IEEE P802.11
Wireless LANs

|  |
| --- |
| CC35 CIDs for 45, 528, 603, 604 for 11ah |
| Date: 2021-11-09 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dave Goodall | Morse Micro |  |  | dave@morsemicro.com |
| Dave Halasz | Morse Micro |  |  | dave.halasz@morsemicro.com |

Abstract

This submission proposes resolutions for the following comments from comment collection 35 on P802.11-REVmeD0.0:

45, 528, 603, 604

**Revision History:**

R0: Initial version

R1: Added to discussion of 45 and 603

# CID 528

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Clause | Comment | Proposed Change |
| 528 |  | There are approximately 100 instances of "relay STA", of which approximately 58 are "S1G relay STA". This seems to falsely suggest that the others are or can be non-S1G relay STAs | Change all instances of "relay STA" and "Relay STA" that are not preceded by "S1G" or "DMG" to "S1G relay STA" throughout, adjusting the preceding indefinite article "a" if present to "an". Change all instances of "relay AP" and "Relay AP" that are not preceded by "S1G" or "DMG" to "S1G relay AP" throughout, adjusting the preceding indefinite article "a" if present to "an" |

## Discussion:

The 802.11ad-2012 specification included the RLS (relay link setup) feature. There are some instances of relay STA that are not preceded by DMG for which the proposed change is incorrect. Such instances could be preceded by DMG but that needs discussion. See 9.4.2.147 Relay Capabilities element for examples.

There is probably good reason to differentiate DMG relay functionality from S1G relay functionality, but it will take more analysis. For example, both 802.11ad and 802.11ah added relay related MIB variables which do not indicate whether they apply to S1G or DMG. A search on dot11Relay shows:

DMG: dot11RelayActivated

S1G: dot11RelayAPImplemented,

S1G: dot11RelayAPOperationActivated,

S1G: dot11RelaySTAImplemented,

S1G: dot11RelaySTAOperationActivated,

S1G: dot11RelayDiscoveryOptionImplemented,

There are also various references to “relay” which are not preceded by DMG or S1G.

## Proposed Resolution:

REJECTED: Insufficient details are provided to incorporate this change correctly, as the global change is not always correct. Consider, for example, 9.4.2.127 where "relay STA" (without DMG) is referring to a DMG relay STA and adding "S1G" would be incorrect.

# CID 45

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Clause | Comment | Proposed Change |
| 45 | 12.5.3 | I'm not sure which section to make this comment. PV1 frame security does not cater for protected QoS management frames for a number of reasons: 1. There doesn't seem to be a default QMF policy for PV1 management frames, but I may have missed it.2. The Packet Number creation/management for encrypted PV1 frames assumes a 12 bit sequence number. The sequence number for QMF is 10 bits and is a separate number space for each AC.3. Base packet numbers for PV1 encryption are associated with keyid and PTID/ACI so it appears that two separate sequence number spaces, i.e. PV1 data and PV1 QMF at the same priority, could end up using the same BPN which I assume voids the security properties of the underlying cipher. | We can either address the points raised in the comment or put a note somewhere that PV1 management frames do not support QoS. |

## Discussion:

Protocol Version 1 (PV1) frames were introduced in 802.11ah-2016 to reduce MAC layer overheads, for example to save power and/or assist in meeting duty cycle requirements in some regulatory domains. Encrypted PV1 frames do not include a CCMP header. The packet number (PN) for CCMP encrypted frames is maintained by the end points and consists of a base packet number BPN concatenated with the sequence control field that is in the transmitted frames.

Section 12.5.3.3.2 PN processing states:

The PN is incremented by a positive number for each MPDU. The PN shall be incremented in steps of 1

for constituent MPDUs of fragmented MSDUs, (11ax)A-MSDUs, and MMPDUs. For PV0 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key. For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and TID/ACI.

Given that the PN for PV1 frames is dependent on the sequence number we need to consider sequence number spaces for:

* QoS data frame priorities (voice, video, best effort, and background)
* Non-QoS management frames which are specified to have a priority value of 0 in the nonce block (See Section 12.5.3.3.1 General, CCMP cryptographic encapsulation process, part b) number 3))
* QoS management frame (QMF) priorities (voice, video, best effort, and background)

Questions:

1. The CCM RFC (<https://datatracker.ietf.org/doc/html/rfc3610>) indicates that it is the nonce that must be unique. To differentiate the number spaces between PV1 data and PV1 management frames should the sentence relating to PN processing for PV1 frames be modified?

“For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and CCM Nonce Flags field.”

If that is acceptable there are other instances of the same or similar PV1 related text that would also need to change.

1. To differentiate the number spaces between PV1 QMF and PV1 non-QMF should a bit be added to the Nonce Flags field? This could be one of the unused bits (6 or 7) or one of the unused priority bits when both bits b4 and b5 are set to 1 (borrowing the latter from proposed resolution of CID 604).


## Proposed Resolution:

Reject: There is insufficient detail in the proposed resolution. It needs more work and discussion around the differentiating the sequence number spaces of PV1 data and management frames that have been raised above.

This CID is related to CC35 comments 603 and 604 which also concern PV1 QMF frames.

# CID 603

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Clause | Comment | Proposed Change |
| 603 | 9.8.5.1 | QMF and non-QMF is not clearly and precisely defined for the Protocol Version 1 (PV1) frames. QMF is distinguished with non-QMF frame through "To DS" subfield in PV0 format, but there is no "To DS" subfield in the PV1 management frame. | Add PTID/Subtype to indicate QMF in PV1 management frame in Table 9-539 |

## Discussion:

802.11ae-2012 introduced QMFs (quality-of-service management frames) for Protocol Version 0 (PV0). To differentiate QMFs from non QoS management frames, the To DS bit in QMFs is set to 1. The access category of the frame is then provided in bits 14 and 15 of the sequence number field which is the AC Index subfield.

802.11ah-2016 introduced PV1 frames which have a compressed header format. The frame control field for a PV1 management frame is shown in Figure 9-979:

In PV1 management frames there is no To DS bit to differentiate between QMF and non-QMF. The proposed change is to add a PTID/Subtype to differentiate QMF but the PTID/Subtype field is either a PTID, used by PV1 data frames to indicate the three LSBs of a traffic identifier, or a Subtype, used for differentiating between PV1 management frame types as shown in Table 9-539 below.

Adding one extra subtype for QMF does not allow definition of which management subtype QoS would apply to. Also note that the tables that define PTID/Subtype values appear to reference the incorrect bits in the Frame Control field, which are b7, b6 and b5.

A possible alternative would be to define a QoS Management Type in Table 9-535—PV1 frame types, but that needs more discussion.

Resolution of this comment may also depend on resolution of CID 45.

REJECTED (MAC: 2021-11-09 16:24:07Z): Insufficient details are provided to incorporate this change correctly, as defining an additional PTID/Subtype has the effect of adding an extra PV1 management frame type but does not differentiate between QMF and non-QMF in general for PV1 management frames.

# CID 604

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Clause | Comment | Proposed Change |
| 604 | 9.4.2.213 | The PV1 header compression has not been clearly described. PV1 frame doesn't contain a cipher header which is used for encryption and decryption. Instead of the cipher header, PV1 frame uses other parameters from compressed header and uses a base packet number (BPN) and Key ID, which is stored and managed in locally.STA receiving PV1 frame decides whether the sequence number was wrap-around or not, and it will increase the BPN in case that the sequence number wraps around. The BPN is stored locally and configured by "TID/ACI" value by using the header compression frame. STA can request and response the update of BPN and Key ID with a header compression action frame. "TID/ACI" field notifies which information would be updated in the peer STA. TID is used for data frame and ACI is used for management frame. However, in header compression frame, there is no proper indication whether the incoming CCMP update field corresponds to data frame or management frame. It can cause two issues. The same value of "TID/ACI" between data frame and management frame indicates the different access category. Both data frame and management frame which has a same value of TID and ACI uses the same sequence number space identifiers. | In Figure 9-722 (CCMP Update field format), TID/ACI (B34 to B37) should be 3 bits of PTID/ACI and 1 bit of Management.- PTID: The 3 LSBs of the TID for PV1 QoS Data frames.- ACI: The Access Category Index of PV1 Management frames. B2 is reserved (e.g. and set to '1'.)- Management: Indication flag that the field is PTID or ACI. If it is set to '1', the field is PTID. Otherwise, the field is ACI.Given that when the STA uses EDCA mechanism, the sequence numbers are managed by STA address and PTID in the PV1 data frame with SNS6, and those are managed by STA address in the PV1 management frame with SNS7, update the Table 10-5 (Transmitter sequence number spaces). For example, for SNS4 it should be for QMF for PV0 and add SNS8 for QMF for PV1.Table 10-6 (Receiver caches) should be also updated. For example, for RC6, it should be QMFs for PV0. And add RC13 for QMF for PV1. |

## Proposed Resolution:

Accept/Revise, pending resolution of CIDs 45 and 603, and creation of text changes.

**References:**