IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some comments on 11me/D4.0 (initial SA ballot) | | | | |
| Date: 2024-01-05 | | | | |
| 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/D4.0. 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 6401  Mark RISON | "assumes" -- the standard should not assume, it should require | Make the changes highlighted in red under CIDs 1397/1398/1794 in 22/0353r10 |

Discussion:

As it says in the comment. However, there are concerns about “shall”s for entities that are not specified by 802.11.

Proposed changes:

Make the changes indicated at the following locations:

171.32: In this document, the word *shall* is used to indicate a mandatory requirement. The word *should* is used to indicate a recommendation. The word *may* is used to indicate a permissible action. The word *can* is used for statements of possibility and capability. The words *need(s) to* are used to indicate a requirement on an entity outside the scope of this standard.

342.16: In order for the MAC to operate properly, ~~this standard assumes that~~ the DS needs to meet~~s~~ the MSDU (“object”) reordering requirements of IEEE Std 802.1AC-2012 [B17].

2630.51: In an infrastructure BSS, the Interworking element contains signaling for HeSSs(M12). The HESSID is a (#2047)MAC address that identifies the HeSS(M12). The HESSID value shall be the universal MAC address of one of the APs(#1347) in the HeSS(M12) and all BSSs in the HeSS use the same value. Thus, it is a globally unique identifier that, in conjunction with the SSID, may be used to provide network identification for an SSPN.

NOTE 1—T~~his standard assumes that t~~he HESSID field in the Interworking element ~~is~~needs to be administered ~~consistently~~to have the same value across all BSSs in an HeSS(M12).

2663.22: NOTE—~~This standard assumes that all APs in an ESS are configured consistently for QMF service~~ All APs in an ESS need to have the same QMF settings when GQMF has been enabled for use by associated non-AP STAs.

2884.10: When the IEEE 802.1X authentication completes successfully, ~~the standard assumes that~~ the STA’s IEEE 802.1X Supplicant and the IEEE 802.1X AS share a secret, called an MSK and used to generate a PMK.

2900.41: Upon a successful authentication, the R0KH shall delete any prior PMK-R0 security association for this mobility domain pertaining to this S0KH. The R0KH shall also delete all PMK-R1 security associations derived from that prior PMK-R0 security association.

***<para break>***

The R0KH generates the PMK-R1s ~~are generated by the R0KH~~ and ~~are assumed to be delivered from the R0KH~~ delivers them to the R1KHs within the same mobility domain. The PMK-R1s are used for PTK generation. Upon receiving a new PMK-R1 for an S0KH, an R1KH deletes the prior PMK-R1 security association and PTKSAs derived from the prior PMK-R1.

~~It is assumed by this standard that the PSK is specific to a single S0KH and a single R0KH.~~

2901.39: The distribution of keys from the R0KH to the R1KHs is outside the scope of this standard. ~~It is assumed that t~~The PMK-R1s are distributed from the R0KH to the R1KHs following the requirements specified in 13.2.2 (Authenticator key holders).

2975.48: Each R0KH-ID and R1KH-ID ~~is assumed to be expressed as~~ needs to be a unique identifier within the mobility domain.

2976.24: The R0KH and the R1KH ~~are assumed~~need to have a secure channel between them that can be used to exchange cryptographic keys without exposure to any intermediate parties. The cryptographic strength of the secure channel between the R0KH and R1KH ~~is assumed~~needs to be greater than or equal to the cryptographic strength of the channels for which the keys are used. T~~his standard assumes that t~~he key transfer includes the PMK-R1, the PMK-R1 PMKSA, the PMK-R1 context, and the associated key authorizations.

2976.33: The PMK-R1 distribution from the R0KH to the R1KHs within the same mobility domain shall satisfy the following ~~assumptions~~:

2976.45: The S0KH and S1KH ~~are entities that are assumed to~~ ~~physically~~ reside in the Supplicant.

2977.23: NOTE—~~It is assumed by this standard that t~~The Fast BSS Transition Policy bits in the MDE ~~are administered consistently~~need to be the same across the mobility domain.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6401 in <this document URL>, which address the locations identified in the comment, using “needs to” for entities not specified by 802.11.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6268  Mark RISON | There are ~16 "MAC layer"s but these should be "MAC sublayer" | As it says in the comment |

Discussion:

It was discussed during LB that the MAC is a sublayer, not a layer (unlike the PHY, which is a layer).

Proposed changes:

Change as follows:

282.56: From the data delivery point of view, ~~it appears as if all STAs in a mesh BSS are directly connected at the MAC layer~~ the MAC service of a STA in an MBSS appears to provide the exchange of MSDUs directly to any other STA in the MBSS, even if the STAs are not within range of each other.

311.57: The deauthentication notification is provided ~~to (#3469)IEEE Std 802.1X-2020 via the MAC layer~~ by the MLME to the SME. The SME then notifies the 802.1X Authenticator or Supplicant, and the 802.1X entity blocks the IEEE 802.1X Controlled Port from passing any further general data traffic.

314.3: When a non-AP STA searches for, and connects to, an infrastructure BSS, IBSS, or PBSS or attempts to discover services on a network preassociation, it ~~defines the addressing of its MAC layer~~ selects a MAC address for the particular connection.

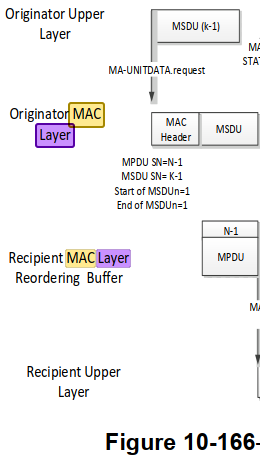
322.22: In 4.3.23 (Mesh BSS), the concept of the MBSS LAN was introduced. It was noted that, using the multi-hop capability ~~it appears as if all mesh STAs are directly connected at the MAC layer~~, the MAC service of a STA in an MBSS appears to provide the exchange of MSDUs directly to any other STA in the MBSS, even if the STAs are not within range of each other. This is different from an IBSS, where STAs cannot communicate if they are not within range of each other.

Unlike the IBSS, an MBSS might have access to the DS. An MBSS connects through one or more mesh gates to the DS. Since in an MBSS it appears ~~as if all mesh STAs are directly connected at the MAC layer~~ at the MAC service interface as if all mesh STAs provide the direct exchange of MSDUs, the MBSS can be used as a DSM. APs, a portal, and mesh gates might use the MBSS as a DSM to provide the DSS. Thus, different infrastructure BSSs can unite over the MBSS to form an ESS for example.

693.28: The maximum length of the Frame Body field can be determined from the maximum MSDU length plus the length of the Mesh Control field (if present) plus any overhead from encapsulation for encryption (i.e., it is always possible to send a maximum length MSDU, with any encapsulations provided by the MAC ~~layer~~ within a single Data frame).

2340.43: In this example, the upper layer of the originator uses the MA-UNITDATA.request primitive to pass MSDUs to the MAC ~~layer~~ for delivery to the recipient.

2341.1: Delete the “Layer”s highlighted in purple in Figure 10-166:



2459.50: TSPECs and DMG TSPECs are constructed at the SME, from application requirements supplied via the SME, and with information specific to the MAC ~~layer~~.

2536.50: Access delay is measured by the AP’s or PCP’s MAC ~~layer~~ being the average medium access delay for transmitted frames

2578.13: The WNM log event report is intended to capture PHY and MAC ~~layer~~ events ~~related to the operation of those layers~~

4450.6: The PHY layer shall issue a PHY-TXSTART.confirm primitive to the MAC in response to the PHY-TXSTART.request(TXVECTOR) primitive when it is ready to receive an MPDU/A-MPDU from the MAC ~~layer~~.

5705.6: TSPECs are constructed at the SME from application requirements supplied via the SME and with information specific to the MAC ~~layer~~.

5757.31: The EDCA and HCCA mechanism defined in 10.23 (HCF) provide QoS control at the MAC sublayer.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6268 in <this document URL>, which reword the instances of “MAC layer”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6366  Mark RISON  C.3 | dot11GroupAddressesTable should also mention the broadcast address where relevant, since this address does not appear in the table | As it says in the comment |

Discussion:

In generic locations the broadcast address is explicitly covered:

1777.33: when the Address 1 field or DA field contains a group address, address filtering is performed by (#1815)comparing the value in the Address 1 field or DA field to all values in the dot11GroupAddressesTable and the broadcast address value

1827.65: the value in the Address 1 field matches any value in the dot11GroupAddressesTable or is the broadcast address(#3522)

In GCR locations not, but GCR uses non-broadcast multicast addresses, e.g.:

1922.20: When using the GCR unsolicited retry retransmission policy for a group address, an AP or mesh STA may retransmit an MPDU to increase the probability of correct reception at the STAs that are listening to this group address (i.e., the group address is in their dot11GroupAddressesTable).

Proposed resolution:

REJECTED

Where a broadcast address might be used, this is already covered. In GCR contexts the broadcast address is not mentioned since GCR does not use the broadcast address.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6320  Mark RISON | CID 4114 follow-up: there are also references to PHY (or PHY SAP) sublayers, but the PHY is a layer not a sublayer. Search for "sublayer-to-sublayer", "PLME SAP sublayer", "between the two sublayers", "the ERP sublayers" and fix those | As it says in the comment |

Discussion:

We agreed that the MAC is a sublayer (of the Data Link layer) but the PHY is a layer.

Proposed resolution:

REVISED

In 6.2 change “The management information specific to each layer is represented as a MIB for that layer. The MLME and PLME are viewed as “containing” the MIB for that layer. […] The invocation of a SET.request primitive might require that the layer entity perform certain defined actions.” to “The management information specific to each of the MAC sublayer and PHY layer is represented as a MIB for each. The MLME and PLME are viewed as “containing” the MIB for each. […] The invocation of a SET.request primitive might require that the entity perform certain defined actions.”

In 8.3.3 change “support sublayer-to-sublayer interactions” to “support interactions between the MAC sublayer and the PHY layer”.

In 8.3.4.2 change “the primitives for sublayer-to-sublayer interactions” to “the primitives for interactions between the MAC sublayer and the PHY layer”.

In the caption for 15.4.1, 16.3.1, 17.4.1, 19.4.1, 20.11.1, 21.4.1, 22.4.1 24.10.1, 25.14.1, change “PLME SAP sublayer management primitives” to “PLME SAP layer management primitives”.

In 17.2.3 change “The MAC and PHY use this value to determine the number of octet transfers that will occur between the two sublayers during the transfer of the received PSDU.” to “The MAC and PHY use this value to determine the number of octet transfers that will occur between them during the transfer of the received PSDU.”

In 18.4.1 change “Subclauses 18.4.2 (Regulatory requirements) to 18.4.7 (PHY transmit specifications) provide general specifications for the ERP sublayers.” to “Subclauses 18.4.2 (Regulatory requirements) to 18.4.7 (PHY transmit specifications) provide general specifications for the ERP.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6420  Mark RISON | There are references to channel "frequency index" but this is not defined | Change "frequency index" to "number" throughout. Change "ChannelCenterFrequencyIndex" to "ChannelCenterNumber" throughout, except in "dot11CurrentChannelCenterFrequencyIndex" |

Discussion:

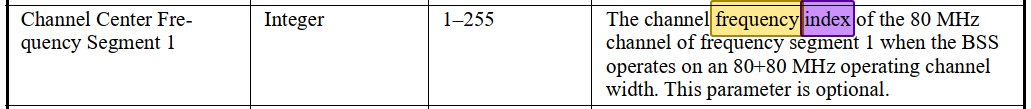
The rules for channel number are well-defined (e.g. in terms of the frequency being (for the “traditional” PHYs) some base frequency plus 5 MHz times the channel number). The “frequency index” is not so defined.

Proposed changes:

In D4.1:

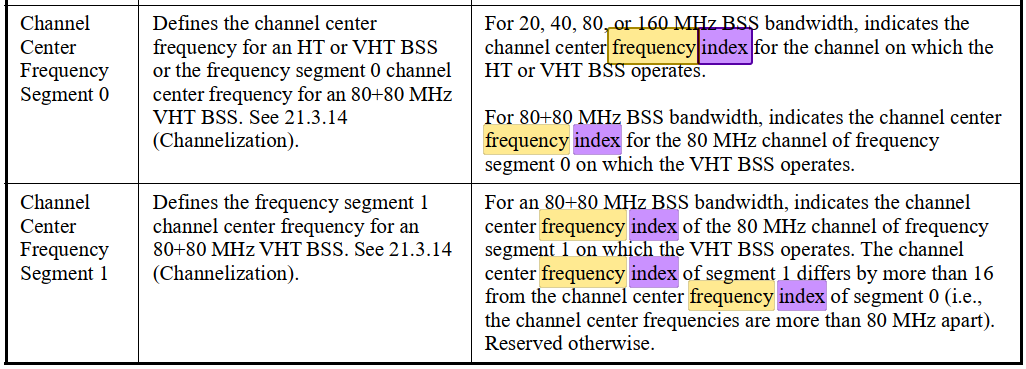
Change “frequency index” to “number” in the highlighted locations:

In 6.5.3.3.2 Semantics of the service primitive:

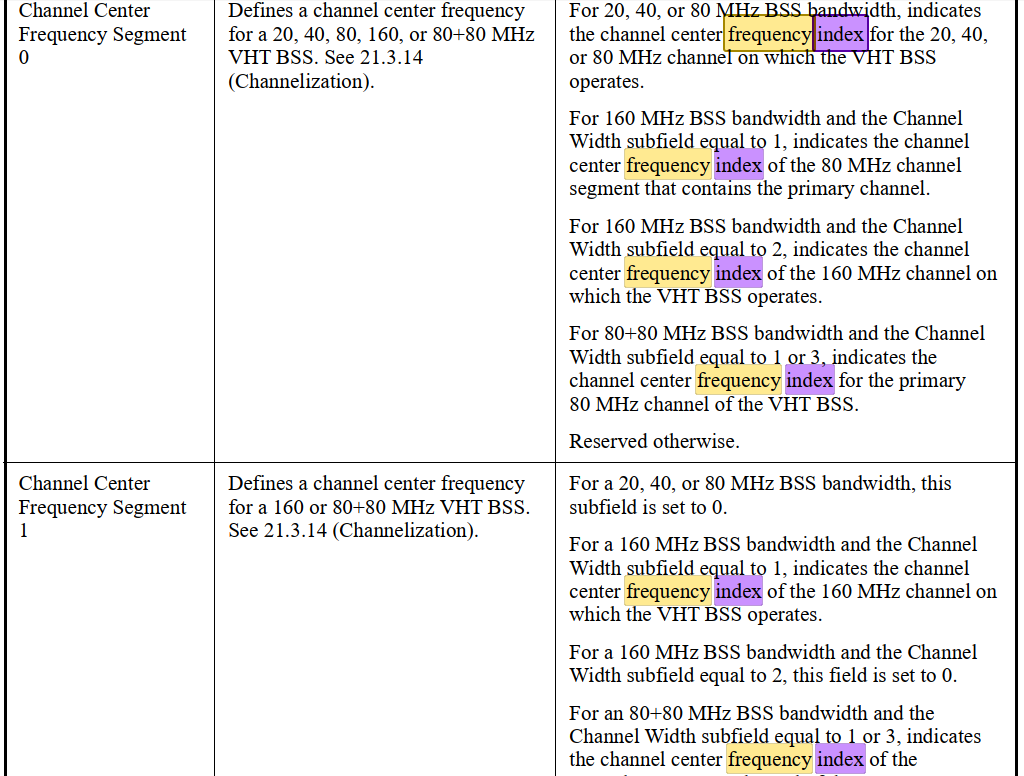


Change “channel center frequency index” to “channel number of the center frequency” in the highlighted locations:

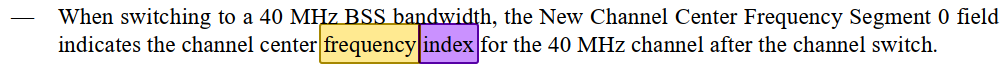
In Table 9-214—HT/VHT Operation Information subfields:



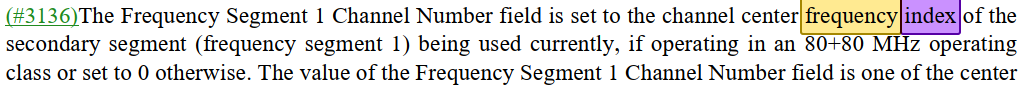
In Table 9-316—VHT Operation Information subfields:



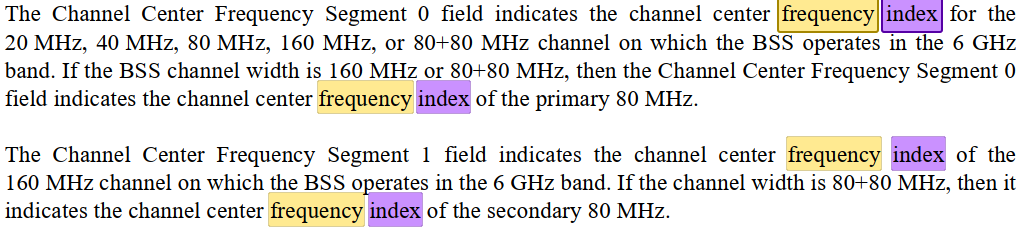
In 9.4.2.161 Channel Switch Wrapper element:



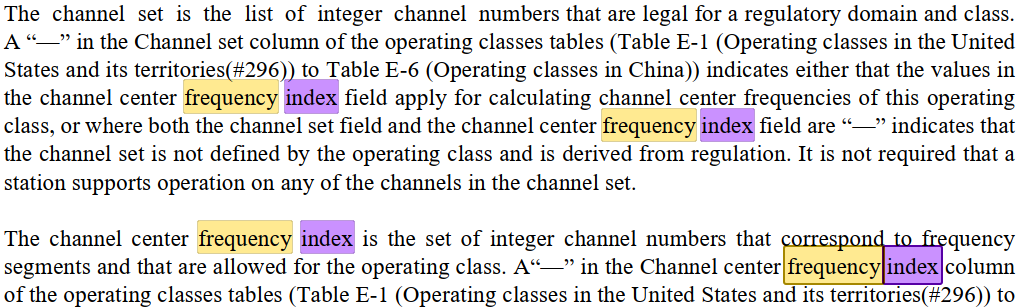
In 9.4.2.235 OCI element:

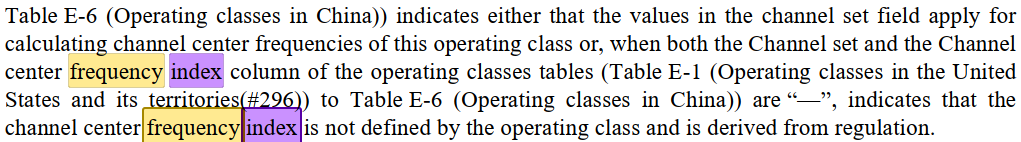


In 9.4.2.248 HE Operation element:



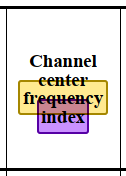
In E.1 Country information and operating classes:





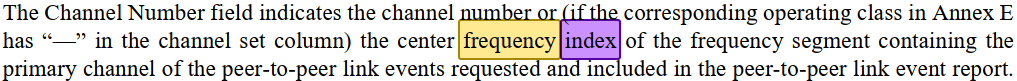
Change “Channel center frequency index” to “Channel number of the center frequency” in the highlighted locations:

In Table E-1—Operating classes in the United States and its territories(#296) to Table E-6—Operating classes in China:

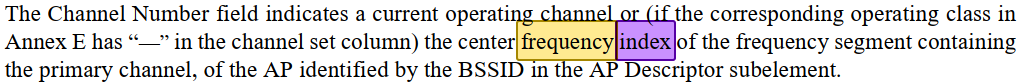


Change “center frequency index” to “channel number of the center frequency” in the highlighted locations:

In 9.4.2.65.4 Peer-to-peer link event request:

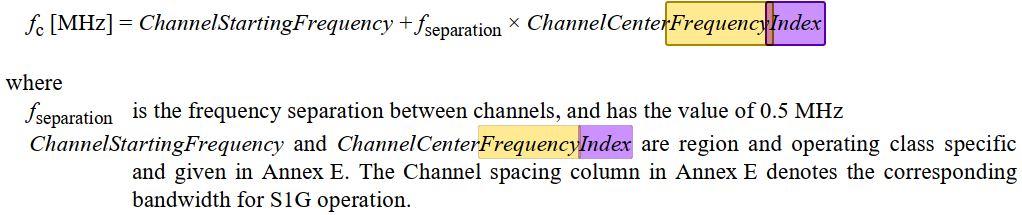


In 9.4.2.67.5 Diagnostic subelement descriptions:



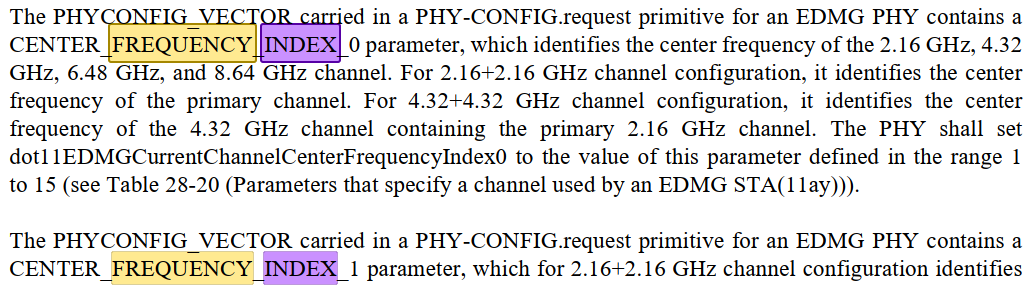
Change “ChannelCenterFrequencyIndex” to “ChannelCenterChannelNumber” in the highlighted locations:

In 23.3.14 Channelization:



Change “CENTER\_FREQUENCY\_INDEX” to “CHANNEL\_CENTER\_CHANNEL\_NUMBER” in the highlighted locations:

In 28.2.3 PHYCONFIG\_VECTOR parameters:



Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6420 in <this document URL>, which refer to channel numbers (of the center frequency, where appropriate).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6171  Mark RISON | (Follow-up of CID 4341). It is not clear how modifying the BA timeout, the buffer size or indeed any other BA agreement parameter works. The only one that is relatively easy to deal with is modification of the BA timeout. | In 10.25.2 and 11.5.1 change "All parameters of [the/an] agreement may be modified except for the TID." to "Only the block ack agreement timeout may be modified." In 11.5.4 change "The inactivity timer at the recipient is also reset when a BlockAckReq frame with the TID for the block ack agreement is received. The inactivity timer at the originator is reset when a BlockAck frame with the TID for the block ack agreement is received." to "The inactivity timer at the recipient is also reset when a BlockAckReq or ADDBA Request frame with the TID for the block ack agreement is received. The inactivity timer at the originator is reset when a BlockAck or ADDBA Response frame with the TID for the block ack agreement is received." |

Discussion:

We discussed BA modification during letter ballot, but did not reach consensus on how it worked.

During the TGme session on 2023-11-13 there seemed to be consensus that BA modification behaves, when the modification is accepted, as if there had been a DELBA immediately prior to the ADDBA exchange. This has the merit of not requiring clarification of how each parameter signalled in ADDBA is handled, since all the BA-related state is cleared by the DELBA, though it does mean that anything “in transit” is potentially lost.

However, the behaviour w.r.t. MPDUs that have been transmitted but not acked (and any MPDUs before the last MPDU that was transmitted) is not clear. There is some discussion in:

**11.5.4 Error recovery upon a peer failure**

When a recipient does not have an active block ack for a TID, but receives QoS Data frames with Block Ack ack policy, it shall discard them and shall send a DELBA frame within its own TXOP. If such a STA receives a BlockAckReq frame, it may respond with an Ack frame and shall respond with a DELBA frame within its own TXOP. The originator may attempt to set up the use of block ack or may send the MPDUs using an alternative acknowledgment mechanism. When the recipient transmits a DELBA frame, it shall set the last sequence number received value to the sequence number of the last received MPDU, regardless of the ack policy used in that frame. 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.

which clarifies some points (though it’s a bit unhelpful to bury generic DELBA behaviour under a “Error recovery”/“peer failure” heading), but:

* The first 3 sentences seem to be about Block Ack ack policy (which is generally not used) and it’s not entirely clear how they relate to the rest
* This describes what happens if the recipient sends the DELBA, but not what happens if the originator sends the DELBA (which is what’s important if we consider BA modification to have an implicit DELBA beforehand)
* This doesn’t cover the (admittedly obscure) case where the originator sent say SN 1, 2 and 4 but not 3 and all the three MPDUs were acked -- in this case the third MPDU has to be discarded too (note “MPDU that has been transmitted and not acknowledged” doesn’t cover such an MPDU)
* “that of the last MPDU that is sent” should presumably be “that of the last MPDU that it sent”
* “Set the sequence number” of what? Presumably the next MPDU it transmits
* It is not clear why the last MPDU can be retained if “it was not a retransmission” but not if it was a retx

Proposed changes:

Modify Subclauses 10.25.2, 11.5.1, 11.5.3.2/3 and 11.5.4, and add Subclauses 11.5.3.4/5as follows:

**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 by the originator(#4352)). All parameters of the agreement may be modified except for the TID. If the request is not successful, the existing agreement is not modified. If the request is successful, the behavior is as if a DELBA frame for the block ack agreement had been transmitted by the originator and received by the recipient immediately prior to the ADDBA Request frame.

**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) (#4353)and 10.25.4 (Teardown of the block ack mechanism)) 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. If the request is not successful, the existing agreement is not modified. If the request is successful, the behavior is as if a DELBA frame for the block ack agreement had been transmitted by the originator and received by the recipient immediately prior to the ADDBA Request frame.

**11.5.3.2 Procedure at the initiator of the block ack agreement teardown**

Upon receipt of an MLME-DELBA.request primitive, the MLME shall tear down the block ack agreement by transmitting a DELBA frame.

~~The encoding of ReasonCode values to Reason Code field (see 9.4.1.7 (Reason Code field)) values is defined in Table 9-79 (Reason codes).~~

**11.5.3.3 Procedure at the recipient of the DELBA frame**

A STA shall issue an MLME-DELBA.indication primitive with the parameter ReasonCode having a value of REQUESTED when a DELBA frame is received.

**11.5.3.4 Procedure at the block ack originator**

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:

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.

**11.5.3.5 Procedure at the block ack recipient**

When a block ack agreement is torn down, the recipient shall, irrespective of whether it transmitted or received a DELBA frame, set the last sequence number received value for MPDUs for the block ack agreement’s originator and TID to the sequence number of the last (highest in sequence number space) MPDU received, regardless of the ack policy used in that MPDU.

**11.5.4 Error recovery upon a peer failure**

When a recipient does not have an active block ack agreement for a TID, but receives one or more QoS Data frames with Block Ack ack policy, it shall discard them and shall send a DELBA frame ~~within its own TXOP~~. ~~If such a STA receives a BlockAckReq frame,~~ When a recipient does not have an active block ack agreement for a TID, but receives a BlockAckReq frame, it may respond with an Ack frame and shall ~~respond with~~ send a DELBA frame ~~within its own TXOP~~. The originator may attempt to set up ~~the use of~~ a block ack agreement again or may send ~~the~~ MPDUs using an alternative acknowledgment mechanism. ~~When the recipient transmits a DELBA frame, it shall set the last sequence number received value to the sequence number of the last received MPDU, regardless of the ack policy used in that frame. 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.~~

Add “agreement” after “the block ack” in the quoted body text of the following subclauses:

9.3.1.8.8 EDMG Compressed BlockAck variant: “The size of the Block Ack Bitmap subfield is negotiated during the block ack establishment”

9.4.1.16 DELBA Parameter Set field: “UP for which the block ack has been originally set up”

9.6.4.4 DELBA frame format: “to terminate the block ack participation” [also delete “participation”]

10.25.2 Setup and modification of the block ack parameters: “The ADDBA Request and Response frames exchanged to set up the block ack”

10.25.2 Setup and modification of the block ack parameters: “Once the block ack exchange has been setup” [also delete “exchange”]

10.25.4 Teardown of the block ack mechanism [title itself; also delete “mechanism”]

10.25.4 Teardown of the block ack mechanism: “for the block ack’s TID”

10.25.4 Teardown of the block ack mechanism: “explicit teardown of the block ack mechanism”

11.5.2.2 Procedure at the originator: “modified the block ack mechanism with the recipient STA” (2x) [also delete “mechanism”]

11.5.3 Teardown of the block ack mechanism [title itself; also delete “mechanism”]

In 9.3.1.8.9 EDMG Multi-TID BlockAck variant change “negotiated during the Block Ack establishment” to “negotiated during the block ack agreement establishment” (2x).

Change “it implies that the originator of the block ack has no information” to “it implies that the block ack originator has no information” in 9.4.1.13 Block Ack Parameter Set field.

Change “which is equal to twice the Block Ack reorder window” to “which is equal to twice the block ack agreement reordering buffer” in 12.5.2.3.6 Construct CCMP header for PV1 MPDUs.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6171 in <this document URL>, which cause BA modification, if successful, to be handled as if the block ack agreement had been deleted immediately prior to the modification, and clarify the behaviour w.r.t. MPDUs that have not been acknowledged.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6173  Mark RISON  10.25.4 | 11.5.4 requires the BA agreement to be torn down on timeout ("When a timeout of BlockAckTimeout is detected, the STA shall send a DELBA") | Change "The block ack agreement may be torn down if" to "The block ack agreement shall be torn down if" |

Discussion:

10.25.4 at 1962.8 says:

The block ack agreement may be torn down if there are no BlockAck, BlockAckReq, or MPDUs received from the peer under the block ack agreement, for the block ack’s TID, within a duration of block ack timeout value (see 11.5.4 (Error recovery upon a peer failure)).

but 11.5.4 at 2482.26 says:

When a timeout of BlockAckTimeout is detected, the STA shall send a DELBA frame to the peer STA

ADACHI Tomo had previously suggested the apparent contradiction might be because the 10.25.4 text is trying to say that the BA agreement can be torn down before the inactivity timeout expires. However, she has subsequently indicated that she is happy with the proposed direction, but thinks that the “within” is unclear; she suggests something like “when an inactivity timer set by a duration of block ack timeout value expires”.

Note that CID 6172, which has been ACCEPTED motioned, has tried to canonicalise the BA timeout wording and here calls for:

In 10.25.4 change "within a duration of block ack timeout value" to "within the block ack agreement inactivity timeout"

Proposed resolution:

REVISED

Change the para at 1962.8 to:

The block ack agreement can be torn down if there are no BlockAck, BlockAckReq, or Data frames received from the peer under the block ack agreement, for the block ack’s TID (even before block ack agreement inactivity timeout) (see 11.5.4).

OR

REVISED

Change the para at 1962.8 to:

The block ack agreement shall be torn down if there are no BlockAck, BlockAckReq, or Data frames received from the peer under the block ack agreement, for the block ack’s TID, when an inactivity timer set by a duration of block ack timeout value expires (see 11.5.4).

OR (given acceptance of CID 6172)

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6166  Mark RISON  12 | Determination of the TDLS responder's RSN capabilities is problematic, because in the TPK handshake the TDLS responder echoes the TDLS initiator's RSNE, so the TDLS initiator does not receive the TDLS responder's RSN capabilities. The TDLS responder's RSN capabilities are present in the TDLS Discovery Response frame, but TDLS discovery is not mandatory, and anyway this frame is not protected. In turn, this means that the number of replay counters supported by the TDLS responder is not always known, nor is its MFP support. It was asserted during a TGme session at the September 2023 F2F that "nobody" does PMF with TDLS and "nobody" pays attention to the number of replay counters advertised. | In Table 9-189—PTKSA/GTKSA/TPKSA replay counters usage delete "/TPKSA" (5x inc. caption) At 4974.17 delete "and the number of TPKSA replay counters per (#2152)TDLS direct link" At 2852.52 and 2862.47 change "subject to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.23 (RSNE))." to "subject if not for a TPKSA to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.23 (RSNE)). A TDLS STA shall support 16 replay counters per TPKSA and shall ignore the PTKSA Replay Counter field in RSNEs received from a TDLS peer STA." At 2874.36 change "(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS peer STA during TDLS discovery or in the RSNEs exchanged in the 3-way handshake with the TDLS peer STA to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0." to "(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS responder STA during TDLS discovery, if performed, or in the RSNE received from the TDLS initiator STA in the TPK handshake to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0. If TDLS discovery was not performed, the TDLS initiator STA shall set the MFPC and MFRP bits in its RSNE to the same value; if the TDLS initiator STA set them to 0 in its RSNE it shall behave as if the MFPC and MFPR bits from the TDLS responder STA were 0, and as if those bits were 1 otherwise. NOTE---This means that if a TDLS initiator STA requires MFP but does not know whether the TDLS responder is MFP-capable, it assumes it is (any mismatch will be discovered when a Management frame exchange is performed); otherwise MFP is not used. The TDLS responder STA might preemptively tear down the TDLS link if this assumption is wrong, i.e. the TDLS initiator STA requires MFP but the TDLS responder STA is not MFP-capable or vice-versa, or it might hope Management frames are not used (e.g. there is no attempt to set up a block ack agreement)." At 2875.37 change "3-way handshake" to "TPK handshake". |
| CID 6150  Mark RISON  12.7.8.4  2937.20 | The number of replay counters supported by a TDLS responder is not known (T2's RSN Capabilities field is a copy of T1's), and though the number supported by the TDLS responder is advertised in T1's RSN Capabilities field, in practice existing deployments just assume this will always be 16, i.e. one per TID. See other comment for more expansive proposed change | At 2937.50 change "In the RSN Capabilities field, (#3056)the PeerKey Enabled subfield shall be set to 1." to "In the RSN Capabilities field, (#3056)the PeerKey Enabled subfield shall be set to 1, the PTKSA Replay Counter field in the shall be set to 3 (to indicate 16 replay counters for the TPKSA) and the GTKSA Replay Counter field shall be reserved." At 2939.17 add a para "The RSN capabilities of the TDLS responder STA are not communicated to TDLS initiator STA during the TPK handshake. A TDLS initiator STA shall assume that a TDLS responder STA supports 16 replay counters for the TPKSA." |
| CID 6149  Mark RISON  9.4.2.23.4  985.17 | Table 9-189—PTKSA/GTKSA/TPKSA replay counters usage is referred to in the context of PTKSAs and GTKSAs, but not in the context of TPKSAs | Delete the "/TPKSA"s from the caption and the cells |

Discussion:

As the comments say, because the RSNE in T2 is required to be a copy of the RSNE in T1, the TDLS initiator either doesn’t receive the TDLS responder’s RSN capabilities, or only receives them unprotected (in the TDLS Discovery Response frame).

The proposals above were to just require support for 16 (well, in practice 8 suffice) replay counters and to use heuristics to determine MFP use, but the group expressed on 2023-12-08 a preference for instead requiring the TDLS responder to align with the TDLS initiator’s RSN capabilities, and if this is not acceptable/possible, to abandon the TPK handshake.

Proposed changes:

Do not make the changes proposed in CID 6149 (this is a reversal of the ACCEPTED in motion 119).

Change 12.6.3 RSNA policy selection in an infrastructure BSS as follows:

(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the value~~s~~ of the MFPC ~~and MFPR~~ bit~~s advertised~~ in the RSNE ~~received from the TDLS peer STA during TDLS discovery or in the RSNEs exchanged in the 3-way handshake with the TDLS peer STA~~ transmitted by the TDLS initiator STA in the TDLS Setup Request frame to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. ~~If either the TDLS initiator STA does not advertise an RSN Capabilities field in anthe RSNE, this shall be treated as if its MFPC and MFPR bits were 0.~~ A TDLS STA should, in the context of TDLS, set the MFPC bit to 1 if dot11RSNAProtectedManagementFramesActivated is true, and shall set it to 0 unless dot11RSNAProtectedManagementFramesActivated is true. ~~A TDLS initiator STA should, in the context of TDLS, set the MFPR bit to the same value as it advertised to the AP with which it is associated.~~(#3056)

NOTE—The MFPR bit from the TDLS initiator STA is ignored by the TDLS responder STA, and (if a TDLS Discovery Response frame is sent) the MFPC and MFPR bits from the TDLS responder STA are ignored by the TDLS initiator STA, except that a TDLS initiator STA might set its MFPC bit to 0 if the MFPC bit from the TDLS responder STA is 0.

Replace Table 12-6—Robust management frame selection between TDLS STAs(#199) with:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TDLS initiator STA MFPC** | **TDLS responder STA MFPC (might not be transmitted)** | **TDLS initiator STA action** | **TDLS responder STA action** | **MFP used?** |
| 0 | 1 | The TDLS initiator STA may establish a TDLS direct link with the TDLS responder STA | The TDLS responder STA may establish a TDLS direct link with the TDLS initiator STA (see NOTE 1) | No |
| 0 | 0 | The TDLS responder STA may establish a TDLS direct link with the TDLS initiator STA |
| 1 | 1 | Yes |
| 1 | 0 | See NOTE 2 | The TDLS responder STA shall reject attempts by the TDLS initiator STA to establish a TDLS direct link with the Status Code ROBUST\_MANAGEMENT\_ POLICY\_VIOLATION | N/A |
| NOTE 1—If the TDLS responder requires MFP, it can cause the TDLS direct link establishment to fail by using the Status Code ROBUST\_MANAGEMENT\_POLICY\_VIOLATION in the TDLS Setup Response frame. | | | | |
| NOTE 2—If a TDLS initiator STA has performed TDLS discovery and determined that the TDLS responder STA is not MFPC, it might, if it trusts the authenticity of the TDLS Discovery Response frame, avoid this situation, i.e. it might set its MFPC bit to 0 and not use MFP. | | | | |

OR with (same information, just different layout):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TDLS initiator STA MFPC** | **TDLS responder STA MFPC (might not be transmitted)** | **TDLS initiator STA action** | **TDLS responder STA action** | **MFP used?** |
| 1 | 1 | The TDLS initiator STA may establish a TDLS direct link with the TDLS responder STA | The TDLS responder STA may establish a TDLS direct link with the TDLS initiator STA | Yes |
| 0 | 0 | No |
| 0 | 1 | The TDLS responder STA may establish a TDLS direct link with the TDLS initiator STA (see NOTE 1) |
| 1 | 0 | See NOTE 2 | The TDLS responder STA shall reject attempts by the TDLS initiator STA to establish a TDLS direct link with the Status Code ROBUST\_MANAGEMENT\_ POLICY\_VIOLATION | N/A |
| NOTE 1—If the TDLS responder requires MFP, it can cause the TDLS direct link establishment to fail by using the Status Code ROBUST\_MANAGEMENT\_POLICY\_VIOLATION in the TDLS Setup Response frame. | | | | |
| NOTE 2—If a TDLS initiator STA has performed TDLS discovery and determined that the TDLS responder STA is not MFPC, it might, if it trusts the authenticity of the TDLS Discovery Response frame, avoid this situation, i.e. it might set its MFPC bit to 0 and not use MFP. | | | | |

Change 12.5.2.4.4 PN and replay detection and 12.5.4.4.4 PN and replay detection as follows:

b) For each PTKSA, (#166)TPKSA, GTKSA, mesh PTKSA, and mesh GTKSA(#239), the (#4212)receiver 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). In the case of a TPKSA, this shall for both the TDLS initiator STA and the TDLS responder STA be the number indicated by the TDLS initiator STA in the PTKSA Replay Counter field in the TDLS Setup Request frame.

NOTE—The number indicated by the TDLS responder STA (if a TDLS Discovery Response frame is sent) is ignored, as is the GTKSA Replay Counter field in the TDLS Setup Request frame and any TDLS Discovery Response frame.

Change 12.7.8.4.2 TPK handshake message 1 as follows:

On reception of message 1, the TDLS responder STA ~~checks whether the RSNE is present.~~ proceeds as follows:

If security is not required on the TDLS direct link (see 12.7.8.1 (General)) and the request includes an RSNE, ~~it~~the TDLS responder STA shall reject the request with status code SECURITY\_DISABLED.

If security is required on the TDLS direct link (see 12.7.8.1 (General))~~, it checks whether~~ and the request does not include~~s~~ both an RSNE and an FTE~~. If not~~, the TDLS responder STA shall reject the request with status code INVALID\_PARAMETERS.

If the version field of the RSNE is 0, ~~then~~ the TDLS responder STA shall reject the request with status code UNSUPPORTED\_RSNE\_VERSION.

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

***<deindent subsequent paras to be at the same level as above>***

If (#3488)the RSNE does not indicate (#4225)the single (#3266)AKM 00-0F-AC:7(TPK handshake), the TDLS responder STA shall reject the request with status code STATUS\_INVALID\_AKMP.

If none of the pairwise cipher suites are acceptable, or pairwise ciphers include (#3056)TKIP, ~~then~~ the TDLS responder STA shall reject the ~~TDLS Setup Request frame~~ request with status code STATUS\_INVALID\_PAIRWISE\_CIPHER.

If the RSN Capabilities field has not been set ~~the subfields~~ according to the described rules for this message, ~~then~~ the TDLS responder STA shall reject~~s~~ the request with status code INVALID\_RSNE\_CAPABILITIES.

If the number of replay counters indicated by the TDLS initiator STA is not acceptable to the TDLS responder STA at both the TDLS initiator STA and the TDLS responder STA (see 12.5.2.4.4 and 12.5.4.4.4), the TDLS responder STA shall reject the request with status code INVALID\_RSNE\_CAPABILITIES.

If the suggested lifetime is unacceptable or below the default value, the TDLS responder STA shall reject the ~~TDLS Setup Request frame~~ request with status code UNACCEPTABLE\_LIFETIME.

If the contents of the FTE are not as per specified for this message, ~~then~~ the TDLS responder STA shall reject the ~~TDLS Setup Request frame~~ request with status code STATUS\_INVALID\_FTE.

The TDLS responder STA shall ignore the remaining fields in the RSNE, FTE, and (#1776)TIE.

Otherwise, the TDLS responder STA shall respond as specified in 11.20.4 (TDLS direct link establishment(#1356)).

Change 12.7.8.4.3 TPK handshake message 2 as follows:

The TDLS responder STA sends message 2 to the TDLS initiator STA. ~~The TDLS initiator STA shall process message 2 as follows:~~

On reception of message 2, the TDLS initiator STA proceeds as follows:

If the TDLS initiator STA Address and TDLS responder STA Address of the Link Identifier element do not match those for an outstanding TDLS Setup Request, the TDLS initiator STA shall silently discard the ~~received TDLS Setup Response frame~~ response.

If the SNonce field of the FTE does not match that of an outstanding request to the TDLS responder STA, ~~then~~ the TDLS initiator STA shall silently discard the ~~received TDLS Setup Response frame~~ response.

Otherwise, the TDLS initiator STA shall compute the TPK and then validate the MIC in the FTE as specified in MIC calculation procedure for TPK handshake message 2. If invalid, the TDLS initiator STA shall discard the ~~message~~response.

If the version of the RSNE is 0 or is greater than the version of the RSNE sent in message 1, ~~then~~ the TDLS initiator STA shall reject the response with status code UNSUPPORTED\_RSNE\_VERSION.

~~Otherwise,~~

***<deindent subsequent paras to be at the same level as above>***

If the (#3488)Information field of the RSNE, with the exception of the pairwise cipher suite count and pairwise cipher suite list, is not the same as that sent by the TDLS initiator STA in message 1 of this sequence, ~~then~~ the TDLS initiator STA shall reject the response with status code INVALID\_RSNE.

If the pairwise cipher suite count is ~~other than~~not 1, ~~then~~ the TDLS initiator STA shall reject the response with status code STATUS\_INVALID\_PAIRWISE\_CIPHER.

If the ~~selected~~ pairwise cipher suite was not included in the ~~Initiator’s~~ request, ~~then~~ the TDLS initiator STA shall reject the ~~TDLS Setup Response frame~~ response with status code STATUS\_INVALID\_PAIRWISE\_CIPHER.

If the (#1776)TIE is not the same as that sent in message 1, the TDLS initiator STA shall reject the ~~TDLS Setup Response frame~~ response with status code UNACCEPTABLE\_LIFETIME.

If the BSSID in the Link Identifier element is different from the one sent in message 1, ~~then~~ the TDLS initiator STA shall reject the response with status code NOT\_IN\_SAME\_BSS.

Change 12.7.8.4.4 TPK handshake message 3 as follows:

The TDLS initiator STA sends message 3 to the TDLS responder STA. ~~The TDLS responder STA shall process message 3 as follows:~~

On reception of message 3, the TDLS responder STA proceeds as follows:

[…]

If any of the above conditions are not met, the TDLS responder STA shall discard the ~~message~~confirmation.

[…]

If any ~~one~~ of the above conditions are not met, the TDLS responder STA shall discard the ~~message~~confirmation

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6166, 6150, 6149 in <this document URL>, which make the RSN capabilities specified by the TDLS initiator apply to the TDLS responder too.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6332  Mark RISON  4.3.1 | "The collection of all possible directional transmissions by a member STA defines the coverage area. (The concept of area, while not precise, is often good enough.) This area is called the Basic Service Area (BSA)" -- no, the BSA is defined as "The area containing the members of a basic service set (BSS)." And how can a STA possibly move out of its BSA? | Change "This area is called the Basic Service Area (BSA)." to "The area containing the members of a BSS is called the Basic Service Area (BSA)." (though this makes the next sentence a bit tautological) |

Discussion:

The paras in question say:

The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN. Figure 4-1 (BSSs) shows two BSSs, each of which has two STAs that are members of the BSS.

It is useful to think of each oval depicting a BSS as the coverage area within which the member STAs of the BSS can remain in communication. In the case of transmissions such as in a directional multi-gigabit (DMG) BSS, the individual coverage area of a transmission from one member STA to another can be thought of as a cone and hence is referred to as a *directional transmission*. The collection of all possible directional transmissions by a member STA defines the coverage area. (The concept of area, while not precise, is often good enough.) This area is called the *Basic Service Area* (BSA). If a STA moves out of its BSA, it can no longer directly communicate with other STAs present in the BSA.

In 802.11-2012 they said:

The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN. Figure 4-1 shows two BSSs, each of which has two STAs that are members of the BSS.

It is useful to think of the ovals used to depict a BSS as the coverage area within which the member STAs of the BSS may remain in communication. (The concept of area, while not precise, is often good enough.) This area is called the Basic Service Area (BSA). If a STA moves out of its BSA, it can no longer directly communicate with other STAs present in the BSA.

So 11ad has confusingly inserted some directional stuff in the middle of the discussion. The current wording reads as if the coverage area defined by directional transmissions by a member STA is the BSA, but that is in contradiction to common sense, because in that case it would not be possible for a STA to move out of its BSA. In addition it is contrary to the definition:

**basic service area:** [BSA] The area containing the members of a basic service set (BSS). It might contain members of other BSSs.

Having said that, “its BSA” doesn’t make sense, and a STA might still be able to communicate with some members even if it moves out of range of some of the other STAs.

It’s also not clear what:

The collection of all possible directional transmissions by a member STA defines the coverage area.

is trying to say. My guess is that it’s trying to say that:

The intersection of all possible directional transmissions by all the member STAs defines the coverage area [in the case of DMG].

Proposed resolution:

REVISED

Change the third para of 4.3.1 General to:

It is useful to think of each oval depicting a BSS as the coverage area within which all the member STAs of the BSS can remain in communication. (The concept of area, while not precise, is often good enough.) This area is called the *basic service area* (BSA). If a STA moves out of the BSA, it can no longer directly communicate with all the other STAs present in the BSA.

NOTE—In the case of transmissions such as in a directional multi-gigabit (DMG) BSS, the individual coverage area of a transmission from one member STA to another can be thought of as a cone and hence is referred to as a *directional transmission*. The intersection of all possible directional transmissions by all the member STAs defines the coverage area.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6213  Mark RISON  9.8.3.1 | "The A1 field is an SID and the A2 field is either an SID or contains a MAC address." -- not clear how you know which it is | Give a xref to where it is described how you know which it is (as for the rows above). Probably needs S1G SME input |

Discussion:

David GOODALL has provided the following input:

the information is in section 9.8.4 (PV1 Control frames). There are currently only two PV1 control frames detailed in sections 9.8.4.2 (STACK frame format) and 9.8.4.3 (BAT frame format).

Proposed resolution:

REVISED

Change the cited text to “The A1 field is a SID field and the A2 field is either a SID field or contains a MAC address, depending on the PV1 Control frame subtype (see 9.8.4 (PV1 Control frames)).”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6277  Mark RISON  10 | Sentence starting "The values of the BlockAck ID" appears twice | Delete one of them |

Discussion:

The contexts are:

**10.3.2.12 Fragment BA procedure**

The originator STA shall consider an NDP\_1M BlockAck frame (or an NDP\_2M BlockAck frame) as received if the BlockAck ID field value equals the 2 LSBs (or 6 LSBs) of the Scrambler Initialization value in the (#3409)SERVICE field and the Starting Sequence Control field value equals the Sequence Number of the fragment that elicited the response. The Scrambler Initialization value shall be obtained from the PHY-TXEND.confirm parameter SCRAMBLER\_OR\_CRC.

The values of the BlockAck ID and Starting Sequence Number fields(#4200) are obtained after decoding the NDP BlockAck frame as described in 10.56 (Bitmap protection for NDP BlockAck frames).

**10.25.6 HT-immediate block ack extensions**

**10.25.6.7 Originator’s behavior**

**10.25.6.7.1 General(11ay)**

If the received BlockAck response is of an expected NDP\_1M BlockAck frame (or an NDP\_2M BlockAck frame), the S1G originator shall accept it as correctly received if the value obtained from the BlockAck ID field equals the 2 LSBs (or the 6 LSBs) of the Scrambler Initialization value of the immediately previously transmitted A-MPDU that is not an S-MPDU, or BlockAckReq frame,(#4200) and the Starting Sequence Number obtained from the Starting Sequence Control field equals WinStartO. The Scrambler Initialization value is obtained from the PHY-TXEND.confirm parameter SCRAMBLER\_OR\_CRC. The values of the BlockAck ID and Starting Sequence Number fields are obtained after decoding the NDP BlockAck frame as described in 10.56 (Bitmap protection for NDP BlockAck frames). The S1G originator shall otherwise consider the NDP BlockAck frame to be lost.

David GOODALL has provided the following input:

I think the instance in the Fragment BA procedure can be removed on the basis that someone implementing that procedure would already have a working implementation of NDP Block Acks.

Proposed resolution:

REVISED

In 10.3.2.12 move “The Scrambler Initialization value shall be obtained from the PHY-TXEND.confirm parameter SCRAMBLER\_OR\_CRC.” to the start of the next para (to be followed by “The values of the BlockAck ID and Starting Sequence Number fields(#4200) are obtained after decoding the NDP BlockAck frame as described in 10.56 (Bitmap protection for NDP BlockAck frames).”), change “shall be” to “is” and prepend “NOTE—”.

In 10.25.6.7.1 prepend “NOTE—” to “The Scrambler Initialization value is obtained from the PHY-TXEND.confirm parameter SCRAMBLER\_OR\_CRC. The values of the BlockAck ID and Starting Sequence Number fields are obtained after decoding the NDP BlockAck frame as described in 10.56 (Bitmap protection for NDP BlockAck frames).” and move it to after the para it is currently in.

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

**References:**

802.11me/D4.0 except where otherwise specified