IEEE P802.11
Wireless LANs

|  |
| --- |
| Some TGm CC35 CRs |
| Date: June 12 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | nehru.bhandaru@broadcom.com |

Abstract

This document contains discussion and proposed resolutions for the following comments from TGme CC35 on IEEE P802.11-REVme/D0.0:

163, 215, 199, 360, 171, 37, 486, 217, 357, 384

**Revision Notes**

R0 – initial version

R1 – Incorporate feedback from Mark Rison

R1 – Changes made during 11me call

R3 – Incorporate feedback from Mark Rison

R4 – Incorporate comments over email thread

**References**

[1] IEEE P802.11-REVme/D0.0, March 2021

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause/Page** | **Comment** | **Proposed Change** | **Resolution** |
| **163** | 12.5.2.6 | "For MSDUs sent using the block ack feature, reordering of received MSDUs according to the block ack receiver operation is performed prior to replay detection." -- TKIP is not allowed in 11n, so this cannot happen, unless this is referring to non-HT block ack, which no longer exists. Ditto "TKIP replay detection takes place after the MIC verification and any reordering required by ack processing." | Delete the cited texts, and change "Thus, a" to "A" | Resolution: ReviseAgree with the commentor. TKIP does not support MPDU aggregation.TGm editor: Please make changes as described in https://mentor.ieee.org/802.11/dcn/21/11-21-0809-04-000m-cc35-crs-a.docx |
| **215** | 12.5 | There are references to "Nonce field" in F12-21/28 and 12.5.3/5.3.4 but there is no such field, it's just an input to [CG]CM {en|de}cryption | In 12.5.3.3.4 change "Nonce field" to "CCM nonce" (3x inc. caption). in 12.5.5.3.4 change "Nonce field" to "GCM nonce" (2x inc. caption) | Resolution: ReviseAgree in principle with the commentor. In addition, there is usage of “Nonce Flags” in the §12.5.3.3.4 (CCM) that also merits a similar change.TGm editor: Please make changes as described in https://mentor.ieee.org/802.11/dcn/21/11-21-0809-01-000m-cc35-crs-a.docx |
| **199** | 12.6.3 | There is information on how MFP is negotiated for infrastructure BSS (Table 12-5--Robust management frame selection in an infrastructure BSS) and for IBSS (Table 12-6--Robust management frame selection in an IBSS) but not for TDLS. More generally, the use of MFP on a TDLS direct link is lacking (there's just "After receiving a Deauthentication frame or a Disassociation frame from the AP, a Deauthentication frame with Reason Code LEAVING\_NETWORK\_DEAUTH shall be transmitted via the direct path to all TDLS peer STAs that are in the awake state, if management frame protection has not been negotiated on the TDLS direct link." buried in 11.20.5 TDLS direct-link teardown) | Change "Table 12-6--Robust management frame selection in an IBSS" to "Table 12-6--Robust management frame selection in an IBSS or between TDLS peer STAs". In that table change "The peer STA shall not" to "The STA shall not". At 2598.50 change "An STA" to "A STA" and after that sentence add "A TDLS STA shall use Table 12-6 and thevalues of the MFPC and MFPR bits advertised in the RSNEs to determine if it may establish a TDLS link with another a TDLS peer STA." | Resolution: ReviseAgree in principle with the commentor. TDLS direct-link is neither an IBSS or infra BSS. So the current proposal is to add a small subclause for RSNA policy selection for TDLS direct link.TGm editor: Please make changes as described in [https://mentor.ieee.org/802.11/dcn/21/11-21-0809-04-000m-cc35-crs-a.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0809-02-000m-cc35-crs-a.docx) |
| **360** | 12.5 | For AAD construction, what is the difference between "not modified" and "not masked"? How does "masked to <n>" differ from "set to <n>" anyway? | In 12.5.3.3.3, 12.5.4.3, 12.5.3.3.1, 12.5.3.3.6, 12.5.4.5, 12.5.4.6, 12.5.5.3.1 change "masked to" to "set to" and "unmasked" to "not modified" (case-preservingly) | Resolution: ReviseAgree with the commentor, set to 0 and ‘not modified’ is clearer terminology. masked could imply setting it to some value hiding the actual value and setting 0 is a special case that is more precise and required for the algorithms to work.TGm editor: Please make changes as described in https://mentor.ieee.org/802.11/dcn/21/11-21-0809-01-000m-cc35-crs-a.docx |
| **171** | 12.5.3.4.4 | It is not clear what replay counter to use for non-QoS Data frames. 5.1.1.3 suggests TID 0: "At QoS STAs associated in a QoS BSS, MSDUs with a priority of Contention are considered equivalent to MSDUs with TID 0." (this is perhaps tx not rx though) | At the end of item b) in 12.5.3.4.4 PN and replay detection and 12.5.5.4.4 PN and replay detection add "For the purposes of replay detection Data frames that have the QoS subfield of the Subtype subfield equal to 0 are treated as having TID 0.". At the start of each subclause change "To effect replay detection," to "To effect replay detection for (QoS) Data frames," | Resolution: ReviseQoS subfield of the Subtype subfield ... seems a bit long winded. We could use the phrase non-QoS Data frames – used elsewhere in the spec.TGm Editor: Please add the following sentence at the end of item b) in § 12.5.3.4.4 PN and replay detection and § 12.5.5.4.4 PN and replay detectionTGm editor: Please make changes as described in https://mentor.ieee.org/802.11/dcn/21/11-21-0809-01-000m-cc35-crs-a.docx |
| **37** | 12.5.3.3.22572.38 | The fixed version of PV1 CCMP in REVmd still has a potential security flaw due to CCM nonce reuse. From an email from Jouni: The language we use for enforcing unique PN values for the same TK, Priority pair is using "TID", not "PTID". As such, there might be a case where two different TID values (e.g., 1 and 9) getting mapped to the same PTID value (1). The current language would allow the same PN to be used for frames using those two TIDs and this would result in CCM nonce reuse and loss of CCMP security protection. I hope that no one would be allowing TIDs 9..15 to be used with PV1 QoS Data frames, but if those are allowed, we do need to fix this by modifying the rule on PN reuse to not allow reuse for same TK/PTID instead TK/TID. | As suggested by Jouni, change the sentence: "For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and TID/ACI." to: "For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and PTID/ACI." | Resolution: **TBD****See discussion** |
| **486** | 12.5.3.3.32573.26 | "Subtype subfield (bits 4 5 6) in a Data frame masked to 0" is confusing because the Subtype subfield is b4-b7 | Change to "The 3 LSBs of the Subtype subfield (bits 4 5 6) in a Data frame masked to 0" | Resolution: ReviseAgree with the commentor.TGm Editor: please change the text as follows"The 3 LSBs of the Subtype subfield (bits 4 5 6) in a Data frame ~~masked~~ set to 0. Bit 7 is not modified" |
| **217** | 12.5.3.3.32573.47 | *"QC - QoS Control field contains the MSDU priority, if present. The QC TID isused in the construction of the AAD. When in a non-DMG BSS and both the STA and its peerhave their SPP A-MSDU Capable fields equal to 1, bit 7 (the A-MSDU Present field) is used inthe construction of the AAD. The remaining QC fields are masked to 0 for the AAD calculation(bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDUCapable field equal to 0). When in a DMG BSS, the A-MSDU Present bit 7 and A-MSDUType bit 8 are used in the construction of the AAD, and the remaining QC fields are masked to0 for the AAD calculation (bits 4 to 6, bits 9 to 15)."* is a bit ambiguous. "The remaining QC fields are masked to 0 for the AAD calculation(bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDUCapable field equal to 0)." only applies to non-DMG | Change to "QC - QoS Control field contains the MSDU priority, if present. The QC TID isused in the construction of the AAD. When in a non-DMG BSS, if both the STA and its peerhave their SPP A-MSDU Capable fields equal to 1, the A-MSDU Present field is also used in the construction of the AAD. When in a DMG BSS, the A-MSDU Present field and A-MSDUType field are also used in the construction of the AAD. The remaining QC fields are not used and are masked to 0 for the AAD calculation(for a non-DMG BSS, bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDU Capable field equal to 0; for a DMG BSS, bits 4 to 6 and bits 9 to 15)." | Resolution: ReviseAgree in principle with the commentor. Mostly accept, but for clarity, the DMG and non-DMG behavior can be in different paragraphs and change masked to set.TGm Editor: please change the text in quotes in the comment to the following:QC - QoS Control field contains the MSDU priority, if present. The QC TID isused in the construction of the AAD.When in a non-DMG BSS if both the STA and its peerhave their SPP A-MSDU Capable fields equal to 1, the A-MSDU Present field (bit 7) is also used in the construction of the AAD. The remaining QC fields (bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDU Capable field equal to 0) are set to 0 for the AAD calculation.When in a DMG BSS, the A-MSDU Present (bit 7) and A-MSDU Type (bit 8) are also used in the construction of the AAD. The remaining QC fields (bits 4 to 6, bits 9 to 15) are set to 0 for the AAD calculation." |
| **357** | 12.5.5.3.12585.10 | "Construct the GCM nonce block as defined in 12.5.3.3.4 (Construct CCM nonce)" -- xref should be to 12.5.5.3.4 | As it says in the comment | Resolution: AcceptAgree. the reference is wrong |
| **384** | 12.6.1.1.102593.41  | Describe how MGTKs are wrapped, or delete "wrapped" | Describe how MGTKs are wrapped, or delete "wrapped" | Resolution: ReviseThe wrapping is specified in the AMPE; perhaps it would be good to add a reference to AMPE section here and delete the word wrapped as it does not add much.TGm Editor: change the text as followsA receive mesh GTKSA is created by a mesh STA aftersuccessfully completing the AMPE in which a ~~wrapped~~ MGTK has been received (see 14.5.4 Distribution of group transient keys in an MBSS) |

**CID 163**

**Discussion**

A-MPDU (advertised in HT capabilities) and block ack re-ordering are not allowed with TKIP. The corresponding text in §**12.5.2.6 TKIP replay protection procedures** needs to be deleted.

TKIP is also deprecated p300.45

HT STA shall not use TKIP for pairwise cipher suite selector p2521.13

Block ack agreement shall not be setup between non-HT.. and another STA p1851.25

A clarificatory note might help.

**Proposed Changes**

TGm Editor: Change bullets f) p2569.3 and i) p2569.25 follows

f) TKIP replay detection takes place after the MIC verification ~~and any reordering required by ack~~

~~processing~~. Thus, a receiver shall delay advancing a TKIP TSC replay counter until an MSDU

passes the MIC check, to prevent attackers from injecting MPDUs with valid ICVs and TSCs, but

invalid MICs.

...

~~i) For MSDUs sent using the block ack feature, reordering of received MSDUs according to the block~~

~~ack receiver operation is performed prior to replay detection.~~

**CID 215**

Nonce field vs. CCM Nonce field in § 12.5.3.3.4 and 12.5.5.3.4 – should use CCM/GCM Nonce consistently

**Discussion**

There are phrases Nonce field, Nonce flags in text and figures in the clause. The title for the subclause is Construct CCM nonce. They should be replaced with CCM Nonce

**Proposed Changes**

TGm Editor: modify p2574.61 § **12.5.3.3.4 Construct CCM nonce** as follows

The CCM ~~N~~nonce occupies 13 octets, and its structure is shown in Figure 12-21 (CCM ~~N~~nonce). The structure of the CCM Nonce Flags field of the CCM ~~N~~nonce is shown in Figure 12-22 (CCM Nonce Flags field).

TGm Editor: modify figures 12-21 and 12-22 p257*5*.1-14 in § **12.5.3.3.4 Construct CCM nonce** by replacing the phrase ‘Nonce Flags’ (in Figure 12-21) and caption of figure 12-22 with ‘CCM Nonce Flags’ and phrase ‘Nonce field’ (in Figure 12-21 caption) with ‘CCM Nonce

TGm Editor: modify p2585.52 § **12.5.5.3.4 Construct GCM nonce** as follows

The GCM ~~N~~nonce occupies 12 octets, and its structure is shown in Figure 12-28 (GCM ~~N~~nonce format).

TGm Editor: modify figure 12-28 p2585.55 by replacing the phrase ‘Nonce field’ (caption of figure 12-28) with ‘GCM nonce

**CID 199**

Need clarification on MFPC/MFPR usage in TDLS link

**Discussion**

The commentor suggests using Table 12-6 Robust Management frame selection in an IBSS for TDLS link. That seems reasonable

Is TDLS direct link a Infra BSS or IBSS or is that frames transmitted outside of a BSS? It might be better to have a small subclause to specify the behavior for a TDLS direct link.

<MR> TDLS is neither an IBSS or an Infra BSS

Does this render existing implementations incompatible – send mail to Menzo and Jouni

Discussion over email – Mark provided a proposal with a merged table as well as some text

 “An TDLS STA shall use Table 12-6 (Robust management frame selection in an IBSS) and the values of the MFPC and MFPR bits advertised in the RSNEs exchanged in the 4-way handshake with the TDLS peer STA to determine if the communication is allowed, and if so whether management frame protection is enabled.

“

Jouni was not sure if the tables for IBSS and TDLS and the related text should me merged

We agreed to consider a separate table for TDLS

TDLS does not use the 4-way handshake, it uses TPK handshake. Once TDLS link is established, (certain) management frames also use the direct link – teardown, channel switch etc. (11.20.5, 11.20.6)

**Proposed Changes**

TGm Editor: add a subclause 12.6.x with the following text after §**12.6.5 RSNA policy selection in an IBSS** p.2600.48 and re-number the subsequent subclauses 12.6.6-23 accordingly

12.6.6 RSNA policy selection for a TDLS direct-link

When dot11RSNAProtectedManagementFramesActivated is set to 1, to establish a direct-link with a peer TDLS STA (See 11.20 Tunneled direct-link setup), an RSNA enabled TDLS STA that implements management frame protection shall use Table 12-6t (Robust management frame selection between TDLS peer STAs) and the MFPC and MFPR values advertised in the RSNEs exchanged in the TPK handshake messages included in the TDLS setup frames.

**Table 12-6t—Robust management frame selection between TDLS STAs**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STA MFPC** | **STA MFPR** | **STA action** | **Peer STA MFPC** | **Peer STA MFPR** | **Peer STA action** | **MFP used?** |
| 0 | 0 | May exchange data with peer STA | 0 or 1 | 0 | May exchange data with the STA | No |
| 1 | 0 | 0 | 0 |
| 1 | 0 or 1 | May exchange data with peer STA | 1 | 0 or 1 | May exchange data with the STA | Yes |
| 1 | 1 | Shall not exchange data with peer STA | 0 | 0 | N/A | N/A |
| 0 | 0 | Should not exchange data with peer STA  | 1 | 1 | Shall reject security association attempts from the STA with the Status Code ROBUST\_MANAGEMENT\_POLICY\_VIOLATION and shall not exchange data with the STA | N/A |
| 0 | 1 | Shall not use this combination |  |  | N/A | N/A |
|  |  |  | 0 | 1 | Shall not use this combination | N/A |

**CID 171**

*5.1.1.3 suggests TID 0: "At QoS STAs associated in a QoS BSS, MSDUs with a priority of Contention are considered equivalent to MSDUs with TID 0.*

and proposes

*At the end of item b) in 12.5.3.4.4 PN and replay detection and 12.5.5.4.4 PN and replay detection add "For the purposes of replay detection Data frames that have the QoS subfield of the Subtype subfield equal to 0 are treated as having TID 0.". At the start of each subclause change "To effect replay detection," to "To effect replay detection for (QoS) Data frames,"*

**Discussion**

~~There is no QoS subfield of the Subtype subfield~~. We could use the phrase non-QoS Data frames – used elsewhere in the spec.

<MR> **9.2.4.1.3 Type and Subtype subfields**

In Data frames, the

most significant bit (MSB) of the Subtype subfield, B7, is defined as the QoS subfield.

What does this mean? And what about other SAs?

-

CCM/GCM replay detection applies to PTKSA and GTKSA. IGTK/BIGTK do not use

CCM/GCM

<MR 06/07> No, this is confusing because there might not be a RC corresponding to TID 0 specifically (e.g. if the number of RCs per GTKSA is 1). If you prefer “non-QoS Data frames” then do this:

At the end of item b) in 12.5.3.4.4 PN and replay detection and 12.5.5.4.4 PN and replay detection add "For the purposes of replay detection non-QoS Data frames are treated as having TID 0.". At the start of each subclause change "To effect replay detection," to "To effect replay detection for (QoS) Data frames,"

<nb> Replay detection appies to non-QoS data frames too – which is covered by this section.

**Proposed Changes**

TGm Editor: At the end of item b) in 12.5.3.4.4 PN and replay detection and 12.5.5.4.4 PN and replay detection add

For the purpose of replay detection, non-QoS Data frames shall be treated as having TID 0.

**CID 37**

p2572.38 For PV1 MPDUs, the PN shall never repeat for a

series of encrypted MPDUs using the same temporal key and TID/ACI.

*For PV1, PN can be reused used for frames using two TIDs but same PTID and this would result in CCM nonce reuse and loss of CCMP security protection.*

**Discussion**

CCM Nonce construction uses TID/Priority – not sure if there is a security issue – as nonce/AES counter will not be the same.

**CID 360**

**Discussion**

<MR> At 2573.31, 2574.34 change “always set to 1” to “not modified (left as 1)”.

At 2571.21, 2585.8 change “may change when” to “might change when” (matching 2571.54).

2573.31 is covered by the below (12.5.3.3.3)

2574.34 – does not seem to need a change because protected frame always set to 1 – net result is the same.

Changing masked seems to imply that we are changing the frame. However we are not changing the frame – the field is used in AAD construction, for example.

No consensus yet. masked is not a good phrase to use. Can we add a note? More work required – send mail to reflector.

TGm Editor: In 12.5.3.3.3, 12.5.4.3, 12.5.3.3.1, 12.5.3.3.6, 12.5.4.5, 12.5.4.6, 12.5.5.3.1 change "masked to" to "set to" and "unmasked" to "not modified" (preserve the case)

Also at 2571.21and 2585.8 change ‘may change when’ to ‘might change when’