IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some comments on 11me/D3.0 (LB273) | | | | |
| Date: 2023-05-26 | | | | |
| 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 4139  Mark RISON  13.1  2967.40 | "Throughout this clause, the notation Authentication-Request refers to an Authentication frame with the  Authentication Transaction Sequence Number field equal to 1; Authentication-Response refers to an  Authentication frame with the Authentication Transaction Sequence Number field equal to 2;  Authentication-Confirm refers to an Authentication frame with the Authentication Transaction Sequence  Number field equal to 3; Authentication-Ack refers to an Authentication frame with the Authentication  Transaction 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 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. ", 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:

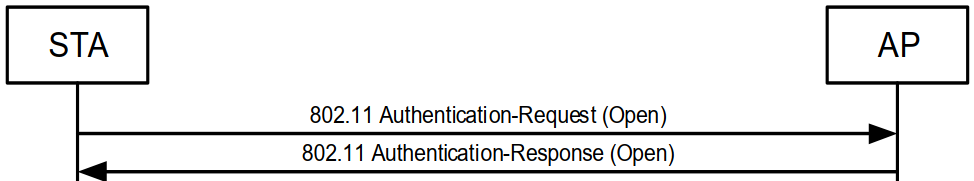
There are a lot of instances of “Authentication-Request frame” etc., so it’s probably better to just define things that way, though note that in MSCs etc. the word “frame” is not used, so should not be part of the term itself (so not italicised). The proposed change in 13.1 is as follows:

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:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4162  Mark RISON  9.4.2.74 | "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 Beamforming  Report 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 4170  Mark RISON  9.4 | Saying in text that a field "is 2 octets" duplicates the figure | Delete "The length of the Authentication 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, "The length of the Block Ack Timeout Value field is 2 octets." in 9.4.1.14, "The length of the Originator Preferred MCS field is 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 4179  Mark RISON  10.3.2.4  1780.23 | "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

Note also at 1796.1: “3) The recognition of a valid S1G RTS frame” and at 1794.53: “If the STA recognizes a valid Ack frame addressed to the STA and corresponding to this PHY-RXEND.indication primitive, this recognition shall be interpreted as successful acknowledgment.” and at 1896.18: “the STA shall wait for the corresponding PHY-RXEND.indication primitive to recognize 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”.

Proposed resolution:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4183  Mark RISON  12 | "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 4225  Mark RISON  12.7.8.4.2  2928.62 | "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 “single AKM”?

Proposed changes:

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4225 in <this document>, which xxx

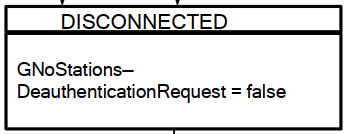
|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4350  Mark RISON  12 | "GNoStations--" in Figure 12-53--Authenticator state machines, part 2 at 2938.13 should be "GNoStations--". Ditto "GKeyDoneStation--". Ditto "GKeyDoneStations -" | At 2938.13 change "GNoStations--" 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:

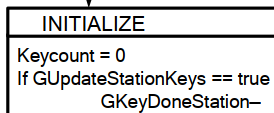
Somehow the comment and proposed change got garbled a bit!

Proposed changes:

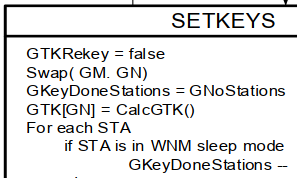
At 2938.13 should be -- not –:



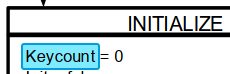
At 2938.22 should be plural and -- not –:



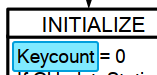
At 2940.34 should be no space:



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 4184  Mark RISON  12.5.3.3 | 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

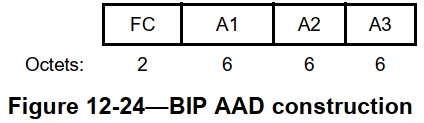
4) Other subfields are not modified

b) A1—MPDU Address 1 field.

c) A2—MPDU Address 2 field.

d) A3—MPDU Address 3 field.

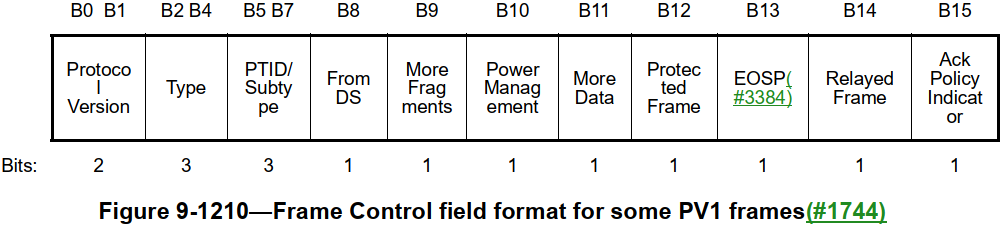
Figure 12-24 (BIP AAD construction) depicts the format of the AAD. The length of the AAD is 20 octets.



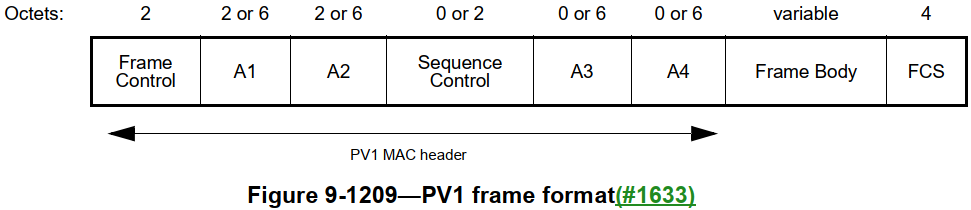
However, the Frame Control field for PV1 Management frames other than PV1 Probe Response frames does not contain a Retry field, and the Power Management and More Data fields are in different positions:

**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:



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.

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 4212  Mark RISON  12.5 | In 12.5.2.4.4 PN and replay detection  12.5.3.4 BIP replay protection  12.5.4.4.4 PN and replay detection  14.6.3 Mesh Group Key Inform frame construction and processing  recipient 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 4261  Mark RISON  11.22.3.4  2645.41 | "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 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)". 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 4341  Mark RISON  10.25.2 | 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?**

Proposed changes:

Proposed resolution:

REVISED

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID xxx  Mark RISON |  |  |

Discussion:

Proposed changes:

Proposed resolution:

REVISED

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

**TBD:**

~~4212 recipient v receiver in some specific subclauses~~

**References:**

802.11me/D3.0 except where otherwise specified