IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for some comments on 11me/D5.0 (SA2) |
| Date: 2024-05-14 |
| 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/D5.0. 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 7165Mark RISON12.4.7.2.13008.60 | "integer-to-octet string conversion" should be spaces not hyphens | As it says in the comment |

Discussion:

802.11 editorial policy is to not use hyphens even when the grammar would demand them.

The instances of octet-string conversion (or octet string conversion) are:

**11.21.6.4.5.4 Overview of secure HE-LTF octet stream generation(11az)**

Integer to octet string conversion (MSB first) specified in 12.4.7.2.2 (Integer to octet string conversion) shall be used to encode the value of the Secure HE-LTF Counter subfield in the KDF as well as in the transmitted LTF sequence information.

**12.4.2 Assumptions on SAE**

D2OS() represents the data to octet string conversion functions in 12.4.7.2 (Data type conversion)

**12.4.7.2 Data type conversion**

**12.4.7.2.1 General**

This protocol requires elements in finite cyclic groups to be converted to octet strings prior to transmission and back again upon receipt. To convert an element into an octet string, the first step is to represent the element in integer format and then employ an integer-to-octet string conversion prior to transmission. To convert an octet string into an element requires an octet string to integer conversion and then representing the integer(s) as an element.

**12.4.7.2.2 Integer to octet string conversion**

An integer, x, shall be converted into an octet string whose length is the smallest integer m such that 28m > x by first representing x in its binary form and then converting the result to an (#1288)octet string.

Given x, m, represent x as […]

**12.4.7.2.3 Octet string to integer conversion**

An octet string shall be converted into an integer by […]

**12.4.7.2.4 Element to octet string conversion**

For ECC groups, each element, except the “point at infinity,” is a point on the elliptic curve satisfying the curve equation and consists of two components: an x-coordinate and a y-coordinate. To convert this point to an octet string, […]

**12.4.7.2.5 Octet string to element conversion**

To convert an octet string into a point on an elliptic curve it is necessary to […]

To convert an octet string into an element in a prime modulus group the octet string shall […]

**12.4.7.3 Encoding and decoding of SAE Commit messages**

When transmitting an SAE Commit message, the scalar and element shall be converted to octet strings […]

**12.10.2 AP PeerKey protocol**

Q1 is the public key used by AP1 in the AP PeerKey protocol encoded as an octet stream using the Element to Octet string conversion from 12.4.7.2.3 (Octet string to integer conversion).

Q2 is the public key used by AP2 in the AP PeerKey protocol encoded as an octet stream using the Element to Octet string conversion from 12.4.7.2.3 (Octet string to integer conversion).

**12.11.2.3.2 Non-AP STA construction of Authentication frame**

and the ephemeral public key shall be encoded in the FFE field (see 9.4.1.38 (FFE field)) according to the element to (#1288)octet string conversion in 12.4.7.2.4 (Element to octet string conversion).

**12.11.2.3.3 AP processing of Authentication frame**

If PFS is being used, the STA’s public key shall be converted from an octet string to an element according to the conversion in 12.4.7.2.5 (Octet string to element conversion).

**12.11.2.3.5 Non-AP STA processing of Authentication frame**

If PFS is being used for the exchange, the AP’s public key shall be converted from an octet string to an element according to the conversion in 12.4.7.2.5 (Octet string to element conversion).

**12.11.2.4.2 Prior to exchange**

The STA’s ephemeral public key shall be encoded into the FFE field (see 9.4.1.38 (FFE field)) according to the element to (#1288)octet string conversion in 12.4.7.2.4 (Element to octet string conversion).

**12.11.2.4.3 Processing after receipt**

The public key is converted from an octet string to an element according to the conversion in 12.4.7.2.5 (Octet string to element conversion).

**12.11.2.4.4 Post processing**

The AP’s ephemeral public key is encoded in the FFE field (see 9.4.1.38 (FFE field)) according to the element to (#1288)octet string conversion in 12.4.7.2.4 (Element to octet string conversion).

**12.11.2.4.5 Upon receipt**

The public key is converted from an octet string to an element according to the conversion in 12.4.7.2.5 (Octet string to element conversion).

It was suggested at the Denver F2F that the conversion functions are canonically defined in <https://secg.org/sec1-v2.pdf> and that the terms there should be used. This defines the following conversions involving octet strings:

2.3.1 Bit-String-to-Octet-String Conversion

2.3.2 Octet-String-to-Bit-String Conversion

2.3.3 Elliptic-Curve-Point-to-Octet-String Conversion

2.3.4 Octet-String-to-Elliptic-Curve-Point Conversion

2.3.5 Field-Element-to-Octet-String Conversion

2.3.6 Octet-String-to-Field-Element Conversion

2.3.7 Integer-to-Octet-String Conversion

2.3.8 Octet-String-to-Integer Conversion

However, these appear to be just section headings, not actual function names, e.g.:



This is grammatical (“integer-to-octet-string” is an adjective for the “conversion”); the capitals are just because in that document the convention is to use uppercase initials for non-trivial words in section headings. Also note it’s not OctetString as had been suggested in Denver.

So since we have a hatred of hyphens, they just have to be replaced by spaces. The instance identified in the comment is the only one.

Proposed resolution:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7198Mark RISON | Should say "m" not "meter[s]" | As it says in the comment |

Discussion:

The name of the unit is “meter” (in American) but the SI abbreviation “m” should be used after numbers. However there was some debate in Denver about whether this is distributive.

Proposed resolution:

REVISED

At 980.2 change

The top of the building is 67.4 meters above sea level, and a starting altitude of 0 meters above sea level is assumed.

to

The top of the building is 67.4 m above sea level, and a starting altitude of 0 m above sea level is assumed.

At 1000.41 change

NOTE 5—Seven decimal places of latitude and longitude provide sufficient resolution to achieve under 0.01 meters of latitude error and longitude error throughout the globe. Considering the sizes of devices whose positions are being estimated and the use cases for the estimated positions, a map georegistration error of under 0.01 meters is generally regarded as sufficient to avoid compromise of the estimated positions.(#6068)

to

NOTE 5—Seven decimal places of latitude and longitude provide sufficient resolution to achieve under 0.01 m of latitude error and longitude error throughout the globe. Considering the sizes of devices whose positions are being estimated and the use cases for the estimated positions, a map georegistration error of under 0.01 m is generally regarded as sufficient to avoid compromise of the estimated positions.(#6068)

At 2634.7 change

the user interface might retrieve the map image and display it from (–50, –100) to (49.9, 0) meters, place a pin at (0, 0) meters labelled “Lobby Entrance”, and place a second pin at (0, –1.5) meters labelled “You Are Here”.

to

the user interface might retrieve the map image and display it from (–50 m, –100 m) to (49.9 m, 0 m), place a pin at (0 m, 0 m) labelled “Lobby Entrance”, and place a second pin at (0 m, –1.5 m) labelled “You Are Here”.

At 1118.2 change “1 microsecond units” to “1 <micro>s units”.

At 1228.37 change “50 milliseconds” to “50 ms”.

At 2025.6 change “8 microsecond” to “8 <micro>s”.

At 2465.26, 2478.38 change “231–1 microseconds” to “231–1 <micro>s”.

At 2653.55 change “30 seconds” to “30 s”.

At 2911.51, 5294.41, 5296.62, 5347.24 change “60 seconds” to “60 s”.

At 3119.24 change “300 seconds” to “300 s”.

At 3136.45 change “five seconds” to “5 s”.

At 3136.61 change “5 seconds” to “5 s”.

At 3340.17 change “1 microsecond” to “1 <micro>s”.

At 3556.41, 3557.60, 3935.29, 3936.47 change “100 nanosecond” to “100 ns”.

At 3881.34/57 change “1 microsecond” to “1 <micro>s”.

At 3965.52 change “100 picosecond” to “100 ps”.

At 4490.52 change “0.1 nanosecond” to “100 ps”.

At 4892.27 change “10 nanosecond” to “10 ns”.

At 5296.29, 5346.57 change “32 seconds” to “32 s”.

At 5296.46 change “256 seconds” to “256 s”.

At 5347.9 change “512 seconds” to “512 s”.

At 5575.5 change “1stream” to “1 stream”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7220Mark RISON | The 11az amendment uses the term "if and only if". This was sadly retired a few generations ago in favour of an explicit blah; otherwise blah | Change the "X if and only if Y"s to "X if Y; otherwise Z"s (17x) |

Discussion:

In TGmb or something all the “if and only if”s were abandoned in favour of the much more verbose (and inconsistently worded) “if X; otherwise Y”. This was a mistake, but we are where we are.

Proposed changes:

At 1454.28 change

The Index Adjustment TBTT Count field is present if and only if the Index Adjustment Factor field is present and nonzero.

to

The Index Adjustment TBTT Count field is present if the Index Adjustment Factor field is present and nonzero; otherwise it is not present.

At 2383.61 change

A STA that has sent an NDP Paging Response with the TWT Setup Command field equal to 4 (Accept TWT) shall schedule an NDP Paging frame as the first frame for transmission at the TWTs indicated by the NDP Paging Response, if any of the following conditions is satisfied:

— There are BUs for the requesting STA.

— No NDP Paging frame was sent in the N consecutive preceding TWT(s), where N is equal to the

value of the Max NDP Paging Period subfield in the NDP Paging Response.

to

A STA that has sent an NDP Paging Response with the TWT Setup Command field equal to 4 (Accept TWT) shall schedule an NDP Paging frame as the first frame for transmission at the TWTs indicated by the NDP Paging Response, if any of the following conditions is satisfied:

— There are BUs for the requesting STA.

— No NDP Paging frame was sent in the N consecutive preceding TWT(s), where N is equal to the

value of the Max NDP Paging Period subfield in the NDP Paging Response.

Otherwise the STA shall not schedule an NDP Paging frame.

At 2384.18 change

The P-ID field of the NDP Paging frame shall be set to the same value as P-ID field in the NDP Paging Response if and only if there are BUs for the STA identified by the partial AID indicated in the P-ID field of the NDP Paging Request.

to

The P-ID field of an NDP Paging frame shall be set to the same value as the P-ID field in the NDP Paging Response.

At 2509.27 change

A TPU buffer STA shall transmit an individually addressed TDLS Peer Traffic Indication frame to a TPU sleep STA, through the AP, if and only if all of the following conditions are met:

— A BU destined for a TPU sleep STA was placed into a buffer at the TPU buffer STA;

— The buffer into which the BU was placed contained no other frames with the same RA; and

— One or more periods of dot11TDLSPeerUAPSDIndicationWindow beacon intervals have expired

after the last service period.

to

A TPU buffer STA shall transmit an individually addressed TDLS Peer Traffic Indication frame to a TPU sleep STA, through the AP, if all of the following conditions are met:

— A BU destined for a TPU sleep STA was placed into a buffer at the TPU buffer STA;

— The buffer into which the BU was placed contained no other frames with the same RA; and

— One or more periods of dot11TDLSPeerUAPSDIndicationWindow beacon intervals have expired

after the last service period.

Otherwise it shall not transmit this frame.

At 2093.36 change

An SLS shall include a BRP if and only if the RequestBRP parameter of the MLME-BF-TRAINING.request primitive is true.

to

An SLS shall include a BRP if the RequestBRP parameter of the MLME-BF-TRAINING.request primitive is true; otherwise it shall not include a BRP.

At 2958.56 change

dot11GLKImplemented is true if and only if a STA implements the GLK facility.

to

dot11GLKImplemented is true if a STA implements the GLK facility, and false or absent otherwise.

At 3030.34 change

the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of CCMP Header (Figure 12-15 (Expanded CCMP MPDU(#3525)(11az))) signals that the management PDU is a Protected Fine Timing frame.

to

the separate replay counter for individually addressed Protected Fine Timing frames shall be used if the FTM subfield of the CCMP Header (Figure 12-15 (Expanded CCMP MPDU(#3525)(11az))) signals that the management PDU is a Protected Fine Timing frame; it shall not be used otherwise.

At 3077.7 change

A KDK is derived if and only if any of the following are true:

— WUR frame protection is negotiated(11az)

— dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support

capability in its RSNXE (see 9.4.2.240 (RSNXE(#1776))))(11az)

to

A KDK is derived if any of the following are true:

— WUR frame protection is negotiated(11az)

— dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support

capability in its RSNXE (see 9.4.2.240 (RSNXE(#1776))))(11az)

 Otherwise, it is not derived.

At 3086.33 change

A KDK shall be derived if and only if any of the following are true:(11az)

—WUR frame protection is negotiated(11az)

—dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support capability in its RSNXE (see 9.4.2.240 (RSNXE(#1776)))(11az)

to

A KDK shall be derived if any of the following are true:(11az)

—WUR frame protection is negotiated(11az)

—dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support capability in its RSNXE (see 9.4.2.240 (RSNXE(#1776)))(11az)

 Otherwise, it shall not be derived.

At 3147.63 change

a KDK shall be derived if and only if any of the following are true:(11az)

— WUR frame protection is negotiated(11az)

— dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support

capability in its RSNXE (see 9.4.2.241 (RSN Extension element (RSNXE)))(11az)

to

a KDK shall be derived if any of the following are true:(11az)

— WUR frame protection is negotiated(11az)

— dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support

capability in its RSNXE (see 9.4.2.241 (RSN Extension element (RSNXE)))(11az);

otherwise it shall not be derived.

At 3233.17 change

The discovered neighbor mesh STA shall be considered a candidate peer mesh STA if and only if all of the following conditions are met:

[…]

to

The discovered neighbor mesh STA shall be considered a candidate peer mesh STA if all of the following conditions are met:

[…]

Otherwise it shall not be considered a candidate peer mesh STA.

At 3268.2 change

A mesh STA updates its current path to the root mesh STA if and only if the PREQ element contains a greater HWMP SN, or the HWMP SN is the same as the current path and the PREQ element offers a better metric than the current path to the root mesh STA.

to

A mesh STA updates its current path to the root mesh STA if the PREQ element contains a greater HWMP SN, or the HWMP SN is the same as the current path and the PREQ element offers a better metric than the current path to the root mesh STA; otherwise it does not update its current path.

At 4050.32 change

A STA shall update the intra-BSS NAV with the duration information indicated by the received frame in a PSDU if and only if all the following conditions are met:

[…]

A STA shall update the basic NAV with the duration information indicated by the received frame in a PSDU if and only if all the following conditions are met:

[…]

A STA that is a TXOP holder shall not update the intra-BSS NAV with the duration information indicated by the RXVECTOR parameter TXOP\_DURATION.

A STA that is not a TXOP holder shall update the intra-BSS NAV with the duration information indicated by the RXVECTOR parameter TXOP\_DURATION for an HE PPDU if and only if all the following conditions are met:

[…]

A STA shall update the basic NAV with the duration information indicated by the RXVECTOR parameter TXOP\_DURATION for an HE PPDU if and only if all the following conditions are met:

[…]

to

A STA shall update the intra-BSS NAV with the duration information indicated by the received frame in a PSDU if all the following conditions are met:

[…]

Otherwise it shall not so update the intra-BSS NAV.

A STA shall update the basic NAV with the duration information indicated by the received frame in a PSDU if all the following conditions are met:

[…]

Otherwise it shall not so update the basic NAV.

A STA that is a TXOP holder shall not update the intra-BSS NAV with the duration information indicated by the RXVECTOR parameter TXOP\_DURATION.

A STA that is not a TXOP holder shall update the intra-BSS NAV with the duration information indicated by the RXVECTOR parameter TXOP\_DURATION for an HE PPDU if all the following conditions are met:

[…]

Otherwise it shall not so update the intra-BSS NAV.

A STA shall update the basic NAV with the duration information indicated by the RXVECTOR parameter TXOP\_DURATION for an HE PPDU if all the following conditions are met:

 […]

Otherwise it shall not so update the basic NAV.

At 4911.21 change

A transmitter shall use the NGV-LTF-2x-Repeat format if and only if the NGV Data field of a 10 MHz NGV PPDU is modulated with BPSK-DCM and one spatial stream; the transmitter shall use the NGV-LTF-2x if the NGV Data field is modulated with two spatial streams; the transmitter shall use the NGV-LTF-2x for NGV ranging NDP; otherwise, the transmitter can choose either NGV-LTF-2x or NGV-LTF-1x.

to

A transmitter shall use the NGV-LTF-2x-Repeat format if the NGV Data field of a 10 MHz NGV PPDU is modulated with BPSK-DCM and one spatial stream; the transmitter shall use the NGV-LTF-2x format if the NGV Data field is modulated with two spatial streams; the transmitter shall use the NGV-LTF-2x format for an NGV ranging NDP; otherwise, the transmitter can choose either NGV-LTF-2x or NGV-LTF-1x format.

At 5284.15 change

A STA uses the defined outside the context of a BSS procedures if and only if this attribute is true.

to

A STA uses the defined outside the context of a BSS procedures if this attribute is true; otherwise it does not use them.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7220 in <this document URL>, which transform the “if and only if”s into a more verbose form.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7166Mark RISON2 | Some months are abbreviated and some not | Abbreivate all months to three letters |

Discussion:

At the moment it’s inconsistent, though generally it’s abbreviated with a full stop (except for May, of course).

Proposed resolution:

REVISED

At 189.1 change “October 1969” to “Oct. 1969”.

At 189.3 change “Sept. 1981” to “Sep. 1981”.

At 189.31 change “April 1999” to “Apr. 1999”.

At 189.37 change “July 2003” to “Jul. 2003”.

At 189.40 change “Sept. 2002” to “Sep. 2002”.

At 189.46 change “Sept. 2003” to “Sep. 2003”.

At 189.51 change “June 2004” to “Jun. 2004”.

At 189.61 change “June 2005” to “Jun. 2005”.

At 190.10/13 change “Sept. 2007” to “Sep. 2007”.

At 190.20 change “July 2008” to “Jul. 2008”.

At 190.45 change “Sept. 2010” to “Sep. 2010”.

At 190.49 change “July 2011” to “Jul. 2011”.

At 190.55 change “July 2012” to “Jul. 2012”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7199Mark RISON3 | Is it not clear whether group addressed frames are "addressed to" STAs | Clarify, maybe under the definition of group addressed in C3 |
| CID 7200Mark RISON9.2.21891.23 | "A STA that receives at least one (#4179)frame in a PSDU can update its NAV" -- that one for example doesn't have to be addressed to the STA | After the para in 9.2.2 "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, where the frame is addressed to the STA (individually addressed or group addressed).(#6185)" add " except that in some contexts the frame can be addressed to another STA" |

Discussion:

Jouni MALINEN comments:

There are some clear cases where broadcast frames are addressed to all non-AP STAs associated with an AP, but there are places that I cannot easily determine whether they include all, some, or even none, group addressed frames..

For many (most?) cases I’d expect FromDS=1 ToDS=0 Data frames with A1=group A2=BSSID to not be addressed to STAs that are not associated in the identified BSS, but even if a STA is associated with that BSS, the frame might not be addressed to it for non-broadcast (i.e., multicast) cases. Probe Request frames use A1=broadcast, but I would not claim them to be addressed to all STAs listening on the channel. It should also be noted that we cases uses “addressed to the same RA” instead of the “addressed to a STA” and that RA might be group address (or a combination of individual and group addresses in some cases). We also use “addressed to one or more WUR non-AP STAs that are identified by the WUR IDs included in the Frame Body field” which seems to imply that something the frame body can actually determine whether the frame is addressed a particular STA. The definition of reception by the MAC sublayer (D5.0 P603 L55-60) is somewhat interesting in this context as well.

Making this all clear would be a significant effort and would likely require going through all those hundreds of places one by one.. It might actually make sense to do that for \_*some*\_ more interesting/complex/meaningful ones, since some of these could likely result in unexpected behavior if things are interpreted differently. I’d do this only based on specific comments identifying each such place instead of a generic comment (which could just get a sentence […] getting added as a lazy way of “fixing” this).

Proposed resolution:

REVISED

In 9.2.2 Conventions, at the end of the para:

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, where the frame is addressed to the STA (individually addressed or group addressed).(#6185)

add:

Unless explicitly specified, a group addressed frame might or might not, depending on the context, be considered “addressed to” a particular STA. Additionally, in certain contexts a frame individually addressed to a STA might be considered “received” by another STA (see e.g. 10.3.2.4).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7201Mark RISON9.6.19.171786.23 | "The Block Ack Starting Sequence Control field is set to the corresponding value within the immediately previously received Relay Ack Request frame." is behaviour | Move to Clause 10 |

Discussion:

It is indeed behaviour, not format. This is in Subclause 9.6.19.17 Relay Ack Response frame format.

Proposed changes:

REVISED

At 1786.23 delete “The Block Ack Starting Sequence Control field is set to the corresponding value within the immediately previously received Relay Ack Request frame.”

At 2365.55 change “Upon reception of a Relay Ack Request frame, the RDS shall respond with a Relay Ack Response frame and set the BlockAck Bitmap field to indicate which frames have been received by the destination REDS.” to “Upon reception of a Relay Ack Request frame, the RDS shall respond with a Relay Ack Response frame with the Block Ack Starting Sequence Control field set to the same value as in the Relay Ack Request frame and the BlockAck Bitmap field set to indicate which frames have been received by the destination REDS.”

At 674.26 change “The Fragment Number subfield of the Block Ack Starting Sequence Control subfield is set to all 0s” to “The Fragment Number subfield of the Block Ack Starting Sequence Control subfield is set to 0”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7160Mark RISON9.6.7.7 | It should be possible to specify a Max Channel Switch Time in an ECSA frame | At the end of Figure 9-1191—Extended Channel Switch Announcement frame Action field format add a cell "Max Channel Switch Time element" with "Zero or more" above and "6" below. Ditto in Figure 9-1178—Channel Switch Announcement frame Action field format |

Discussion:

The Max Channel Switch Time element can currently be passed in a beacon/probe rsp when a Channel Switch Announcement or an Extended Channel Switch Announcement element is also present. The behaviour is:

**11.8 DFS procedures**

**11.8.8 Selecting and advertising a new channel**

**11.8.8.2 Selecting and advertising a new channel in a non-DMG infrastructure BSS**

When an AP transmits a frame containing an Extended Channel Switch Announcement element, it should include a Max Channel Switch Time element in the frame if the Channel Switch Count field is nonzero and it may include the element if the field is 0.(#6027) When the AP includes the Max Channel Switch Time element(#6), the AP shall transmit the first Beacon frame in the new channel no later than the time indicated in the Switch Time field of the Max Channel Switch Time element after the last Beacon frame transmitted in the current channel, unless the AP determines that it is unable to operate on the new channel.(#1812)

(#6)A STA that receives a Max Channel Switch Time element from its associated AP should not transmit a frame to the AP on the new channel until it receives a frame on the new channel from the AP.

**11.9 Extended channel switching (ECS)**

**11.9.3 Selecting and advertising a new channel and/or operating class**

**11.9.3.2 Selecting and advertising a new channel in an infrastructure BSS**

When an AP transmits a frame containing an Extended Channel Switch Announcement element, it should include a Max Channel Switch Time element in the frame if the Channel Switch Count field is nonzero and it may include the element if the field is 0.(#6027) When the AP includes the Max Channel Switch Time element(#6), the AP shall transmit the first Beacon frame in the new channel no later than the time indicated in the Switch Time field of the Max Channel Switch Time element after the last Beacon frame transmitted in the current channel, unless the AP determines that it is unable to operate on the new channel.

(#6027)NOTE 1—An Extended Channel Switch Announcement frame does not contain an Extended Channel Switch Announcement element (see 9.6.7.7 (Extended Channel Switch Announcement frame format)).

A STA that receives a Max Channel Switch Time element from its associated AP should not transmit a frame to the AP on the new channel until it receives a frame on the new channel from the AP.

However, this means that the STA doesn’t get to find out the channel switch time if it’s not listening for, or not receiving, beacons, or if the channel switch is non-extended. The mechanism should be extended to CSA and ECSA frames, and to CSA elements, keeping it as a “should” so that existing implementations are not affected.

Proposed changes:

In 9.6.2.6 Channel Switch Announcement frame format and 9.6.7.7 Extended Channel Switch Announcement frame format:

At the end of Figure 9-1178—Channel Switch Announcement frame Action field format and Figure 9-1191—Extended Channel Switch Announcement frame Action field format add a cell “Max Channel Switch Time element” with “Zero or one” above and “0 or 6” below.

At the end of the subclause add a para:

The Max Channel Switch Time element is defined in 9.4.2.216 (Max Channel Switch Time element).

Change as follows:

**11.8 DFS procedures**

**11.8.8 Selecting and advertising a new channel**

**11.8.8.2 Selecting and advertising a new channel in a non-DMG infrastructure BSS**

When an AP transmits an Extended Channel Switch Announcement frame or a frame containing a Channel Switch Announcement element or an Extended Channel Switch Announcement element, it should include a Max Channel Switch Time element in the frame if the Channel Switch Count field is nonzero and it may include the element if the field is 0.(#6027) When the AP includes the Max Channel Switch Time element(#6), the AP shall transmit the first Beacon frame in the new channel no later than the time indicated in the Switch Time field of the Max Channel Switch Time element after the last Beacon frame transmitted in the current channel, unless the AP determines that it is unable to operate on the new channel.(#1812)

(#6)A STA that receives a Max Channel Switch Time element from its associated AP should not transmit a frame to the AP on the new channel until it receives a frame on the new channel from the AP.

**11.9 Extended channel switching (ECS)**

**11.9.3 Selecting and advertising a new channel and/or operating class**

**11.9.3.2 Selecting and advertising a new channel in an infrastructure BSS**

When an AP transmits an Extended Channel Switch Announcement frame or a frame containing a Channel Switch Announcement element or an Extended Channel Switch Announcement element, it should include a Max Channel Switch Time element in the frame if the Channel Switch Count field is nonzero and it may include the element if the field is 0.(#6027) When the AP includes the Max Channel Switch Time element(#6), the AP shall transmit the first Beacon frame in the new channel no later than the time indicated in the Switch Time field of the Max Channel Switch Time element after the last Beacon frame transmitted in the current channel, unless the AP determines that it is unable to operate on the new channel.

~~(#6027)NOTE 1—An Extended Channel Switch Announcement frame does not contain an Extended Channel Switch Announcement element (see 9.6.7.7 (Extended Channel Switch Announcement frame format)).~~

A STA that receives a Max Channel Switch Time element from its associated AP should not transmit a frame to the AP on the new channel until it receives a frame on the new channel from the AP.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7160 in <this document URL>, which allow the max channel switch time to be communicated for ECSA frames and for frames containing a CSA element (including CSA frames).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7213Mark RISON11.5.3.42588.63 | "a) Discard all MPDUs that have not been acknowledged, up to and including the last (highest in sequence number space) MPDU transmitted, and b) Set the sequence number of the next MPDU to be transmitted outside the block ack agreement to the sequence number immediately after that of the last (highest in sequence number space) MPDU transmitted." should allow last one to be retxed, i.e. a) to allow not last if not acked and b) to say use that SN if retxing | Commenter to bring specific wording proposal |

Discussion:

The D4.0 wording was:

When the originator receives a DELBA frame, it shall

a) Discard any MPDU that has been transmitted and not acknowledged, with the possible exception if it was the last MPDU to be sent and it was not a retransmission, and

b) Set the sequence number to either that of the last MPDU that is sent if it intends to retransmit or one beyond the last MPDU sent.

This meant that if SN 42 was transmitted but not acked and not retried, and SN 43 was never transmitted, then the originator could choose to retry SN 42 after the DELBA (the D5.0 wording doesn’t allow this). If, however, SN 42 was retried at least once, it could not. It is not clear why the latter restriction was applied: the recipient might have received the initial transmission of SN 42 in any case. But the point is that if the originator wants to keep trying SN 42, it should be allowed to do so.

Proposed changes:

Change 11.5.3.4 Procedure at the block ack originator(#6171) as follows:

When a block ack agreement is torn down, the originator shall, for MPDUs under that block ack agreement (i.e., recipient and TID), irrespective of whether it transmitted or received a DELBA frame, behave as follows:

If the last (highest in sequence number space) MPDU transmitted was not acknowledged, and the originator wishes to retry this, the originator shall:

a) Discard all MPDUs that have not been acknowledged, up to and excluding the last (highest in sequence number space) MPDU transmitted, and

b) Retry that last MPDU first, outside the block ack agreement, retaining its sequence number.

NOTE—The MPDU cannot be retried in a subsequent new block ack agreement.

Otherwise, the originator shall:

a) Discard all MPDUs that have not been acknowledged, up to and including the last (highest in sequence number space) MPDU transmitted, and

b) Set the sequence number of the next MPDU to be transmitted outside the block ack agreement to the sequence number immediately after that of the last (highest in sequence number space) MPDU transmitted.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7213 in <this document URL>, which allow the originator to keep trying the last MPDU if this was not acknowledged (even if it had been retried).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7191Mark RISON12.7.6.43107.29 | "the Supplicant verifies that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2 and verifies that" should be "the Supplicant shall verifiy that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2 and shall verify that" (maybe other bullets) | As it says in the comment |

Discussion:

It is not clear that the “shall” that introduces all the bullets applies to anything beyond the first verb in each line.

Proposed changes:

Change from 3107.26 as follows:

The Supplicant (#1243)shall also:

a) (#1243)Verify the RSNE and, if present, the RSNXE. If this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the Supplicant shall verify~~ies~~ that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2, ~~and verifies~~ that all other fields of the RSNE are identical to the fields in the RSNE present in the Beacon or Probe Response frames and ~~verifies~~ that the FTE and MDE are the same as in the (Re)Association Response frame. Otherwise, the Supplicant shall verify~~ies~~ that the RSNE is identical to that the STA received in the Beacon or Probe Response frame. If the RSNXE is present, the Supplicant shall verify~~ies~~ that the RSNXE is identical to that the STA received in the Beacon or Probe Response frame. If any of these verification steps indicates a mismatch, the STA shall disassociate or deauthenticate. If a second RSNE is provided in the message, the Supplicant shall use~~s~~ the pairwise cipher suite specified in the second RSNE or deauthenticate~~s~~.

b) (#1243)Verify the message 3 MIC or AEAD decryption operation result. If the calculated MIC does not match the MIC that the Authenticator included in the (#1836)EAPOL-Key PDU or AEAD decryption operation returns failure, (#6110)the Supplicant shall silently discard message 3.

c) (#1243)Update the last-seen value of the Key Replay Counter field.

d) If the Extended Key ID for Individually Addressed Frames subfield of the RSN Capabilities field is 1 for both the Authenticator and Supplicant: Use~~s~~ the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to receive individually addressed MPDUs protected by the PTK with the assigned (#3493)key ID.

e) (#1243)Construct message 4.

f) (#1243)Send message 4 to the Authenticator.

g) (#1243)Use the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to send and, if the receive key has not yet been installed, to receive individually addressed MPDUs protected by the PTK. The GTK is also configured by MLME-SETKEYS.request primitive. (11ba)If WUR frame protection is negotiated, the WTK, and if applicable the WIGTK, is also configured by using the MLME-SETKEYS.request primitive.

At 3108.58 change “the MLME-SETKEYS primitive” to “the MLME-SETKEYS.request primitive”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7191 in <this document URL>, which make everything a “shall”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7217Mark RISON9.4.2.5.1 | I see no behavioural references to the Traffic Indicator field (whether in S1G or in non-S1G). I do see some behavioural references to "AID 0" | Add some behavioural rules for the Traffic Indicator field (tx and rx) |

Discussion:

Here are the AID 0 instances:

**Table 9-9—Duration/ID field encoding**

AID 0 is used for broadcast transmission in S1G PPDU, reserved if not in S1G PPDU.

*[not relevant to the Traffic Indicator field]*

**9.4.2.5 TIM element**

(#6033)The Traffic Indicator field contains the traffic indication virtual bitmap bit associated with AID 0. This bit is set to 1 in TIM elements with the DTIM Count field set to 0 when one or more group addressed MSDUs/MMPDUs are buffered at the AP or the mesh STA and they are not to be delivered using group AID as described in 10.54 (Group AID).

**11.2.3.3 AP TIM transmissions**

AID 0 (zero) is reserved to indicate the presence of buffered non-GCR-SP group addressed BUs (M118)to be delivered using MPDUs with an RA other than a SYNRA but that are not delivered using group AID. The AP shall identify those STAs for which it is prepared to deliver38 buffered BUs by setting bits in the TIM’s partial virtual bitmap that correspond to the appropriate AIDs.

**11.2.3.6 AP operation**

The bit for AID 0 (zero) in the Bitmap Control field of the TIM element shall be set to 1 when non-GCR-SP non-SYNRA group addressed traffic that is not to be delivered using group AID is buffered, according to 9.4.2.5 (TIM element).

[…]

the AP shall set the bit for AID 0 (zero) in the TIM element to 1 for a single BSSID or set the corresponding group address bit to 1 for multiple BSSIDs, as defined in 9.4.2.5 (TIM element)

**14.4 Mesh peering management (MPM)**

AID 0 (zero) is reserved to indicate the presence of buffered group addressed MSDUs and MMPDUs (see 14.15.4 (TIM transmissions in an MBSS)).

**14.15.4 TIM transmissions in an MBSS**

The TIM element identifies the peer mesh STAs for which traffic is pending and buffered in the reporting mesh STA. This information is coded in a partial virtual bitmap, as described in 9.4.2.5 (TIM element). In addition, the TIM contains an indication whether group addressed traffic is pending. Every neighbor peer mesh STA is assigned an AID by the reporting mesh STA as part of the mesh peering establishment process (see 14.4.1 (General)). The mesh STA shall identify those peer mesh STAs for which it is prepared to deliver41 buffered MSDUs and MMPDUs by setting bits in the TIM’s partial virtual bitmap that correspond to the appropriate AIDs.

**14.15.7 Power save support**

The mesh STA sets the bit for AID 0 (zero) in the Bitmap Control field of the TIM element to 1 when group addressed traffic is buffered, according to 9.4.2.5 (TIM element).

**Figure 26-6—Illustration of UORA procedure**

*[not relevant to the Traffic Indicator field]*

**Figure L-1/2/3/5/6/7 (not 4/8/9/10/11/12/13/14/15)— Partial Virtual Bitmap examples** (not all searchable)

*[Being handled by Dave HALASZ under CID 7218.]*

So there’s some behavioural description, but it’s hidden behind references to AID 0.

Having said that, I can’t find anything to describe the rx behaviour for the Traffic Indicator field!

Note also the subtlety that the AID 0 bit in the bitmap is replicated in the Traffic Indicator field, and indeed the AID 0 bit need not be transmitted in the PVB:

NOTE 1—The bit numbered 0 in the traffic indication virtual bitmap need not be included in the Partial Virtual Bitmap field even if that bit is set.

Proposed changes:

Change as follows:

**9.4.2.5 TIM element**

(#6033)The Traffic Indicator field contains the traffic indication virtual bitmap bit associated with AID 0. This bit is set to 1 in TIM elements with the DTIM Count field set to 0 when one or more group addressed MSDUs/MMPDUs are buffered at the AP or the mesh STA and they are not to be delivered using group AID as described in 10.54 (Group AID).

*[no change needed]*

**11.2.3.3 AP TIM transmissions**

AID 0 ~~(zero)~~ is reserved to indicate the presence of buffered non-GCR-SP group addressed BUs (M118)to be delivered using MPDUs with an RA other than a SYNRA but that are not delivered using group AID. The AP shall identify those STAs for which it is prepared to deliver38 buffered BUs by setting bits in the TIM’s partial virtual bitmap that correspond to the appropriate AIDs.

NOTE—AID 0 is signalled in the Traffic Indicator field when the DTIM Count field is zero.

**11.2.3.6 AP operation**

The Traffic Indicator field ~~bit for AID 0 (zero)~~ in the Bitmap Control field of the TIM element shall be set to 1 when non-GCR-SP non-SYNRA group addressed traffic that is not to be delivered using group AID is buffered, according to 9.4.2.5 (TIM element).

[…]

the AP shall set the Traffic Indicator field ~~bit for AID 0 (zero)~~ in the TIM element to 1 for a single BSSID or set the corresponding group address bit to 1 for multiple BSSIDs, as defined in 9.4.2.5 (TIM element)

**11.2.3.7 Receive operation for STAs in PS mode**

e) When dot11FMSActivated is false and ReceiveDTIMBeacons(#4221) is true, the STA shall transition to awake state(#6038) early enough to be able to receive either every non-STBC DTIM beacon or every STBC DTIM beacon sent by the AP of the BSS. If the Traffic Indicator field in the TIM element in the DTIM beacon is equal to 1, the STA shall remain in the awake state to receive the group addressed MPDUs transmitted by the AP as described in 11.2.3.1 General and 11.2.3.4 TIM types.

**14.4 Mesh peering management (MPM)**

AID 0 ~~(zero)~~ is reserved to indicate the presence of buffered group addressed MSDUs and MMPDUs (see 14.15.4 (TIM transmissions in an MBSS)).

**14.15.4 TIM transmissions in an MBSS**

The TIM element identifies the peer mesh STAs for which traffic is pending and buffered in the reporting mesh STA. This information is coded in a partial virtual bitmap, as described in 9.4.2.5 (TIM element). In addition, the TIM contains an indication whether group addressed traffic is pending, in the Traffic Indicator field, which signals AID 0. Every neighbor peer mesh STA is assigned an AID by the reporting mesh STA as part of the mesh peering establishment process (see 14.4.1 (General)). The mesh STA shall identify those peer mesh STAs for which it is prepared to deliver41 buffered MSDUs and MMPDUs by setting bits in the TIM’s partial virtual bitmap that correspond to the appropriate AIDs.

**14.15.7 Power save support**

The mesh STA sets the Traffic Indicator field ~~bit for AID 0 (zero)~~ in the Bitmap Control field of the TIM element to 1 when group addressed traffic is buffered, according to 9.4.2.5 (TIM element).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7217 in <this document URL>, which address the issue raised.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7208Mark RISONC.35637.29 | Definition of dot11TransmittedFragmentCount is "This is a status variable. This counter is incremented when a Data or Management frame (which may or may not be a fragment) is successfully transmitted." Does this include (QoS) Null? Similarly for definition of dot11QoSTransmittedFragmentCount | Add a NOTE to say this includes (QoS) Null frames |

Discussion:

This is part of the wider problem that we have both a Data frame type and a Data frame subtype.

It seems easiest to include all Data frames for the first MIB attribute, and QoS Null frames for the second.

Proposed resolution:

REVISED

At 5639.29 change “This counter is incremented when a Data or Management frame (which may or may not be a fragment) is successfully transmitted.” to “This counter is incremented when a Data (including QoS Data and (QoS) Null) or Management frame is successfully transmitted; the frame may or may not be a fragment.”

At 5658.32 change “This counter is incremented when a QoS Data frame (which may or may not be a fragment) for a particular UP is successfully transmitted.” to “This counter is incremented when a QoS Data frame (which may or may not be a fragment) or QoS Null frame for a particular UP is successfully transmitted.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7224Mark RISON9 | Units for Length fields should be specified (typically octets) | Fix in Cookie Length in 9.4.2.306, Emergency Call Number in 9.4.5.5, Redict URL in 9.4.5.6, NAI Realm Data Field Length in 9.4.5.10 |

Discussion:

As it says in the comment, units should be stated.

Proposed resolution:

REVISED

At 1554.13 change “The Cookie Length subfield value is the length of the following Cookie subfield.” to “The Cookie Length subfield contains the length in octets of the Cookie subfield.”

At 1572.36 change “The Length of Emergency Call Number field is set to the length of the Emergency Call Number field.” to “The Length of Emergency Call Number field contains the length in octets of the Emergency Call Number field.”

At 1573.56 change “The Redirect URL Length field contains the length of the Redirect URL.” to “The Redirect URL Length field contains the length in octets of the Redirect URL field.” At 1573.48 change “The ReDirect URL” to “The Redirect URL field”. On page 1573 change “the Redirect URL Length” not followed by “field” to “the Redirect URL Length field” (3x) and “Redirect URL” where followed by “can” or “is” to “Redirect URL field” (6x not including the specific instances above). At 6130.18 change “Redirect URL” to “redirect URL”.

At 1576.51 change “The NAI Realm Data Field Length subfield is equal to 3 plus the length of the NAI Realm subfield plus the length of the EAP Method Tuples subfield.(#1611)” to “The NAI Realm Data Field Length subfield is equal to 3 plus the length in octets of the NAI Realm subfield plus the length in octets of the EAP Method Tuples subfield.(#1611)”

At 1577.40 change “The Length subfield is 2 plus the length of the Authentication Parameters subfield.” to “The Length subfield is 2 plus the length in octets of the Authentication Parameters subfield.”

At 1578.3 change “The Length subfield indicates the length of the Authentication Parameter Value subfield.” to “The Length subfield indicates the length in octets of the Authentication Parameter Value subfield.”

At 1587.54 change “The AP List Length field indicates the length of the BSSIDs field.” to “The AP List Length field indicates the length in octets of the BSSIDs field.”

At 1589.46 change “The Service Information Request Attribute Length subfield indicates the length of the Service Information Request Attribute subfield.” to “The Service Information Request Attribute Length subfield indicates the length in octets of the Service Information Request Attribute subfield.”

At 1590.28 change “The Service Information Response Attribute Length subfield indicates the length of the Service Information Response Attribute subfield.” to “The Service Information Response Attribute Length subfield indicates the length in octets of the Service Information Response Attribute subfield.”

At 1605.59 change “The Excluded NAI Realm Data Field Length subfield is equal to 1 plus the length of the Excluded NAI Realm subfield.” to “The Excluded NAI Realm Data Field Length subfield is equal to 1 plus the length in octets of the Excluded NAI Realm subfield.”

At 1702.61 change “The EBCS TIM Length field indicates the length of the EBCS TIM field.” to “The EBCS TIM Length field indicates the length in octets of the EBCS TIM field.”

At 1738.62 change “The URL Length field is the value of the length of the URL field.” to “The URL Length field is the length in octets of the URL field.”

At 1746.12 change “The Key Data Length field is the length of the Key Data field.” to “The Key Data Length field is the length in octets of the Key Data field.”

At 1864.14 change “The Length subfield indicates the length of the Frame Body field as defined in 9.9.2.3 (Frame Body field).” to “The Length subfield indicates the length in octets of the Frame Body field as defined in 9.9.2.3 (Frame Body field).”

At 1865.1 change “If present, the length of the Frame Body field is in units of octets and is equal to 2 × (L + 1)” to “If present, the length of the Frame Body field is 2 × (L + 1) octets”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7151Mark RISON9.4.2.2611455.41 | "The Short SSID List field contains the one or more four octet Short SSID fields" -- but "The Short SSID field is defined in 9.4.2.169.3 (Calculating the short SSID)." and that defines the size | Delete " four octet" |

Discussion:

It has been argued that the fact that the short SSID is defined as being a 32-bit quantity does not mean that a Short SSID field is necessarily a 4-octet field. More generally, it’s a bit weird that we refer to Short SSID fields but don’t actually define them.

Proposed changes:

Change as follows:

**6.5.3.2 MLME-SCAN.request**

One or more ~~S~~short SSID ~~field~~s that are optionally present if dot11ShortSSIDList is true.

**9.4.1.x Short SSID field**

The Short SSID field is used to carry a short SSID (see 9.4.2.169.3). The Short SSID field is shown in Figure 9-xxx (Short SSID field format); the short SSID is transmitted commencing with the coefficient of the highest-order term of the short SSID.

***<Add a figure with caption Figure 9-xxx—Short SSID field format with the standard field format showing just a 4-octet field called Short SSID, similar to e.g. 9.4.1.12 Dialog Token field>***

**9.4.2.169.2 Neighbor AP Information field**

The Short SSID subfield is defined in 9.4.1.x ~~calculated as given in 9.4.2.169.3 (Calculating the short SSID)~~.

**9.4.2.169.3 Calculating the short SSID**

A short SSID is a 32-bit value calculated over an SSID. The SSID is referred to as the calculation fields. The ~~value of the S~~short SSID ~~field~~ is calculated using the following standard generator polynomial of degree 32:

[…]

The ~~value of the S~~short SSID ~~field~~ is the 1s complement of the sum (modulo 2) of the following:

[…]

~~The Short SSID field is transmitted commencing with the coefficient of the highest-order term.~~

**9.4.2.261 Short SSID List element(11ax)**

The Short SSID List field contains the one or more ~~four octet~~ Short SSID fields for which the STA is requesting information. The use of the Short SSID List element and frames is described in 11.1.4.3.2 (Active scanning procedure for a non-DMG STA). The Short SSID field is defined in 9.4.1.x ~~9.4.2.169.3 (Calculating the short SSID)~~.

**9.4.2.294 WUR Discovery element(11ba)**

***<In this subclause change “Short-SSID” to “Short SSID” (6x).>***

The Short~~-~~ SSID field is defined in 9.4.1.x and contains the short SSID of the WUR AP identified by the WUR AP Parameters subfield ~~as defined in 9.4.2.169.3 (Calculating the short SSID)~~.

**9.6.7.36 FILS Discovery frame format**

A value of 1 in the Short SSID Indicator subfield indicates that a short SSID is contained in the SSID/Short SSID field of the FILS Discovery frame. A value of 0 indicates that an SSID is contained in the SSID/Short SSID field of the FILS Discovery frame.

~~The SSID/Short SSID subfield is variable length between 1 and 32 octets.~~ When the Short SSID Indicator subfield is 1, the SSID/Short SSID field contains ~~the s~~a Short SSID field (see 9.4.1.x ~~9.4.2.169 (Reduced Neighbor Report element)~~). Otherwise, the SSID/Short SSID field contains the SSID, whose length in octets is specified by the ~~5-bit~~ SSID Length subfield in the FILS Discovery Frame Control of the FILS Discovery frame (see 9.4.2.2 (SSID element)).

**9.9.3.3 WUR Discovery frame format**

The Compressed SSID field contains 16 LSBs of the short SSID as defined in 9.4.2.169.3 (Calculating the short SSID).

**11.1.4.3.4 Criteria for sending a response**

7) dot11ShortSSIDListImplemented is true, and the Short SSID List element is present in the Probe Request frame and includes the ~~S~~short SSID ~~field~~ corresponding to the SSID of the STA’s BSS.(11ax)

8) dot11ShortSSIDListImplemented is true, the STA is an AP that is in the same (#2210)colocated AP set as a 6 GHz AP, the Short SSID List element is present in the Probe Request frame and includes the ~~S~~short SSID ~~field~~ corresponding to the SSID of the 6 GHz AP,

**29.12 WUR discovery**

The Compressed SSID parameter, if present in the primitive, indicates the 16 LSBs of the ~~Short-~~ short SSID of the WUR AP to be discovered, as defined in 9.4.2.169.3 (Calculating the short SSID).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7151 in <this document URL>, which define explicitly a (4-octet) Short SSID field.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7078Emily QI12.6.173068.17 | 11az work item - Changes in 12.6.19 of 11az cannot be incorporated in this section. Please review. | as in comment. |

Discussion:

802.11az-2022 shows the following:

**12.6.19 Protection of robust Management frames**

***Change the fourth and fifth paragraphs of 12.6.19 as follows:***

A STA with dot11RSNAProtectedManagementFramesActivated equal to true and dot11RSNAUnprotectedManagementFramesAllowed equal to true shall transmit and receive protected individually addressed robust Management frames to and from any associated STA that advertised MFPC = 1, shall discard unprotected individually addressed robust Action frames and robust Action No Ack frames received from any STA that advertised MFPC = 1, and shall discard unprotected individually addressed Disassociation and Deauthentication frames received from a STA that advertised MFPC = 1 after the PTK and IGTK have been installed. The receiver shall process unprotected individually addressed Disassociation and Deauthentication frames before the PTK and IGTK are installed.

A STA with dot11RSNAProtectedManagementFramesActivated equal to true and dot11RSNAUnprotectedManagementFramesAllowed equal to false shall transmit and receive protected individually addressed robust Action frames and robust Action No Ack frames to and from any STA, shall not transmit unprotected individually addressed robust Action frames and robust Action No Ack frames to any STA, and shall discard unprotected individually addressed robust Action frames and robust Action No Ack frames received from a STA after the PTK and IGTK have been installed. The receiver shall process unprotected individually addressed Disassociation and Deauthentication frames before the PTK and IGTK are installed.

***Change the last paragraph of 12.6.19 as follows:***

Management frame protection cannot be applied until the PTK and IGTK has been established with the STA. A STA shall not transmit robust Action frames and robust Action No Ack frames until it has installed the PTK for the peer STA, or in the case of group addressed frames, has installed the IGTK. The STA shall discard any robust Action frames and robust Action No Ack frames received before the PTK and IGTK are installed.

So basically this is about treating Action No Ack frames the same as Action frames.

In D5.0 the bit of the subclause that discusses Action frames is:

**12.6.17 Protection of robust Management frames**

(#2128)If management frame protection is negotiated for the link, a STA shall not transmit any of the following, and shall discard all of the following:

— An unprotected individually addressed Deauthentication or Disassociation frame(#1922).

— An unprotected individually addressed robust Action frame

The bit about no robust until PTK/IGTK is covered by:

(#2128)NOTE 2—Management frame protection cannot be applied until the PTK and (except for a TDLS direct link) IGTK have been set.

(#2128)NOTE 6—The STA is not(M118) sent any protected individually addressed robust Management frames before the PTKSA has been established.

Proposed resolution:

REVISED

At 3069.1 change “An unprotected individually addressed robust Action frame” to “An unprotected individually addressed robust Action or robust Action No Ack frame”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7228Mark RISONC.3 | Some DESCRIPTIONs have standalone phrases like "Responder Sector Sweep Retry Limit" and "Responder Sector Sweep Backoff" and "A-BFT Transmit Sector Sweep Switch." | Replace them with an actual sentence giving behaviour in each case |

Discussion:

DESCRIPTIONs need to be, like, descriptions rather than, like, field names, you know?

All the MIB attributes in Dot11DMGBeamformingConfigEntry seem to be afflicted.

I am grateful for Claudio DA SILVA for providing the full descriptions (I have only made editorial changes).

Proposed changes:

Change in C.3 as follows:

dot11MaxBFTime OBJECT-TYPE

SYNTAX Unsigned32 (1..16)

UNITS "beacon intervals"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or an external management entity.

Changes take effect as soon as practical in the implementation.

~~Maximum Beamforming Time~~This attribute indicates the maximum duration supported by the STA for beamforming training (SLS and BRP)."

DEFVAL { 4 }

::= { dot11DMGBeamformingConfigEntry 1 }

dot11BFTXSSTime OBJECT-TYPE

SYNTAX Unsigned32 (1..256)

UNITS "milliseconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or an external management entity.

Changes take effect as soon as practical in the implementation.

~~Timeout until the initiator restarts ISS~~This attribute indicates the maximum TXSS duration supported by the non-AP STA."

DEFVAL { 100 }

::= { dot11DMGBeamformingConfigEntry 2 }

dot11MaximalSectorScan OBJECT-TYPE

SYNTAX Unsigned32 (1..32)

UNITS "beacon intervals"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or an external management entity.

Changes take effect as soon as practical in the implementation.

~~Maximal Sector Scan~~This attribute indicates the maximum TXSS duration supported by the AP or PCP."

DEFVAL { 8 }

::= { dot11DMGBeamformingConfigEntry 3 }

dot11ABFTRTXSSSwitch OBJECT-TYPE

SYNTAX Unsigned32 (1..32)

UNITS "beacon intervals"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or an external management entity.

Changes take effect as soon as practical in the implementation.

~~A-BFT Transmit Sector Sweep Switch~~This attribute indicates the maximum duration in which an A-BFT is present, in which the AP or PCP allocates an A-BFT as a responder TXSS."

DEFVAL { 4 }

::= { dot11DMGBeamformingConfigEntry 4 }

dot11RSSRetryLimit OBJECT-TYPE

SYNTAX Unsigned32 (~~1..32~~0..3)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or an external management entity.

Changes take effect as soon as practical in the implementation.

~~Responder Sector Sweep Retry Limit~~This attribute indicates the retry limit that a STA attempting to access the A-BFT of a BSS uses:

0, for 2 retries;

1, for 4 retries;

2, for 6 retries;

3, for 8 retries."

DEFVAL { ~~8~~3 }

::= { dot11DMGBeamformingConfigEntry 5 }

dot11RSSBackoff OBJECT-TYPE

SYNTAX Unsigned32 (1..32)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or an external management entity.

Changes take effect as soon as practical in the implementation.

~~Responder Sector Sweep Backoff~~This attribute indicates the maximum number of A-BFT periods that the STA waits after a consecutive number of times (FailedRSSAttempts) the STA initiates RSS during A-BFTs but does not receive an SSW-Feedback frame as a response."

DEFVAL { 8 }

::= { dot11DMGBeamformingConfigEntry 6 }

dot11BFRetryLimit OBJECT-TYPE

SYNTAX Unsigned32 (1..32)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or an external management entity.

Changes take effect as soon as practical in the implementation.

~~Beamforming Retry Limit~~This attribute indicates the number of times an initiator may start an SSW feedback procedure if it does not receive an SSW-Ack frame from the responder following the completion of the SSW feedback procedure."

DEFVAL { 8 }

::= { dot11DMGBeamformingConfigEntry 7 }

dot11BeamLinkMaintenanceTime OBJECT-TYPE

SYNTAX Unsigned32 (0..64000000)

UNITS "microseconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC or SME.

Changes take effect as soon as practical in the implementation.

~~Beam Link Maintenance Time~~

~~dot11BeamLinkMaintenanceTime = BeamLink\_Maintenance\_Unit \* BeamLink\_Maintenance\_Value.~~

This attribute indicates the beam link maintenance time. ~~Otherwise, the dot11BeamLinkMaintenanceTime is left undefined. An~~

~~undefined~~ The value 0 ~~of the dot11BeamLinkMaintenanceTime~~ indicates

that the STA does not participate in beamformed link maintenance."

DEFVAL { 0 }

::= { dot11DMGBeamformingConfigEntry 8 }

dot11AntennaSwitchingTime OBJECT-TYPE

SYNTAX Unsigned32 (0..64000000)

UNITS "microseconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC or SME.

Changes take effect as soon as practical in the implementation.

This attribute indicates the time it takes the STA to switch DMG antennas."

DEFVAL { 0 }

::= { dot11DMGBeamformingConfigEntry 9 }

dot11ChanMeasFBCKNtaps OBJECT-TYPE

SYNTAX Unsigned32 (0..64000000)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC or SME.

Changes take effect as soon as practical in the implementation.

~~Number of channel measurement taps~~This attribute indicates the number of channel impulse response taps measured by the STA."

DEFVAL { 0 }

::= { dot11DMGBeamformingConfigEntry 10 }

dot11BeamTrackingTimeLimit OBJECT-TYPE

SYNTAX Unsigned32 (0..65535)

UNITS "microseconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC or SME.

Changes take effect as soon as practical in the implementation.

~~BRP tracking initiator time limit~~This attribute indicates the maximum time in which a feedback response is sent after a request for beam tracking feedback is received."

DEFVAL { 10000 }

::= { dot11DMGBeamformingConfigEntry 11 }

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7228 in <this document URL>, which fix the DESCRIPTIONs for attributes in Dot11DMGBeamformingConfigEntry, and fix a few other items.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7159Mark RISON21.3.203709.63 | It is not clear what action causes transition out of the End Of Wait state in the PHY receive state machines (the location given is just one example) | Have a statement at the start of every subclause with PHY receive state machines: "If no condition is shown for a transition, the transition is unconditional and immediate." |

Discussion:

When you have a state machine, you need to define what triggers a change of state. Here is an example where no trigger is specified:



However, it’s only immediate insofar as you have to complete the actions defined for that state, e.g. setting something, or waiting for something to happen.

Proposed resolution:

REVISED

At the end of Subclause 1.4 add a para:

“Where a transition is shown a state machine figure, but no transition condition is shown, the transition occurs as soon as all the state actions have been performed.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7219Mark RISON | I also note that in some of the Annex L figures the Traffic Indicator field is described as Transmitted BSSID group addressed traffic indication/AID 0 and Nontransmitted BSSID group addressed traffic indication though some of the figures aren't searchable (grrr…) | Use consistent wording and make figures searchable |

Discussion:

Embrace and extend the work started by Dave HALASZ on this topic.

Note only the MBSSID figures have been fixed, not the non-MBSSID figures and the S1G figures, other than Figure L-1, because it is currently unsearchable.

Proposed changes:

In each case the original figure and the new figure are shown.

**Figure L-4—Partial Virtual Bitmap example #4, Method A and Method B**



→



**Figure L-5—Partial Virtual Bitmap example #5, Method A or Method B**



→



**Figure L-6—Partial Virtual Bitmap example #6, Method A**



→



**Figure L-7—Partial Virtual Bitmap example #6, Method B**



→



**Figure L-1—Partial Virtual Bitmap example #1**



→

****

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 7219 in <this document URL>, which effect the improvements requested by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7211Mark RISONC.35325.25 | "and the num-ber of TPKSA replay counters per (#2152)TDLS direct link" is no longer applicable | Delete the cited text |

Discussion:

The comment is calling for the following deletion:

dot11RSNAConfigNumberOfPTKSAReplayCounters OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by (#3375)STA capabilities.

Specifies the number of PTKSA replay counters per association ~~and the number of TPKSA replay counters per (#2152)TDLS direct link~~:(#167)

0 -> 1 replay counter,

1 -> 2 replay counters,

2 -> 4 replay counters,

3 -> 16 replay counters"

::= { dot11RSNAConfigEntry 18 }

However, per the final resolution of CID 6149 (which was unfortunately missed in D5.0, so it got an earlier resolution) the PTKSA Replay Counter field in the TDLS Setup Requeset frame is used to determine the number of replay counters on both sides of a TDLS link, and we have:

**9.4.2.23.4 RSN capabilities**

— Bits 2–3: PTKSA Replay Counter. A STA sets the PTKSA Replay Counter subfield(#1801) to the value contained in dot11RSNAConfigNumberOfPTKSAReplayCounters(#1391).

Proposed resolution:

REJECTED

The PTKSA Replay Counter field in the RSNE in the TDLS Setup Request frame is used for the TDLS, and its value comes from this MIB attribute.

Note to the Editor: this is a reversal of a prior motioned ACCEPTED, so the deletion in the current draft has to be reverted.

|  |  |  |
| --- | --- | --- |
| 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 URL>, which xxx

**References:**

802.11me/D5.0 except where otherwise specified