IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for some comments on 11me/D3.0 (LB273) |
| Date: 2023-07-09 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Mark RISON | Samsung Cambridge Solution Centre | SJH, CB4 0DS, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |

Abstract

This submission proposes resolutions for various CIDs on 11me/D3.0. Green indicates material agreed to in the group, yellow material to be discussed, red material rejected by the group and cyan material not to be overlooked. The “Final”/“No Markup” view should be selected in Word (this means Word comments can be disregarded by the Editor).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4139Mark RISON13.12967.40 | "Throughout this clause, the notation Authentication-Request refers to an Authentication frame with theAuthentication Transaction Sequence Number field equal to 1; Authentication-Response refers to anAuthentication frame with the Authentication Transaction Sequence Number field equal to 2;Authentication-Confirm refers to an Authentication frame with the Authentication Transaction SequenceNumber field equal to 3; Authentication-Ack refers to an Authentication frame with the AuthenticationTransaction Sequence Number field equal to 4. " -- so the text should not say "Authentication-Request frame" but just "Authentication-Request". Or better, say "frame" in the notation | Change the cited text to (additions between \*\*\*): "Throughout this clause, the notation Authentication-Request \*\*\*frame\*\*\* refers to an Authentication frame with theAuthentication Transaction Sequence Number field equal to 1; Authentication-Response \*\*\*frame\*\*\* refers to anAuthentication frame with the Authentication Transaction Sequence Number field equal to 2;Authentication-Confirm \*\*\*frame\*\*\* refers to an Authentication frame with the Authentication Transaction SequenceNumber field equal to 3; Authentication-Ack \*\*\*frame\*\*\* refers to an Authentication frame with the AuthenticationTransaction Sequence Number field equal to 4. ", keeping the insertion roman. At 1307.36 change "Clause 13" to "Subclause 13.1". In Figure 13-3—FT initial mobility domain association in a non-RSN, Figure 13-5—Over-the-air FT protocol in an RSN, Figure 13-8—Over-the-air FT protocol in a non-RSN, Figure 13-10—Over-the-air FT resource request protocol in an RSN, Figure 13-11—Over-the-air FT resource request protocol in a non-RSN, delete "802.11 " before "Authentication-" |

Discussion:

There are a lot of instances of “Authentication-Request frame” etc., so it’s probably better to just define things that way, though note that in MSCs etc. the word “frame” is not used, so should not be part of the term itself (so not italicised). The proposed change in 13.1 is as follows:

Throughout this clause, the notation *Authentication-Request* frame refers to an Authentication frame with the Authentication Transaction Sequence Number field equal to 1; *Authentication-Response* frame refers to an Authentication frame with the Authentication Transaction Sequence Number field equal to 2; *Authentication-Confirm* frame refers to an Authentication frame with the Authentication Transaction Sequence Number field equal to 3; *Authentication-Ack* frame refers to an Authentication frame with the Authentication Transaction Sequence Number field equal to 4.

and in 9.4.2.201:

The notation of Authentication-Request and Authentication-Response refers to the definition in ~~Clause 13 (Fast BSS transition)~~ Subclause 13.1.

The identified figures have an “802.11” that is spurious since all frames transmitted by 802.11 STAs are by definition 802.11 frames, and the definition in 13.1 doesn’t include “802.11” either. E.g. in Figure 13-3:



Proposed resolution:

REVISED

Make the changes proposed by the commenter except say just “13.1” not “Subclause 13.1” in 9.4.2.201.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4162Mark RISON9.4.2.74 | "The FMS Counter ID field is a 3- bit value that represents" (1104.50) should be "The FMS Counter ID field represents" since the size is already shown in the figure. Similarly other locations "The Buffered AC subfield is a 4-bit bitmap that" (597.45), "The Enablement Identifier field is a 16-bit number assigned" (1557.44), "The Queue Size subfield is an 8-bit field that indicates" (594.9), "The Average SNR of Space-Time Stream i subfield in the Table 9-103 (VHT Compressed BeamformingReport information) is an 8-bit" (but keep "2s complement after") (804.2, 822.36, 833.48), "is represented as a 48-bit MAC address" (1141.23), "the offset value is an 8-bit" (885.7), "The MPDU delimiter CRC field is an 8-bit CRC value" (1728.8), "Each Address field contains a 48-bit address" (586.45) | As it says in the comment |

Discussion:

More instances of duplication between the text and the normative figure.

Proposed changes:

The FMS Counter ID field ~~is a 3- bit value that~~ represents (1104.50)

The Buffered AC subfield ~~is a 4-bit bitmap that~~ indicates (597.45)

The Enablement Identifier field is ~~a 16-bit number~~ assigned (1557.44)

The Queue Size subfield ~~is an 8-bit field that~~ indicates" (594.9)

The Average SNR of Space-Time Stream i subfield in the Table 9-103 (VHT Compressed Beamforming Report information) is a~~n 8-bit~~ 2s complement integer whose definition is shown in Table 9-105 (804.2, 822.36, 833.48)

The Destination Mesh STA Address field ~~is represented as a 48-bit MAC address and~~ is set (1141.23)

the offset value is a~~n 8-bit~~ 2s complement integer (885.7)

The MPDU delimiter CRC field is a~~n 8-bit~~ CRC value (1728.8)

Each Address field contains an ~~48-bit~~ address as defined in Clause 8 of IEEE Std 802-2014 (586.45)

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4162 in <this document>, which identify the specific changes in each case.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4170Mark RISON9.4 | Saying in text that a field "is 2 octets" duplicates the figure | Delete "The length of theAuthentication Algorithm Number field is 2 octets." in 9.4.1.1, "The length of the Authentication Transaction Sequence Number field is 2 octets." in 9.4.1.2, "The length of the Beacon Interval field is 2 octets." in 9.4.1.3, "The length of the Capability Information field is 2 octets." in 9.4.1.4, "The length of the Listen Interval field is 2 octets." in 9.4.1.6, "The length of the Reason Code field is 2 octets." in 9.4.1.7, "The length of the AID field is 2 octets." in 9.4.1.8, "The length of the Block Ack Parameter Set field is 2 octets." in 9.4.1.13, "Thelength of the Block Ack Timeout Value field is 2 octets." in 9.4.1.14, "The length of the Originator Preferred MCS fieldis 2 octets." in 9.4.1.15, "The length of the DELBA Parameter Set field is 2 octets." in 9.4.1.16, "The length of the RSN Capabilities field is 2 octets." in 9.4.2.23.4, "is 2 octets and" in 9.4.2.46,  |

Discussion:

More instances of duplication between the text and the normative figure.

Proposed resolution:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4179Mark RISON10.3.2.41780.23 | "valid frame" -- what exactly does this mean? 573.46 indicates we cannot "receive" invalid frames | Delete "valid" at the referenced location. Also at 1789.12, 1795.27, 1896.22, 2089.63, 2091.41, |

Discussion:

573.46 says:

Reception, in references to frames or fields within frames (e.g., received Beacon frames or a received Duration/ID field), applies to MPDUs indicated from the PHY without error and validated by FCS within the MAC sublayer. Without further qualification, reception by the MAC sublayer implies that the frame contents are valid, and that the protocol version is supported (see 9.2.4.1.2 (Protocol Version subfield)), with no implication regarding frame addressing or regarding whether the frame type or other fields in the MAC header are meaningful to the MAC entity that receives the frame.

The proposed changes are the following deletions:

A STA that receives at least one ~~valid~~ frame in a PSDU can update its NAV with the information from any valid Duration field in the PSDU.

The recognition of a valid CTS frame sent by the recipient of the RTS frame, corresponding to this PHY-RXEND.indication primitive, shall be interpreted as successful response, permitting the frame exchange sequence to continue(#109). The recognition of anything else, including any other ~~valid~~ frame, shall be interpreted as failure of the RTS frame transmission.

Additional exceptions exist for S1G STAs for accepting a ~~valid~~ frame as successful acknowledgment as described in the following three paragraphs:

If anything else, including any other ~~valid~~ frame, is recognized, the transmission of the MPDU has failed.

DMG STAs receiving any ~~valid~~ frame shall perform the following NAV update operation

CMMG STAs receiving any ~~valid~~ frame shall perform the following NAV update operation

However, the text at 573.46 is about “reception” rather than “recognition”, so it would be better to align the terminology throughout (there are other locations beyond those highlighted in yellow above).

Proposed changes:

At 1780.23:

A STA that receives at least one ~~valid~~ frame in a PSDU can update its NAV with the information from any valid Duration field in the PSDU.

At 1789.12:

The ~~recognition~~reception of a ~~valid~~ CTS frame sent by the recipient of the RTS frame, corresponding to this PHY-RXEND.indication primitive, shall be interpreted as successful response, permitting the frame exchange sequence to continue(#109). ~~The recognition of a~~Anything else, including the reception of any other ~~valid~~ frame, shall be interpreted as failure of the RTS frame transmission.

At 1794.53:

If the STA ~~recognizes~~receives an ~~valid~~ Ack frame addressed to the STA and corresponding to this PHY-RXEND.indication primitive, this ~~recognition~~ shall be interpreted as successful acknowledgment.

At 1795.7:

If the STA does not ~~recognize~~receive an ~~valid~~ Ack frame addressed to the STA, this condition shall be interpreted as failure of its MPDU transmission, except as defined below. In this instance, the STA shall invoke its backoff procedure at the PHY-RXEND.indication primitive and may process the received frame. If the STA has transmitted a PS-Poll frame, then the STA’s receipt ~~and recognition~~ of a ~~valid~~ Data or Management frame transmitted by the recipient of the PS-Poll frame shall also be accepted as successful acknowledgment of the PS-Poll frame.

At 1795.27:

Additional exceptions exist for S1G STAs for accepting a ~~valid~~ frame as successful acknowledgment as described in the following three paragraphs:

At 1796.1:

3) The ~~recognition~~reception of an ~~valid~~ S1G RTS frame, sent by the recipient of a PS-Poll frame or of a PS-Poll+BDT frame shall be accepted as successful acknowledgment of the PS-Poll or of the PS‑Poll+BDT frame.

At 1896.18:

the STA shall wait for the corresponding PHY-RXEND.indication primitive to ~~recognize~~receive a ~~valid~~ response MPDU(#109) that either does not have a TA field or is sent by the recipient of the MPDU requiring a response

At 1896.22:

~~If a~~Anything else, including the reception of any other ~~valid~~ frame, is ~~recognized, the transmission of the MPDU has failed~~ defined to be a failure.

At 2089.63:

DMG STAs receiving any ~~valid~~ frame shall perform the following NAV update operation

At 2091.41:

CMMG STAs receiving any ~~valid~~ frame shall perform the following NAV update operation

Proposed resolution:

REVISED

Incorporate the changes shown in <this document> for CID 4179, which removes "valids", and also changes "recognizes" wording to "receives" wording.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4183Mark RISON12 | "FC—MPDU Frame Control field, with the following modifications:" for BIP should be just "FC—MPDU Frame Control field, with:" and then for all cases (CCMP, BIP, GCMP) the last subbullet should be "No modifications to other subfields" | Fix the lists at 2837.45, 2838.52, 2845.31 |

Discussion:

The wording is broken. Each bullet item needs to make sense when preceded by “with”.

Proposed changes:

At 2837.45:

1) FC – MPDU Frame Control field, with

i) (#486)The 3 LSBs of the Subtype subfield (bits 4 5 6) in a Data frame (#1951)masked out.

Bit 7 is not modified

ii) Retry subfield (bit 11) (#1951)masked out

iii) Power Management subfield (bit 12) (#1951)masked out

iv) More Data subfield (bit 13) (#1951)masked out

v) Protected Frame subfield (bit 14) (#1951)not modified (left as 1)

vi) +HTC subfield (bit 15) as follows:

— (#1951)Masked out in all Data frames containing a QoS Control field

— (#1951)Not modified otherwise

vii) No modifications to o~~O~~ther subfields ~~are not modified~~

At 2838.52:

1) FC – MPDU Frame Control field, with

i) Power Management subfield (bit 10) (#1951)masked out

ii) More Data subfield (bit 11) (#1951)masked out

iii) Protected Frame subfield (bit 12) (#1951)not modified (left as 1)

iv) EOSP subfield (bit 13) (#1951)masked out

v) Relayed Frame subfield (bit 14) (#1951)masked out

vi) Ack Policy Indicator subfield (bit 15) (#1951)masked out

vii) No modifications to o~~O~~ther subfields ~~are not modified~~

At 2845.31:

a) FC—MPDU Frame Control field, with the following modifications:

1) Retry subfield (bit 11) (#1951)masked out

2) Power Management subfield (bit 12) (#1951)masked out

3) More Data subfield (bit 13) (#1951)masked out

4) No modifications to o~~O~~ther subfields ~~are not modified~~

Proposed resolution:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4225Mark RISON12.7.8.4.22928.62 | "indicate (#3266)AKM 00-0F-AC:7(TPK handshake)" -- what if it includes >1 AKM? Ditto "indicate a negotiated AKM" for FT (but maybe that's OK because it's in the assoc req where you can only have a single AKM -- but is that specified anywhere and what about 2975.42, 2977.54, 2980.9?) | Change the former to "indicate the single (#3266)AKM 00-0F-AC:7(TPK handshake)". |

Discussion:

The context is:

Otherwise, the TDLS responder STA processes the message as follows:

If (#3488)the RSNE does not indicate (#3266)AKM 00-0F-AC:7(TPK handshake), the TDLS responder STA shall reject the request with status code STATUS\_INVALID\_AKMP.

T1 should only contain a single AKM (“The AKM (#3241)Suite Count field shall be set to 1.”)

Therefore it seems better to reduce the attack surface by being clear that only :7 should be specified:

Otherwise, the TDLS responder STA processes the message as follows:

If (#3488)the RSNE does not indicate the single (#3266)AKM 00-0F-AC:7(TPK handshake), the TDLS responder STA shall reject the request with status code STATUS\_INVALID\_AKMP.

The other instances are:

2975.42: If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the Authentication frame with status code 54 (“Invalid MDE”). If an MDE is present in the Authentication frame and (#3488)the RSNE does not indicate AKM(#3266) 00-0F-AC:16 or 00-0F-AC:17 (Fast BSS Transition over FILS), the AP shall reject the Authentication frame with status code 43 (“Invalid AKMP”).

2977.54: If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the authentication request with status code STATUS\_INVALID\_MDE. If the Authentication-Request frame contains an authentication algorithm equal to FT authentication and (#3488)the RSNE does not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-188 (AKM suite selectors)), the AP shall reject the authentication request with status code STATUS\_INVALID\_AKMP.

2980.9: If the contents of the MDE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the FT Request frame with status code STATUS\_INVALID\_MDE. If (#3488)the RSNE does not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-188 (AKM suite selectors)), the AP shall reject the FT Request frame with status code STATUS\_INVALID\_AKMP.

Should these also be explicitly “AKM” to “the single AKM” for the first and “a negotiated AKM for which the … indicates FT” to “a single AKM, and the … for that AKM indicates FT”?

Proposed changes:

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4225 in <this document>, which make it clear that it has to be a single AKM.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4350Mark RISON12 | "GNoStations--" in Figure 12-53--Authenticator state machines, part 2 at 2938.13 should be "GNoStations--". Ditto "GKeyDoneStation--". Ditto "GKeyDoneStations -" | At 2938.13 change "GNoStations--" to "GNoStations--". At 2938.22 change "GKeyDoneStation--" to "GKeyDoneStations--" (2 fixes). At 2940.34 change "GKeyDoneStations --" to "GKeyDoneStations--". At 2934.14 and 2938.20 change "Keycount" to "keycount" |

Discussion:

The comment and proposed change got garbled by the comment processing system. The proposed change was submitted as:

At 2938.13 change "GNoStations—" to "GNoStations--". At 2938.22 change "GKeyDoneStation—" to "GKeyDoneStations--" (2 fixes). At 2940.34 change "GKeyDoneStations --" to "GKeyDoneStations--". At 2934.14 and 2938.20 change "Keycount" to "keycount"

Proposed changes:

At 2938.13 should be -- not –:



At 2938.22 should be plural and -- not –:



At 2940.34 should be no space:



At 2932.14 should be keycount not Keycount:



At 2938.20 should be keycount not Keycount:



Proposed resolution:

ACCEPTED

Note to the Editor: change given as at 2934.14 is actually at 2932.14.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4184Mark RISON12.5.3.3 | BIP doesn't work for S1G because the AAD doesn't account for PV1 frames | At the start of 12.6.17 add "An S1G STA shall not support PMF." |

Discussion:

12.5.3.3 says:

**12.5.3.3 BIP AAD construction**

The BIP Additional Authentication Data (AAD) is constructed from the MPDU header. AAD construction is performed as follows:

a) FC—MPDU Frame Control field, with the following modifications:

1) Retry subfield (bit 11) (#1951)masked out

2) Power Management subfield (bit 12) (#1951)masked out

3) More Data subfield (bit 13) (#1951)masked out

4) Other subfields are not modified

b) A1—MPDU Address 1 field.

c) A2—MPDU Address 2 field.

d) A3—MPDU Address 3 field.

Figure 12-24 (BIP AAD construction) depicts the format of the AAD. The length of the AAD is 20 octets.



However, the Frame Control field for PV1 Management frames other than PV1 Probe Response frames does not contain a Retry field, and the Power Management and More Data fields are in different positions:

**9.8.3.1 Frame Control field**

The Frame Control field of the PV1 MAC header for PV1 frames except the PV1 Probe Response(#3384) frame, PV1 Resource Allocation frame, and PV1 Control frames, is defined in Figure 9-1210 (Frame Control field format for some PV1 frames(#1744)).



Furthermore the PV1 MAC header doesn’t have explicit Address 1-3 fields, it has A1-A3 fields, and these don’t always contain a MAC address anyway (and A3 is not always present):



So as things stand BIP cannot be used with PV1 frames. Having said that, PV1 Probe Response frames are not robust Management frames (see 12.2.7: “The robust Management frames are Disassociation, Deauthentication, and robust Action frames.”) and hence do not use BIP, and so S1G STAs can still, and do, do MFP.

Note that 10.57 requires use of PV1 Management frames when both sides support this, but only for individually addressed frames:

An S1G STA with dot11PV1MACHeaderOptionImplemented equal to true shall use the PV1 format instead of the PV0 format to transmit QoS Data, Action, and Action No Ack frames that are individually addressed to a peer STA from which it has received an S1G Capabilities element with PV1 Frame Supported subfield equal to 1.

Proposed resolution:

REVISED

At the end of 12.6.17 add a para “When management frame protection is negotiated, an S1G STA shall not transmit group addressed robust PV1 Management frames.”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4212Mark RISON12.5 | In 12.5.2.4.4 PN and replay detection12.5.3.4 BIP replay protection12.5.4.4.4 PN and replay detection14.6.3 Mesh Group Key Inform frame construction and processingrecipient should be receiver | As it says in the comment [I can provide locations if needed; confirm direction] |

Discussion:

In general the security clauses use “receiver” not “recipient” when discussing 802.11-specific functionality. However, some of the clause numbers are wrong, and the Clause 14 subclause actually has a different problem.

Proposed changes:

Change the “recipient”s highlighted in yellow to “receiver”.

**12.5.2.4.4 PN and replay detection**

To effect replay detection, the receiver extracts the PN from the CCMP header.

(#171)NOTE 1—The CCMP header is not present in secure PV1 MPDUs, but constructed locally at the STA as defined in 12.5.2.3.6 (Construct CCMP header for PV1 MPDUs).

See 12.5.2.2 (CCMP MPDU format) for a description of how the PN is encoded in the CCMP header. The following processing rules are used to detect replay:

a) The receiver shall maintain a separate set of replay counters for each PTKSA, (#166)TPKSA, GTKSA, (#1627)mesh PTKSA, and mesh GTKSA(#239). (#1508)The receiver initializes these replay counters to 0 when it resets the TK, TPK-TK or MTK for a peer, and to the value indicated by the peer when it sets the GTK or MGTK. The replay counter is set to the PN value of accepted CCMP MPDUs.

b) For each PTKSA, (#166)TPKSA, GTKSA, (#1627)mesh PTKSA, and mesh GTKSA(#239), the recipient shall maintain a separate replay counter for each TID, subject to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.23 (RSNE))(#3573).

(#171)NOTE 2—For the purpose of replay detection, non-QoS Data frames are treated as having TID 0, and use the reply counter corresponding to MSDU priority 0.

c) If the recipient set the MFPC bit on a given link to 1, it(#199) shall maintain a single replay counter for received individually addressed robust (#3573)PV0 Management frames that are received with the To DS subfield equal to 0, and (#3573)(S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames. If dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust (#3573)PV0 Management frames that are received with the To DS subfield equal to 1.

(#3573)NOTE 3—QMF is not supported for PV1 Management frames (see 11.24.1.1 (Overview)).

d) The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA(#3573), RA (individual or group address; not if TDLS) and priority value of the received MPDU. The receiver shall discard (#3573)fragmented MSDUs, A-MSDUs(#3089) and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1. (#199)If the receiver set the MFPC bit on a given link to 1, it shall discard any individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter associated with the TA(#3573), (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI, and (S1G STA only) Protocol Version subfield of that individually addressed Management frame.

e) When discarding a frame, the receiver shall increment by 1 dot11RSNAStatsCCMPReplays for Data frames or dot11RSNAStatsRobustMgmtCCMPReplays for robust Management frames.

f) For MSDUs or A-MSDUs sent using the block ack feature, reordering of received MSDUs or A-MSDUs according to the block ack receiver operation is performed prior to replay detection.

**12.5.3.5 BIP transmission**

When a STA transmits a protected group addressed robust Management frame, it shall

a) Select the IGTK or BIGTK currently active for transmission of frames to the intended group of recipients and construct the MME (see 9.4.2.53 (MME(#1517))) with the MIC field (#1951)masked out and the Key ID field set to the corresponding IGTK (#3493)key ID. […]

**12.5.4.4.4 PN and replay detection**

*[same as 12.5.2.4.4 PN and replay detection above]*

At 3046.60 change “MGTK receiver” to “MGTK recipient” (term defined in 14.7.1: “A “MGTK recipient” is a mesh STA receiving the MGTK being sent by the MGTK Source.”).

At 3038.57, 3044.63 change “MGTK Source” to “MGTK source”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4212 in <this document>, which make the changes requested by the commenter, and also fix one spurious “MGTK receiver” and two spuriously cased “MGTK Source”s.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4261Mark RISON11.22.3.42645.41 | "NOTE--When RLQP is transmitted between the GDD enabling STA and the RLSS, it uses [...]" -- it's not clear all this is stated normatively elsewhere. Also the element is Advertisement Protocol not Advertising Protocol. Also "the [AP] element is missing an antecedent" | Change to:When RLQP is transmitted between the GDD enabling STA and the RLSS, (#3370)MSDUs with(#2186)EtherType 89-0d shall be used, as defined in Annex H. The Payload field of the MSDUs contains RLQP-elements as specifiedin 9.4.6 (Registered location query protocol (RLQP) elements) and an Advertisement Protocol element with anAdvertisement Protocol tuple whose Advertisement Protocol ID field is set to the value of RLQP specified in Table 9-275(Advertisement protocol ID definitions). When an RLQP-element is transmitted between the GDD dependent STA andits GDD enabling STA, protected Action frames shall be used, not MSDUs with (#2186)EtherType 89-0d.NOTE---Insome regulatory domains, the GDD enabling STA might be required to have secured connection with the RLSS.(#399)". At 2635.37 change "Advertisement protocol element" to "Advertisement Protocol element" |

Discussion:

This NOTE seems to actually mostly be normative, not informative:

NOTE—When RLQP is transmitted between the GDD enabling STA and the RLSS, (#3370)it uses MSDUs with (#2186)EtherType 89-0d, as defined in Annex H. The Payload field of the MSDUs contains RLQP-elements as specified in 9.4.6 (Registered location query protocol (RLQP) elements) and the Advertising Protocol element with an Advertising Protocol tuple whose Advertisement Protocol ID field is set to the value of RLQP specified in Table 9-275 (Advertisement protocol ID definitions). When an RLQP-element is transmitted between the GDD dependent STA and its GDD enabling STA, it uses protected Action frames, but does not use MSDUs with (#2186)EtherType 89-0d. In some regulatory domains, the GDD enabling STA may be required to have secured connection with the RLSS.(#399)

Proposed changes:

The commenter’s proposed change was to make most of the text normative, and in the informative bit make it a might not a may:

When RLQP is transmitted between the GDD enabling STA and the RLSS, (#3370)MSDUs with (#2186)EtherType 89-0d shall be used, as defined in Annex H. The Payload field of the MSDUs contains RLQP-elements as specified in 9.4.6 (Registered location query protocol (RLQP) elements) and an Advertisement Protocol element with an Advertisement Protocol tuple whose Advertisement Protocol ID field is set to the value of RLQP specified in Table 9-275 (Advertisement protocol ID definitions). When an RLQP-element is transmitted between the GDD dependent STA and its GDD enabling STA, protected Action frames shall be used, not MSDUs with (#2186)EtherType 89-0d.

NOTE—In some regulatory domains, the GDD enabling STA might be required to have secured connection with the RLSS.(#399)

However, an article is missing before “secured” since it seems this is an adjective not a participle, and the “the GDD”s should be “a GDD” since there is no clear antecedent.

The commenter also proposed to fix the element capitalisation in:

As described in 11.22.3.2 (GAS Protocol), APs indicate their support for a particular GAS advertisement protocol by including an Advertisement protocol element with that Advertisement protocol ID in Beacon and Probe Response frames

However, “Advertisement protocol ID” also has the wrong capitalisation. This is also the case at 1131.44 (“The Advertisement protocol ID value 221 is reserved”). But anyway it’s not “reserved”, it’s allocated, and furthermore this duplicates Table 9-275—Advertisement protocol ID definitions.

Proposed resolution:

REVISED

Make the changes proposed by the commenter, and additionally:

- in the replacement para say “between a GDD” not “between the GDD” (2x)

- before “secured connection” in the NOTE add “a ”

- at 2635.37 change “Advertisement protocol ID” to “advertisement protocol ID”

- at 1131.44 delete “The Advertisement protocol ID value 221 is reserved for vendor specific advertisement protocols.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4341Mark RISON10.25.2 | 9.6.4.1 says "When Block Ack operation is modified, only the timeout can be changed." but 10.25.2 says "All parameters of the agreement may be changed except for the TID." and 11.5.1 says something similar | Decide one way or the other. If buffer size and timeout can be changed, describe what happens if the new values are smaller than the current, and the current window/idle time exceed the new limits [needs discussion] |

Discussion:

We currently have:

**9.6.4.1 Block Ack Action field(#3729)**

ADDBA Request and ADDBA Response frames are used to set up or to modify block ack operation(#3518) for a specific TC, TS, or GCR group address. (#3172)When Block Ack operation is modified, only the timeout can be changed.

**10.25.2 Setup and modification of the block ack parameters**

(#1807)A block ack agreement may be modified by the originator by sending an ADDBA Request frame ((#3174)see 11.5.2 (Setup and modification of the block ack parameters), except that MLME-ADDBA primitives are not used). All parameters of the agreement may be modified except for the TID.

**11.5 Block ack operation**

**11.5.1 Introduction**

(#3174)Block ack agreements may be set up, modified by the originator, or deleted from the MAC (see 10.25.2 (Setup and modification of the block ack parameters)) or from the SME. The setup, modification by the originator and deletion of block ack agreements from the SME is described in this subclause. All parameters of an agreement may be modified except for the TID.

An ADDBA Request frame is defined in Table 9-445—ADDBA Request frame Action field format and contains the following fields:

Block Ack Parameter Set, which contains A-MSDU Supported, Block Ack Policy, TID and Buffer Size subfields

Block Ack Timeout Value

Block Ack Starting Sequence Control, which contains a SSN

GCR Group Address element (optional), which contains a GCR group address

Multi-band (optional), which contains loads of stuff

TCLAS (optional), which contains loads of stuff

ADDBA Extension (optional), which contains No-Fragmentation and HE Fragmentation Operation subfields

EDMG Flow Control Extension Configuration (optional), which contains loads of stuff

SAR Configuration (optional), which contains quite a lot of stuff

**Q1: is it really OK for all of these to be modified? E.g. change A-MSDU support or GCR address or TCLAS or fragmentation or Multi-band/EDMG/SAR config?**

An ADDBA Response frame is defined in Table 9-446—ADDBA Response frame Action field format and contains the following fields:

Block Ack Parameter Set

Block Ack Timeout Value

GCR Group Address element (optional)

Multi-band (optional)

TCLAS (optional)

ADDBA Extension (optional)

EDMG Flow Control Extension Configuration (optional)

SAR Configuration (optional)

Originator Preferred MCS element (optional)

**Q2: is it really OK for all of these to be modified, even if not modified in the request (either w.r.t. the original request, or the original response)?**

**Q3: even if we focus on the “core” parameters, i.e. timeout and buffer size, what if the new values are smaller than the current values, i.e. there has been no traffic for more than the new timeout, or the new buffer size is smaller than the current outstanding window size?**

**Q4: what happens if some MPDUs have been transmitted under a BA agreement but the originator has not seen the ack (either the recipient did not receive the MPDU or the originator did not receive the ack), and the BA agreement is modified? Are all these MPDUs lost? Can the new SSN be less than the last SN transmitted (whether acked or not)?**

Proposed changes:

In 9.6.4.1 delete “(#3172)When Block Ack operation is modified, only the timeout can be changed.”

In 10.25.2 and 11.5.1 make “All parameters of an agreement may be modified except for the TID.” into a separate para and then append:

Alternative 1:

When an agreement is modified, at the originator any frames in the transmit buffer are discarded (even if they have not been acknowledged), and at the receiver:

* the scoreboard is cleared
* the reordering buffer is flushed
* the replay counter, if any, is not modified
* the inactivity timeout is restarted

NOTE 1—The originator might wait until any frames in the transmit buffer have been acknowledged before modifying the agreement, to avoid loss of data.

NOTE 2—Modification of a parameter can be requested by the originator, but, except for the starting sequence number, the recipient might reject the request (by specifying the current value in the ADDBA Response frame), or modify differently.

NOTE 3—The effect of modification of any parameter other than the starting sequence number, buffer size and timeout is parameter-dependent.

Alternative 2:

When an agreement is modified, at the originator the transmit buffer is not modified except for possible discarding of frames that precede the new starting sequence number or are beyond the window, and at the receiver the scoreboard and reordering buffer are not modified except for possible flushing of frames that precede the new starting sequence number or are beyond the window, and corresponding updating of the scoreboard; the inactivity timeout is also restarted at the receiver.

NOTE 1—The originator might choose a new starting sequence number that does not exceed the sequence number of any frame that has not been acknowledged, to avoid loss of data. The originator and responder might choose a buffer size that does not leave frames beyond it, to avoid loss of data.

NOTE 2—Modification of a parameter can be requested by the originator, but, except for the starting sequence number, the recipient might reject the request (by specifying the current value in the ADDBA Response frame), or modify differently.

NOTE 3—The effect of modification of any parameter other than the starting sequence number, buffer size and timeout is parameter-dependent.

[Alternative 3: pick one of alternatives 1 and 2 above, then make the change in 10.25.1 and just xref to there from 11.5.1, or vice-versa.]

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4341 in <this document>, which xxx

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4140Mark RISON7.2.2.2.4 | "A group addressed MAC service tuple from an AP is distributed to all APs, mesh gates,and the portal, including the originating entity. A group addressed MAC service tuple from a portal isdistributed to all APs and mesh gates." -- does this mean that a group addressed MSDU is expected to be transmitted by all APs in an ESS? This seems excessive, depending on the definition of an ESS | Clarify |

Discussion:

As discussed in 20/0177 and incorporated into 802.11-2020, the BSSes in an ESS are connected by a single DS, and the ESS appears to be a single IEEE Std 802™ access domain to the LLC sublayer. On this basis, it is reasonable to distribute all group traffic to all APs, mesh gates, and the portal (if any) within the ESS.

Having said that, the text above fails to cover tuples from mesh gates. Also “entity” is a bit vague.

Proposed resolution:

REVISED

At the referenced location, change

(#3422)A MAC service tuple with a destination address that is a group address

from an AP is distributed

to all APs, mesh gates, and the portal, including the originating entity.

(#3422)A MAC service tuple with a destination address that is a group address

from a portal is distributed

to all APs and mesh gates.

to

 (#3422)A MAC service tuple that has a destination address that is a group address

and that is delivered to the DS from an AP or mesh gate is distributed

to the portal, if any, and to all APs and mesh gates connected to the DS, including the originating AP or mesh gate.

(#3422)A MAC service tuple that has a destination address that is a group address

and that is delivered to the DS from a portal is distributed

to all APs and mesh gates connected to the DS.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4199Mark RISON9.6 | There are 7 "Action field is set"s in 9.6 that should just be "The <blah> Action field is defined in 9.6.<blah>.1." | As it says in the comment [I can provide locations if needed; confirm direction] |

Discussion:

In general, for each Action frame category, there is a Subclause 9.6.n.1 that contains a table giving the <blah> Action field values (the octet after the Category field octet), e.g.:



Then for each Action frame in that category, a reference back to 9.6.n.1 is just given, e.g.:

**9.6.2.2 Spectrum Measurement Request frame format**

The Spectrum Measurement Request frame is transmitted to request another STA to measure one or more channels. The format of the Spectrum Measurement Request frame Action field is shown in Figure 9-1081 (Spectrum Measurement Request frame Action field format).

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

The Spectrum Management Action field is defined in 9.6.2.1 (Spectrum Management Action field(#3729)).

However, sometimes some ad libbing appears instead.

Proposed changes:

Change at 1544.41:

The Block Ack Action field is ~~set to 0, 128, or 132 (representing ADDBA request). The meaning for each value is described~~ defined in 9.6.4.1 (Block Ack Action field(#3729)) for each of the ADDBA request variants.

Change at 1545.58:

The Block Ack Action field is ~~set to 1, 129, or 133 (representing ADDBA response). The meaning for each value is described~~ defined in 9.6.4.1 (Block Ack Action field(#3729)) for each of the ADDBA response variants.

Change at 1547.3:

The Block Ack Action field is ~~set to 2, 130, or 134 (representing DELBA). The meaning for each value is described~~ defined in 9.6.4.1 (Block Ack Action field(#3729)) for each of the DELBA variants.

Change at 1547.44:

The Block Ack Action field is ~~set as~~ defined in ~~Table 9-444 (Block Ack Action field values) to represent PBAC WinStart Update~~ 9.6.4.1.

At 1696.54 change “Table 9-583—FILS Action frame values” to “Table 9-583—FILS Action field values”.

At 1696.59 delete “ frame”.

At 1687.40 change “The DMG Action field is defined in DMG Action field” to “The DMG Action field is defined in 9.6.19.1”.

Change at 1697.18:

The FILS Action field is ~~set to the value given in Table 9-583 (FILS Action frame values) for FILS Container frame~~ defined in 9.6.23.1.

Change at 1719.41, 1920.23/51:

The HE Action field is defined in ~~Table 9-617 (HE Action field values(#3764)(11ax))~~ 9.6.31.1.

Change at 1721.41, 1722.1:

The Protected HE Action field is defined in ~~Table 9-621 (Protected HE Action field values(11ax))~~ 9.6.32.1.

Change at 1723.24:

The WUR Action field is ~~set to 0 as~~ defined in ~~Table 9-624 (WUR Action field values(11ba))~~ 9.6.33.1.

Change at 1724.23:

The WUR Action field is ~~set to 1 as~~ defined in ~~Table 9-624 (WUR Action field values(11ba))~~ 9.6.33.1.

Change at 1724.48:

The WUR Action field is ~~set to 2 as~~ defined in ~~Table 9-624 (WUR Action field values(11ba))~~ 9.6.33.1.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4199 in <this document>, which ensure that consistent wording is used throughout 9.6.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4303Mark RISON9 | "Service period request (SPR) frame", "Sector sweep (SSW) frame", "Sector sweep feedback (SSW-Feedback) frame", "Sector sweep Ack (SSW-Ack) frame" -- frames should have just one name | As it says in the comment [confirm direction] |

Discussion:

As the commenter says, it is established that frames (and indeed also elements etc.) should always be referred to in the same way. This helps finding all uses of the frame. If an abbreviation is used, the full form should only appear in 3.4 and at the start of the subclause defining the frame (but not its heading).

Proposed changes:

Change as follows:

**9.3.1.11 ~~Service period request (~~SPR~~)~~ frame format**

The format of the service period request (SPR) frame is shown in Figure 9-68 (SPR frame format).

**9.3.1.15 ~~Sector sweep (~~SSW~~)~~ frame format**

The frame format for the sector sweep (SSW) frame is defined in Figure 9-72 (SSW frame format).

 […]

The RA field contains the MAC address of the STA that is the intended receiver of the ~~sector sweep~~ SSW frame.

The TA field contains the MAC address of the transmitter STA of the ~~sector sweep~~SSW frame.

**9.3.1.16 ~~Sector sweep feedback (~~SSW-Feedback~~)~~ frame format**

The format of the sector sweep feedback (SSW-Feedback) frame is shown in Figure 9-73 (SSW-Feedback frame format).

**9.3.1.17 ~~Sector sweep Ack (~~SSW-Ack~~)~~ frame format**

The format of the sector sweep acknowledgement (SSW-Ack) frame is shown in Figure 9-74 (SSW-Ack frame format).

**9.5.1 ~~Sector Sweep~~SSW field**

(11ay)When the ~~Sector Sweep (~~SSW~~)~~ field is not transmitted in a DMG Beacon frame, the format of the

SSW field is shown in Figure 9-1067

**9.5.3 ~~Sector Sweep~~SSW Feedback field**

Change at 226.60 as follows:

**receive sector sweep:** [RXSS] Reception of ~~Sector Sweep (~~SSW~~)~~ frames via different sectors, in which a sweep is performed between consecutive receptions.

Change at 230.1 as follows:

**(11ay)short sector sweep (SSW) physical layer (PHY) protocol data unit (PPDU):** [Short SSW PPDU] A directional multi-gigabit (DMG) control mode physical layer (PHY) protocol data unit (PPDU) that has the Length field in the PHY header equal to 6 and the PPDU Type subfield within the Short SSW Payload field equal to 0.

Change at 234.4 as follows:

**transmit sector sweep:** [TXSS] Transmission of multiple ~~sector sweep (~~SSW~~)~~ or ~~directional multi-gigabit (~~DMG~~)~~ Beacon frames via different sectors, in which a sweep is performed between consecutive transmissions.

At 396.30, 1521.9, 2134.16, 2136.27, 2137.37, 2139.19/44, 2151.2/4, 2159.1 change “Sector Sweep field” to “SSW field”.

At 1523.37 change “Sector Sweep Feedback field” to “SSW Feedback field”.

At 1426.15 change “the Time to Switch to Complete Sector Sweep field” to “the Time to Switch to Full Sector Sweep field”.

At 2678.37 change “the Time to Switch to Full Sweep field” to “the Time to Switch to Full Sector Sweep field”.

At 2130.38, 2135.19/49 change “Sector Sweep Ack” to “SSW-Ack”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4303 in <this document>, which ensure that frames/fields related to SPR/SSW have only one name.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4356Mark RISON9 | Is the field "Comeback Delay" or "GAS Comeback Delay"? Also sometimes missing "frame" | As it says in the comment |

Discussion:

There are in fact two comeback delay fields. The GASsy one has “GAS” prepended. The EDMGy one does not.

It’s “field” that’s sometimes missing, not “frame”.

Sometimes it is suggested that a delay expires. It’s actually the delay timer that expires.

Proposed changes:

At 1567.17 change “nonzero GAS Comeback Delay value” to “nonzero GAS Comeback Delay field”.

At 1567.21 change “the expiration of the GAS Comeback Delay timer” to “the expiration of the GAS comeback delay timer”.

At 2172.44 change “If the TXOP or SP ended before the comeback delay elapses,” to “If the TXOP or SP ended before the comeback delay elapsed,” (cf. 2170.58).

At 2630.44 change “and Comeback Delay and Query Response Length fields both set to 0” to “and GAS Comeback Delay and Query Response Length fields both set to 0”.

At 2630.51 change “a Comeback Delay and Query Response Length both set to 0” to “GAS Comeback Delay and Query Response Length fields both set to 0”.

At 2631.2 change “a GAS Comeback Delay and Query Response Length both set to 0” to “GAS Comeback Delay and Query Response Length fields both set to 0”.

At 2631.42, 2634.8 change “the expiration of the GAS Comeback Delay” to “the expiration of the GAS comeback delay timer”.

At 2632.25/36 change “a GAS Comeback Delay set to 0, the Query Response and a Query Response Length set to the query response length” to “a GAS Comeback Delay field set to 0, a Query Response field, and a Query Response Length field set to the query response length”.

At 2633.14 change “a GAS Comeback Delay set to 1 TU, and a Query Response Length set to 0” to “a GAS Comeback Delay field set to 1 (TU), and a Query Response Length field set to 0”.

At 2633.60 change “and GAS Comeback Delay set to the value in dot11GASComebackDelay” to “and a GAS Comeback Delay field set to the value in dot11GASComebackDelay”.

At 2634.35 change “shall wait for the GAS Comeback Delay from that frame and upon expiration of the GAS Comeback Delay” to “shall wait for the expiration of the GAS comeback delay timer from that frame”.

At 5411.12 change “GAS Comeback Delay” to “GAS comeback delay”.

At 5411.28 change “the time after the expiration of the GAS comeback delay that a STA will buffer a Query Response.” to “the time after the expiration of the GAS comeback delay timer that a STA will buffer a Query Response.”

At 2562.40 change “Status Code” to “Status Code field”.

At 2632.23/33 change “a Status Code” to “the Status Code field”.

At 2659.10/14/16/52, 2661.25/27 change “Status Code” to “the Status Code field”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4356 in <this document>, which add “GAS” and “frame” where missing, and other minor editorial tweaks.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4278Mark RISON1.4 | We should have something in 1.4 to say that e.g. "beacon" refers to a Beacon, DMG Beacon or S1G Beacon frame | As it says in the comment [needs discussion] |

Discussion:

We sometimes use “beacon” to refer to one of the three flavours of beacon frame. However, this is never made clear.

Perhaps we should also do this for “probe request” (there exists an NDP flavour of this)? CID 4329 is about this, though it erroneously talked of probe responses rather than probe requests.

Proposed resolution:

REVISED

At 173.17 add a para “References in this standard to a “beacon” (with a lowercase initial) are to be understood as being to a Beacon, DMG Beacon or S1G Beacon frame, as the context permits.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4220Mark RISON | Shouldn't say values are reserved for the WFA, as then they would not be allowed to be used by 802.11 STAs. Just say used/defined by the WFA | As it says in the comment [needs discussion] |

Discussion:

The “reserved” terminology is well-defined in the MAC to mean (for a field) set to 0 on tx and ignored on rx or (for a value) do not use. It is therefore inappropriate to talk of fields/values being reserved by the WFA (or any other body) as this would suggest IEEE Std 802.11-conformant STAs could not use them. A formal process exists that allows the WFA (and any other SDO) to request allocation; if this is granted then the field/value can legitimately be used by IEEE Std 802.11 implementations.

Proposed changes:

At 762.54 change “Reserved (used by the Wi-Fi Alliance® a)” to “*Allocated to the Wi-Fi Alliance® a*” (note italicisation).

At 1357.23 delete “Reserved” (leave cell blank) and change “Used by the Wi-Fi Alliance® a” to “Allocated to the Wi-Fi Alliancea” (note can delete the ® since already at 762.54).

At 1586.47, 2657.53 change “Reserved (used by the Wi-Fi Alliancea)” to “*Allocated to the Wi-Fi Alliancea*” (note italicisation).”

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4220 in <this document>, which describe fields/values as being allocated to the WFA rather than reserved.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4219Mark RISON10.52285.30 | "include a Page Slice Number that matches its Page Slice Number and a page index that matches its Page index" has bogus capitalisation and missing "field"s | As it says in the comment [needs submission] |

Discussion:

A veritable cornucopia of editorial horror.

Proposed changes:

Change as follows:

An S1G STA for which dot11PageSlicingImplemented is true shall process all received TIM elements that include a Page Slice Number field that matches its ~~P~~page ~~S~~slice ~~N~~number and a ~~p~~Page ~~i~~Index field that matches its ~~P~~page index

At 2286.3/10/20, 2378.48/50 change “Page Slice Number” to “Page Slice Number field”.

Proposed resolution:

REVISED

Change the para at the referenced location to:

An S1G STA for which dot11PageSlicingImplemented is true shall process all received TIM elements that include a Page Slice Number field that matches its page slice number and a Page Index field that matches its page index

At 2286.3/10/20, 2378.48/50 change “Page Slice Number” to “Page Slice Number field”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4201Mark RISON10 | There are a few "successfully negotiated"s, which implies that the other "negotiated"s include unsuccessful negotiation | Delete "successfully" in each case [I can provide locations if needed; confirm direction] |

Discussion:

As the comment indicates, in general if you talk of negotiating something then unless there are words to the contrary that implies success.

Proposed resolution:

REVISED

Delete “successfully”/”a successful” at:

1871.23: An AP may transmit an SPP A-MSDU for a GCR group address if it has **successfully** negotiated RSNA (re)associations with all associated STAs that have an active GCR agreement for this group address.

1953.43: (11ay)An EDMG STA that has **successfully** negotiated a block ack agreement shall obey the following rules as a recipient in addition to the rules specified in 10.25.6 (HT-immediate block ack extensions).

1954.1: (11ay)An EDMG STA that has **successfully** negotiated a block ack agreement shall obey the following rules as an originator in addition to rules specified in 10.25.6 (HT-immediate block ack extensions).

1973.62: A block ack agreement that is **successfully** negotiated between two PBAC STAs is a protected block ack agreement.

1974.1: A block ack agreement that is **successfully** negotiated between two STAs when either or both of the STAs is not a PBAC STA is a block ack agreement that is not a protected block ack agreement.

1974.10: A STA that has **successfully** negotiated a protected block ack agreement shall obey the following rule as a block ack originator in addition to rules specified in 10.25.6.7 (Originator’s behavior) and 10.25.6.8 (Maintaining block ack state at the originator):

1974.18: A STA that has **successfully** negotiated a protected block ack agreement shall obey the following rules for that agreement(#1014) as a block ack recipient in addition to rules specified from(#1014) 10.25.6.3 (Scoreboard context control during full-state operation) to 10.25.6.6 (Receive reordering buffer control operation):

2451.41: Following **a successful** negotiation, a TS is created, identified within the non-AP STA by its TSID and direction, and identified within the HC by a combination of TSID, direction, and STA address.

2451.43: Following **a successful** negotiation of a DMG TSPEC in a PBSS or in a DMG infrastructure BSS, a new allocation is created, or an existing allocation is modified.

2451.47: Following **a successful** negotiation of a PTP TSPEC or a TSPEC in a DMG BSS, the frames corresponding to the PTP TSPEC or TSPEC are identified within the STA by the combination of TSID, requesting non-AP DMG STA address, and responding non-AP DMG STA address and direction.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4367Mark RISON9 | The field is now called EOF/Tag but there are ~9 instances of "EOF (sub)field" | Add "/Tag" to the errant instances |

Discussion:

/Tag got appended by HE, since the bit stopped always meaning end-of-frame.

Proposed resolution:

REVISED

Add “/Tag” after “EOF” at 206.57, 230.18, 1725.43, 1726.18, 1812.15, 1875.40, 1876.6/36, 1877.20, 3580.16.

At 1726.1 change “TThe” to “The”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4223Mark RISON6 | "Specifies the address of the peer MACentity with which to perform thedisassociation process." -- there's more than one entity if the address is the group address | Change to "Specifies the address of the peer MACentity with which to perform thedisassociation process, if individual." for those where broadcast is possible [I can provide locations; confirm direction] |

Discussion:

If the address is the broadcast address doesn’t specify “the” peer MAC entity.

Lots of other problems become apparent once you look at the peer MAC address stuff…

Why no PeerSTAAddress in MLME-(RE)ASSOCIATE.confirm? Maybe at 425.54 and 452.20 add “PeerSTAAddress,” and at 427.2 and 453.36 add a row with cells PeerSTAAddress / MAC address / Any valid individual address / Specifies the address of the peer MAC entity to which the [re]association request was sent.

Why only REASSOC has [New]PCPorAPAddress? Maybe at 446.63 and 447.55 change “NewPCPorAPAddress” to “NewPeerSTAAddress”.

Proposed resolution:

REVISED

At 365.26 change “ASSOCIATE” to “AUTHENTICATE”.

At 416.28 (AUTH.ind) change “Specifies the address of the peer MAC entity with which the authentication relationship was established.” to “Specifies the address of the peer MAC entity from which the authentication

request was received.”

At 419.34, 420.11/47, 474.45 change “Any valid individual address, or broadcast address” to “Any valid individual address, or the broadcast address”.

At 419.34 (DEAUTH.req) change “Specifies the address of the peer MAC entity with which to perform the deauthentication process.” to “Specifies the address of the peer MAC entity(ies) with which to perform the deauthentication process.”

At 420.11 (DEAUTH.cfm) change “Specifies the address of the peer MAC entity with which the deauthentication process was attempted.” to “Specifies the address of the peer MAC entity(ies) with which the deauthentication process was attempted.”

At 420.47 (DEAUTH.ind) change “Any valid individual address, or broadcast address” to “Any valid individual address”.

At 435.25 (ASSOC.ind) change “Specifies the address of the peer MAC entity from which the association was received.” to “Specifies the address of the peer MAC entity from which the association request was received.”

At 474.45 (DISASSOC.req) change “Specifies the address of the peer MAC entity with which to perform the disassociation process.” to “Specifies the address of the peer MAC entity(ies) with which to perform the disassociation process.”

At 505.34 (BF-TRAINING.ind) change “Specifies the address of the peer MAC entity with which beamforming training was performed.” to “Specifies the address of the peer MAC entity with which beamforming training was performed or attempted.”

At 507.12 (SU-MIMO-BF-TRAINING.cfm) change “Specifies the address of the peer MAC entity with which to perform SU-MIMO beamforming training.” to “Specifies the address of the peer MAC entity with which SU-MIMO beamforming training was performed or attempted.”

At 508.3 (SU-MIMO-BF-TRAINING.ind) change “Specifies the address of the peer MAC entity with which to perform SU-MIMO beamforming training.” to “Specifies the address of the peer MAC entity with which SU-MIMO beamforming training was performed or attempted.”

At 509.47 (MU-MIMO-BF-TRAINING.cfm) change “Specifies the group of peer MAC entities with which to perform MU-MIMO beamforming training.” to “Specifies the group of peer MAC entities with which MU-MIMO beamforming training was performed or attempted.”

At 510.45 (MU-MIMO-BF-TRAINING.ind) change “Specifies the address of the peer MAC entity with which to perform MU-MIMO beamforming training.” to “Specifies the address of the peer MAC entity with which MU-MIMO beamforming training was performed or attempted.”

At 512.24 (SU-MIMO-HYBRID-BF-PROTOCOL.cfm), 513.25 (SU-MIMO-HYBRID-BF-PROTOCOL.ind) change “Specifies the address of the peer MAC entity with which to perform the SU-MIMO hybrid beamforming protocol.” to “Specifies the address of the peer MAC entity with which the SU-MIMO hybrid beamforming protocol was performed or attempted.”

At 515.24 (MU-MIMO-HYBRID-BF-PROTOCOL.cfm) change “Specifies the group of peer MAC entities with which to perform the MU-MIMO hybrid beamforming protocol.” to “Specifies the group of peer MAC entities with which the MU-MIMO hybrid beamforming protocol was performed or attempted.”

At 516.24 (MU-MIMO-HYBRID-BF-PROTOCOL.ind) change “Specifies the address of the peer MAC entity with which to perform the SU-MIMO hybrid beamforming protocol.” to “Specifies the address of the peer MAC entity with which the SU-MIMO hybrid beamforming protocol was performed or attempted.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4134Mark RISON6.5.3.3.2 | Load in BSSDescription should be conditional on dot11QBSSLoadImplemented, as for HE BSS Load. Also rename to BSS Load | As it says in the comment [confirm direction] |

Discussion:

In the table in 6.5.3.3.2 we have:



but also:



Note that e.g. in the Beacon frame:





What about the Extended BSS Load element? Why not in the 6.5.3.3.2 table at all? Maybe add a row after the BSS Load row (the one at 393.14) with the following cells:

Extended BSS Load / Extended BSS Load element / As defined in <Extended BSS Load element> / The values from the Extended BSS Load element. The parameter is present if dot11QBSSLoadImplemented, and dot11VHTOptionImplemented are both true and an Extended BSS Load element was present in the Probe Response or Beacon frame from which the BSSDescriptionSet was determined. Otherwise, the parameter is not present. / Do not adopt

Proposed resolution:

REVISED

At 393.14 change the first cell to “BSS Load” and the fourth cell to “The values from the BSS Load element. The parameter is present if dot11QosOptionImplemented and dot11QBSSLoadImplemented are both true and a BSS Load element was present in the Probe Response or Beacon frame from which the BSSDescriptionSet was determined. Otherwise, the parameter is not present.”

At 404.14 delete “optionally”.

At 404.18 change “are true” to “are both true”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4195Mark RISON10.25.6 | "MSDU SSN" and "MSDU\_SSN" are each used once and not defined | Replace with "MPDU SSN" and "MPDU\_SSN" [needs discussion] |
| CID 4196Mark RISON10.25 | "MPDU SSN" is used in 10.25.6.3 Scoreboard context control during full-state operation and 10.25.6.4 Scoreboard context control during partial-state operation and 10.25.7 Protected block ack agreement but not defined | I think it might refer to the Starting Sequence Number field, but if so say that not "SSN" |
| CID 4197Mark RISON10.25.6 | "the MPDU Starting Sequence Number subfield" (5x) -- no such field | I think it might refer to the Starting Sequence Number field, but if so say that not "MPDU Starting Sequence Number" |
| CID 4187Mark RISON | There are references to "MPDU SSN" or "MPDU\_SSN" (sometimes italicised) but it's not clear what these are in 10.25.6.4/10.25.7 (maybe just referring to abbreviated field name?), 10.25.6.7.1, | Define MPDU\_SSN and use that term throughout (non-italic) [needs discussion] |
| CID 4200Mark RISON10.25.6.7.1 | "and the PBAC WinStart Update frame shall contain only MPDU\_SSN and MSDU\_SSN fields of an MPDU that has the value of the Start of MSDU subfield equal to 1" -- an MPDU doesn't have MPDU\_SSN and MSDU\_SSN fields (note also that 10.25.6.6.3.2 does define MPDU\_SSN for BAR frames, but not for PWU frames) | Refer to fields that exist [needs discussion] |

Discussion:

The term “SSN” is not defined in Clause 3. The term “MPDU\_SSN” is defined in 10.25.6.6.3.2 Block ack agreements using segmentation and reassembly(11ay): MPDU\_SSN is the MPDU Starting Sequence Number subfield value of the received BlockAckReq frame, although there is no such thing as an MPDU Starting Sequence Number (sub)field. BAR (and BA etc.) frames have Starting Sequence Number fields.

Notes on SAR (11ay): the SAR Configuration element can be included in ADDBA Request/Response frames, and contains MSDU Buffer Size, MPDU Buffer Size, MSDU Modulo and MPDU Modulo fields. When SAR is used the Sequence Control field has MSDU Sequence Number and MPDU Sequence Number fields. However, the BAR and BA frames are apparently unchanged; they still just have a Starting Sequence Number field (not an “MPDU Starting Sequence Number” field). Ditto the PBAC WinStart Update frame.

Proposed changes:

**10.3.2.12 Fragment BA procedure**

The values of the BlockAck ID and Starting Sequence Number fields are obtained after decoding the NDP BlockAck frame as described in 10.56 (Bitmap protection for NDP BlockAck frames).

**10.25.1 Introduction**

The Block Ack Starting Sequence Control subfield within the BlockAckReq frame represents the MPDU starting sequence number.

**10.25.6.2 HT-immediate block ack architecture**

(11ay)In a block ack agreement with segmentation and reassembly, the originator maintains a transmit buffer control that uses *WinStartOJ* and *WinSizeOJ* to submit MPDUs for transmission and releases transmit buffers upon reception of BlockAck frames from the recipient. *WinStartOJ* is the ~~MSDU SSN value~~ starting sequence number of the transmit window and *WinSizeOJ* is the value of the MSDU Buffer Size field in the recipient’s SAR Configuration element that established the block ack agreement.

**10.25.6.3 Scoreboard context control during full-state operation**

a) At HT-immediate block ack agreement establishment:

1) (11ay)~~In a block ack agreement that does not use segmentation and reassembly,~~ *WinStartR = ~~SSN~~*Starting Sequence Number subfield in ~~from~~ the ADDBA Request frame that elicited the ADDBA Response frame that established the HT-immediate block ack agreement or from an MPDU that synchronized an unsolicited block ack agreement. ~~Otherwise,~~ *~~WinStart~~~~R~~ ~~= MPDU SSN~~* ~~from the ADDBA Request frame that elicited the ADDBA Response frame that established the block ack agreement.~~

[…]

c) For each received BlockAckReq frame that is (#407)related to a specific full-state operation HT-immediate block ack agreement that is not a protected block ack agreement, the block acknowledgment record for that agreement is modified as follows, where *SSN* is the ~~value from the~~ Starting Sequence Number subfield of the received BlockAckReq frame (11ay)~~if segmentation and reassembly is not used and is the value from the MPDU Starting Sequence Number subfield of the received BlockAckReq frame when segmentation and reassembly is used~~:

**10.25.6.4 Scoreboard context control during partial-state operation**

a) During partial-state operation (11ay)~~without segmentation and reassembly~~, *WinStartR* is determined by the Sequence Number subfield value of received Data frames and by the Starting Sequence Number subfield value of received BlockAckReq frames as described below. (11ay)~~During partial-state operation with segmentation and reassembly,~~ *~~WinStart~~~~R~~ ~~= MPDU SSN~~* ~~from the ADDBA Request frame that elicited the ADDBA Response frame that established the block ack agreement.~~

[…]

d) For each received BlockAckReq frame that is (#407)related to a specific partial-state operation HT-immediate block ack agreement that is not a protected block ack agreement, when no temporary record for the agreement (#407)related to the received frame exists at the time of receipt of the frame, a temporary block acknowledgment record is created as follows, where *SSN* is the ~~starting value of the~~ Starting Sequence Number subfield of the received BlockAckReq frame (11ay)~~if segmentation and reassembly is not used and is the value of the MPDU Starting Sequence Number subfield of the received BlockAck frame when segmentation and reassembly is used~~:

**10.25.6.6.1 General**

(11ay)For each HT-immediate block ack agreement that uses segmentation and reassembly, *WinStartB* and *WinEndB* *[Editor: note formatting change too]* variables shall be initialized as follows:

— *WinStartB* is initialized to the ~~MPDU~~ Starting Sequence Number subfield value of the ADDBA Request frame that elicited the ADDBA Response frame that established the block ack agreement.

— *WinEndB* is initialized to *WinStartB* + *WinSizeB* – 1, where *WinSizeB* is set to the smaller of 1024 and the value of the MPDU Buffer Size field of the ADDBA Response frame that established the block ack agreement.

**10.25.6.6.3.2 Block ack agreements using segmentation and reassembly(11ay)**

For each received BlockAckReq frame that is (#407)related to a specific block ack agreement that uses segmentation and reassembly, the receive reordering buffer record is modified as follows, where *MPDU\_SSN* is the ~~MPDU~~ Starting Sequence Number subfield value of the received BlockAckReq frame:

**10.25.6.7.1 General(11ay)**

If the received BlockAck response is of an expected NDP\_1M BlockAck frame (or an NDP\_2M BlockAck frame), the S1G originator shall accept it as correctly received if the value obtained from the BlockAck ID field equals the 2 LSBs (or the 6 LSBs) of the Scrambler Initialization value of the immediately previously transmitted A-MPDU that is not an S-MPDU, or BlockAckReq frame, and the Starting Sequence Number obtained from the Starting Sequence Control field equals *WinStartO*.

[…]

(11ay)Under a block ack agreement with segmentation and reassembly, the BlockAckReq ~~frame shall contain only~~ *~~MPDU\_SSN~~*and ~~the~~ PBAC WinStart Update frames shall ~~contain only~~ *~~MPDU\_SSN~~* ~~and MSDU\_SSN fields of~~ have a Starting Sequence Number field that corresponds to an MPDU that has the Start of MSDU subfield equal to 1. (#3169)(#3014)

**10.25.6.8 Maintaining block ack state at the originator**

— The originator shall not update the status of MPDUs with Sequence Number subfield values between *WinStartO* and *SSN* – 1 of the received BlockAck frame, where *SSN* is the Starting Sequence Number subfield in the received BlockAck frame.~~, and~~

NOTE 1—It is possible for *SSN* *[Editor: note italicisation]* ~~the Starting Sequence Number subfield value (SSN) of the received BlockAck frame~~ to be greater than *WinStartO* because of the lack of reception of a nonzero number of MPDUs beginning with the MPDU with Sequence Number subfield value equal to *WinStartO* at a recipient that is using partial-state operation.

— For each MPDU for which the status is not acknowledged, and for which the corresponding bit of the received bitmap contains a value of 1, and for which the Sequence Number subfield value is between *SSN* *[Editor: note italicisation]* ~~of the received BlockAck frame~~ and *WinStartO* + *WinSizeO* – 1, the originator shall change its status to acknowledged.

**10.25.7 Protected block ack agreement**

A STA that has successfully negotiated a protected block ack agreement shall obey the following rules for that agreement(#1014) as a block ack recipient in addition to rules specified from(#1014) 10.25.6.3 (Scoreboard context control during full-state operation) to 10.25.6.6 (Receive reordering buffer control operation):

— (#1014)(#1017)The STA shall not use the Starting Sequence Number subfield of the Block Ack Starting Sequence Control field in a BlockAckReq, MU-BAR Trigger or GCR-MU BAR Trigger frame(#3015) to update *WinStartB* and *WinStartR*. If the Starting Sequence Number subfield is greater than *WinEndB* or less than *WinStartB*, dot11PBACErrors shall be incremented by 1.(11ay) ~~If, for a block ack agreement with segmentation and reassembly, the MPDU Starting Sequence Number subfield is greater than~~ *~~WinEnd~~~~B~~*~~or less than~~ *~~WinStart~~~~B~~*~~, dot11PBACErrors shall be incremented by 1.(#3014)~~

— Upon receipt of a PBAC WinStart Update frame whose TID and transmitter address are the same as those of the protected block ack agreement, the STA shall update its *WinStartR* and *WinStartB* values based on the starting sequence number in the PBAC WinStart Update frame according to the procedures outlined for reception of BlockAckReq frames in 10.25.6.3 (Scoreboard context control during full-state operation), 10.25.6.4 (Scoreboard context control during partial-state operation), 10.25.6.6.1 (General), and 10.25.6.6.3 (Operation for each received BlockAckReq), while treating the starting sequence number as though it were the *~~SSN~~*Starting Sequence Number field of a received BlockAckReq frame (11ay)~~or, in case of a block ack agreement with segmentation and reassembly, treating the MPDU starting sequence number as though it were the MPDU SSN of a received BlockAckReq frame~~.(#3014)

**10.25.8.2 Scoreboard context control during GCR block ack**

1) *WinStartR* = the Starting Sequence Number subfield value ~~(SSN) from~~ in the ADDBA Request frame that elicited the ADDBA Response frame that established the GCR block ack agreement.

**10.25.8.3 Scoreboard context control during GLK-GCR block ack**

1) *WinStartR* = the Starting Sequence Number subfield value ~~(SSN) from~~ in the GLK-GCR Parameter Set element included in the Association Response frame, Reassociation Response frame or in the GLK-GCR Groupcast Mode Change Notification frame.

**10.25.9.2 DMG block ack architecture with flow control**

The scoreboard context control provides the *WinCapacityB*, actually controlled by the Reordering buffer in addition to the bitmap field and the Starting Sequence Number ~~(SSN)~~ field value (SSN) to be sent in BlockAck frame responses to the originator.

**10.25.9.4.2 Operation for DMG block ack agreement initialization**

a) *WinStartB = SSN*, where *SSN* is the Starting Sequence Number field in ~~from~~ the ADDBA Request frame that elicited the ADDBA Response frame that established the DMG block ack agreement

**10.25.10.6 Originator behavior and block ack state maintenance**

At the start of the next TXOP or SP, may transmit all the MPDUs with *SN* equal or higher than the first unsuccessful MPDU, or may send a BlockAckReq frame with *~~SSN~~*Starting Sequence Number field equal to the *SN* of the first unsuccessful MPDU

**9.6.19.16 Relay Ack Request frame format**

|  |  |
| --- | --- |
| 4 | Block Ack Starting Sequence Control |

The BAR Control field and Block Ack Starting Sequence Control fields are defined in 9.3.1.7 (BlockAckReq frame format).

**9.6.19.17 Relay Ack Response frame format**

|  |  |
| --- | --- |
| 4 | Block Ack Starting Sequence Control |

The Block Ack Starting Sequence Control field is defined in 9.3.1.8 (BlockAck frame format) and is set to

the corresponding value within the immediately previously received Relay Ack Request frame.

**26.4.2 Acknowledgment context in a Multi-STA BlockAck frame**

If the AID subfield is 0 for an AP originator or the non-AP STA’s AID for a non-AP STA originator, the Ack Type field is 0, and the TID field is less than 8, then the Block Ack Starting Sequence Control, TID, and Block Ack Bitmap fields

**26.4.5 HE block acknowledgment request and response rules**

An HE STA that receives a BlockAckReq frame or an MU-BAR Trigger frame that contains a Compressed BlockAckReq variant in the User Info field addressed to the STA or receives a GCR MU-BAR Trigger frame that contains a Compressed BlockAckReq variant in the Common Info field shall respond with a Compressed BlockAck frame as defined in 10.25.6 (HT-immediate block ack extensions) or a Multi-STA BlockAck frame as defined in 26.4 (HE acknowledgment procedure) with the Starting Sequence Number subfield set to the Starting Sequence Number subfield of the Block Ack ~~Request~~ Starting Sequence Control subfield and the length of the Block Ack Bitmap subfield calculated as defined in 26.4.3 (Negotiation of block ack bitmap lengths).

An HE STA that receives a Multi-TID BlockAckReq frame or an MU-BAR Trigger frame that contains a Multi-TID BlockAckReq variant in the User Info field addressed to the STA or receives a GCR MU-BAR Trigger frame that contains a Multi-TID BlockAckReq variant in the Common Info field shall respond with a Multi-STA BlockAck frame that contains a Per AID TID Info field with a Block Ack Bitmap subfield for each of the TIDs (with values less than 8) contained in the BlockAckReq frame, with the Starting Sequence Number subfield set to the Starting Sequence Number subfield of the Block Ack ~~Request~~ Starting Sequence Control subfield, and with the length of the Block Ack Bitmap subfield calculated as defined in 26.4.3 (Negotiation of block ack bitmap lengths).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CIDs 4195, 4196, 4197, 4187, 4200 in <this document>, which address various issues related to field names and variables for BA.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4226Mark RISON12 | There needs to be something to specify the restrictions on the RSNE in (re)assoc req, e.g. that there be a single paiwise cipher suite | As it says in the comment [confirm direction] |

Discussion:

All the restrictions are already specified.

Proposed resolution:

REJECTED

All the restrictions are already specified in 11.3.5.2/11.3.5.4: "The RSNE shall specify exactly one pairwise cipher suite and exactly one AKM suite."

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4141Mark RISON12.7 | "Error = 0 - same as message 1" is spurious. Yes, it's the same, but so is e.g. the Install bit, but this isn't flagged | Remove the spurious "same as message"s [confirm direction] |

Discussion:

In general, things might happen to be, or are by necessity, the same as in previous messages, but this should only be flagged when it has particular significance.

Proposed changes:

**12.7.6.3 4-way handshake message 2**

Message 2 uses the following values for each of the (#1836)EAPOL-Key PDU fields:

Descriptor Type = N – see 12.7.2 (EAPOL-Key frames)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 ~~– same as message 1~~

Key Type = 1 (Pairwise) ~~– same as message 1~~

Reserved = 0

Install = 0

Key Ack = 0

(#1829)Key MIC Present = 0 when using an AEAD cipher or 1 otherwise

Secure = (#3302)(#3596)0 in initial 4-way handshake, or 1 when PTK rekeying (but see 12.7.2

(EAPOL-Key frames))

Error = 0 ~~– same as message 1~~

Request = 0 ~~– same as message 1~~

Encrypted Key Data = 1 when using an AEAD cipher or 0 otherwise

Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = n – same as message 1, to let the Authenticator or initiator STA know to which message 1 this corresponds

**12.7.6.4 4-way handshake message 3**

Message 3 uses the following values for each of the (#1836)EAPOL-Key PDU fields:

Descriptor Type = N – see 12.7.2 (EAPOL-Key frames)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 ~~– same as message 1~~

Key Type = 1 (Pairwise) ~~– same as message 1~~

Reserved = 0

Install = (#3056)1

Key Ack = 1

(#1829)Key MIC Present = 0 when using an AEAD cipher or 1 otherwise

Secure = 1 (keys installed)

Error = 0 ~~– same as message 1~~

Request = 0 ~~– same as message 1~~

Encrypted Key Data = 1

Reserved = 0 – unused by this protocol version

Key Length = (#3270)Cipher suite dependent; see Table 12-8 (Cipher suite key

lengths(#1083)(#3532))

Key Replay Counter = n+1 – to allow Authenticator or initiator STA to match the right message 4 from Supplicant or peer STA

Key Nonce = ANonce – same as message 1

**12.7.6.5 4-way handshake message 4**

Message 4 uses the following values for each of the (#1836)EAPOL-Key PDU fields:

Descriptor Type = N – see 12.7.2 (EAPOL-Key frames)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 ~~– same as message 1~~

Key Type = 1 (Pairwise) ~~– same as message 1~~

Reserved = 0

Install = 0

Key Ack = 0(#1824)

(#1829)Key MIC Present = 0 when using an AEAD cipher or 1 otherwise

Secure = 1

Error = 0

Request = 0

Encrypted Key Data = 1 when using an AEAD cipher or 0 otherwise

Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = n+1 – same as message 3, to let the Authenticator or initiator STA know to which message 3 this corresponds

**12.7.7.3 Group key handshake message 2**

Message 2 uses the following values for each of the (#1836)EAPOL-Key PDU fields:

Descriptor Type = N – see 12.7.2 (EAPOL-Key frames)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 ~~– same as message 1~~

Key Type = 0 (Group) ~~– same as message 1~~

Install = 0

Key Ack = 0

(#1829)Key MIC Present = 0 when using an AEAD cipher or 1 otherwise

Secure = 1

Error = 0

Request = 0

Encrypted Key Data = 1 when using an AEAD cipher or 0 otherwise

Reserved = 0

Key Length = 0

Key Replay Counter = m (#1475)– same as message 1, to let the Authenticator or initiator STA know to which message 1 this corresponds

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4141 in <this document>, which delete the spurious “same as message”s.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4233Mark RISON12.7.22898.54 | It would be helpful to show what the packet body is | In Figure 12-32--EAPOL-Key PDU format add a vertical bidi arrow from the top of the Descriptor Type cell to the bottom of the Key Data Length + Key Data cells, labelled Packet body |

Discussion:

There are references to a Packet Body field, but nothing actually shows this.

Proposed changes:

Add a labelled bidi arrow as shown:



Proposed resolution:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4158Mark RISON2507.34 | "If dot11RMBeaconActiveMeasurementActivated is true and the Measurement Mode in the measurementrequest is Active, the measuring STA shall perform the following procedure (or an equivalent procedure) onthe requested channel, if permitted (e.g. the channel is not subject to DFS)" -- should say should respond with reject if not permitted | Add a sentence to that effect |

Discussion:

At the moment the behaviour under DFS is vague. Refusing is probably better than declaring incapability.

Proposed resolution:

REVISED

At 2507.56 add a para:

If dot11RMBeaconActiveMeasurementActivated is true, the Measurement Mode in the measurement request is Active, and the measurement on the requested channel is not permitted (e.g. the channel is subject to DFS), the measuring STA shall reject the measurement request by returning a Beacon report with the Refused subfield in the Measurement Report Mode field set to 1.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4221Mark RISON | Sometimes "DTIMs" is used as an interval | Change to "DTIM intervals" [confirm direction] |

Discussion:

We have two specific terms:

**delivery traffic indication map (DTIM) beacon:** [DTIM beacon] A Beacon frame or an S1G Beacon frame after which any buffered group addressed bufferable units (BUs) are transmitted.

**delivery traffic indication map (DTIM) interval:** [DTIM interval] The interval between the consecutive target beacon transmission times (TBTTs) of DTIM beacons.

Proposed changes:

REVISED

Change “DTIM frame” to “DTIM beacon” at 383.10 (in “receive all DTIM frames”), 2286.54 (in “check the DTIM frame comprising of […]”).

Change “ReceiveDTIMs” to “ReceiveDTIMBeacons” at 383.2/10, 1089.22/26, 2378.60, 2382.34, 2391.31/33.

Change “DTIMs” to “DTIM intervals” at 695.48 (in “every dot11QLoadReportIntervalDTIM DTIMs”), 1106.3/9 (in “in units of DTIMs”), 2554.22 (in “every dot11TimeAdvertisementDTIMInterval DTIMs”), 2668.31 (in “every dot11QLoadReportIntervalDTIM DTIMs”).

Change “DTIMs” to “DTIM beacons” at 858.2 (2x) (in “successive DTIMs. If all TIMs are DTIMs”), 2382.33 (in “they contain TIMs, some of which are DTIMs”), 2382.34 (in “power-on its receiver for all DTIMs”), 2551.8 (in “if no DTIMs are transmitted”).

At 4926.60 change “UNITS "dtims"” to “UNITS "DTIM intervals"”. At 4927.4 delete “in number of DTIMS”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4228Mark RISON9.4.2.66.3 | What does "negotiated RSNE" mean? Does it mean the last one sent? | Change to "last RSNE transmitted" (1x in 9.4.2.66.3 and 2x in C.3) |
| CID 4263Mark RISON12 | Re CID 3488. What does "the negotiated RSNE" mean? The one sent last? The one sent last locally?Also, in relation to RSNE contents and whether they include the element ID and length: what about "All other fields in the second RSNE shall be identical to the first RSNE.(#190)" at 2905.55 [not clear: does the first RSNE have all suites or just one?], "all other fields of the RSNE shall be identical to the RSNE present in" on p. 2976 (2x) [for first, not sure if auth frame can contain a PMKID; for second beacon/prsp frame does not contain a PMKID so Length field will differ], "The RSNE shall be identical to the RSNE in the STA's Beacon and Probe Response frames." at 3038.14 [OK?]? | As it says in the comment [needs discussion] |

Discussion:

Jouni MALINEN comments on CID 4263:

There are two completely separate topics here.

“The negotiated RSNE” is used (at least in D3.0) only in WNM event reporting. I doubt anyone has ever implemented that or has any intent of implementing it, so this is of not much interest to real world. I’d guess the original intent was for this to refer to the RSNE sent by the non-AP STA in the (Re)Association Request frame that resulted in successful completion of the current RSN association.

2905.55: The first RSNE in EAPOL-Key msg 3/4 includes all the pairwise cipher suites to match the RSNE in the Beacon frames. The second RSNE is otherwise identical to the first one except for having only a single pairwise cipher suite and well, having a smaller Length field value (which the current text does not seem to strictly speaking state). By the way, this is yet another one of those not-implemented-by-anyone case, I’d assume.

2976: Should really allow the Length field value to be different for the second instance of RSNE (in another frame) (for both L2 and L12).

3038.14: This looks correct.

The “negotiated RSNE” instances are:

1078.36: The RSNE field contains the (#3488)Information field of the negotiated RSNE at the time of the authentication attempt, truncated to the maximum length allowed for the RSNE field if necessary.

5006.60: This attribute contains (#3488)the negotiated RSNE at the time of the authentication attempt.

5142.5: This attribute contains the (#3488)Information field of the negotiated RSNE at the time of the authentication attempt, truncated to the maximum length allowed for the RSNE field in the RSNA event report, if necessary.

3038.14 says:

In addition to contents for establishing a mesh peering as specified in 14.4.6.1 (Generating Mesh Peering Open frames), the Mesh Peering Open frame, if used for the AMPE, shall contain the following:

[…]

— The RSNE shall be identical to the RSNE in the STA’s Beacon and Probe Response frames.

In a couple of locations reference is made to “the Authentication frame” without specifying which one this actually is (AP’s or STA’s). Mike MONTEMURRO has kindly clarified this.

Proposed changes:

At 1078.36, 5006.60, 5142.5 change “the negotiated RSNE at the time of the authentication attempt” to “the RSNE in the (Re)Association Request frame that resulted in the current RSNA”.

Change at 2095.50 (in 4-way handshake message 3):

It may happen, for example, that a Supplicant selects a pairwise cipher suite which is advertised by an AP, but which policy disallows for this particular STA. An Authenticator may, therefore, insert a second RSNE to overrule the STA’s selection. An Authenticator’s SME shall insert the second RSNE, after the first RSNE, only for this purpose. The Pairwise Cipher Suite Count field in the second RSNE included shall be set to 1 and the ~~p~~Pairwise ~~c~~Cipher ~~s~~Suite List field ~~in the second RSNE included~~ shall ~~be~~contain one of the ciphers advertised by the Authenticator. All other fields in the second RSNE, disregarding the Length field, shall be identical to those in the first RSNE.(#190)

Change at 2975.62 (FT initial mobility domain association over FILS in an RSN):

The S1KH ~~on STA~~ provides the PMKR1Name in the PMKID List field of the RSNE to be included in the (Re)Association Request frame. The PMKR1Name shall be as calculated by the S1KH according to the procedures of 12.7.1.6.4 (PMK-R1); all other fields of the RSNE, disregarding the Length field, shall be identical to those in the RSNE present in the STA’s Authentication frame. The S1KH shall also provide the FTE and MDE; they ~~FTE and MDE~~ shall be the same as those ~~provided~~ in the AP’s Authentication frame. If the S1KH set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in the RSNXE, the S1KH shall also provide the RSNXE.

Finally, the R1KH provides the PMKR1Name in the PMKID List field of the RSNE to be included in the (Re)Association Response frame. The PMKR1Name shall be as calculated by the R1KH according to the procedures of 12.7.1.6.4 (PMK-R1) and shall be the same as the PMKR1Name in the (Re)Association Request frame; all other fields of the RSNE, disregarding the Length field, shall be identical to those in the RSNE present in the Beacon or Probe Response frames. The R1KH shall also provide the FTE and the MDE; they~~. The FTE and MDE~~ shall be the same as those in the AP’s Authentication frame. If the RSNXE is present in the Beacon or Probe Response frames ~~that the AP transmits~~, the ~~AP~~R1KH shall also provide the RSNXE.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4228 and 4263 in <this document>, which clarify that the “negotiated RSNE” is the one in the (re)assoc req, and that the Length field can indeed vary in some of the locations identified. Some editorial fixes are also made.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID xxxMark RISON |  |  |

Discussion:

Proposed changes:

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID xxx in <this document>, which xxx

**TBD:**

4340: lowercase frame names in 3.1/2 left of colon

4242: only one abbrev (cf. 22/1993 -- {fast BSS transition, FT} {over-the-air fast BSS transition, over-the-air FT} {over-the-DS fast BSS transition, over-the-DS FT} {fast BSS transition initial mobility domain association, FT initial mobility domain association} {fast BSS transition originator, FT originator, FTO} {TDLS peer U-APSD, TPU})

**References:**

802.11me/D3.0 except where otherwise specified