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

# 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:

Reject: Insufficient detail.

This CID is related to CC35 comments 603 and 604 which also concern PV1 QMF frames. If QMF is not supported for robust PV1 management frames, then CIDs 603 and 604 would be rejected.

# 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:

Reject: Insufficient detail.

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.

# 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:

Reject: Insufficient detail.

Resolution of this comment depends on resolution of CID 45.

# 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. | 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. |

## Discussion:

Reject: Insufficient detail.

Resolution of this comment depends on resolution of CID 45.

**References:**