall be set using the MLME- SETPROTECTION.request primitive with the Protectlist including a Key Type value of IGTK. A non-AP STA shall also set the Protect Type value to Rx. In an IBSS, a STA shall set the ProtectType value to Rx\_Tx. An AP shall set the Protect Type value to Tx. -- The IGTK shall be installed using the MLME-SETKEYS.request primitive with the value IGTK for the Key Type parameter of the SetKeyDescriptor. -- The frames shall be encapsulated and protected using BIP (see 12.5.4 (Broadcast/multicast integrity protocol (BIP)))." -- should be clearer that there is also a protection service for Beacon frames, though it is not 100% clear what the scope of "the group addressed frame protection service" is)" |

### Discussion:

* The comment is “-- should be clearer that there is also a protection service for Beacon frames, though it is not 100% clear what the scope of "the group addressed frame protection service" is”
* The cited text is:

Graphical user interface, text, application

Description automatically generated

* The proposed change is:

Change

“For all other group addressed Management frames, the group addressed frame protection service shall take the following actions:”

To

“For all other group addressed Management frames except for Beacon frames, the group addressed frame protection service shall take the following actions:”

* Since Beacon frames are group-addressed and are covered by beacon protection, the proposed text change makes sense.
* Feedback from reflector: “We have already discussed and resolved CID 1813, which adds the word “robust”, so the “For all other…” bullet now only includes robust Management frames. Beacon frames are excluded with this change.
* No additional changes required beyond the changes for CID 1813.

### Proposed Resolution: (1689)

REVISED. The resolution to CID 1813 addresses the issue described in this comment. Make the changes marked as "The proposed changes for CID 1813" in 11-22/0740r3 (https://mentor.ieee.org/802.11/dcn/22/11-22-0740-03-000m-proposed-resolutions-to-some-lb258-comments.docx). This includes the changes proposed in the comment and additional changes to 4.5.4.9 to clean up the description of management frame protection protocol applicability to group addressed frames.

Note to Editor: No addition changes required.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1756 | 3320.00 | 14.2.6 |  |  | "To actively scan, the mesh STA shall transmit Probe Request frame containing a wildcard Mesh ID or the desired Mesh ID." -- needs to obey various other rules about backoff etc. Also missing article | Change to "To actively scan, the mesh STA shall follow the procedures in 11.1.4.3, using a wildcard Mesh ID or the desired Mesh ID in the Probe Request frame(s)." |

### Discussion:

* Cited text is:

A screenshot of a computer

Description automatically generated with medium confidence

* The proposed change is:

Change

“To actively scan, the mesh STA shall transmit Probe Request frame containing a wildcard Mesh ID or the desired Mesh ID.”

To

“To actively scan, the mesh STA shall follow the procedures in 11.1.4.3, using a wildcard Mesh ID or the desired Mesh ID in the Probe Request frame(s)."

* Clause 11.1.4.3 is the Clause describing active scanning and probing procedures
* The proposed change looks to improve the text.

### Proposed Resolution: (1756)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1792 | 2083.00 | 10.2.8 |  |  | "the STA also validates the BSSID to verify either that the group addressed frame originated from a STA in the BSS of which the receiving STA is a member, or that it contains the wildcard BSSID value" | Change to "the STA also validates the BSSID to verify that it corresponds to the BSS of which the receiving STA is a member, or it is the wildcard BSSID value" |
| 1796 | 2083.00 | 10.2.8 |  |  | "the STA also validates the BSSID to verify either that the group addressed frame originated from a STA in the BSS of which the receiving STA is a member, or that it contains the wildcard BSSID value, indicating a Data frame sent outside the context of a BSS (dot11OCBActivated is true in the transmitting STA)." -- a STA should not be required to receive OCB data | "the STA also validates the BSSID to verify either that the group addressed frame originated from a STA in the BSS of which the receiving STA is a member, or, if dot11OCBActivated is true, that it contains the wildcard BSSID value, indicating a Data frame sent outside the context of a BSS." |

### Discussion:

* Updated based on comments from Mark Rison.
* The clause is 10.2.8 which describes the MAC data service.
* The cited paragraph is:

Text

Description automatically generated with low confidence

* Updated based on comments from Mark Rison
* The proposed change for CID 1792 is, change:

“the STA also validates the BSSID to verify either that the group addressed frame originated from a STA in the BSS of which the receiving STA is a member, or that it contains the wildcard BSSID value,”

To

“the STA also validates the BSSID to verify that it corresponds to the BSS of which the receiving STA is a member, or it is the wildcard BSSID value,”

* + The quoted sentence refers to the frame as being received either in a BSS or OCB. The either/or should remain.
  + It would be better to make this cited text a separate sentence since the beginning of the sentence refers to the Address 1 or DA field.
* The proposed change for CID 1796 is, change”

“, or that it contains the wildcard BSSID value, indicating a Data frame sent outside the context of a BSS (dot11OCBActivated is true in the transmitting STA).”

To

“, or, if dot11OCBActivated is true, that it contains the

wildcard BSSID value, indicating a Data frame sent outside the context of a BSS.”

* The change looks OK since dot11OCBActivated is true when the STA is operating in OCB mode.

### Proposed Resolution: (1792, 1796)

REVISED. Change

“, and the STA also validates the BSSID to verify either that the group addressed frame originated from a STA in the BSS of which the receiving STA is a member, or that it contains the wildcard BSSID value, indicating a Data frame sent outside the context of a BSS (dot11OCBActivated is true in the transmitting STA).”

To

“. The STA also validates the BSSID to verify that it either corresponds to the BSS of which the receiving STA is a member, or if dot11OCBActivated is true, that it contains the wildcard BSSID value, indicating a Data frame sent outside the context of a BSS.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1835 | 1538.00 | 9.4.2.153 |  |  | "NOTE--The structure of the LLC header is defined in IEEE Std 802.2-1998. The structure of the LLC with SNAP extension is defined in IEEE Std 802.2-1998. " -- 802.2 doesn't exist anymore | Delete the cited text |

### Discussion:

* The cited text in context is:

Table

Description automatically generated

* This element refers to LPD behavior and the element is used in an ADDTS.
* In other clauses that provide a reference to the LLC header, the standard uses the ISO/IEC document: “ISO/IEC 8802-2:1998, Information technology — Telecommunications and information exchange between systems—Local and metropolitan area networks — Specific requirements — Part 2: Logical link control.”
* For examples, see Clause 5.1.4 MSDU format (p353.35) “There are two LLC sublayer protocols used (see IEEE Std 802): LLC Protocol Discrimination (LPD) (see ISO/IEC 8802-2:1998) and Ethertype Protocol Discrimination (EPD) (see IEEE Std 802.3-2018).”
* Also see Annex H Usage of Ethertype 89-0d (5841.21) - LLC is defined in ISO/IEC 8802-2:1998.

### Proposed Resolution: (1835)

REVISED. Cross references to the LLC header definition cites ISO/IEC 8802-2:1998. At 1538.49, change “IEEE Std 802.2-1998” to “ISO/IEC 8802-2:1998” in two locations in the note.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 1551 | 1290.00 | 9.4.2.24.2 |  |  | It is not clear whether you are allowed to use CCMP with BIP-GMAC | At the end of the para at the referenced location add "Use of BIP-CMAC with a GCMP data cipher suite is valid." |
| 1552 | 1290.00 | 9.4.2.24.2 |  |  | It is not clear whether you are allowed to use CCMP-m with BIP-CMAC-n, where n != m | At the end of the para at the referenced location add "Use of BIP-CMAC-n with CCMP-m as the data cipher suite, where n is not the same as m, is valid." where n and m should be italicised |

### Discussion:

* The cited text in context is:

Graphical user interface, text, application, email

Description automatically generated

* As described in the text preceding the cited text, there can be multiple pairwise cipher suites and a single group data cipher suite. The cited paragraph indicates that when management frame protection is negotiated, the negotiated pairwise cipher is used to protect individually addressed management frames and the group management cipher is used to protect group addressed robust management frames. The only restriction is that the BIP suites cannot be used as a data cipher suite.
* Furthermore if the proposed text was added in clause 9, the proposed text would impose normative requirements on cipher suite advertisement.
* *Comment from Mark Rison: But still I think it’s worth stating that you can use GCMP-256 with BIP-CMAC-128, say* – The choice of unicast cipher suites, group cipher suite, and group management cipher suite are dependent on the security requirements of the deployment and interoperability of the STAs that connect to the network. Cipher suites can be advertised with different key lengths.

### Proposed Resolution: (1551, 1552)

REJECTED. The cited text and the entire clause describe how cipher suites are encoded and how they are included in the appropriate RSNE fields. There can be multiple CCMP and GCMP suites advertised with different key lengths, so no additional clarification is needed at the cited location on cipher suites and how they relate to advertised BIP-CMAC cipher suites. The choice of unicast cipher suites, group cipher suite, and group management cipher suite are dependent on the security requirements of the deployment and interoperability of the STAs that connect to the network. Cipher suites can be advertised with different key lengths.