IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some comments on 11me/D2.0 (LB270) | | | | |
| Date: 2023-03-14 | | | | |
| 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/D2.0. 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 3510  Mark RISON  9.4.2.17 | The Supported Channels element stuff is a mess.  Some bits of the spec suggest this element only applies to DFS operation  (e.g. Clause 6), others that that it doesn't apply if you support ECSA  (e.g. Clause 9). 9.2.4.17 even suggests it only applies to 11a!  But 9.6.7.16/12.2/12.3 indicates it's also used for TDLS. 11.8.2/8  suggest it's about letting the AP decide whether to allow a STA to  associate, based on the channels it supports, and if so what channels  to use when changing channels. 11.20.6 says that for TDLS you include  both that a Supported Operating Classes element, but it doesn't describe  how you determine which OC in the SOCe a given channel in the SCe  applies to | At the start of the referenced subclause add "The Supported Channels element means completely different things in different contexts." |

Discussion:

Here are the key instances of “Supported Channels”:

**4.5.5.3 DFS**

[…]

The DFS service provides for the following:

— Association of STAs with an AP based on the STAs’ supported channels.

**4.5.8 Radio measurement service**

The Radio measurement service provides the following:

— The ability to request and report radio measurements in supported channels.

— The ability to perform radio measurements in supported channels.

**6.5.7.2.2 Semantics of the service primitive [ditto reassoc]**

The primitive parameters are as follows:

MLME-ASSOCIATE.request(

[…]

Supported Channels

The list of channels in which the STA is capable of operating.

Present if DFS functionality is required, as specified in 11.8 (DFS procedures); otherwise not present.

=> DFS-only

**Table 9-62—Association Request frame body [ditto reassoc]**

The Supported Channels element is present if dot11SpectrumManagementRequired is true and dot11ExtendedChannelSwitchActivated is false.

=> suggests not present if ECSA supported; at least not required

**9.4.2.17 Supported Channels element**

The Supported Channels element contains a list of channel subbands (from those channels defined in 17.3.8.4.3 (Channelization)) in which a STA is capable of operating.

=> 11a-only

[…]

The use of the Supported Channels element is described in 11.8.2 (Association based on supported channels) and 11.8.8 (Selecting and advertising a new channel).

=> about letting the AP decide whether to allow a STA to associate based on the channels it supports, and what channel to switch to

**9.4.2.20.7 Beacon request**

[…]

For operating classes that identify the location of the primary channel, a Channel Number field set to 0 indicates a request to make iterative measurements for all supported channels in the operating class where the measurement is permitted on the channel and the channel is valid for the current regulatory domain.

For operating classes that encompass a primary channel but do not identify the location of the primary channel, a Channel Number field set to 0 indicates a request to make iterative measurements for all primary channel positions within all requested and supported channels where the measurement is permitted on the channel and the channel is valid for the current regulatory domain.

For operating classes that identify the location of the primary channel, a Channel Number field set to 255 indicates a request to make iterative measurements for all supported channels in the current operating class listed in the latest AP Channel Report received from the serving AP.

**Table 9-457—TDLS Discovery Response frame Action field format [ditto setup req]**

[…]

The Supported Channels element is present if the TDLS Channel Switching subfield is equal to 1.

The Supported Channels element is defined in 9.4.2.17 (Supported Channels element).

=> also used for TDLS

**Table 9-498—Information for TDLS Setup Response Action field**

[…]

The Supported Channels element is defined in 9.4.2.17 (Supported Channels element). It is present if the TDLS Channel Switching subfield is equal to 1 and the Status Code is SUCCESS, and not present otherwise.

=> also used for TDLS

**Table 9-519—Mesh Peering Open frame Action field format**

[…]

The Supported Channels element is present if dot11SpectrumManagementRequired is true and dot11ExtendedChannelSwitchActivated is false.

=> suggests not present if ECSA supported; at least not required

**10.39.12.2.1 Channel access rules**

[…]

An EDMG STA shall not transmit an EDMG PPDU to a peer EDMG STA over a channel that is not supported by the peer STA as indicated in the Supported Channels field [I think subelement is intended here] in the peer STA’s EDMG Capabilities element.

**11.8 DFS procedures**

**11.8.1 General [ditto DMG]**

[…]

Attribute dot11SpectrumManagementRequired shall be set to true (#1038)if regulatory authorities require DFS. It may also be set to true in other circumstances. The DFS procedures provide for the following:

— Associating STAs with an AP based on the STAs’ supported channels (see 11.8.2 (Association based on supported channels)).

=> about letting the AP decide whether to allow a STA to associate based on the channels it supports

**11.8.2.1 Association based on supported channels in a non-DMG BSS [similar DMG]**

A STA shall provide an AP with a list of the channels in which the STA can operate when associating or reassociating by including a Supported Channels element in its (Re)Association Request frames.

=> about letting the AP decide whether to allow a STA to associate based on the channels it supports

An AP may use the supported channels list for associated STAs as an input into an algorithm used to select a new channel for the BSS. The specification of this algorithm is beyond the scope of this standard.

=> about helping the AP choose which channel to switch to

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

[…]

The decision to switch to a new operating channel in an infrastructure BSS shall be made only by the AP. An AP may make use of the information in Supported Channel [should be Channels, also in MBSS and DMG] elements and the results of measurements undertaken by the AP and other STAs in the BSS to assist the selection of the new channel. The algorithm to choose a new channel is beyond the scope of this standard. The AP shall attempt to select a new channel that is supported by all associated STAs.

=> about helping the AP choose which channel to switch to

**11.9.3.2 Selecting and advertising a new channel in an infrastructure BSS [similar MBSS]**

[…]

The decision to switch to a new operating channel and/or operating class in an infrastructure BSS is made by the AP when dot11DSERequired is false. An AP may make use of the information in the Supported Channels element, Supported Operating Classes element, and the results of measurements undertaken by the AP and other STAs in the BSS to assist the selection of the new channel and/or operating class.

=> about helping the AP choose which channel to switch to

**11.20.6.1 General**

The STA shall include a Supported Channels element and a Supported Operating Classes element in all TDLS Setup Request and TDLS Setup Response frames that have a TDLS Channel Switching subfield equal to 1. The STA shall include only channels in the Supported Channels element for which it can adhere to the local power constraint.

=> how do you determine which OC in the SOCe a given channel in the SCe applies to?

**B.4.10 Spectrum management extensions**

SM3 Power Capability and Supported Channels elements in (Re)Association Request and Response frames

CFSM:M

=> so not if spectrum management not supported

My starting suggestion would be:

* the bits that suggest it's 11a-only or DFS-only or SM-only are just wrong
* the bits that suggest it's not used if ECSA is supported are misleading
* the combined use of SC and SOC in TDLS needs clarification (or just delete the SOC from the TDLS frames?)
* the EDMG typo should be fixed
* the Supported Channel element typos should be fixed

Proposed changes:

Make the following changes:

**6.5.7.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-ASSOCIATE.request(

[…]

Supported Channels

The list of channels in which the STA is capable of operating.

Present if DFS functionality is required, as specified in 11.8 (DFS procedures); otherwise ~~not~~optionally present.

**6.5.8.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-REASSOCIATE.request(

[…]

Supported Channels

The list of channels in which the STA is capable of operating.

Present if DFS functionality is required, as specified in 11.8 (DFS procedures); otherwise ~~not~~optionally present.

**Table 9-62—Association Request frame body**

The Supported Channels element is present if dot11SpectrumManagementRequired is true and dot11ExtendedChannelSwitchActivated is false.

The Supported Channels element is optionally present, otherwise.

**Table 9-64—Reassociation Request frame body**

The Supported Channels element is present if dot11SpectrumManagementRequired is true and dot11ExtendedChannelSwitchActivated is false.

The Supported Channels element is optionally present, otherwise.

**9.4.2.17 Supported Channels element**

The Supported Channels element contains a list of channel subbands ~~(from those channels defined in 17.3.8.4.3 (Channelization))~~ in which a STA is capable of operating.

[…]

~~The use of the Supported Channels element is described in 11.8.2 (Association based on supported channels) and 11.8.8 (Selecting and advertising a new channel).~~

**Table 9-519—Mesh Peering Open frame Action field format**

The Supported Channels element is present if dot11SpectrumManagementRequired is true and dot11ExtendedChannelSwitchActivated is false.

The Supported Channels element is optionally present, otherwise.

**10.39.12.2.1 Channel access rules**

An EDMG STA shall not transmit an EDMG PPDU to a peer EDMG STA over a channel that is not supported by the peer STA as indicated in the Supported Channels ~~field~~subelement in the peer STA’s EDMG Capabilities element.

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

The decision to switch to a new operating channel in an infrastructure BSS shall be made only by the AP. An AP may make use of the information in Supported Channels elements and the results of measurements undertaken by the AP and other STAs in the BSS to assist the selection of the new channel.

**11.8.8.4.1 General**

A mesh STA may make use of the information in Supported Channels elements, Supported Operating Classes

elements, and the results of measurements undertaken by the mesh STAs in the MBSS to assist the selection of

the new channel.

**11.8.8.6 Selecting and advertising a new channel in a DMG BSS**

The decision to switch to a new operating channel in a DMG BSS shall be made only by an AP or PCP. An AP

or PCP may make use of the information in received Supported Channels elements and the results of

measurements undertaken by the AP or PCP and other STAs in the BSS to assist the selection of the new

channel.

**11.20.6.1 General**

The STA shall include a Supported Channels element and a Supported Operating Classes element in all TDLS Setup Request and TDLS Setup Response frames that have a TDLS Channel Switching subfield equal to 1. The Supported Channels element shall indicate the channels supported for the current operating class. The STA shall include only channels in the Supported Channels element for which it can adhere to the local power constraint.

**B.4.10 Spectrum management extensions**

SM3 Power Capability and Supported Channels elements in (Re)Association Request and Response frames

CFSM:M

NOT CFSM:O

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3510 in <this document>, which clarify the usage of the Supported Channels element.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3338  Mark RISON | Sometimes it's "The BSS Load element is optionally present if  dot11QosOptionImplemented and dot11QBSSLoadImplemented" and sometimes "is present". Also a DMG STA is a QoS STA | At 737.31 change "The BSS Load element is optionally present if  dot11QosOptionImplemented and dot11QBSSLoadImplemented are  both true; otherwise not present.(#1598-Ed1)" to "The BSS Load element is present if  dot11QBSSLoadImplemented is true; otherwise not present.(#1598-Ed1)" |

Discussion:

Solomon TRAININ has clarified that:

The general approach in the DMG is to have an alternative way to deliver elements. This element same like some others may be delivered in the Announce frame instead or in addition to the DMG beacon

[Note: it doesn’t in fact seem to be possible to deliver a BSS Load element in an Announce frame. Something for D3.0!]

So the element should remain optional in DMG beacons. But it’s mandatory in Probe Responses sent by a DMG AP (or indeed a PCP).

It is also the case that DMG APs are QoS STAs, so checking dot11QosOptionImplemented is otiose. Ditto for VHT APs.

Dave GOODALL has clarified that:

It is optional for S1G to support BSS Load. We would typically put the element in a Probe Response but it is optional to put it in an S1G Beacon.

So this is the same behaviour as for DMG.

Proposed changes:

Change at 697.25 (in Table 9-60—Beacon frame body) and 725.15 (in Table 9-67—Probe Response frame body):

The Extended BSS Load element is optionally present if

~~dot11QosOptionImplemented,~~ dot11QBSSLoadImplemented~~,~~ and

dot11VHTOptionImplemented are both true.

Change at 737.31 (in Table 9-73—DMG Beacon frame body):

The BSS Load element is optionally present if

~~dot11QosOptionImplemented and~~ dot11QBSSLoadImplemented ~~are~~

~~both~~is true; otherwise not present.

Change at 4903.3 (in C.3 MIB):

dot11QBSSLoadImplemented OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute is available only at a~~n~~ QoS AP or PCP. This attribute, when true, indicates that the AP or PCP ~~implementation is capable of generating and transmitting~~transmits the BSS ~~l~~Load element in ~~the~~ Beacon frames (non-DMG non-S1G AP only) and Probe Response frames, and optionally in DMG Beacon frames (DMG AP or PCP only) and S1G Beacon frames (S1G AP only); optionally transmits the Extended BSS Load element in Beacon and Probe Response frames (VHT AP only); and optionally transmits the HE BSS Load element in Beacon and Probe Response frames (HE AP only). These elements are not transmitted~~The capability is disabled~~, otherwise."

::= { dot11StationConfigEntry 36 }

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3338 in <this document>, which make changes in the suggested direction (including recognising VHT and DMG APs as necessarily QoS APs), but keep the BSS Load element optional in DMG beacons. The description of the dot11QBSSLoadImplemented attribute is aligned with Clause 9.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3541  Mark RISON  C.3 | Can read-create MIB attributes have a DEFVAL? What does read-create mean anyway? | Delete DEFVAL lines for MIB attributes that are read-create |

Discussion:

Here are examples:

dot11PPEThresholdsMappingStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The status column used for creating, modifying, and deleting instances of the columnar objects in the PPE thresholds mapping table."

DEFVAL { active }

::= { dot11PPEThresholdsMappingsEntry 6 }

dot11RMRqstDuration OBJECT-TYPE

SYNTAX Unsigned32

UNITS "TUs"

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity when requesting a

measurement.

Changes take effect when dot11RMRqstRowStatus is set to Active.

This attribute indicates the preferred or mandatory measurement duration

for this Measurement Request. This attribute is ignored if dot11RMRqstType = LCI or Measurement Pause."

DEFVAL { 0 }

::= { dot11RMRequestEntry 12 }

RFC 2578 (Structure of Management Information Version 2 (SMIv2)) says:

The MAX-ACCESS clause, which must be present, defines whether it

makes "protocol sense" to read, write and/or create an instance of

the object, or to include its value in a notification. This is the

maximal level of access for the object. (This maximal level of

access is independent of any administrative authorization policy.)

The value "read-write" indicates that read and write access make

"protocol sense", but create does not. The value "read-create"

indicates that read, write and create access make "protocol sense".

The value "not-accessible" indicates an auxiliary object (see Section

7.7). The value "accessible-for-notify" indicates an object which is

accessible only via a notification (e.g., snmpTrapOID [5]).

These values are ordered, from least to greatest: "not-accessible",

"accessible-for-notify", "read-only", "read-write", "read-create".

If any columnar object in a conceptual row has "read-create" as its

maximal level of access, then no other columnar object of the same

conceptual row may have a maximal access of "read-write". (Note that

"read-create" is a superset of "read-write".)

and:

The DEFVAL clause, which need not be present, defines an acceptable

default value which may be used at the discretion of an agent when an

object instance is created. That is, the value is a "hint" to

implementors.

During conceptual row creation, if an instance of a columnar object

is not present as one of the operands in the correspondent management

protocol set operation, then the value of the DEFVAL clause, if

present, indicates an acceptable default value that an agent might

use (especially for a read-only object).

Note that with this definition of the DEFVAL clause, it is

appropriate to use it for any columnar object of a read-create table.

It is also permitted to use it for scalar objects dynamically created

by an agent, or for columnar objects of a read-write table

dynamically created by an agent.

and:

For newly-defined conceptual rows which allow the creation of new

object instances and/or the deletion of existing object instances,

there should be one columnar object with a SYNTAX clause value of

RowStatus (a textual convention defined in [[3](https://www.rfc-editor.org/rfc/rfc2578.html#ref-3)]) and a MAX-ACCESS

clause value of read-create. By convention, this is termed the

status column for the conceptual row.

Proposed resolution:

REJECTED

RFC 2578 specifies that read-create means that “read, write and create access make "protocol sense"” (and requires that read-write not be used for a table if read-create is used). It also specifies that a DEFVAL can be used “for any columnar object of a read-create table”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3290  Mark RISON | "ERP-DSSS modes" is not clear since ERP-DSSS is itself defined as a mode of a PHY. Ditto CCK and OFDM | Use better terminology |

Discussion:

Instances (note no instances of “ERP-CCK mode”):

18.1.3: For example, a BSS could operate in an ERP-OFDM-only mode, a mixed mode of ERP-OFDM and ERP-DSSS/CCK, or a mixed mode of ERP-DSSS/CCK and non-ERP. When options are enabled, combinations are also allowed. [Arguably is about the mode of the BSS]

18.3.2.4: The format, preamble, and headers for the ERP-OFDM PPDU are described in 17.3.2 (PPDU format) to 17.3.5 (DATA field). For the ERP-OFDM modes, the DATA field that contains the SERVICE field, the PSDU, the TAIL bits, and the PAD bits shall follow 17.3.5 (DATA field).

For ERP-OFDM modes, an ERP PPDU is (#14)immediately followed by a period of no transmission with a duration of aSignalExtension(#14)

18.4.7.3: The transmit spectral mask for the ERP-OFDM modes shall follow 17.3.9.3 (Transmit spectrum mask) and is shown in Figure 17-13 (Transmit spectrum mask for 20 MHz transmission) therein. The transmit spectral mask for the ERP-DSSS modes shall follow 16.3.7.4 (Transmit spectrum mask) and is shown in Figure 16-8 (Transmit spectrum mask) therein.

18.4.8.1: Subclause 18.4.8 (PHY receive specifications) describes the receive specifications for the PHY sublayer. The receive specification for the ERP-OFDM modes shall follow 17.3.10 (PHY receiver specifications) with the exception of the receiver maximum input level (17.3.10.5 (Receiver maximum input level)) and the adjacent channel rejection (17.3.10.3 (Adjacent channel rejection)). The receive specifications for the ERP-DSSS modes shall follow 16.3.8 (PHY receiver specifications) with the exception of the receiver maximum input level (16.3.8.3 (Receiver maximum input level)).

18.4.8.2: The PER of the ERP-OFDM modes shall be less than 10% at a PSDU length of 1000 octets for the input levels of Table 17-18 (Receiver performance requirements) of 17.3.10 (PHY receiver specifications). […] The PER for ERP-CCK shall be as specified in 16.3.8.2 (Receiver minimum input level sensitivity).

18.4.8.3: The adjacent channel rejection of the ERP-DSSS modes shall follow 16.3.8.4 (Receiver adjacent channel

rejection).

Proposed changes:

18.1.3: For example, a BSS could operate in an ERP-OFDM-only mode, a mixed mode of ERP-OFDM and ERP-DSSS/CCK, or a mixed mode of ERP-DSSS/CCK and non-ERP. When options are enabled, combinations are also allowed. *[No change]*

18.3.2.4: The format, preamble, and headers for the ERP-OFDM PPDU are described in 17.3.2 (PPDU format) to 17.3.5 (DATA field). For ERP-OFDM PPDUs, the DATA field that contains the SERVICE field, the PSDU, the TAIL bits, and the PAD bits shall follow 17.3.5 (DATA field).

An ERP-OFDM PPDU is (#14)immediately followed by a period of no transmission with a duration of aSignalExtension(#14)

18.4.7.3: The transmit spectral mask for ERP-OFDM PPDUs shall follow 17.3.9.3 (Transmit spectrum mask) and is shown in Figure 17-13 (Transmit spectrum mask for 20 MHz transmission) therein. The transmit spectral mask for ERP-DSSS PPDUs shall follow 16.3.7.4 (Transmit spectrum mask) and is shown in Figure 16-8 (Transmit spectrum mask) therein.

18.4.8.1: Subclause 18.4.8 (PHY receive specifications) describes the receive specifications for the PHY sublayer. The receive specification for ERP-OFDM PPDUs shall follow 17.3.10 (PHY receiver specifications) with the exception of the receiver maximum input level (17.3.10.5 (Receiver maximum input level)) and the adjacent channel rejection (17.3.10.3 (Adjacent channel rejection)). The receive specification for ERP-DSSS PPDUs shall follow 16.3.8 (PHY receiver specifications) with the exception of the receiver maximum input level (16.3.8.3 (Receiver maximum input level)).

18.4.8.2: The PER for ERP-OFDM PPDUs shall be less than 10% at a PSDU length of 1000 octets for the input levels of Table 17-18 (Receiver performance requirements) of 17.3.10 (PHY receiver specifications). […] The PER for ERP-CCK PPDUs shall be as specified in 16.3.8.2 (Receiver minimum input level sensitivity).

18.4.8.3: Adjacent channels at 2.4 GHz are defined to be at ± 25 MHz spacing. ***<para break>***

For ERP-OFDM PPDUs, the adjacent channel rejection shall be measured by setting the desired signal’s strength 3 dB above the rate-dependent sensitivity specified in Table 17-18 (Receiver performance requirements) of 17.3.10 (PHY receiver specifications) […]

The adjacent channel rejection for ERP-DSSS PPDUs shall follow 16.3.8.4 (Receiver adjacent channel

rejection).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3290 in <this document>, which refer to ERP PPDUs rather than modes, and add flavours where missing.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3719  Mark RISON  C.3 | dot11RSNAConfigGroupRekeyPackets should be stated to apply only if dot11RSNAConfigGroupRekeyMethod is packetBased(3) or timepacketBased(4) | As it says in the comment |

Discussion:

We have:

dot11RSNAConfigGroupRekeyTime OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

UNITS "seconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

The time after which the (#1980)(#1509)GTK is (#1382)refreshed (by rekeying). The timer starts at the moment the GTK was set using the MLME-SETKEYS.request primitive."

DEFVAL { 86400 } -- once per day

::= { dot11RSNAConfigEntry 6 }

dot11RSNAConfigGroupRekeyPackets OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

UNITS "1000 packets"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

A packet count after which the (#1980)(#1509)GTK is (#1382)refreshed (by rekeying). The packet counter starts at the moment the GTK was set using the MLME-SETKEYS.request primitive and it counts all packets encrypted using the current GTK."

::= { dot11RSNAConfigEntry 7 }

but these only apply for certain values of dot11RSNAConfigGroupRekeyMethod.

Proposed changes:

Change from 4952.15 as follows:

dot11RSNAConfigGroupRekeyTime OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

UNITS "seconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

The time after which the (#1980)(#1509)GTK is (#1382)refreshed (by rekeying), if dot11RSNAConfigGroupRekeyMethod is timeBased(2) or timepacketBased(4). The timer starts at the moment the GTK was set using the MLME-SETKEYS.request primitive."

DEFVAL { 86400 } -- once per day

::= { dot11RSNAConfigEntry 6 }

dot11RSNAConfigGroupRekeyPackets OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

UNITS "1000 packets"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

~~A~~The packet count after which the (#1980)(#1509)GTK is (#1382)refreshed (by rekeying), if dot11RSNAConfigGroupRekeyMethod is packetBased(3) or timepacketBased(4). The packet counter starts at the moment the GTK was set using the MLME-SETKEYS.request primitive and it counts all packets encrypted using th~~e current~~at GTK."

::= { dot11RSNAConfigEntry 7 }

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3719 in <this document>, which make the changes requested.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3409  Mark RISON | CID 1927: add a NOTE to say that the SCRAMBLER\_INITIAL\_VALUE is equal to the value in the SERVICE field after scrambling | As it says in the comment |

Discussion:

I think Youhan KIM presented some figures to demonstrate that the initial value of the scrambler (which is what the transmitter cares about) is also the value in the SERVICE field after scrambling (which is what the receiver cares about) is. However, I can’t find these (not in 22/0990 for instance).

In any case, the point is that the receiver doesn’t care about the initial value of the scrambler at the transmitter, the receiver cares about the value in the SERVICE field after scrambling (because that’s what’s used for e.g. MU-RTS/CTS). In general this is made clear through wording like “(the first 7 bits received in the SERVICE field prior to descrambling)”, but not always.

Proposed changes:

Change from 3180.45 as follows:

During reception, an HE STA shall generate the RXVECTOR parameter SCRAMBLER\_INITIAL\_VALUE as the ~~integer representation of the first 7 bits of the scrambling sequence, with the first bit of the scrambling sequence being the LSB of the SCRAMBER\_INITIAL\_VALUE~~ value in the first 7 bits of the SERVICE field prior to descrambling.

Change “Service field” to “SERVICE field” at 559.36/37, 1739.44, 1793.23, 3579.10, 3658.43, 3659.20, 3687.39.

Delete the second “]” at 559.37.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3409 in <this document>, which clarify that on rx the value is the SERVICE field prior to descrambling, and fix the case of “SERVICE field”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3795  Xiangxin GU  B.4.4.2  4651.16 | not CFDMG:O or not CFDMG:M for CF-End frame? | as commented |

Discussion:

It is indeed the case that a M/O indication is missing:



CF-End can be used to truncate a TXOP under EDCA, but I am not aware of any situations in which CF-End transmission is mandatory, at least when disregarding deprecated/obsolete features. I find evidence that CF-End can be used with DMG, so I am not sure what the “not CFDMG” pertained to. However, FR16 is a reminder that CF-End does not apply to OCB operation.

Proposed resolution:

REVISED

At the referenced location change “not CFDMG” to “NOT CFOCB:O”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3321  Mark RISON  C.3 | The DESCRIPTION of dot11SPIdleTimeout is far too generic. This is a DMG service period thing only | As it says in the comment |

Discussion:

dot11SPIdleTimeout is only used in these subclauses:

* 10.39.6.7 Service period recovery (under 10.39.6 Channel access in scheduled DTI (under 10.39 DMG and CMMG channel access))
* 11.3.5.2 Non-AP and non-PCP STA association initiation procedures [in a DMG list item]
* 11.3.5.4 Non-AP and non-PCP STA reassociation initiation procedures [in a DMG list item]

However, only DMG is mentioned, not CMMG, in those subclauses, so this seems to be a DMG-only thing.

Proposed changes:

Change from 5283.40 as follows:

dot11SPIdleTimeout OBJECT-TYPE

SYNTAX Unsigned32 (1..100000)

UNITS "microseconds"

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.

This attribute~~e SPIdleTimeout subfield~~ indicates the time during which a DMG STA expects to receive a frame from its partner STA."

DEFVAL { 200 }

::= { dot11DMGOperationEntry 9 }

Proposed resolution:

REVISED

At 5283.50 change “The SPIdleTimeout subfield indicates time during which a STA” to “This attribute indicates the time during which a DMG STA”.

At 5283.34 change “The MinPPDuration subfield” to “This attribute”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3200  Mark RISON  C.3 | "The default is" should not appear in the DESCRIPTION, but in a DEFVAL | As it says in the comment |

Discussion:

As it says in the comment, we have DEFVAL for defaults.

Proposed changes:

REVISED

In dot11StationID at 4894.59 delete “Its syntax is MAC address, and the default value is the STA's assigned, unique MAC address.” and after the DESCRIPTION add “DEFVAL { the STA's MAC address }”.

In dot11RMMeasurementPilotPeriod at 4907.3 delete “The default period is 25% of dot11BeaconPeriod.” and after the DESCRIPTION add “DEFVAL { dot11BeaconPeriod / 4 }”.

In dot11RSNAConfigGroupRekeyMethod at 4951.55 delete “The default is time-based, once per day.”

In dot11EDMGOptionImplemented at 5238.61 delete “The default value of this attribute is false.”

In dot11QAPEDCATableMandatory at 5275.57 delete “The default value for this parameter is false.” and after the DESCRIPTION add “DEFVAL { false }”.

In dot11NonAPStationAuthMaxVoiceRate at 5378.41 delete “, which is the default value,”. Ditto for dot11NonAPStationAuthMaxVideoRate, dot11NonAPStationAuthMaxBestEffortRate, dot11NonAPStationAuthMaxBackgroundRate, dot11NonAPStationAuthMaxHCCAHEMMRate, dot11NonAPStationAuthHCCAHEMMDelay, dot11NonAPStationAuthMaxSourceMulticastRate.

What about things like

See Table 9-192

(Default EDCA Parameter Set element (#1660)parameters

if dot11OCBActivated is false and the STA is a non-sensor STA(#251)) and

Table 9-193 (Default EDCA parameter set for STA operation if dot11OCBActi-

vated is true).

?

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3493  Mark RISON | The interpretation of the Key ID field in KDEs is not specified | Add sentences of the form "The Key ID field contains ..." |
| CID 3494  Mark RISON | The interpretation of some of the fields in KDEs is not specified, e.g. GTK in GTK KDE, MAC Address in MAC Address KDE, | Add sentences of the form "The <blah> field contains ..." |

Discussion:

As these comments say, some KDE fields are not described. Ditto some TK subelement fields.

Also, “Key ID” should have lowercase “key” when not about the name of a field etc., and not at the start of a sentence etc.

Miscellaneous additional small horrors have come to light in the course of examining these issues.

Proposed changes:

At 1038.46 add a para “The Key ID field contains the GTK key ID.”

At 2905.6 add a para “The Key ID field contains the GTK key ID.”

At 2905.12 add a para “The GTK field contains the GTK.”

At 2905.22 add a para “The MAC Address field contains a MAC address.”

At 2905.31 add a para “The PMKID field contains a PMKID.”

At 2905.40 add a para “The Key Nonce field contains a key nonce.”

At 2905.41 change “The Key Lifetime value is expressed in seconds and uses big endian octet order.” to “The Key Lifetime field contains a key lifetime in seconds, in big endian octet order.”

At 2905.45 delete “(in seconds)”.

At 2905.51 change “The Error Type field is in big endian octet order.” to “The Error Type field contains an error type, in big endian octet order.”

At 2906.12 add three paras “The Key ID field contains the IGTK key ID.”, “The IPN field contains the IPN.” and “The IGTK field contains the IGTK.” Move the sentence “The IPN corresponds…” above to the end of the second new para.

At 2908.6 add a para “The Key ID field contains the BIGTK key ID.”

At 2908.10 add a para “The BIGTK field contains the BIGTK.”

At 2908.21 add a para “The Key ID field contains the WIGTK key ID.”

At 2908.26 add a para “The WIGTK field contains the WIGTK.”

At 1038.35 change “The GTK subelement Key Info subfield” to “The Key Info subfield”.

At 2908.16 change “(Length-12)” to “variable”.

At 2908.18 change “WIGTK KDE” to “WIGTK KDE format”.

At 1039.16 change “indicates the value of the BIP key identifier” to “contains the IGTK key ID”.

At 1040.1 change “indicates the value of the BIGTK identifier” to “contains the BIGTK key ID”.

At 1040.25 change “indicates the WIGTK identifier” to “contains the WIGTK key ID”.

At 1634.15 change “indicates the value of the BIP key identifier” to “contains the IGTK key ID”.

At 1634.41 change “indicates the value of the BIGTK identifier” to “contains the BIGTK key ID”.

Change “Key ID” to “key ID” at 492.5/6, 978.56/57, 1046.11(2x)/12, 1159.1, 1320.54, 1321.14 (rightmost), 1476.47 (rightmost), 1722.64, 2313.49, 2841.8/10, 2847.31 (rightmost, also delete “value”), 2859.49/58/59, 2871.8, 2876.60/61, 2881.43/44/45/48/50/51/53, 2907.18 (rightmost), 2917.14/15/18(2x)/63, 3034.41, 4572.17(2x, also delete “value”)/53/54(also delete “value”), 4573.13/14 (also delete “value”), 4575.50/56, 4576.2,

At 338.57/59 change “key identifier” to “PMK identifier”.

Change at 1258.53 as follows:

The Number of Public Key Identifiers subfield ~~lists~~contains the number of Public Key Identifier fields that are present in the Public Key Identifiers field in the FILS Indication element. When the Number of Public Key Identifiers subfield is 0, the Public Key Identifiers field is not present in the FILS Indication element. Each Public Key Identifier field is formatted per Figure 9-729 (Public Key Identifier field format). Up to seven Public Key Identifier~~s~~ fields may be carried in a FILS Indication element.

At 1258.24 change “Public Key Identifier” to “Public Key Identifiers”.

Change at 2911.16 as follows:

{Key Data} is a sequence of zero or more elements and KDEs, concatenated and contained in the Key Data field, where

RSNE is the RSNE, described in 9.4.2.24 (RSNE)

RSNE[KeyName] is the RSNE, with the PMKID List field set to KeyName

GTK[N] is the GTK KDE, with the ~~k~~Key ID~~identifier~~ field set to N (The key ID~~identifier~~ specifies which index is used for this GTK. Index 0 shall not be used for GTKs, except in mixed environments, as described in 12.7.1 (Key hierarchy). (#1457)Index 3 shall not be used for GTKs)

FTE is the (#1776)FTE, described in 9.4.2.47 (FTE(#1776))

MDE is the (#1776)MDE, described in 9.4.2.46 (MDE(#1776))

TIE[IntervalType] is a (#1776)TIE of type IntervalType, as described in 9.4.2.48 (TIE(#1776)), containing e.g., for type KeyLifetime, the lifetime of the FT key hierarchy

IGTK[M] is the IGTK KDE, with the ~~k~~Key ID~~identifier~~ field set to M

IPN is the current IGTK replay counter value provided by the IGTK KDE

BIGTK[Q] is the BIGTK KDE, with the ~~k~~Key ID~~identifier~~ field set to Q

BIPN is the current BIGTK replay counter value provided by the BIGTK KDE

(11ba)WIGTK[R] is the WIGTK KDE, with the ~~k~~Key ID~~identifier~~ field set to R

(11ba)WIPN is the current WIGTK replay counter value provided by the WIGTK KDE

PMKID is ~~of type~~the PMKID KDE and is the ~~key~~PMK identifier used during the 4-way ~~PTK~~ handshake for PMK identification

OCI KDE is ~~a~~the OCI KDE ~~containing operating channel information~~

RSNXE is the RSNXE, described in 9.4.2.241 (RSNXE(#1776))

PMKID is the PMK identifier for~~identifies~~ the PMKSA selected by the Authenticator

“{a} or {b}” means that exactly one of either {a} or {b} is present as the {Key Data}

Change “key identifier” to “key ID” at 2912.42, 2916.25/50, 2922.50/54/58/62, 2923.61/62, 2924.1/3.

Change “TK identifier” to “TK key ID” at 1752.46/49, 2845.53/57/60.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3493 and 3494 in <this document>, which make the changes requested by the commenter, and fix related issues.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3631  Mark RISON  12 | The setting of the Secure bit in M1 and M2 of a rekeying 4WH is not clear | Specify that it is indeterminate, and hence must be ignored by the receiver |
| CID 3596  Mark RISON  12.7.6.1 | It is not clear whether 12.7.6.1 General applies to rekeying, e.g. whether the Secure bit is 0 in M1 and M2 even in rekeying (when it has the old PTK and GTK). Ditto 12.7.2.b)7) Note that if the Secure bit is 1 in M2 rekeying then the Key Information field is the same for M2 and M4 | Clarify the rules for rekeying |

Discussion:

In 12.7.2 we have:

Secure (bit 9) indicates whether the Authenticator and the Supplicant share a PTKSA. It is set to 0 in messages 1 and 2 of the 4-way handshake if the Authenticator and the Supplicant do not share a PTKSA. Otherwise, it is set to 1.

NOTE 1—Some deployed Authenticator and Supplicant implementations set the Secure bit to 0 in messages 1 and 2 of the 4-way handshake that is used for PTK rekeying even when they already share a previously generated PTKSA. In the interests of interoperability, implementations might ignore the Secure bit in received frames.

NOTE 2—The Secure bit is set to 1 in messages 3 and 4 of the 4-way handshake.

I think we ended up with NOTE 1 as a compromise between saying “it shall be 1 when PTK rekeying (because a PTKSA exists at that point)” and “it shall be ignored when PTK rekeying (because some existing implementations set it to 0)”.

However, 12.7.6.1 suggests the Secure bit is always set to 0 in M1 and M2:

Message 1: Authenticator → Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID})

Message 2: Supplicant → Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE} or

{RSNE, OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE})

And in fact so does 12.7.6.2/3:

Message 1 uses the following values for each of the (#1836)EAPOL-Key PDU fields:

[…]

Secure = 0

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

[…]

Secure = 0 – same as message 1

And in fact various state machines assume 0. And indeed fail to cover all the messages!

Also, as CID 3596 points out, the statements about how you can distinguish M1-M4 and G1-G2 are no longer correct.

Proposed changes:

Change 12.7.6.1 as follows:

Message 1: Authenticator → Supplicant: EAPOL-Key(0 or 1,0,1,0,P,0,0,ANonce,0,{} or {PMKID})

Message 2: Supplicant → Authenticator: EAPOL-Key(0 or 1,1,0,0,P,0,0,SNonce,MIC,{RSNE} or

{RSNE, OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE})

Change 12.7.6.2 as follows:

Message 1 uses the following values for each of the (#1836)EAPOL-Key PDU fields:

[…]

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

Change 12.7.6.3 as follows:

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

[…]

Secure = 0 in initial 4-way handshake, or 1 when PTK rekeying (but see 12.7.2) ~~– same as message 1~~

In the list in 12.7.9.3 Supplicant state machine variables immediately before SNonce add:

— *PTKSAEstablished*. The Supplicant sets this variable to 0 on initialisation and to 1 when a PTKSA has been established.

Change at 2935.52 from:

**if** *A* = 1 && *State* ≠ Failed **then**

Send EAPOL-Key(0,1,0,0,K,0,0,TSNonce,MIC(TPTK),{RSNE})

**endif**

**if** UpdatePTK = 1 **then**

*MLME-SETPROTECTION.request(TA, Rx\_Tx)*

**endif**

to:

**if** *State* ≠ Failed **then**

**if** *K* = P && *M* = 0 && *A* = 1 **then**

Send EAPOL-Key(*PTKSAEstablished*,1,0,0,P,0,0,TSNonce,MIC(*TPTK*),{RSNE}) // M2

**else if** *K* = P && *M* = 1 && *A* = 1 **then**

Send EAPOL-Key(1,1,0,0,P,0,0,0,MIC(*TPTK*),{}) // M4

**else if** *K* = G && *A* = 1 **then**

Send EAPOL-Key(1,1,0,0,G,0,0,0,MIC,{}) // G2

**else**

*State* ← FAILED

**endif**

**endif**

**if** *State* ≠ Failed && *UpdatePTK* = 1 **then**

*MLME-SETPROTECTION.request(TA, Rx\_Tx)*

*PTKSAEstablished* ← 1

**endif**

At 2934.39 romanise “*P”*.

At 2934.42 change “–“ to “//”.

At 2935.28 change “*KeyData* = GTK” to “*K* = G”.

At 2937.28 change

Send EAPOL-Key( 0, 0, 1, 0, P, 0, 0, ANonce, 0, {})

to:

Send EAPOL-Key(PTK = 0 ? 0 : 1, 0, 1, 0, P, 0, 0, ANonce, 0, {}) // M1

At 2937.44 append “ // M3” after “Send EAPOL-Key(1, 1, 1, Pair, P, 0, RSC, ANonce, MIC(PTK),

{RSNE, GTK[N], IGTK [M]})”.

At 2939.16 append “ // G1” after “Send EAPOL-Key (1, 1, 1, !Pair, G, 0, RSC, 0, MIC(PTK), {GTK[GN]})” and delete the space before the opening paren.

Change 12.7.6.8 as follows:

It is critical to the correctness of the 4-way handshake that at least one bit differs in each message. Within the 4-way handshake, ~~message 1 can be recognized as the only one in which the (#1829)Key MIC Present bit is 0, meaning message 1 does not include the MIC, while message 2 to message 4 do. Message 3 differs from message 2 by not asserting the Ack bit and from message 4 by asserting the Ack Bit. Message 2 differs from message 4 by including the RSNE~~ the messages are distinguished by the Key MIC and Encrypted Key Data bits (not both 0 except in message 1), the Key Ack bit (1 in message 1 and message 3 only) and the presence of RSNEs and/or Multi-Band elements (in message 2 but not in message 4).

~~Request messages are distinct from 4-way handshake messages because the former assert(#1826) the Request bit and 4-way handshake messages do not. Group key handshake messages are distinct from 4-way handshake messages because they assert a different key type.~~

Group key handshake messages are distinct from 4-way handshake messages because they set the Key Type bit differently (0 in group key handshake messages only), and are distinguished from each other by the Key Ack bit (1 in message 1 only). Request messages are distinct from 4-way handshake and group key handshake messages because they set the Request bit differently (1 in request messages only).

At 2918.47 change “none require” to “none required”.

Change 12.7.9.3 as follows:

— AuthenticationRequest. The Supplicant sets this variable to true if its STA’s IEEE 802.11 management entity reports that an SSID is to be authenticated. ~~This might be on association or at other times.~~

Change 12.7.10.3 as follows:

— AuthenticationRequest. This variable is set to true by the STA’s IEEE 802.11 management entity in order to authenticate an association. ~~This can be set to true when the STA associates or at other times.~~

At 2950.32, restore Figure 12-56—FILS Shared Key authentication to what it was in D1.0.

At 2969.57 insert a para:

The same FT 4-way handshake is performed for PTK rekeying, except that the Secure bit is set in the first two messages (but see 12.7.2).

In Figure 13-15—R1KH state machine, including portions of the SME (part 1) move “PTK‑RekeyRequest = false” from the FT-INIT-R1\_SA state to the end of the FT-PTK-START state and in the latter change:

Send EAPOL-Key (0, 0, 1, 0, P, 0, 0, ANonce, 0, {})

to (note deletion of space before the opening paren):

Send EAPOL-Key(PTK-RekeyRequest ? 1 : 0, 0, 1, 0, P, 0, 0, ANonce, 0, {}) // M1

At 2997.46 append “ // M3” after “Send EAPOL-Key (1, 1, 1, 1, P, 0, 0, ANonce, MIC, {RSNE[PMKR1Name],

MDE, GTK[N],  IGTK[M], BIGTK[Q], FTE, TIE[ReassociationDeadline], TIE[KeyLifetime], RSNXE})” and delete the space before the opening paren.

In Figure 13-18—S1KH state machine, including portions of the SME (part 1):

* At the end of R1-START add “PTKRekeying = false”
* Add a new state FT-REKEY that sets “PTKRekeying = true” and then does UCT into FT-INIT-R1-SA
* Move the side arrow into FT-INIT-R1-SA to go into the new FT-REKEY
* In FT-PTK-START change “Send EAPOL-Key (0, 1, 0, 0, P, 0, SNonce, […])” to “Send EAPOL-Key(PTKRekeying ? 1 : 0, 1, 0, 0, P, 0, SNonce, […]) // M2” (note deletion of space before opening paren)

At 3002.36 append “ // M4” after “Send EAPOL-Key (1, 1, 0, 0, P, 0, 0, MIC-KCK)” and delete the space before the opening paren.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3631, 3596 in <this document>, which indicate that the Secure bit in M1 and M2 is not necessarily 0, and fix various issues with the security pseudocode/state machines.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3532  Mark RISON  12 | The row ordering in Table 12-7--Cipher suite key lengths seems haphazard | Sort alphabetically |

Discussion:

The reference is incorrect; it should be to Table 12-8:

**Table 12-8—Cipher suite key lengths**

|  |  |  |
| --- | --- | --- |
| **Cipher suite** | **Key length (octets)** | **TK\_bits (bits)** |
| TKIP | 32 | 256 |
| CCMP-128 | 16 | 128 |
| BIP-CMAC-128 | 16 | 128 |
| GCMP-128 | 16 | 128 |
| GCMP-256 | 32 | 256 |
| CCMP-256 | 32 | 256 |
| BIP-GMAC-128 | 16 | 128 |
| BIP-GMAC-256 | 32 | 256 |
| BIP-CMAC-256 | 32 | 256 |

It might be that this is historically the order in which these suites were added to the standard, but that’s not helpful to the reader.

Proposed changes:

Change Table 12-8 to have the following order:

**Table 12-8—Cipher suite key lengths**

|  |  |  |
| --- | --- | --- |
| **Cipher suite** | **Key length (octets)** | **TK\_bits (bits)** |
| BIP-CMAC-128 | 16 | 128 |
| BIP-CMAC-256 | 32 | 256 |
| BIP-GMAC-128 | 16 | 128 |
| BIP-GMAC-256 | 32 | 256 |
| CCMP-128 | 16 | 128 |
| CCMP-256 | 32 | 256 |
| GCMP-128 | 16 | 128 |
| GCMP-256 | 32 | 256 |
| TKIP | 32 | 256 |

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3532 in <this document>, which use alphanumeric order for Table 12-8 (Cipher suite key lengths).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3326  Mark RISON  9.4.1.9  755.21 | "Status code" (name of field) should be "Status Code" | I can provide locations |

Discussion:

There are 75x “Status code” and 354 “Status Code”.

Proposed resolution:

REVISED

Change “Status code” to “Status Code” at 712.15, 728.33, 730.18, 1535.7, 1674.5, 3011.44/47, 3013.11/13.

At 1089.37 change “The Status Code field contains the final IEEE 802.11 Status code, as defined in Table 9-78 (Status codes) in 9.4.1.9 (Status Code field), received at the end of the applicable operation.” to “The Status Code field contains the status code, as defined in Table 9-78 (Status codes) in 9.4.1.9 (Status Code field), received at the end of the applicable operation.”

At 1559.46, 1561.60 change “The Status Code values” to “The Status Code field values”.

At 1626.54 change “the Status code field value is not set to 5” to “the BTM Status Code field is not 5”.

At 1626.56 change “if the Status code subfield contains 0” to “if the BTM Status Code field is 0”.

At 1658.30, 1660.26 change “indicated” to “defined”.

At 2396.26 change “FMS Status code” to “FMS status code”.

At 2627.40 change “Status Code” to “Status Code field”.

At 2627.43 change “a Comeback Delay and Query Response Length both set to 0” to “Comeback Delay and Query Response Length fields both set to 0”.

At 2629.45 change “Status Code” to “Status Code field”.

At 2629.47 change “a GAS Comeback Delay set to 0 and a Query Response Length set to 0” to “and GAS Comeback Delay and Query Response Length fields both set to 0”.

At 2630.1 change “Status Code” to “Status Code field”.

At 2630.3 change “a GAS Comeback Delay set to 0 and a Query Response Length set to 0” to “and GAS Comeback Delay and Query Response Length fields both set to 0”.

At 2630.23 change “a status code equal to GAS\_QUERY\_TIMEOUT” to “a Status Code field set to GAS\_QUERY\_TIMEOUT”.

At 2630.57 change “with status code equal to GAS\_RESPONSE\_NOT\_RECEIVED\_FROM \_SERVER” to “with a Status Code field set to GAS\_RESPONSE\_NOT\_RECEIVED\_FROM\_SERVER”.

At 2825.33 change “a Transaction Sequence Number of 1 and a Status Code of SUCCESS or SAE\_HASH\_TO\_ELEMENT” to “a Transaction Sequence Number field set to 1 and a Status Code field set to indicate SUCCESS or SAE\_HASH\_TO\_ELEMENT”.

At 2826.21 change “a Transaction Sequence Number of 2 and a Status Code of SUCCESS” to “a Transaction Sequence Number field set to 2 and a Status Code field set to indicate SUCCESS”.

Change “Status code” to “status code” at 2831.43/46 (and delete “set to”)/51, 2832.11/13/19/22/33/37/44.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3291  Mark RISON  21.1  3387.4 | L\_DATARATE is missing in Table 21-1--TXVECTOR and RXVECTOR parameters (cf. CID 1057) | As it says in the comment |

Discussion:

CID 1057’s resolution was to add the following row to Table 27-1—TXVECTOR and RXVECTOR parameters for HE:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L\_DATARATE | FORMAT is NON\_HT | Indicates the rate used to transmit the PSDU in megabits per second.  Allowed values depend on the value of the NON\_HT\_MODULATION  parameter as follows:  ERP-DSSS: 1 and 2  ERP-CCK: 5.5 and 11  ERP-OFDM, NON\_HT\_DUP\_OFDM:  6, 9, 12, 18, 24, 36, 48, and 54  OFDM: 6, 9, 12, 18, 24, 36, 48, and 54 | Y | Y |
| Otherwise | Not present | | |

Note there was already an L\_LENGTH row, though this just xreffed back to earlier PHYs for non-HE:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L\_LENGTH | FORMAT is HE\_SU,  HE\_MU, or HE\_ER\_SU | Not present  NOTE—The LENGTH field of the L-SIG field for HE PPDU  is defined in Equation (27-11) using the TXTIME value  defined in 27.4.3 (TXTIME and PSDU\_LENGTH  calculation), which in turn depends on other parameters  including the TXVECTOR parameter APEP\_LENGTH. | N | N |
| FORMAT is HE\_TB | Indicates the value in the LENGTH field of the L-SIG field in  the range of 1 to 4095. The value is obtained from the  triggering frame to which the HE TB PPDU is a response. | Y | N |
| Otherwise | See corresponding entry in Table 19-1 (TXVECTOR and RXVECTOR  parameters) or Table 21-1 (TXVECTOR and RXVECTOR  parameters(#12)). | | |

Table 19-1—TXVECTOR and RXVECTOR parameters for HT already has L\_DATARATE (and L\_LENGTH), for NON\_HT, HT\_MF and HT\_GF formats.

Table 22-1—TXVECTOR and RXVECTOR parameters for TVHT already has L\_DATARATE (and L\_LENGTH), for NON\_HT and VHT formats.

But Table 21-1—TXVECTOR and RXVECTOR parameters has no L\_DATARATE (or L\_LENGTH).

Proposed changes:

In Table 21-1—TXVECTOR and RXVECTOR parameters, after the NON\_HT\_MODULATION row add the following:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L\_DATARATE | FORMAT is NON\_HT | Indicates the rate used to transmit the PSDU in megabits per second. The allowed values are 6, 9, 12, 18, 24, 36, 48, and 54. | Y | Y |
| Otherwise | Not present | | |
| L\_LENGTH | FORMAT is NON\_HT | See corresponding entry in Table 19-1 (TXVECTOR and RXVECTOR parameters). | Y | Y |
| Otherwise | Not present | | |

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3291 in <this document>, which add L\_DATARATE and L\_LENGTH parameters to the VHT TXVECTOR/RXVECTOR.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3262  Mark RISON  G.1  5528.12 | "BlockAck or BlockAckReq frame has the BA Ack Policy or BAR Ack Policy  Indicator field, respectively" -- no such fields | Delete " with the BAR Ack Policy  subfield equal to No Acknowledgment"" at 1727.55, "with the BA Ack Policy subfield set to 1 (representing  No Acknowledgment)" at 2002.15, "with the BAR Ack Policy subfield set to 1 (representing  No Acknowledgment)" at 2002.17, the delayed-no-ack row at 5528.12, "sent with the BAR/BA Ack Policy subfield set to No  Acknowledgment" at 5535.32, |

Discussion:

There are indeed no such fields.

Here are the proposed changes:

1727.55: At most one Multi-TID BlockAckReq frame ~~with the BAR Ack Policy subfield equal to No Acknowledgment~~.

2002.15/17: — BlockAck under an immediate policy ~~with the BA Ack Policy subfield set to 1 (representing~~

~~No Acknowledgment)~~

— BlockAckReq under an immediate policy ~~with the BAR Ack Policy subfield set to 1 (representing~~

~~No Acknowledgment)~~

5528.12: *~~delayed-no-ack~~* ~~BlockAck or BlockAckReq frame has the BA Ack Policy or BAR Ack Policy~~

~~Indicator field, respectively, equal to No Acknowlegement.~~

However, the things that use delayed-no-ack also need to be deleted:

5535.31:

(\* A frame-not-requiring-response-ampdu is a frame that does not require a response and can be sent within an A-MPDU. It is ~~one of the delayed BlockAck frames sent with the BAR/BA Ack Policy subfield set to No~~  ~~Acknowledgment, or~~ a Data frame that does not require an immediate ack~~,~~ or an Action No Ack frame. A frame-not-requiring-response may be included with any of the following sequences in any position, except the initial position when this contains a BlockAck frame or Multi-TID BlockAck frame: ppdu-bar, ppdu-ba-bar, ppdu-ba, ppdu-rd, ppdu-rd-bar, ppdu-ba-rd-bar, psmp-ppdu \*)

frame-not-requiring-response-ampdu =

**~~BlockAck~~**~~[+~~*~~HTC~~*~~]+~~*~~delayed-no-ack~~* ~~|~~

**~~BlockAckReq~~**~~[+~~*~~HTC~~*~~]+~~*~~delayed-no-ack~~* ~~|~~

**Data**[+*HTC*]+QoS+block-ack |

ma-no-ack-htc;

Proposed resolution:

REVISED

Make the changes proposed by the commenter and additionally at 5535.32 change “It is one of the delayed BlockAck frames sent with the BAR/BA Ack Policy subfield set to No Acknowledgment, or Data that does not require an immediate ack, or an Action No Ack frame.” to “It is a Data frame that does not require an immediate ack or an Action No Ack frame.” and delete the first two lines after the = (the ones starting BlockAck/BlockAckReq).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3089  John WULLERT  10.4  1820.18 | Notes 1 on this page (and Notes 1 and 2 on page 1821) seem to impose requirements without using normative language, which violates the spirit, but perhaps not the letter, of the rule that Notes cannot be normative. Furthermore, there are no matching requirements in the referenced sections, but rather the required mechanism for constructing the packet numbers will result in them being consecutive. | Revise to state "PN processing will generate consecutive PN numbers for constituent MPDUs of fragmented MSDUs (see 12.5.2.3.2 (PN processing) and 12.5.4.3.2 (PN processing))." |
| CID 3396  Mark RISON  10.4  1820.18 | "NOTE 1--Packet numbers for consecutive fragments of an MSDU or MMPDU in an RSNA are required to be  consecutive" should also cover A-MSDUs | Change "of an MSDU or MMPDU" to "of an MSDU, A-MSDU or MMPDU" at 1820.18 and 1821.40 |

Discussion:

With dynamic fragmentation A-MSDUs can now be fragmented too (this was missed in the PN and replay detection subclauses, too).

It is critical that the PNs of a fragmented MSDU/A-MSDU/MMPDU increment by exactly 1, otherwise you get one of the FragAttacks that made the headlines in 2021.

However, it is arguable that “consecutive” is not immediately obviously the same as “increment by 1”.

Proposed changes:

Change at 1820.18 as follows:

NOTE 1—Packet numbers for consecutive fragments of an MSDU, A-MSDU or MMPDU in an RSNA are required to ~~be consecutive~~increment in steps of 1 (see 12.5.2.3.2 (PN processing) and 12.5.4.3.2 (PN processing)).

Change at 1821.40 as follows:

NOTE 1—Packet numbers for consecutive fragments of an MSDU, A-MSDU or MMPDU in an RSNA are required to ~~be consecutive~~increment in steps of 1 (see 12.5.2.4.4 (PN and replay detection) and 12.5.4.4.4 (PN and replay detection) under d)).

Change at 2845.7 and 2854.49 as follows:

The receiver shall discard MSDUs, A-MSDUs and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1.

Change at 2587.5 as follows:

Dialog Token field values of consecutive Fine Timing Measurement frames shall ~~be consecutive~~increment in steps of 1

Proposed resolution:

REVISED

In NOTE 1 at 1820.18 and 1821.40 change “be consecutive” to “increment in steps of 1” and add “, A-MSDU” after “MSDU”. Add a full stop at the end of the sentence at 1821.40. At 2845.8 and 2854.50 add “, A-MSDUs” after “MSDUs”. At 2587.6 change “be consecutive” to “increment in steps of 1”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3312  Mark RISON  28.2.2  4237.54 | "If the CH\_BANDWIDTH parameter has two contiguous bits" -> has exactly two contiguous bits set to 1 and no other bits set to 1 | Change from line 54 to:  -- If the CH\_BANDWIDTH parameter has a single bit equal to 1 (#2349)(e.g., "01000000") or if the  CH\_BANDWIDTH parameter has exactly two bits equal to 1 and they are noncontiguous (e.g., "01001000") and the  CHANNEL\_AGGREGATION parameter is set to AGGREGATE, then NCB is set to 1.  -- If the CH\_BANDWIDTH parameter has exactly two bits equal to 1 and they are contiguous (e.g., "01100000") and the CHANNEL\_AGGREGATION parameter is set to AGGREGATE, then  NCB is set to 1. Otherwise, if the CHANNEL\_AGGREGATION parameter is set to  NOT\_AGGREGATE, then NCB is set to 2.  -- If the CH\_BANDWIDTH parameter has exactly three bits equal to 1 and they are contiguous (e.g., "00111000"), then NCB is set to 3.  -- If the CH\_BANDWIDTH parameter has exactly four bits equal to 1 and they are contiguous (e.g., "01111000") and the CHANNEL\_AGGREGATION parameter is set to AGGREGATE, then  NCB is set to 2. Otherwise, if CHANNEL\_AGGREGATION parameter is set to  NOT\_AGGREGATE, then NCB is set to 4. |
| CID 3313  Mark RISON  28.2.2  4237.54 | What about other combinations, e.g. 3 or 4 bits equal to 1, but not contiguous, or >4 bits equal to 1, or 2 bits equal to 1 and not contiguous and CHANNEL\_AGGREGATION not set to AGGREGATE? | As it says in the comment |
| CID 3386  Mark RISON  28.2.2  4237.54 | "If the CH\_BANDWIDTH parameter has a single bit equal to 1 (e.g., "01000000") or if the CH\_BANDWIDTH parameter has two non-continguous bits equal to 1 (e.g., "01001000") and the CHANNEL\_AGGREGATION parameter is set to AGGREGATE" precedence unclear | Add comma before "or" |

Discussion:

Yan XIN has provided the following information re EDMG:

* There are only two aggregation cases, 2.16+2.16 GHz and 4.32+4.32 GHz
* If more than 2 bits are set in CH\_BANDWIDTH they are necessarily contiguous
* No more than 4 bits can be set
* For the case that there are exactly 2 bits equal to 1 and these 2 bits are noncontiguous, CHANNEL\_AGGREGATION should be ignored
* “Channel bonding” is different from “channel aggregation”. Channel bonding is defined as two, three or four continuous channels, each 2.16 GHz, bonded together for wide band transmissions (max BW 4x2.16 GHz). Channel aggregation is defined as two contiguous or non-contiguous channels of 2.16 GHz or two contiguous channels of 4.32 GHz (two bonded 2.16 GHz channels), aggregated

Proposed changes:

Change 28.2.2 from:

The NCB parameter represents the number of contiguous (i.e., bonded) 2.16 GHz channels used for a transmission. The value of the CH\_BANDWIDTH and CHANNEL\_AGGREGATION parameters in the TXVECTOR and RXVECTOR define the value of the NCB parameter in the EDMG PHY definition throughout this clause as follows:

— If the CH\_BANDWIDTH parameter has a single bit equal to 1 (#2349)(e.g., “01000000”) or if the CH\_BANDWIDTH parameter has two noncontiguous bits equal to 1 (e.g., “01001000”) and the CHANNEL\_AGGREGATION parameter is set to AGGREGATE, then NCB is set to 1.

— If the CH\_BANDWIDTH parameter has two contiguous bits each of which is equal to 1 (e.g., “01100000”) and the CHANNEL\_AGGREGATION parameter is set to AGGREGATE, then NCB is set to 1. Otherwise, if the CHANNEL\_AGGREGATION parameter is set to NOT\_AGGREGATE, then NCB is set to 2.

— If the CH\_BANDWIDTH parameter has three contiguous bits each of which is equal to 1 (e.g., “00111000”), then NCB is set to 3.

— If the CH\_BANDWIDTH parameter has four contiguous bits each of which is equal to 1 (e.g., “01111000”) and the CHANNEL\_AGGREGATION parameter is set to AGGREGATE, then NCB is set to 2. Otherwise, if CHANNEL\_AGGREGATION parameter is set to NOT\_AGGREGATE, then NCB is set to 4.

to:

The NCB parameter represents the number of contiguous (i.e., bonded) 2.16 GHz channels used for a transmission. The value of the CH\_BANDWIDTH and CHANNEL\_AGGREGATION parameters in the TXVECTOR and RXVECTOR define the value of the NCB parameter in the EDMG PHY definition throughout this clause as follows:

NOTE—Between 1 and 4 bits are set in the CH\_BANDWIDTH parameter.

— If the CH\_BANDWIDTH parameter has exactly 1 bit equal to 1 (#2349)(e.g., “01000000”), then NCB is set to 1.

NOTE—The CHANNEL\_AGGREGATION parameter is ignored in this case.

— If the CH\_BANDWIDTH parameter has exactly 2 bits equal to 1, then:

—If the 2 bits are noncontiguous (e.g., “01001000”), then NCB is set to 1.

NOTE—The CHANNEL\_AGGREGATION parameter is ignored in this case.

— If the 2 bits are contiguous (e.g., “01100000”), then if the CHANNEL\_AGGREGATION parameter is set to AGGREGATE, NCB is set to 1, otherwise NCB is set to 2.

— If the CH\_BANDWIDTH parameter has exactly 3 bits equal to 1 (e.g., “00111000”), then NCB is set to 3.

NOTE—The 3 bits are necessarily contiguous in this case. The CHANNEL\_AGGREGATION parameter is ignored in this case.

— If the CH\_BANDWIDTH parameter has exactly 4 bits equal to 1 (e.g., “01111000”), then if the CHANNEL\_AGGREGATION parameter is set to AGGREGATE, NCB is set to 2, otherwise NCB is set to 4.

NOTE—The 4 bits are necessarily contiguous in this case.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CIDs 3312, 3313, 3386 in <this document>, which address the issues identified (note CHANNEL\_AGGREGATION ignored when two non-contiguous bits, bits necessarily contiguous if >2 set).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3488  Mark RISON  C.3  5136 | dot11WNMEventRsnaRprtRsnElement refers to "RSNE field" but should refer to "RSNE" | Change "RSNE field" to "RSNE" 3x on referenced page |

Discussion:

There is an RSNE field in the RSNA event report (see Figure 9-472—Event Report format for RSNA event). But the descriptions are rather confusing, especially since they talk of “the entire contents of the negotiated RSNE”. This itself is ambiguous: does it include the Element ID and Length fields? The wording “If the contents of the RSNE, with the exception of the pairwise cipher suite count and pairwise cipher suite list are not the same as those sent by the TDLS initiator STA in message 1 of this sequence” in 12.7.8.4.3 indicates that at least in this subclause “contents of the RSNE” is to be understood as excluding the Element ID and Length fields (since if the suite count differs the Length field will differ too).

TBD: What does “the negotiated RSNE” mean? The one sent last? The one sent last locally?

TBD: What about “All other fields in the second RSNE shall be identical to the first RSNE.(#190)” at 2906.57 [not clear: does the first RSNE have all suites or just one?], “all other fields of the RSNE shall be identical to the RSNE present in” on p. 2973 (2x) [for first, not sure if auth frame can contain a PMKID; for second beacon/prsp frame does not contain a PMKID so Length field will differ], “The RSNE shall be identical to the RSNE in the STA’s Beacon and Probe Response frames.” at 3035.14 [OK?]?

Proposed changes:

Change at 758.32 as follows:

Invalid ~~contents of~~ RSNE, other than unsupported RSNE version or invalid RSNE capabilities, AKMP or pairwise cipher.

Change at 1077.36 as follows:

The RSNE field contains the Information field ~~entire contents~~ of the negotiated RSNE at the time of the authentication attempt~~. The maximum length of the RSNE field is less than the maximum length of an RSNE, as defined in 9.4.2.24 (RSNE). If the length of the RSNE included here exceeds the maximum length of the RSNE field, the RSNE is~~, truncated to the maximum length allowed for the RSNE field if necessary.

Change at 2929.47 as follows:

If the ~~contents of the~~ RSNE does not indicate an AKM of TPK handshake (suite type 00-0F-AC:7), the TDLS responder STA shall reject the request with status code STATUS\_INVALID\_AKMP.

Change at 2931.4 as follows:

If the Information field ~~contents of~~ the RSNE, with the exception of the pairwise cipher suite count and pairwise cipher suite list, ~~are~~is not the same as ~~those~~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.

Change at 2932.7 as follows:

Validate that ~~the contents of~~ the RSNE received in message 3 ~~are~~is the same as the RSNE sent by the TDLS responder STA in message 2;

Change at 2968.63 as follows:

If an MDE is present in the (Re)Association Request frame and ~~the contents of~~ the RSNE does not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-188 (AKM suite selectors)), the AP shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_AKMP.

Change at 2972.41 as follows:

If an MDE is present in the Authentication frame and ~~the contents of~~ the RSNE does not indicate a negotiated AKM of Fast BSS Transition over FILS (suite type 00-0F-AC:16 or 00-0F-AC:17), the AP shall reject the Authentication frame with status code 43 (“Invalid AKMP”).

Change at 2974.53 as follows:

If the Authentication-Request frame contains an authentication algorithm equal to FT authentication and the ~~contents of the~~ RSNE does not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-188 (AKM suite selectors)), the AP shall reject the authentication request with status code STATUS\_INVALID\_AKMP.

Change at 2977.7 as follows:

If ~~the contents of~~ the RSNE does not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-188 (AKM suite selectors)), the AP shall reject the FT Request frame with status code STATUS\_INVALID\_AKMP.

Change at 2986.53 as follows:

If those frames did not include the RSNXE or if ~~the contents of the~~ RSNXEs are not identical, the S1KH of the FTO shall discard the response.

Change at 2990.45 as follows:

All other fields of the Information field shall be identical to ~~the contents of~~ those in the RSNE advertised by the AP in Beacon and Probe Response frames.

Change at 2992.20 as follows:

All other fields of the Information field shall be identical to ~~the contents of~~ those in the RSNE advertised by the target AP in Beacon and Probe Response frames.

Change at 5001.55 as follows (dot11WirelessMGTEventRSNARSNElement -- note “SIZE(0..257)”, which implies includes the Element ID and Length fields):

This attribute contains ~~the entire contents of~~ the negotiated RSNE at the time of the authentication attempt. ~~The format of the RSNE is defined in 9.4.2.24 (RSNE).~~

Change at 5136.59 as follows:

This attribute contains the Information field ~~entire contents~~ of the negotiated RSNE at the time of the authentication attempt~~. The maximum length of the RSNE field is less than the maximum length of an RSNE, as defined in 9.4.2.24 (RSNE). If the length of the RSNE included here exceeds the maximum length of the RSNE field, the RSNE shall be~~, truncated to the maximum length allowed for the RSNE field in the RSNA event report, if necessary."

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3488 in <this document>, which clarify the reference to the RSNE field in the RSNA event report.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3384  Mark RISON  9.8.3.1  1735.58 | "PV1 frames with Type subfield value equal to 0 define a PV1 QoS Data frame where either A1 or A2 field is  an SID as indicated in Table 9-639 (From DS subfield values in PV1 frames(#278)) and the other A1 or A2" etc. seems to duplicate the nearby table | Delete the para at the referenced location |

Discussion:

We have (green/cyan = common to both table and text, red/purple = not common to both table and text):

**Table 9-638—PV1 frame types**

|  |  |  |
| --- | --- | --- |
| **Type value** | **Type** | **Description** |
| 0 | QoS Data | Either the A1 field or the A2 field is an SID (defined in 9.8.3.2 (Address fields)),  as determined by the From DS subfield in the Frame Control field. |
| 1 | Management | Both A1 and A2 fields contain MAC addresses for PV1 Probe Response frames,  or  Either the A1 field or the A2 field is an SID (defined in 9.8.3.2 (Address fields)),  as determined by the From DS subfield in the Frame Control field. |
| 2 | Control | The A1 field is an SID and the A2 field is either an SID or contains a MAC  address. |
| 3 | QoS Data | Both A1 and A2 fields contain MAC addresses. |
| 4-6 | Reserved |  |
| 7 | Reserved for extension |  |

PV1 frames with Type subfield value equal to 0 define a PV1 QoS Data frame where either A1 or A2 field is an SID as indicated in Table 9-639 (From DS subfield values in PV1 frames(#278)) and the other A1 or A2 field contains a MAC address. PV1 frames with Type subfield value equal to 1 define a PV1 Management frame where either A1 or A2 field is an SID as indicated in Table 9-639 (From DS subfield values in PV1 frames(#278)) and the other A1 or A2 field contains a MAC address. PV1 frames with Type subfield value equal to 2 define PV1 Control frames. PV1 frames with Type subfield value equal to 3 define a PV1 QoS Data frame where both A1 and A2 fields contain MAC addresses. All other values of the Type subfield are reserved.

Note that the table allows PV1 Probe Response frames to have two MAC addresses, while the text does not. The table is correct.

Proposed changes:

Delete the para at 1735.58 and change Table 9-638 as follows:

**Table 9-638—PV1 frame types**

|  |  |  |
| --- | --- | --- |
| **Type value** | **Type** | **Description** |
| 0 | QoS Data | Either the A1 field or the A2 field is an SID (defined in 9.8.3.2 (Address fields)),  as determined by the From DS subfield in the Frame Control field (see Table 9-639), and the other field contains a MAC address. |
| 1 | Management | For PV1 Probe Response frames: b~~B~~oth A1 and A2 fields contain MAC addresses ~~for PV1 Probe Response frames,~~  Otherwise: e~~or~~  ~~E~~ither the A1 field or the A2 field is an SID (defined in 9.8.3.2 (Address fields)),  as determined by the From DS subfield in the Frame Control field (see Table 9-639), and the other field contains a MAC address. |
| 2 | Control | The A1 field is an SID and the A2 field is either an SID or contains a MAC  address. |
| 3 | QoS Data | Both A1 and A2 fields contain MAC addresses. |
| 4-6 | Reserved |  |
| 7 | Reserved for extension |  |

At 1735.19 change “End of Service Period” to “EOSP”.

At 1736.15 in “The From DS subfield, if present, defines the addressing of PV1 frames with values of the Type field less than 2” delete “, if present, ”.

At 1736.19 change “From DS subfield values in PV1 frames” to “From DS subfield values in type 0 or 1 PV1 frames”.

At 1735.5 change “PV1 Probe Request frame” to “PV1 Probe Response frame”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3384 in <this document>, which merge the material in the text into the table.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3216  Mark RISON  9.4.2.21.13 | It is not clear what angles are relative to, or measured (e.g. is it anticlockwise from X axis +ve, or clockwise from Y-axis +ve), and sometimes not clear what they are for (e.g. for ellipsoids) | Specify that angles are from the positive X-axis, anticlockwise |
| CID 3217  Mark RISON  9.4.2.21.13  951.41 | Figure 9-324-- Ellipse Location Shape Value ... Angle field is angle of what? | Change "The Angle field contains the angle of the ellipse." to "The Angle field contains the angle of the major axis of ellipse anticlockwise from the positive X-axis." |
| CID 3218  Mark RISON  9.4.2.21.13  952.21 | What is an arcband? | Define an arcband |
| CID 3224  Mark RISON  9.4.2.21.13  948.37 | "A Location Reference subelement set to 0" is not clear. If this is trying to say the string "0" is used for the field, then say that | Change to "A Location Reference field set to the string "0"" |
| CID 3226  Mark RISON  9.4.2.21.13  948.55 | "A Shape is specified with respect to either a 2-Dimensional or 3-Dimensional Coordinate Reference  System where each point in the shape defines the direction from the Location Reference value's starting  point. A positive X-axis value corresponds to an easterly direction relative to the Location Reference value's  starting point; a negative X-axis value corresponds to a westerly direction relative to the Location Reference  value's starting point; a positive Y-axis value corresponds to a northerly direction relative to the Location  Reference value's starting point; a negative Y-axis value corresponds to a southerly direction relative to the  Location Reference value's starting point and the Z-axis value corresponds to the altitude above the  horizontal plane at the Location Reference value's starting point." -- need to also define what angles correspond to (which axis, and which direction is a positive angle) | After the cited text add "An angle is measured anticlockwise from the positive X-axis towards the Y-axis." |
| CID 3227  Mark RISON  9.4.2.21.13  952.21 | An "arcband" is not well-defined, especially what "Start Angle" and "Opening Angle" are | Define an arcband and the start/opening angles |

Discussion:

The specification of location references was derived from RFC 5491. This has:

5. Geodetic Shape Representation

Angles

representing bearings are measured in a clockwise direction from

Northing […]

5.2.4. Ellipse

An elliptical area describes an ellipse in two-dimensional space.

The ellipse is described by a center point, the length of its semi-

major and semi-minor axes, and the orientation of the semi-major

axis. […]

The gs:orientation element is the angle by which the semi-major axis

is rotated from the first axis of the CRS towards the second axis.

For WGS 84, the orientation indicates rotation from Northing to

Easting

5.2.5. Arc Band

The arc band shape type is commonly generated in wireless systems

where timing advance or code offsets sequences are used to compensate

for distances between handsets and the access point. The arc band is

represented as two radii emanating from a central point, and two

angles that represent the starting angle and the opening angle of the

arc. […]

For example, Paul is using a cellular wireless device and is 7 timing

advance symbols away from the cell tower. For a GSM-based network,

this would place Paul roughly between 3,594 meters and 4,148 meters

from the cell tower, providing the inner and outer radius values. If

the start angle is 20 degrees from north, and the opening angle is

120 degrees, an arc band representing Paul's location would look

similar to Figure 11.

N ^ ,.\_\_

| a(s) / `-.

| 20 / `-.

|--. / `.

| `/ \

| /\_\_ \

| . `-. \

| . `. \

|. \ \ .

---c-- a(o) -- | | -->

|. / 120 ' | E

| . / '

| . / ;

.,' /

r(i)`. /

(3594m) `. /

`. ,'

`. ,'

r(o)`'

(4148m)

Figure 11: Example of an Arc Band

5.2.7. Ellipsoid

The ellipsoid is the volume most commonly produced by GPS systems.

It is used extensively in navigation systems and wireless location

networks. The ellipsoid is constructed around a central point

specified in three dimensions, and three axes perpendicular to one

another are extended outwards from this point. These axes are

defined as the semi-major (M) axis, the semi-minor (m) axis, and the

vertical (v) axis, respectively. An angle is used to express the

orientation of the ellipsoid. The orientation angle is measured in

degrees from north, and represents the direction of the semi-major

axis from the center point.

\

\_.-\""""^"""""-.\_

.' \ | `.

/ v m \

| \ | |

| -c ----M---->|

| |

\ /

`.\_ \_.'

`-...........-'

Figure 14: Example of an Ellipsoid

Regarding CID 3224, “A Location Reference subelement set to 0” is probably trying to refer to the length of the subelement (i.e. the subelement is not present) or to the Length field of the subelement (i.e. the subelement is present but empty). Also, calling (0, 0) “top north west” is a bit confusing as generally the positive quadrant is thought to originate at the southwestern corner.

The following additional issues have been identified and are to be addressed separately:

* 4.3.21.10 Location services’s claim that “The location reference is a URL that defines from where the location value is retrieved.”
* Which field is being referred to in “The Civic Location Type field contains the format of location information in the Civic Location field” in 9.4.2.21.13 Location Civic report
* Which field is being referred to in “The Civic Location field follows the little-endian octet ordering” in 9.4.2.21.13 Location Civic report
* Which field is being referred to in “If the Location Civic report contains the Location Reference and Location Shape subelements, the receiving STA may use the information specified in those subelements in combination with the Civic Location field value for additional granularity on the position reported in the Civic Location field.” in 11.10.9.9 Location Civic report
* “When the Civic Location Type field is IETF RFC 4776, the list of optional subelements optionally includes the Location Reference, Location Shape, Map Image, and Vendor Specific subelements as defined in Table 9-175 (Subelement IDs for Location Civic report).” in 9.4.2.21.13 Location Civic report is not clear: is it trying to say that no other optional subelements are allowed?
* Dependencies between subelements, e.g.:
  + Location Shape depends on the presence of Location Reference, which in turn depends on this being Civic Location.
  + Map Image depends on this being Civic Location.
* … or maybe:
  + Location Shape depends on the presence of non-empty Location Reference, which in turn depends on this being Civic Location.
  + Location Reference if absent/empty, depends on the presence of Map Image which in turn depends on this being Civic Location.
* … or even:
  + Location Shape depends on the presence of Location Reference which in turn depends on the presence of a Map Image which in turn depends on this being Civic Location (seems to be implicit in “of the floor plan on which the Location Shape is defined”)
* Whether if you don’t have a non-empty Location Reference it should be “… indicates that the position of the Location Shape is the south west corner (i.e., 0,0) of the lowest (or only) floor in the floor plan on which the Location Shape is defined.”
* The axes of the coordinate system are undefined. We probably should require that a Map Image is a prerequisite for a Location Shape

Proposed changes:

In Clause 2 add:

IETF RFC 5941, GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations, Mar. 2001.

Change at 947.56 as follows:

— An unknown civic location is indicated by ~~a subelement Length of 0 and~~ a zero-length Location Civic field

Change at 948.37 as follows:

A missing Location Reference subelement ~~set to 0~~ or one with a zero-length Location Reference field indicates that the position of the Location Shape is ~~top north~~ the south west corner (i.e., 0,0) of the floor plan on which the Location Shape is defined.

Change at 951.41 as follows:

The Angle field contains the angle of the semi-major axis of the ellipse, measured clockwise from north (see IETF RFC 5941).

Change at 952.8 as follows:

The Angle field contains the angle of the semi-major axis of the ellipsoid, measured clockwise from north (see IETF RFC 5941).

NOTE—The semi-major axis lies in the XY-plane.

At the start of the para at 952.21 add:

An arcband is defined in IETF RFC 5941.

Change at 952.45 as follows:

The Start Angle field contains the start angle of the arcband, measured clockwise from north (see IETF RFC 5941).

The Opening Angle field contains the opening angle of the arcband (see IETF RFC 5941).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3216, 3217, 3218, 3224, 3226, 3227 in <this document>, which address the issue raised in the comment.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3502  Mark RISON  9.4.2.62  1064.20 | "The Offset field is the time in microseconds between TSF 0 and the start of a first Awake Window.  See 11.2.3.12 (TDLS peer power save mode). " -- but the TSF is 8 octets and the Offset field is only 4 octets | Change the first cited text to "The Offset field is the time in microseconds between intervals specified by the Interval field, starting at TSF 0, and the start of the Awake Window, in microseconds." |
| CID 3503  Mark RISON  9.4.2.62  1064.20 | "The Offset field is the time in microseconds between TSF 0 and the start of a first Awake Window.  See 11.2.3.12 (TDLS peer power save mode). " -- doesn't seem compatible with "Awake Windows begin at TSF values that satisfy the equation TSF mod Interval = Offset." at 2390.60 | Change the first cited text to "The Offset field is the time in microseconds between intervals specified by the Interval field, starting at TSF 0, and the start of the Awake Window, in microseconds." |

Discussion:

The Offset field cannot be the time of the first Awake Window (sic) since that would mean that you couldn’t set up TDLS peer PSM 232 µs =~ an hour after the BSS had started (or less, since it doesn’t actually seemed to be specified that the TSF shall be 0 when the BSS is started!). This was probably intended to refer to a notional first Awake Window, but this has potential for confusion. The term “TSF 0” also has potential for confusion, as it is not defined.

The way it can all work is if:

* The Interval field defines points in time starting when TSF was 0 and occurring with that interval
* The Offset field defines points in time relative to the points in time defined by the Interval field
* The Awake Windows are those starting at the points in time defined by the (Interval and) Offset field, starting after the TDLS Peer PSM Response frame is received

This matches the equation in 11.2.3.12.

Proposed changes:

Change in 9.4.2.62 Wakeup Schedule element from:

The Offset field is the time in microseconds between TSF 0 and the start of a first Awake Window. See 11.2.3.12 (TDLS peer power save mode).

The Interval field is set to the time in microseconds between the start of two successive Awake Windows. See 11.2.3.12 (TDLS peer power save mode).

to:

The Offset and Interval fields are in microseconds and define when awake windows begin. See Equation (11-x) in 11.2.3.12 (TDLS peer power save mode). The Interval field is nonzero and the Offset field is less than the Interval field.

Change in 11.2.3.12 TDLS peer power save mode from:

Awake Windows begin at TSF values that satisfy the equation TSF mod Interval = Offset. The interval between the start of two successive Awake Windows is equal to the time in microseconds of the Interval field. The periodic wakeup schedule may be unrelated to the target beacon transmission time (TBTT) or the beacon interval.

to:

Awake windows begin at TSF values that satisfy Equation (11-x) and that are after the TDLS Peer PSM Request/Response frame exchange has completed, where Interval and Offset are the fields of the Wakeup Schedule element.

TSF mod Interval = Offset (11-x)

NOTE—The awake window timings might not be related to the beacon timings (TBTTs).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3502 and 3503 in <this document>, which clarify that the awake windows start when TSF % Interval = Offset, after the TDLS Peer PSM Request/Response exchange has completed.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3327  Mark RISON  12.4.8.6.3  2831.49 | "the frame shall be processed by first checking whether  a password identifier is present. If so and there is no password associated with that identifier, BadID shall be set  and the protocol instance shall construct and transmit an Authentication frame with Status Code set to  UNKNOWN\_PASSWORD\_IDENTIFIER" -- no Del event (cf. previous and next step)? | Send a Del event to the parent process in this case |

Discussion:

Jouni MALINEN has confirmed that a Del event is indeed missing (see Figure 12-15).

Proposed resolution:

REVISED

At 2831.45 after “If so and there is no password associated with that identifier, BadID shall be set

and the protocol instance shall construct and transmit an Authentication frame with Status Code set to

UNKNOWN\_PASSWORD\_IDENTIFIER” append “, and a Del event shall be sent to the parent process” (with Del italicised).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3650  Mark RISON  12 | The same SNonce should be reused until a valid M3 has been received, to avoid DoS attacks (see <https://theory.stanford.edu/~jcm/papers/fp09-he.pdf> ) | Make this recommendation (as a "should") |

Discussion:

Jouni MALINEN concurs that it would “make sense for the standard to promote this relatively strongly”.

Proposed resolution:

REVISED

In Clause B add:

[Bxx] He, C. and Mitchell, J.C., *Analysis of the 802.11i 4-Way Handshake*, WiSE’04, Oct. 2004

italicising the title.

At 2913.54, after “Generates a new nonce SNonce” append “, if it has not already generated one for this 4-way handshake (see [Bxx]); otherwise it should reuse the same SNonce”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3573  Mark RISON  12.5 | There are replay counters for PMF (one for each of individually addressed robust Management and individually addressed robust PV1 Management) and for QMF (one for each ACI of individually addressed robust Management -- it's not clear whether this is also used for individually addressed robust PV1 management or whether there's a separate set of 4) | Explicitly identify the full set of replay counters |
| CID 3574  Mark RISON  12.5 | There is one RC for unicast robust Management and there are four RCs for unicast QMF. It is not clear when the former will be used, if QMF is enabled for the link | Explicitly identify the use of the RC for unicast robust Management frames when QMF is enabled |

Discussion:

For PV0 we have in 12.5.2.4.1:

a)5) The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter maintained for the session(#193), and TID (for Data frames) or ACI (for QMFs).

For PV1 we have in 12.5.2.4.1:

b)6) The decryption processing prevents replay of MPDUs by validating that the PN in the (#193)locally constructed CCMP header (see 12.5.2.3.6 (Construct CCMP header for PV1 MPDUs)) is greater than the replay counter maintained for the session, and TID (for Data frames) or ACI (for QMFs).

We also have in 12.5.2.4.4:

b) For each PTKSA, (#166)TPKSA, GTKSA, (#1627)mesh PTKSA, and mesh GTKSA(#239), the recipient shall maintain a separate replay counter for each TID, subject to the limitation of the number of supported replay counters

c) If the recipient set the MFPC bit on a given link to 1, it(#199) shall maintain a single replay counter for received individually addressed robust Management frames that are received with the To DS subfield equal to 0, and a single replay counter for received individually addressed robust PV1 Management frames and shall use the PN from the received frame to detect replays. If dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames and robust PV1 Management frames(#1681), where these frames are received with the To DS subfield equal to 1.

and in 12.5.3.4:

When management frame protection is negotiated, the receiver shall maintain a 48-bit replay counter for each IGTK.

[…]

When dot11QMFActivated is true, the receiver shall maintain an additional replay counter for each ACI for received group addressed robust Management frames that use QMF.

If dot11RSNAProtectedManagementFramesActivated is true and dot11MeshSecurityActivated is true, the recipient shall maintain a single replay counter for received group addressed robust Management frames that do not use the QMF service and shall use the PN from the received frame to detect replays. If dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received group addressed robust Management frames that use the QMF service.

and in 12.5.3.6:

1) If the frame is a robust Management frame but not a GQMF, the receiver shall compare this MME IPN(#1422) to the value of the (#1504)replay counter for the IGTK identified by the MME Key ID field. […]

2) If the frame is a robust Management frame and also a GQMF, the receiver shall compare this MME IPN(#1422) to the value of the (#1504)replay counter for the IGTK identified by the MME Key ID field and the AC represented by the value of the ACI subfield of the received frame.

So for PV0 Management frames, there’s a replay counter for To DS = 0 if PMF and additionally a replay counter per ACI for To DS = 1 if QMF. But for PV1 Management frames the single replay counter appears to be used when To DS = 1 even if there’s also the replay counters per ACI if QMF.

… but PV1 frames don’t have a To DS field! Dave GOODALL has clarified:

* QMF is not supported for PV1. To support it would probably require a number of changes to differentiate between QMF and non-QMF PV1 management frames, provide additional PNs for each traffic priority and modify the language around use of the sequence number for PV1 frame security to account for the different size of the sequence number field in QMF frames.
* PV1 Data and Management frames are supported by sensor non-AP STAs and APs that advertise support for sensor STAs in the STA Type Support field in the S1G Capabilities element. If an AP advertises that it only supports non-sensor STAs then PV1 Management frames are never used by that AP or its associated STAs. Industry currently is only testing non-sensor STA support.
* If we specify that QMF does not apply to PV1 management frames then that will be acceptable.

Hypothesis on replay counters:

* PTK: per-TID Data (subject to max), also iff PMF: one Management, one PV1 Management iff S1G, per-ACI Management iff QMF (then the one Management is for non-QMF, based on To DS field)
* GTK: per-TID Data (subject to max); non-AP STA only
* IGTK (iff PMF): one Management, ?one PV1 Management iff S1G, per-ACI Management iff QMF (then the one Management is for non-QMF, based on To DS field); non-AP STA only

Proposed changes:

In 11.24.1.1 add a bullet “— The frame is not a PV1 Management frame.” at 2652.5/14/23.

Change 12.5.2.4.4 PN and replay detection as follows:

b) For each PTKSA, (#166)TPKSA, GTKSA, (#1627)mesh PTKSA, and mesh GTKSA(#239), the recipient shall maintain a separate replay counter for each TID, subject to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.24 (RSNE))~~, and shall use the PN from a received frame to detect replayed frames~~. ~~A replayed frame occurs when the PN from a received frame is less than or equal to the current replay counter value for the frame’s MSDU or A-MSDU priority and frame type.~~

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

c) If the recipient set the MFPC bit on a given link to 1, it(#199) shall maintain a single replay counter for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to 0, and (S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames ~~and shall use the PN from the received frame to detect replays~~. If dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust PV0 Management frames ~~and robust PV1 Management frames(#1681), where these frames~~that are received with the To DS subfield equal to 1. ~~The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the current value of the management frame replay counter that corresponds to the ACI of the frame.~~

NOTE—QMF is not supported for PV1 Management frames (see 11.24.1.1).

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

Change 12.5.2.3.1 General (under CCMP cryptographic encapsulation) as follows:

b) For secure PV1 MPDUs, CCMP encrypts the Frame Body field of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:

1) When the sequence number of the MPDU is less than the previous sequence number and satisfies the BPN update conditions in 12.5.2.3.6 (Construct CCMP header for PV1 MPDUs), for that (#37)(#193)PTID, ~~(~~for Data frames~~) or ACI (for QMFs)~~, increment the base PN so that the PN never repeats for the same temporal key and (#37)PTID/ACI.

NOTE 2—Retransmitted MPDUs are not modified on retransmission.

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

2) Use the fields in the MPDU header to construct the AAD for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that might change when retransmitted are muted by being (#1951)masked out when calculating the AAD.

3) Construct the (#209)CCM nonce as defined in 12.5.2.3.4 (Construct CCM nonce) from the PN, A2, and the priority value of the MPDU, where A2 is the STA MAC address identified by the A2 field of the MPDU. If the MPDU is a QoS Data MPDU, the priority value of the MPDU is equal to the value of the PTID subfield of the Frame Control field. ~~If the Type field of the Frame Control field is 001 (Management frame) and the frame is a QMF, the priority value of the MPDU is equal to the value in the ACI subfield of the Sequence Number field.~~ Otherwise, the priority value of the MPDU is equal to the fixed value 0.

Change 12.5.2.3.2 PN processing as follows:

The PN is incremented by a positive number for each MPDU. The PN shall be incremented in steps of 1 for constituent MPDUs of fragmented MSDUs, (11ax)A-MSDUs, and MMPDUs. For PV0 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key. For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and (for Data frames) (#37)(#193)PTID ~~(for Data frames) or ACI (for QMFs)~~.

Change 12.5.3.4 BIP replay protection as follows:

**12.5.3.4 BIP replay ~~protection~~counters and packet numbers**

[…]

See 12.5.3.5 (BIP transmission) and 12.5.3.6 (BIP reception) for per frame BIP processing, including detection of replayed frames.

[…]

When dot11QMFActivated is true, the receiver shall maintain an additional replay counter for each ACI for received group addressed robust Management frames that use QMF. ~~The receiver shall use the ACI encoded in the Sequence Number field of received GQMFs protected by BIP to select the replay counter to use for the received frame, and shall use the IPN from the received frame to detect replays.~~

NOTE—QMF is not supported for PV1 Management frames (see 11.24.1.1).

If dot11RSNAProtectedManagementFramesActivated is true and dot11MeshSecurityActivated is true, the recipient shall maintain a single replay counter for received group addressed robust Management frames that do not use the QMF service ~~and shall use the PN from the received frame to detect replays~~. If dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received group addressed robust Management frames that use the QMF service. ~~The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the value of the management frame replay counter that corresponds to the ACI of the frame.~~ When the QMF service is not used, t~~T~~he transmitter shall preserve the order of protected group addressed robust Management frames that are transmitted to the same ~~D~~RA ~~without the QMF service~~. When the QMF service is used, the transmitter shall ~~not reorder~~ preserve the order of protected robust GQMFs within an AC ~~when the frames~~that are transmitted to the same RA.

Change 12.5.2.3.7 CCM originator processing as follows:

When the QMF service is not used, t~~T~~he transmitter shall preserve the order of protected individually addressed robust Management frames that are transmitted to the same ~~D~~RA ~~without the QMF service~~. When the QMF service is used, the transmitter shall ~~not reorder~~ preserve the order of protected robust IQMFs within an AC ~~when the frames~~that are transmitted to the same RA.

In 12.5.3.5 BIP transmission after a) and in 12.5.3.6 BIP reception after b)1) add:

NOTE—QMF is not supported for PV1 Management frames (see 11.24.1.1).

Make equivalent changes in the GCMP subclauses, but only for PV0 (since “An S1G STA shall not use PV1 frames when using GCMP encapsulation.” in 12.5.4.1).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3573, 3574 in <this document>, which clarify the set of replay counters in the possible contexts.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3578  Mark RISON  12.6.21 | It is not clear how rekeying is performed in an MBSS | State that the same rules on Auth/Supp roles are used for the rekeying 4WH as for the initial 4WH |

Discussion:

Mesh doesn’t use the 4WH/GKH, it uses the AMPE/mesh GKH.

This is mentioned at the end of 14.5 for pairwise operation:

The MTK is used to protect communications between two peer STAs. The local STA and peer STA derive an MTK per peering instance and may rekey the MTK using AMPE.

and at the start of 14.6 for group operation:

The mesh group key handshake may be used by either mesh STA, after a secure mesh peering has been established, to update the MGTK that it uses to protect group addressed MPDUs that it transmits to its peer mesh STAs.

Proposed resolution:

REVISED

In 14.5.7 change “using AMPE” to “using the AMPE”.

In 14.6 Mesh group key handshake change “to update the MGTK” to “to rekey the MGTK”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3185  Mark RISON | It's not clear why some things in Figure 5-1--MAC data plane architecture are "(optional)" and some not. E.g. presumably MSDU Integrity and Protection is optional because you're not required to do security, but then shouldn't e.g. "SYNRA Receiver Filtering" and "Block Ack Scoreboarding" be optional because you're not required to do GLK or BA respectively? | In Figures 5-1 and 5-2 add "(optional)" at the end of the "SYNRA Receiver Filtering" and "Block Ack Scoreboarding" boxes |

Discussion:

In fact, almost all of the processes in the data plane architecture figures are optional in some sense, e.g. in general:

* Security is not mandatory so PN assignment, replay detection and encryption/decryption are optional (ditto MSDU Integrity and Protection -- is this referring to the TKIP thing?)
* Fragmentation might not ever occur on tx if the fragmentation limit is high enough and/or if block ack agreements are always used
* A-MSDU aggregation is not mandatory on tx
* Block ack agreements are not required to be set up or accepted, so A-MPDU aggregation is not mandatory, nor are block ack buffering/scoreboarding/reordering
* Segmentation is a DMG thing
* SYNRA filtering is a GLK thing

Proposed changes:

Change 5.1.5.1 General as follows:

During transmission, an MSDU goes through some or all, as applicable, of the processes shown in the left-hand side of Figure 5-1 (MAC data plane architecture(#1001)(11ay)). When transparent FST is used, an MSDU first goes, as shown in Figure 5-2 (MAC data plane architecture (transparent FST)(11ay)(#1938)), through an additional transparent FST entity that contains a demultiplexing process that forwards the MSDU down to the selected TX MSDU Rate Limiting process and from there to MAC data plane processing as described in the previous sentence. IEEE Std 802.1X-2010 may block the MSDU at the Controlled Port before the preceding processing occurs. Otherwise, at some point, the Data frames that contain all or part of the MSDU are queued per AC/TS.

During reception, a received Data frame goes through some or all, as applicable, of the processes shown in the right-hand side of ~~of~~ Figure 5-1 (MAC data plane architecture(#1001)(11ay)). Then, one or more MSDUs are delivered to the MAC SAP or, via the DSAF, to either the DS or an IEEE 802.1Q bridge port. When transparent FST is used, MSDUs originating from different PHY SAPs go, as shown in Figure 5-2 (MAC data plane architecture (transparent FST)(11ay)(#1938)), through a final step of a transparent FST entity that contains a multiplexing process before delivering the MSDU. The IEEE 802.1X Controlled/Uncontrolled Ports discard any received MSDU if the Controlled Port is not enabled and if the MSDU does not represent an IEEE 802.1X frame.

Change 5.1.5.6 S1G relay as follows:

The MAC data plane architecture of an S1G relay is shown in Figure 5-7 (S1G relay data plane architecture). During transmission, an MSDU goes through some or all, as applicable, of the processes shown in the left-hand side of Figure 5-7. During reception, a received Data frame goes through some or all, as applicable, of the processes shown in the right-hand side of Figure 5-7.

In Figures 5-1, 5-2 and 5-7 delete “(optional)” throughout.

In Figure 5-1 delete “(AP or IBSS STA only)” and change “(Rx)” to “(RX)”.

In Figure 5-2 delete “(AP or IBSS STA only)” (2x).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3185 in <this document>, which remove explicit indication of which processes are optional, since most are.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3266  Mark RISON | "AKM 00" should be "AKM suite selector 00" (ditto "intended AKM" stuff). Or maybe "AKMP"? | As it says in the comment |

Discussion:

AKM suites are identified by AKM suite selectors, but often the suite selector value is used to identify the “AKM”.

Proposed changes:

At the end of 1.4 add a para:

A construction of the form “AKM [is] [not] 00-0F-AC:<n>” is to be interpreted as referring to the AKMP identified by AKM suite selector 00-0F-AC:<n>. A construction of the form “intended AKM” or “negotiated AKM” is to be interpreted as referring to the AKMP.

Change at 731.48 as follows:

The AKM Suite Selector element is present if the intended AKM is 00-0F-AC:24 or 00-0F-AC:25 ~~is the intended AKM~~

Change at 970.47 as follows:

In an IBSS only a single AKM suite selector is specified because IBSS STAs use the same AKMP ~~suite~~ and because there is no mechanism to negotiate the AKMP in an IBSS (see 12.6.5 (RSNA policy selection in an IBSS)).

Change at 970.57 as follows:

~~The~~ AKM ~~suite selector value~~ 00-0F-AC:1 (i.e., Authentication negotiated over IEEE Std 802.1X with RSNA key management as defined in 12.7 (Keys and key distribution))(#1545) is the default AKMP ~~suite~~ when the AKM Suite List field is not included in the RSNE.

Change on page 977 as follows:

NOTE 1—~~The~~ AKM ~~selector value~~ 00-0F-AC:1 specifies only that IEEE Std 802.1X-2010 is used as the authentication transport. IEEE Std 802.1X-2010 selects the authentication mechanism.

NOTE 2—~~The~~ AKM ~~suite selector value~~ 00-0F-AC:11 is deprecated.(M20)

NOTE 3—The usage of AKM suite selector values with authentication algorithms is defined in the Authentication algorithm numbers column of Table 9-188 (AKM suite selectors); see 9.4.1.1 (Authentication Algorithm Number field).(M20)

NOTE 4—~~The~~ AKMs ~~selector values~~ 00-0F-AC:8 and 00-0F-AC:9 have the length of the PMK in bits equal to 256, the length of the KCK in bits equal to 128, and the length of the KEK in bits equal to 128 (see 12.4.5.4 (Processing of a peer’s SAE Commit message), 12.7.1.3 (Pairwise key hierarchy), and 12.7.3 (EAPOL-Key PDU construction and processing)). ~~The~~ AKMs ~~selector values~~ 00-0F-AC:24 and 00-0F-AC:25 have the length of the PMK, the length of the KCK, and the length of KEK depending on the hash algorithm specified in 12.4.2 (Assumptions on SAE) (see 12.7.1.3 (Pairwise key hierarchy) and 12.7.3 (EAPOL-Key PDU construction and processing)). (M21)(M67)

~~The~~ AKM ~~suite selector value~~ 00-0F-AC:8 (i.e., SAE authentication with SHA-256)(#1545) is used when either a password or PSK is used with RSNA key management.

NOTE 5—AKMs ~~Selector values~~ 00-0F-AC:1 and 00-0F-AC:8 can simultaneously be enabled by an Authenticator.

~~The~~ AKM ~~suite selector value~~ 00-0F-AC:2 (PSK) is used when an alternate form of

PSK is used with RSNA key management.

NOTE 6—AKMs ~~Selector values~~ 00-0F-AC:1 and 00-0F-AC:2 can simultaneously be enabled by an Authenticator.

Change at 1077.19 as follows:

The Authentication Type field ~~contains~~identifies the ~~Authentication type~~ AKMP in use at the time of the authentication attempt

Change at 1585.28 as follows:

An AKM suite selector is a code identifying an AKMP ~~suite type~~ as specified in Table 9-188 (AKM suite selectors). The definition of the AKM suite selectors is shown in Table 9-472 (AKM suite selector definitions).

**Table 9-472—AKM suite selector definitions**

AKM suite selector AKMP ~~suite type~~

0 Use AKMP from RSN IE Beacon/Probe Response frame

1 Set AKM ~~suite to~~ 00-0F-AC:14 of Table 9-188 (AKM suite selectors)

2 Set AKM ~~suite to~~ 00-0F-AC:15 of Table 9-188 (AKM suite selectors)

3 Set AKM ~~suite to either~~ 00-0F-AC:14 or 00-0F-AC:15 of Table 9-188 (AKM suite selectors)

4 Set AKM ~~suite to~~ 00-0F-AC:17 of Table 9-188 (AKM suite selectors)

5–61 Reserved

62 Vendor Specific

63 No AKMP ~~suite~~ selected

Change at 2821.59 as follows:

If an AKM Suite Selector element is not included in the SAE Commit message from the peer and the state of the SAE finite state machine is Nothing (see 12.4.8.2.2 (Protocol instance states)), then AKM 00-0F-AC:8 or 00-0F-AC:9 shall be the intended AKM.

If the state of the SAE finite state machine is Committed (see 12.4.8.2.2 (Protocol instance states)) and the SAE Commit message that has been sent by the SAE finite state machine to transition into Committed state does not include an AKM Suite Selector element, then AKM 00-0F-AC:8 or 00-0F-AC:9 shall be the intended AKM.

Change at 2856.22 as follows:

— PMK; or if the PMKSA was established with an AKMP ~~suite type~~ for which the Authentication type column includes FT authentication (see Table 9-188 (AKM suite selectors)), MPMK (see 12.7.1.6.3 (PMK-R0)).

Change at 2857.41 as follows:

— Selected AKMP ~~suite~~ (see 9.4.2.24.3 (AKM suites))

Change “depending on the negotiated AKM suite” to “depending on the negotiated AKMP” at 2858.10/12.

Change at 2868.29 as follows:

IBSS STAs use the same AKMP ~~suite~~

Change at 2872.10 as follows:

A STA shall not use preauthentication except when pairwise keys are employed. A STA shall not use preauthentication within the same mobility domain if an AKMP ~~suite type~~ for which the Authentication type column indicates FT authentication (see Table 9-188 (AKM suite selectors)) is used in the current association.

Change at 2872.49 as follows:

The AKMP shall be ~~set to~~AKM 00-0F-AC:1 in the PMKSA that results from preauthentication.

Change at 2873.23 as follows:

A cached PMKSA established using an AKMP ~~suite type~~ for which the Authentication type column indicates FT authentication (see Table 9-188 (AKM suite selectors)) may be used in a subsequent FT Initial Mobility Domain Association using an identical AKMP ~~suite~~. A cached PMKSA is not used in an FT authentication sequence.

Change at 2887.44 as follows:

When using AKM ~~suite selector~~ 00-0F-AC:12, 00-0F-AC:15, 00-0F-AC:20,(#590) 00-0F- AC:23(M20)(M67), the length of the PMK, PMK\_bits, shall be 384 bits. (M67)When using AKM ~~suite selector~~ 00-0F-AC:24 or 00-0F-AC:25, the length of the PMK, PMK\_bits, shall have the length of the digest generated by H() identified in 12.4.2 (Assumptions on SAE).

Change at 2888.62 as follows:

The values of KCK\_bits and KEK\_bits are AKMP ~~suite~~ dependent and are listed in Table 12-11 (Integrity and key wrap algorithms).

Change at 2897.6 as follows:

The length is dependent on the negotiated cipher suites and AKMP ~~suites~~

Change at 2908.34 as follows:

Table 12-11 (Integrity and key wrap algorithms) indicates the particular algorithms to use when constructing and processing EAPOL-Key frames and FT authentication sequence. The AKM of “Deprecated” indicates ~~an~~ AKM ~~of~~ 00-0F-AC:1 or 00-0F-AC:2 when either TKIP or “Use group cipher suite” is the negotiated pairwise cipher. For all other AKMs the negotiated pairwise cipher suite does not influence the algorithms used to process EAPOL-Key frames. For ~~the~~AKMs 00-0F-AC:16 and 00-0F-AC:17 ~~AKMs~~ (FILS with FT), different keys and algorithms are used in EAPOL-Key frames and FT authentication sequence. These different cases are indicated in the table in <EAPOL-Key> / <FT authentication> format.

Change at 2929.47 as follows:

If the contents of the RSNE do not indicate AKM ~~of TPK handshake (suite type~~ 00-0F-AC:7 (TPK handshake),

Change at 2945.22 as follows:

When using AKM ~~suite selector~~ 00-0F-AC:10 to indicate AP PeerKey,

Change at 2963.56 as follows:

— The STA should use SAE (AKM ~~suite selectors~~ 00-0F-AC:8 and/or 00-0F-AC:9) if authenticating using a password where IEEE Std 802.1X is not used (as a replacement for PSK).

Change at 2969.13 as follows:

On successful (re)association, the S0KH on the STA and the R0KH on the AP then proceed with an IEEE 802.1X authentication using EAPOL PDUs carried in IEEE 802.11 Data frames if SAE authentication was not performed (i.e., if the ~~suite type~~AKM is not 00-0F-AC:9 or 00-0F-AC:25(Ed1)(M21)).

Change at 2972.41 as follows:

If an MDE is present in the Authentication frame and the contents of the RSNE do not indicate ~~a negotiated~~ AKM ~~of Fast BSS Transition over FILS (suite type~~ 00-0F-AC:16 or 00-0F-AC:17 (Fast BSS Transition over FILS), the AP shall reject the Authentication frame with status code 43 (“Invalid AKMP”)

Change “is set to the value of either 00-0F-AC:1” to “is set to either 00-0F-AC:1” at 5001.35 and 5136.27.

Change “selected AKM suite” to “selected AKMP” at 4953.5/21, 5180.24.

Change “last AKM suite” to “last AKMP” at 4955.18 and 4956.2.

Change “the AKM suite” to “indicates the AKMP” at 5001.24, 5136.13, 5149.40.

Change at 4961.24 as follows:

"This table lists the AKMP ~~suite~~s supported by this entity. Each AKMP ~~suite~~ can be individually enabled and disabled.

Change at 4961.61 as follows:

The selector of an AKMP ~~suite~~.

Change at 4962.10 as follows:

This variable indicates whether the corresponding AKMP ~~suite~~ is enabled/disabled.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3266 in <this document>, which make “AKM 00-0F-AC:<n>” an acceptable shorthand for the AKMP identified by that AKM suite selector value.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3485  Mark RISON | In Table 27-53--HE PHY MIB attributes why do we have both dot11VHTChannelWidthOptionImplemented and dot11HEChannelWidthOptionImplemented? Per the description of the latter it's equal to the former in the 5G band, and reserved in the 2G4 band | Delete the row at 4194.18, 5343.47 and 5349.36-50 |

Discussion:

The description of dot11HEChannelWidthOptionImplemented is:

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the channel widths supported: 20/40/80 MHz, 20/40/80/160 MHz or 20/40/80/160/80+80 MHz. For the 5 GHz band, the value of dot11HEChannelWidthOptionImplemented equals

dot11VHTChannelWidthOptionImplemented. Reserved in the 2.4 GHz band.

Reserved in a 20 MHz-only non-AP HE STA."

So this is needed for 6 GHz operation and cannot be deleted.

Something is also needed for 2.4 GHz operation, though -- namely dot11FortyMHzOperationActivated/Implemented (which is present in the VHT and HE PHY MIB attribute tables).

Note CID 1072 suggested “a STA could be capable (and signal itself accordingly) as 160M HE but 80M VHT or vice versa” but the discussion in 22/0576r11 disagrees and says:

Note that VHT and HE bandwidth support should be the same, and the HT bandwidth support is 40 MHz if the HE bandwidth support is 40 MHz, and hence these bandwidths can be inferred from the HT/VHT supported bandwidth MIB variables

Proposed changes:

Change C.3 as follows:

dot11FortyMHzOperationImplemented OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute, when true, indicates that the 40 MHz ~~O~~operation is

implemented.

false or not present in a 20 MHz-only non-AP HE STA that is an HT STA.

true in a VHT STA that is not a 20 MHz-only non-AP HE STA."

::= { dot11PhyHTEntry 1 }

dot11FortyMHzOperationActivated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This attribute, when true, indicates that the 40 MHz ~~O~~operation is

enabled.

false or not present in a 20 MHz-only non-AP HE STA that is an HT STA.

true in a VHT STA that is not a 20 MHz-only non-AP HE STA."

DEFVAL { false }

::= { dot11PhyHTEntry 2 }

dot11VHTChannelWidthOptionImplemented OBJECT-TYPE

SYNTAX INTEGER { contiguous80(0), contiguous160(1), noncontiguous80plus80(2)

}

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the channel widths supported: 20/40/80 MHz, 20/40/80/160 MHz or 20/40/80/160/80+80 MHz.

Reserved in a 20 MHz-only non-AP HE STA that is a VHT STA."

::= { dot11PhyVHTEntry 1 }

(#1072)dot11HEChannelWidthOptionImplemented OBJECT-TYPE

SYNTAX INTEGER { contiguous80(0), contiguous160(1), noncontiguous80plus80(2)

}

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the channel widths supported: 20/40/80 MHz, 20/40/80/160 MHz or 20/40/80/160/80+80 MHz. For the 5 GHz band, the value of dot11HEChannelWidthOptionImplemented equals

dot11VHTChannelWidthOptionImplemented. Reserved in the 2.4 GHz band (see dot11FortyMHzOperationImplemented and dot11FortyMHzOperationActivated).

Reserved in a 20 MHz-only non-AP HE STA."

::= { dot11PhyHEEntry 26 }

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3485 in <this document>, which clarify the interplay between HE, VHT and HT requirements. Note to the commenter: dot11HEChannelWidthOptionImplemented is needed for 6 GHz operation.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3480  Mark RISON  17.3.12  3206.21 | The CID 1058 changes have moved PHY-CCA.ind in e.g. Figure 17-19--Receive PHY to well after CCA changes -- is this wise? It doesn't even say "issued at the same time" | Move the CCA.inds back to where they were in D1.0 |

Discussion:

Brian HART has provided the following input:

* Since aCCATime is 4usec, averaging of up to 4usec is implied. In path-of-least-resistance implementations, this cuts both ways – it could be 4usec before the CCA goes idle too.
* It is desirable for CCA to go idle “immediately” after a PPDU[+SigExt], and pretty quickly (e.g., <1usec) after non-802.11 energy (e.g. a microwave oven) drops below -62 dBm.
* However, there is no delay parameter defined in clause 6.7.4.2 from the end of a PPDU to CCA going idle
* And, AFAIK, there is no clear *requirement* that CCA go idle quickly. For instance, the RX procedure just has requirements on when the PHY needs to assert busy: e.g., “17.3.12 Receive PHY: Also, in this case, the CCA of the OFDM PHY shall indicate a busy medium for the intended duration of the transmitted frame, as indicated by the LENGTH field.”
* Related, 8.3.5.12.2 Semantics of the service primitive does say “The parameter value is BUSY if the assessment of the channel(s) by the PHY determines that the channel(s) are not available. Otherwise, the value of the parameter is IDLE.” However, if the PHY determination takes some time, then the IDLE signaling could be delayed
* As well, for 14B in an 54 Mbps 11a/g PPDU, it might be a struggle for CCA to go idle at the immediate end of the PPDU, especially for an 11a/g implementation, because it may not be able to determine the PPDU duration before the PPDU has already ended.
* From Figure 10-29—EDCA mechanism timing relationships, slot timing depends on PHY-RXEND.ind, not PHY-CCA(IDLE).ind. So slot timings are a don’t care. Indeed, as long as CCA goes idle within SIFS, we’re OK.

So I can’t say CCA going idle quickly at the exact end of a **PPDU** is required or especially desirable or even possible for very short PPDUs. And it’s NEVER been drawn so.

On the other hand, CCA going idle quickly at the end of non-802.11 interference does seem important for slot synchronization. And maybe this points out a problem with Figure 10-29??? That discussion I’m happy to continue, but I’ll stop for now …

and re having RXEND and CCA(idle) at the same time:

This has been there for a long time and does make *some* reasonable sense, so my bias is to leave it there.

Except:

* We haven’t identified anywhere else in the spec where this “at the same time” is ever written as normative text
* Consider a received PPDU at -30 dBm and other, continuing energy at -60 dBm. Here the PPDU ends but really CCA shouldn’t go idle until that continuing energy disappears … which implies that CCA should never report idle until there is measurement.

So I guess this overcomes my bias and I *individually* support your changes.

Proposed resolution:

REVISED

Delete “Issue at the same time”/“Issued at the same time” (as appropriate) from Figure 19-25—PHY receive procedure for HT-mixed format PPDU, Figure 19-26—PHY receive procedure for HT-greenfield format PPDU, Figure 20-18—PHY receive procedure, Figure 27-60—PHY receive procedure for an HE SU PPDU, Figure 27-61—PHY receive procedure for an HE ER SU PPDU, Figure 27-62—PHY receive procedure for an HE MU PPDU, Figure 27-63—PHY receive procedure for an HE TB PPDU, and shorten the corresponding arrows to be the same as all the other arrows on that line.

At 4613.42 change “PHY receiver procedure” to “PHY receive procedure”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3174  Mark RISON  11.5.2.1 | "The procedures for setting up and modifying the block ack parameters are described in 11.5.2.2 (Procedure at  the originator)" -- but 11.5.2.2 has nothing about modifying the BA params | Change to "The procedures for setting up the block ack parameters are described in 11.5.2.2 (Procedure at  the originator)" |

Discussion:

10.25.2 Setup and modification of the block ack parameters only has this on BA modification:

(#1807)A block ack agreement may be modified by the originator by sending an ADDBA Request frame. All parameters of the agreement may be changed except for the TID. If the request is not successful, the existing agreement is not modified.

11.5.2 Setup and modification of the block ack parameters has nothing in 11.5.2.2 Procedure at the originator and nothing except the word “modification” in 11.5.2.3 Procedure at the recipient.

11.5.1 Introduction suggests that the original intent was for 10.25.2 to be for MAC-initiated operation while 11.5.2 was for SME-initiated operation:

Block ack may be set up at the MAC (see 10.25.2 (Setup and modification of the block ack parameters)) or by the initiation of SME. The setup and deletion of block ack at the initiation of the SME is described in this subclause.

However, this leaves modification by the MAC undefined, since 11.5.2 is in the context of SME operation.

The changes below are probably not perfect: it is highly suspect to have ADDBA handling in both 10.25(.2) and 11.5(.2), and there might be contradictions/omissions. However, they at least make sure BA modification is covered.

Proposed changes:

Change 10.25.2 Setup and modification of the block ack parameters as follows:

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

Change 11.5.1 Introduction as follows:

Block ack agreements may be set up, modified by the originator, or deleted from ~~at~~ the MAC (see 10.25.2 (Setup and modification of the block ack parameters)) or ~~by the initiation of~~ from the SME. The setup, modification by the originator and deletion of block ack agreements ~~at the initiation of~~ 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.

Change 11.5.2.2 Procedure at the originator as follows:

(#111)Upon receipt of an MLME-ADDBA.request primitive, in order to send QoS Data frames under the block ack mechanism, an initiating STA shall set up or modify a ~~the~~ block ack agreement using the following procedure:

a) If the initiating STA is an HT STA, is an IBSS STA, and has no block ack agreement with the recipient STA, then the initiating STA shall transmit a Probe Request frame to the recipient STA and shall not transmit an ADDBA Request frame unless it receives a Probe Response frame from the recipient.

NOTE—When the block ack agreement is being established between a non-AP STA and its AP, then the originator and the recipient have exchanged capability information during the association exchange that allows them to determine whether the other STA is an HT STA.

b) If the peer STA is an S1G STA, the S1G originator shall send an NDP ADDBA Request to indicate that it expects only NDP BlockAck frames during the block ack agreement with the following exceptions:

1) If the S1G originator’s dot11BATImplemented is true and the BAT Support subfield in the most recently received S1G Capabilities element from the S1G recipient is 1 and a TWT has been set up with the S1G recipient as described in 10.47 (Target wake time (TWT)), then the S1G originator shall send a BAT ADDBA Request to indicate that it expects only BAT frames during the block ack agreement.

2) When any of the conditions below is satisfied then the S1G originator may send an ADDBA request to indicate that it expects only BlockAck frames during the block ack agreement:

i) The value of the Buffer Size field in the ADDBA Request, carried in an S1G\_LONG or S1G\_SHORT PPDU, is greater than 16.

ii) The value of the Buffer Size field of the ADDBA Request, carried in an S1G\_1M PPDU, is greater than 8.

iii) The dot11AsymmetricBlockAckActivated is true and Asymmetric BA Supported field in the most recently received S1G Capabilities element from the S1G recipient is 1.

c) If the recipient is capable of participating, the originator sends an ADDBA Request frame indicating the TID and the buffer size. If the recipient is capable of participating and the GCRGroupAddress parameter of the MLME-ADDBA.request primitive is present, the originator sends an ADDBA Request frame that includes a GCR Group Address element. All DMG STAs are capable of participating in the block ack mechanism.

d) If an ADDBA Response frame is received with the matching dialog token and the TID and with a status code equal to SUCCESS, the STA has established or modified a block ack mechanism with the recipient STA; and the MLME shall issue an MLME-ADDBA.confirm primitive indicating the successful completion of the setup or modification of the block ack agreement.

e) If an ADDBA Response frame is received with the matching dialog token and the TID and with a status code not equal to SUCCESS, the STA has not established or modified the ~~a~~ block ack mechanism with the recipient STA; and the MLME shall issue an MLME-ADDBA.confirm primitive indicating the failure of the setup or modification of the block ack agreement.

Change 11.5.2.3 Procedure at the recipient as follows:

A recipient shall operate as follows in order to support block ack agreement set up and modification:

a) When an ADDBA Request frame is received from another STA, the MLME shall issue an MLME-ADDBA.indication primitive.

b) Upon receipt of the MLME-ADDBA.response primitive, the STA shall respond by an ADDBA Response frame with a status code(#1780) as defined in 9.6.4.3 (ADDBA Response frame format).

1) If the status code(#1780) is SUCCESS, the block ack agreement ~~is considered to be~~ has been established ~~with the originator~~ or modified. Contained in the frame are the type of Block Ack agreement, the type of BlockAck frames, and the number of buffers that have been allocated for the support of this block. If the recipient STA is (#306)a non-AP S1G STA and it has received from the AP a frame containing an S1G Capabilities element with the Asymmetric BA Supported equal to 1, the Originator Preferred MCS field may be contained in the ADDBA Response frame.

2) If the status code(#1780) is REFUSED\_REASON\_UNSPECIFIED(#1780), the block ack agreement ~~is not considered to have~~ has not been established or modified.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3174 in <this document>, which clarify how BA agreement modification operates.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3379  Mark RISON  9.4.2.25 | Vendor-specific fields are not described consistently:  - sometimes not described at all  - sometimes "The Vendor Specific field contains the vendor specific information."  - sometimes "The Vendor Specific Content field is a variable length field whose content is defined by the entity identified  in the OI field."  - sometimes "The Vendor Specific Content field contains vendor-specific field(s)." | Pick one and change the others |

Discussion:

Figure 9-351—Vendor Specific element format:

no definition of Vendor-specific content field

Figure 9-526—TFS Request Vendor Specific subelement format [note: field called “Vender Specific”]:

“The Vendor Specific field contains the vendor specific information.”

Figure 9-529—TFS Response Vendor Specific subelement format:

“The Vendor Specific field contains the vendor specific information.”

Figure 9-810—Request Tuple field format:

“The Requested Vendor Specific Information field is a sequence of octets that comprise individual requests. The requested vendor specific information sequence must start with an Organization Identifier field as described in 9.4.1.31 (Organization Identifier field).”

Figure 9-1017—Vendor Specific ANQP-element format:

“The Vendor Specific Content field is a variable length field whose content is defined by the entity identified in the OI field.”

Figure 9-1069—Vendor Specific RLQP-element format:

no definition of Vendor-specific content field

Figure 9-1089—Vendor Specific frame Action field format:

“The Vendor Specific Content field contains vendor-specific field(s).”

Figure 9-1106—Vendor Specific Public Action frame Action field format:

“The Vendor Specific Content field contains vendor-specific field(s).”

9.9.3.4 WUR Vendor Specific frame format:

The Frame Body field, if present, contains vendor specific information that is out of scope of the standard.

Proposed changes:

At the end of 9.4.2.25 Vendor Specific element add a para:

The Vendor-specific content field contains vendor specific information.

In 9.4.2.79 TFS Request element delete from “The format of the Vendor Specific subelement for a TFS Request element is shown in Figure 9-526” to “The Vendor Specific field contains the vendor specific information.” and replace with this para:

The Vendor Specific subelement has the same format as the corresponding element (see 9.4.2.25 (Vendor Specific element)). Zero or more Vendor Specific subelements are included in the list of optional subelements.

In 9.4.2.80 TFS Response element delete from “The format of the Vendor Specific subelement for a TFS Response element is shown in Figure 9-526” to “The Vendor Specific field contains the vendor specific information.” and replace with this para:

The Vendor Specific subelement has the same format as the corresponding element (see 9.4.2.25 (Vendor Specific element)). Zero or more Vendor Specific subelements are included in the list of optional subelements.

Change 9.4.2.218 Vendor Specific Request element as follows:

The Requested Vendor Specific Information field ~~is a sequence of octets that comprise individual requests. The requested vendor specific information sequence must~~ starts with an Organization Identifier field as described in 9.4.1.31 (Organization Identifier field), followed by vendor specific information.

Change 9.4.5.8 Vendor Specific ANQP-element as follows:

The Vendor Specific Content field ~~is a variable length field whose content is defined by the entity identified in the OI field~~ contains vendor specific information.

At the end of 9.4.6.5 Vendor Specific RLQP-element add a para:

The Vendor-specific content field contains vendor specific information.

Change 9.6.5 Vendor-specific action details and 9.6.7.11 Vendor Specific Public Action frame format as follows:

The Vendor Specific Content field contains vendor~~-~~ specific ~~field(s)~~information.

Change 9.9.3.4 WUR Vendor Specific frame format as follows:

The Frame Body field, if present, contains vendor specific information ~~that is out of scope of the standard~~.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3379 in <this document>, which refer to the fields in question as containing “vendor specific information” (sic) throughout.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3404  Mark RISON | TIME\_OF\_DEPARTURE descriptions in tables are not consistent | As it says in the comment |

Discussion:

These all say “This parameter is present only if TIME\_OF\_DEPARTURE\_REQUESTED is true in the corresponding request.” so omitting it.

The tables are as follows (outliers highlighted):

Table 15-3:

TIME\_OF\_DEPARTURE

0 to 232– 1. The locally measured time when the first (#14)PPDU energy is sent by the transmitting port, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

TIME\_OF\_DEPARTURE\_ClockRate

0 to 216– 1. The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.

TX\_START\_OF\_FRAME\_OFFSET (#1373)(#1370)

0 to 232– 1. ***[description below table]*** (#1373)(#1370)TX\_START\_OF\_FRAME\_OFFSET is an estimate of the offset (in 10 ns units) from the point in time at which the start of the preamble (#14)of the PPDU was transmitted at the transmit antenna connector to the point in time at which this primitive is issued to the MAC.

Table 16-5:

TIME\_OF\_DEPARTURE TXSTATUS

0 to 232– 1. The time when the first frame energy is sent by the transmitting port, measured by the local PHY entity, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

TIME\_OF\_DEPARTURE\_ClockRate TXSTATUS

0 to 216– 1. The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.

***[TX\_START\_OF\_FRAME\_OFFSET missing]***

Table 17-3:

TIME\_OF\_DEPARTURE PHY-TXSTART.confirm

0 to 232– 1. The locally measured time when the first (#14)PPDU energy is sent by the transmitting port, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

TIME\_OF\_DEPARTURE\_ClockRate PHY-TXSTART.confirm

0 to 216– 1. The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.

TX\_START\_OF\_FRAME\_OFFSET PHY-TXSTART.confirm

0 to 232– 1. An estimate of the offset (in 10 ns units) from the point in time at which the start of the preamble (#14)of the PPDU was transmitted at the transmit antenna connector to the point in time at which this primitive is issued to the MAC.

Table 18-2:

TIME\_OF\_DEPARTURE

0 to 232– 1. The locally measured time when the first (#14)PPDU energy is sent by the transmitting port, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

TIME\_OF\_DEPARTURE\_ClockRate

0 to 216– 1. The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.

TX\_START\_OF\_FRAME\_OFFSET

0 to 232– 1. An estimate of the offset (in 10 ns units) from the point in time at which the start of the preamble (#14)of the PPDU was transmitted at the transmit antenna connector to the point in time at which this primitive is issued to the MAC.

Table 19-4:

TIME\_OF\_DEPARTURE

0 to 232– 1. The locally measured time when the first (#14)PPDU energy is sent by the transmitting port, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

TIME\_OF\_DEPARTURE\_ClockRate

0 to 216– 1. The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.

TX\_START\_OF\_FRAME\_OFFSET

0 to 232– 1. An estimate of the offset (in 10 ns units) from the point in time at which the start of the preamble (#14)of the PPDU was transmitted at the transmit antenna connector to the point in time at which this primitive is issued to the MAC.

Table 20-2:

TIME\_OF\_DEPARTURE

***[missing range]***When the first (#14)PPDU energy is sent by the transmitting port, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

TIME\_OF\_DEPARTURE\_ClockRate

0 to 216–1. The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.

TX\_START\_OF\_FRAME\_OFFSET

0 to 232–1. An estimate of the offset (in 10 nanosecond units) from the point in time at which the start of the preamble (#14)of the PPDU was transmitted at the transmit antenna connector to the point in time at which this primitive is issued to the MAC.

21.2.6 TXSTATUS parameters:

The parameters listed in Table 19-4 (TXSTATUS parameters) are defined as part of the TXSTATUS parameter list in the PHY-TXSTART.confirm primitive.

Clause 22

***[Apparently nothing]***

Table 23-3:

TIME\_OF\_DEPARTURE

0 to 232 – 1. The locally measured time when the first PPDU energy is sent by the transmitting port, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

***[No TIME\_OF\_DEPARTURE\_ClockRate]***

***[No TX\_START\_OF\_FRAME\_OFFSET]***

Table 24-2:

TIME\_OF\_DEPARTURE

***[missing range]***When the first (#14)PPDU energy is sent by the transmitting port, in units equal to 1/TIME\_OF\_DEPARTURE\_ClockRate.

TIME\_OF\_DEPARTURE\_ClockRate

0 to 216–1. The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.

***[No TX\_START\_OF\_FRAME\_OFFSET]***

Clause 25

***[Apparently nothing]***

Clause 27

***[Apparently nothing]***

28.2.5 TXSTATUS parameters

The parameters listed in Table 20-2 (TXSTATUS parameters) (in 28.3.1 (Introduction)) are defined as part of the TXSTATUS parameter list in the PHY-TXSTART.confirm(TXSTATUS) primitive.

Proposed changes:

Add TIME\_OF\_DEPARTURE\_ClockRate to Table 23-3.

Delete “is” in “The clock rate, in units of MHz, is used to generate the TIME\_OF\_DEPARTURE value.” throughout.

Add TIME\_OF\_DEPARTURE range in Tables 20-2, 24-2.

Use canonical TIME\_OF\_DEPARTURE wording in Tables 16-5, 20-2, 24-2.

Add TXSTATUS table in Clauses 22 (TVHT), 25 (CMMG), 27 (HE).

Delete the weird “(in 28.3.1 (Introduction))” in 28.2.5.

Move TX\_START\_OF\_FRAME\_OFFSET description into Table 15-3 (and just start “An estimate…”).

Add TX\_START\_OF\_FRAME\_OFFSET to Tables 16-5, 23-3, 24-2.

Change “nanosecond” to “ns” in Table 20-2.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3404 in <this document>, which make the descriptions consistent.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3683  Mark RISON | "drop" is not clear in the context of a frame | Use "discard" for frames, and "ignore" for everything else |

Discussion:

The proposed change isn’t clear. The intent is to use “discard” for frames and “ignore” for fields etc.

Proposed changes:

Here are the instances of “drop” excluding those adjacent to { eligib protectedframe dot11 level eaves } -- it is proposed to change “drop”/“dropped” highlighted in yellow to “discard”/“discarded”:

1860.54: With the information from the DEI subfield, a STA may selectively drop frames with the DEI subfield set to 1

2496.52: The STA may pause Data frame transmission and may drop any received Data frames until the SA query procedure has completed successfully

2526.47: the AP shall delay the actual transmission of a Measurement Pilot frame according to the basic medium access rules specified in Clause 10 (MAC sublayer functional description) for a maximum period of one dot11RMMeasurementPilotPeriod and drop the delayed Measurement Pilot frame at the next TMPTT. In this way, a continuously busy medium causes multiple successive Measurement Pilot frames to be delayed, then dropped.

2601.65: The proxy ARP function shall drop those messages if the target IP address does not correspond to an associated STA.

2623.61: Figure 11-46—Group addressed GAS frame exchange with a response drop

2625.40: X = frame is dropped

2628.17: If the GAMode associated with the Query Request is true and the advertisement server(#571) has no response to the Query Request, the advertisement server(#571) may drop the request.

2628.41: If the responding STA does not receive a GAS Comeback Request frame whose source MAC address and dialog token match the source MAC address and value of the Dialog Token field respectively of the corresponding GAS Initial Response frame within this time, it may drop the query response.

2629.49: If the query response is subsequently received from the advertisement server(#571), it shall be dropped by the responding STA.

2629.57: NOTE—If there is no response to the Query Request, the advertisement server(#571) may drop the request.

If the Query Response received from the advertisement server(#571) is larger than dot11GASQueryResponseLengthLimit or requires more than 128 fragments for transmission to the requesting STA, it shall be dropped by the responding STA.

2630.24: If the query response is subsequently received from the advertisement server(#571), it shall be dropped by the STA.

2) If the Query Response received from the advertisement server(#571) is larger than dot11GASQueryResponseLengthLimit, it shall be dropped by the responding STA.

2686.32: The AP or PCP should stop the spatial sharing of two or more SPs if it determines that the link quality of any of the links involved in the spatial sharing has dropped below acceptable levels.

2795.22: The receiver drops MPDUs received out of order, i.e., not received with increasing sequence numbers.

2809.6: NOTE—This works because if an attacker modifies the TSC, then the encryption key is modified and hence both the ICV and MIC decrypt incorrectly, causing the received MPDU to be dropped.

2830.57: If it is identical, the frame shall be dropped.

2831.10: If there are no protocol instances indexed by that peer MAC address, the frame shall be dropped.

2832.57: The mesh STA with the numerically greater of the two MAC addresses shall drop the received SAE Commit message

2942.17: Any (#1836)EAPOL-Key PDUs with an invalid MIC are dropped and ignored.

2946.15: An AP that has both dot11ProtectedTXOPNegotiationActivated is false and dot11ProtectedQLoadReportActivated is false shall drop all received Public Key frames.

3022.57: — If the Peer Nonce field is present in the received frame, and the localNonce in the mesh peering instance is different from the Peer Nonce field of the received frame, the frame shall be dropped.

— If the peerNonce in the mesh peering instance exists and is different from the Local Nonce field of the received frame, the frame shall be dropped.

4437.1: The PHY entity shall switch to the IDLE state immediately after the energy drops below the specified threshold.

4571.27: If no such WIGTK exists, the WUR non-AP STA shall silently drop the frame and terminate BIP processing for this reception.

4614.32: Did receive signal strength drop significantly?

4615.3: the PHY shall keep decoding until receive signal strength drops significantly.

5383.34: For EDCA operation, this counter shall be incremented for each MSDU dropped by the AP on the voice access category."

5384.1/30/59: ditto “MSDU dropped by the AP”

5385.25: For EDCA operation, this counter shall be incremented for each MSDU dropped by the AP on the best effort access category and for each MSDU dropped by the AP on either user priority 0 or 3. For DCF operation, this counter shall be incremented for each MSDU dropped by the AP."

5385.59/60/62, 5386.26/57, 5387.21/50, 5388.15/44: ditto “MSDU dropped by the AP”

5411.5/19/34/48: When the RSSI drops below this threshold, a report is issued.

5682.6: If a stream is dropped, the scheduler might use the time available to resume contention. The scheduler might also choose to move the TXOPs for the STAs following the STA dropped to use the unused time.

5682.18: Figure K-3—Reallocation of TXOPs when a stream is dropped

5682.60: For example, UP-based ACU is possible by examining the UP field in TSPEC to decide whether to admit, retain, or drop a stream. If the UP is not specified, a default value of 0 is used. If a higher UP stream needs to be serviced, an ACU might drop lower UP streams.

5683.52: With *p* as the probability of dropping the frame, and *pe* as the

probability of the frame not being transmitted successfully (i.e., either the Data frame or the Ack frame

associated with it is in error), let *Np* be the number of retries required to maintain the probability of dropping

the frame to be *p*.

The probability of any given packet being dropped in such a channel after *Np* retries is given by

*pdrop = peNp + 1*

For example, in such a channel, if *pe* = 0.1 and *pdrop* = 10–8, then up to seven retries within the delay bound

are required, and the scheduler should consider these retransmissions in the cumulative TXOP allocations.

The Surplus Bandwidth Allowance (SBA) parameter causes the requesting STA to be allocated a minimum

amount of excess time by the scheduler so that the application dropped packet rates are bounded.

Also change “ignore” to “discard” in:

**10.23.5.7 RAW Operation with Resource Allocation frame**

The AP transmits the RA frame to non-AP STAs belonging to the RAW group allocated to access the RAW as specified in the previously transmitted RPS element. A non-AP STA that does not belong to the RAW group may ignore the RA frame.

**10.36.5.2 Rules for VHT sounding protocol sequences**

A STA ignores received VHT NDP Announcement, VHT NDP, and Beamforming Report Poll frames if dot11VHTSUBeamformeeOptionImplemented is false.

**10.42.10.2.3.4 MIMO phase–nonreciprocal**

A responder whose corresponding bit in the Group User Mask field of the MIMO Setup Control element included in the received MIMO BF Setup frame is equal to 0 can ignore frames transmitted in the following MU-MIMO BF training subphase and MU-MIMO BF feedback subphase.

**10.53.3 Group sectorization operation**

A non-AP STA that is not group sectorized capable may ignore the sectorized Beacon frame and is not subject to the rules described in this subclause.

**11.2.3.6 AP operation**

Until the transmission of this BU either has succeeded or is presumed failed (when maximum retries are exceeded), the AP shall acknowledge but ignore all PS-Poll frames from the same STA.

**11.3.3 Frame filtering based on STA state**

If an IBSS STA receives a Class 2 or Class 3 frame, it shall ignore the frame.

**11.3.5.3 AP or PCP association receipt procedures**

**11.3.5.5 AP or PCP reassociation receipt procedures**

This MLME-DISASSOCIATE.request primitive generates a protected Disassociation frame. If the association request was genuine, the STA has deleted the PTKSA by this point and so the protected Disassociation frame is ignored.

**11.21.2.8 BSS color in use event**

An AP shall not transmit frames to a non-AP HE STA during a TXOP, if it has received a BSS color in use event report from that non-AP HE STA with a nonzero BSS color in the Event Report field and the AP ignores an inter-BSS PPDU with the same BSS color value as the one carried in the Event Report field to obtain a TXOP by following the procedure in 26.10.2.2 (General operation with non-SRG OBSS PD level) and 26.10.2.3 (General operation with SRG OBSS PD level).

**11.31.3.1 General**

A STA that does not support the FST protocol shall ignore a received FST Setup Request frame.

**11.31.3.2 Transitioning between states**

Upon receipt of an FST Setup Request frame, the responder shall respond with an FST Setup Response frame unless it has a pending FST Setup Request frame addressed to the initiator and the responder has a numerically larger MAC address (see 12.7.1.1 (General) for comparison of MAC addresses) than the initiator’s MAC address, (#274)in which case the responder shall ignore the received FST Setup Request.

**11.31.5 On-channel Tunneling (OCT) operation**

A receiving TR-MLME shall ignore the received On-channel Tunnel Request frame if that frame is not targeting an NT-MLME in the same multi-band capable device as the TR-MLME.

**11.40 Notification of operating mode changes**

A VHT STA associated with a VHT AP shall ignore Notify Channel Width frames received from the VHT AP.

**26.6.3.4 Ack-enabled multi-TID A-MPDU operation**

A STA that transmits an ack-enabled multi-TID A-MPDU that contains at least two tagged MPDUs shall ignore the immediate response if it is an Ack frame.

**26.10.2.2 General operation with non-SRG OBSS PD level**

The received PPDU is an inter-BSS PPDU (see 26.2.2 (Intra-BSS and inter-BSS PPDU classification)), and the received PPDU is not a non-HT PPDU carrying a response frame (Ack, BlockAck, or CTS frame); or the received PPDU contains a CTS, a PHY-CCA.indication transition from BUSY to IDLE occurred within the PIFS time immediately preceding the received CTS, and that transition corresponded to the end of an inter-BSS PPDU that contained an RTS that was ignored following this procedure.

**26.10.3.2 PSR-based spatial reuse initiation**

may issue a PHY-CCARESET.request to ignore the associated HE TB PPDU(s) that are triggered by the Trigger frame

**29.9.2 WUR Short Wake-up frame operation**

Otherwise, a WUR AP shall not transmit WUR Short Wake-up frames to a WUR non-AP STA and the WUR non-AP STA shall ignore received WUR Short Wake-up frames with a matching WUR ID and FCS.

The WUR non-AP STA shall ignore received WUR Short Wake-up frames with a matching WUR ID and FCS after the WUR non-AP STA received a WUR Short Wake-up frame with a matching WUR ID and FCS, until a new WUR ID has been configured at the WUR non-AP STA by the WUR AP.

Proposed resolution:

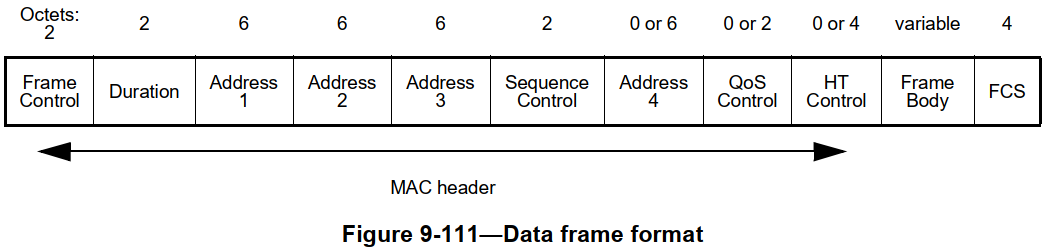
REVISED

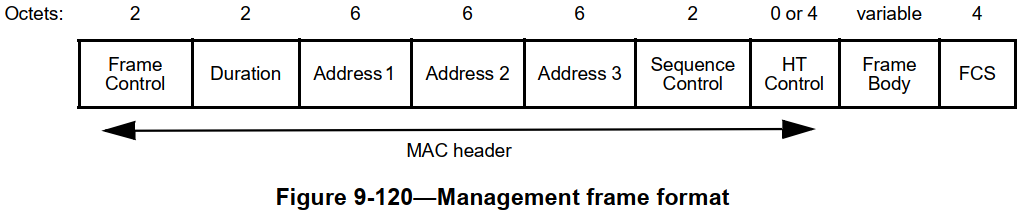
Make the changes shown under “Proposed changes” for CID 3683 in <this document>, which effect the requested changes.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3522  Mark RISON  10 | There are ~10 references to RA and TA "values" but they're not values, they're fields. Dito 3x SA/DA "values" | Make the changes shown under "Proposed changes" under CID 422 in 21/0829 (latest revision) |

Discussion:

Data and Management frames just have Address <n> fields:

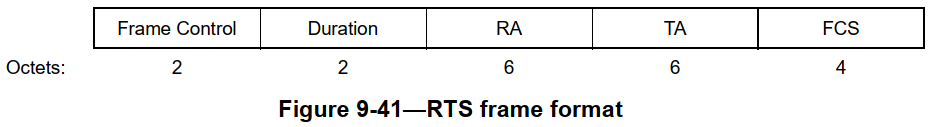




In Control frames, however, the first two address fields have an alternative or additional name:

The Frame Control, Duration and Address 1 (RA) fields are present in all control frame subtypes. The Address 2 (TA) field is present in some control frame subtypes.

and typically explicitly have that name on a per-frame basis, e.g.:



Having said this, the general description of MPDU fields is written as if there are specific field names, e.g.:

**9.2.4.3.7 RA field**

The RA field contains a (#1893)MAC address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field.

There are approximately 500 instances of “[RTSD]A field”, and many of these are for Data frames. So the pragmatic solution is to say that Address 1-4 fields can alternatively be referred to by the name of what they contain in any given context. Also, they can use the general convention that when we walk of “the X field” we mean “the value carried in the X field”, so no “RA field value” etc.

Proposed changes:

Make the following changes:

**9.3.2.1.2 Address and BSSID fields**

The content of the address fields of Data frames is dependent upon the values of the To DS and From DS subfields in the Frame Control field and whether the Frame Body field contains either an MSDU (or fragment thereof) or an A-MSDU (or fragment thereof)(11ax), as determined by the A-MSDU Present subfield of the QoS Control field (see 9.2.4.5.9 (A-MSDU Present subfield)). The content of the address fields transmitted by nonmesh STAs is defined in Table 9-58 (Address field contents for Data frames transmitted by nonmesh STAs(#462)). The content of the address fields transmitted by mesh STAs is defined in 9.3.5 (Frame addressing in an MBSS), and the content of the fields transmitted by GLK STAs is defined in 10.65 (Addressing of GLK Data frame transmission). Where the content of a field is shown as not applicable (N/A), the field is omitted. Note that Address 1 always holds the receiver address of the intended receiver (or, in the case of group addressed frames, receivers) and that Address 2 always holds the address of the STA that is transmitting the frame. Note also that the address fields can be referred to by their contents, e.g., the Address 1 field can be referred to as the RA field and the Address 3 field for a Data frame transmitted by a nonmesh non-GLK STA with To DS and From DS subfields equal to 0 can be referred to as the BSSID field.

**4.3.19 STA transmission of Data frames outside the context of a BSS**

When dot11OCBActivated is true, a sending STA sets the BSSID field to the wildcard BSSID ~~value~~ (see 9.2.4.3.4 (BSSID field)).

**4.3.30.1 General**

As described in 4.3.28.2 (Selective reception of group addressed frames), when a GLK AP transmits a Data frame with a four-address MAC header whose RA field contains a group address, the ~~contents of the~~ RA is a synthetic receiver address (SYNRA), and therefore its RA and DA ~~values~~fields are not equal. A GLK non-AP STA supports selective reception of group addressed frames by supporting SYNRA reception.

**9.3.1.5.1 General**

The BSSID (RA) field is set to the address of the STA contained in the AP. The TA field ~~value~~ is the address of the STA transmitting the frame or a bandwidth signaling TA. In a PS-Poll frame transmitted by a VHT STA or an HE STA(11ax) in a non-HT or non-HT duplicate format and where the scrambling sequence carries the TXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT, the TA field ~~value~~ is a bandwidth signaling TA.

**9.3.1.7.1 Overview**

The TA field ~~value~~ is the address of the STA transmitting the BlockAckReq frame or a bandwidth signaling TA. In a BlockAckReq frame transmitted by a VHT STA or an HE STA(11ax) in a non-HT or non-HT duplicate format and where the scrambling sequence carries the TXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT, the TA field ~~value~~ is a bandwidth signaling TA.

**9.3.1.8.1 Overview**

The TA field ~~value~~ is the address of the STA transmitting the BlockAck frame.

**9.3.2.1.2 Address and BSSID fields**

When a Data frame carries an MSDU (or fragment thereof), the DA and SA ~~values~~ related to that MSDU are carried in the Address 1, Address 2, Address 3, and Address 4 fields (according to the setting of the To DS and From DS subfields) as defined in Table 9-30 (Address field contents).

When a Data frame carries a (#279)Basic A-MSDU (or fragment thereof)(11ax), the DA and SA ~~values~~ related to each MSDU carried by the A-MSDU are carried within the A-MSDU subframe header. Zero, one, or both of these fields are present in the Address 1 and Address 2 fields as indicated in Table 9-30 (Address field contents).

**9.3.2.1.5 Duration field**

The Duration field calculation for the Data frame is based on the rules in 10.6 (Multirate support) that determine the data rate at which the Control frames in the frame exchange sequence are transmitted. If the calculated duration includes a fractional microsecond, that value is rounded up to the next higher integer. All STAs process Duration field ~~value~~s less than or equal to 32 767 from valid Data frames (without regard for the RA, DA, and/or ~~(#365)MAC address~~BSSID fields ~~values~~ that might be present in these frames) to update their NAV settings as appropriate under the coordination function rules.

**9.3.2.2.1 General**

(#462)An A-MSDU contains only MSDUs whose DA and SA parameter values (in the MA-UNITDATA.request primitive) map to the same receiver address (RA) and same transmitter address (TA) field ~~value~~s (see 10.11 (A-MSDU operation)), respectively.

**9.3.3.1 Format of (PV0) Management frames**

When the Address 1 field contains a group address and the frame subtype is either Probe Request or Action with Category Public, a wildcard BSSID ~~value~~ matches all receiving STA’s BSSIDs.

In Public Action frames, the Address 3 field is the BSSID~~. The BSSID value is~~, set according to 11.17 (Public Action frame addressing).

**9.6.8.2 FT Request frame**

The Target AP Address field is set to the BSSID ~~value~~ of the target AP’s BSS.

**9.6.8.3 FT Response frame**

The Target AP Address field is set to the BSSID ~~value~~ of the target AP’s BSS.

**9.6.8.4 FT Confirm frame**

The Target AP Address field is set to the BSSID ~~value~~ of the target AP’s BSS.

**9.6.8.5 FT Ack frame**

The Target AP Address field is set to the BSSID ~~value~~ of the target AP’s BSS.

**10.2.8 MAC data service**

The STA also validates the BSSID to verify that it either corresponds to the BSS of which the receiving STA is a member, or if dot11OCBActivated is true, that it contains the wildcard BSSID ~~value~~, indicating a Data frame sent outside the context of a BSS.

**10.3.2.3.2 RIFS**

RIFS shall not be used between frames with different RA field ~~value~~s.

**10.3.6 Group addressed MPDU transfer procedure**

A STA that is not an S1G relay STA shall discard an MPDU with a group address in the Address 1 field unless one of the following cases applies: (1) the value in the Address 1 field matches any value in the dot11GroupAddressesTable or ~~matches~~is the broadcast address ~~value~~, or (2) the STA is a GLK STA and the address in the Address 1 field is a SYNRA.

**10.11 A-MSDU operation**

An A-MSDU contains only MSDUs whose DA parameter values map to a single RA ~~field value~~ and whose SA parameter values map to a single TA ~~field value~~ (see 9.3.2.2 (Aggregate MSDU (A-MSDU) format)).

**10.23.2.4 Obtaining an EDCA TXOP**

A STA shall save the TXOP holder address for the BSS in which it is associated. (11ax)The TXOP holder address is the MAC address from the Address 2 field of the frame that initiated a frame exchange sequence except (11ax)if this is a CTS frame, in which case the TXOP holder address is the Address 1 field. If the TXOP holder address is obtained from a Control frame, a VHT STA (11ax)or HE STA shall save the nonbandwidth signaling TA ~~value~~ obtained from the Address 2 field. If a non-VHT non-HE STA(11ax) receives an RTS frame with the RA matching the MAC address of the STA and the MAC address in the TA field in the RTS frame matches the saved TXOP holder address, then the STA shall send the CTS frame after SIFS, without regard for, and without resetting, its NAV. If a VHT STA (11ax)or HE STA receives an RTS frame with the RA matching the MAC address of the STA and the nonbandwidth signaling TA ~~value~~ obtained from the Address 2 field in the RTS frame matches the saved TXOP holder address, then the STA shall send the CTS frame after SIFS, without regard for, and without resetting, its NAV. If a CMMG STA receives an RTS frame with the RA matching the MAC address of the STA and the TA ~~value~~ obtained from the Address 2 field in the RTS frame matches the saved TXOP holder address, then the STA shall send the CTS frame after SIFS, without regarding for, and without resetting its NAV. When a STA receives a frame addressed to it that requires an immediate response, except for RTS (11ax)and Trigger frames (see 26.5.2.5 (UL MU CS mechanism)), it shall transmit the response independent of its NAV. The saved TXOP holder address shall be cleared when the NAV is reset or when the NAV counts down to 0.

**10.28.3 Duration/ID field processing**

When the contents of a received Duration/ID field, treated as an unsigned integer and without regard for address ~~valu~~es, type, and subtype (even when type or subtype contain reserved values), are less than 32 768, the duration value is used to

**10.39.10 Updating multiple NAVs**

If a STA receives a valid CF-End frame response with RA and TA field ~~value~~s that match the NAVSRC and NAVDST values, in any order, for any NAV, then the STA shall set the associated NAV to the value of the Duration field in the received CF-End frame. If one of NAVSRC or NAVDST of a NAV is 0 and the corresponding NAVDST or NAVSRC, respectively, of the NAV matches the RA or the TA field ~~value~~ of the received valid CF-End frame, then the STA shall set the associated NAV to the value of the Duration field in the received CF-End frame.

If one of NAVSRC or NAVDST of a NAV is 0 and the nonzero NAVDST or NAVSRC of the NAV match either the RA or the TA field ~~value~~ of a (#1939)received frame, the NAVSRC or NAVDST that is 0 shall be set to the RA or TA that does not match the nonzero NAVSRC or NAVDST.

**11.1.3.8.2 Nontransmitted BSSID profile(11ax)**

(#4)A non-AP and non-PCP STA derives its nontransmitted BSSID ~~value~~ according to 9.4.2.45 (Multiple BSSID element) and 9.4.2.73 (Multiple BSSID-Index element).

**11.15.12 Switching between 40 MHz and 20 MHz**

A VHT STA is not required to perform any of the behavior described in this subclause associated with Information Request and 20 MHz BSS Width Request.

The following events are defined to be BSS channel width trigger events (TEs):

— TE-A: On any of the channels of the channel set defined in Clause 18 (Extended Rate PHY (ERP) specification), reception of a Beacon frame that does not contain an HT Capabilities element.

— TE-B: On any of the channels of the channel set defined in Clause 18 (Extended Rate PHY (ERP) specification), reception of a 20/40 BSS Coexistence Management, Beacon, Probe Request, or Probe Response frame that contains a value of 1 in a Forty MHz Intolerant field and that has the Address 1 field equal to the receiving STA’s address or to a group address ~~value~~, with no further addressing qualifications.

— TE-C: Reception of a 20/40 BSS Coexistence Management frame with the 20 MHz BSS Width Request field equal to 1 and with an Address 1 field that matches the receiving STA using either individual or group addressing and with a TA field that corresponds to the MAC address of a STA with which the receiver is associated.

— TE-D: Reception of a 20/40 BSS Coexistence Management frame containing at least one 20/40 BSS Intolerant Channel Report element with a nonzero length and with an Address 1 field equal to the receiving STA’s address or to a group address ~~value~~, but with no qualification of the Address 3 field.

**11.16 20/40 BSS Coexistence Management frame usage**

NOTE—A 20/40 BSS Coexistence Management frame is a Class 1 frame and, therefore, can be sent to a STA that supports reception of such frames and that is not a member of the same BSS as the transmitting STA. In such a case, the BSSID field of the frame is set to the wildcard BSSID ~~value~~, regardless of whether the Address 1 field contains an individual or group address ~~value~~.

**11.17 Public Action frame addressing**

A STA that is a member of a BSS and that transmits an individually addressed Public Action frame to a STA that is not a member of the same BSS shall set the BSSID field of the frame as follows:

— If the recipient STA is known to be a member of another BSS (including being an AP) and that BSS’s BSSID is known, the BSSID field shall be set to the BSS’s BSSID or the wildcard BSSID ~~value~~.

— Otherwise, the BSSID field of the frame shall be set to the wildcard BSSID ~~value~~.

A STA that is a member of a BSS and that transmits a group addressed Public Action frame shall set the BSSID field of the frame to the BSS’s BSSID or the wildcard BSSID ~~value~~.

A STA that is a member of a BSS and that transmits an individually addressed Public Action frame to a STA that is a member of the same BSS shall set the BSSID field of the frame to the BSS’s BSSID.

A STA that is not a member of a BSS and that transmits a Public Action frame shall set the BSSID field of the frame as follows:

— If the frame is individually addressed, the recipient STA is known to be a member of a BSS (including being an AP), and that BSS’s BSSID is known, the BSSID field shall be set to the BSS’s BSSID or the wildcard BSSID ~~value~~.

— Otherwise, the BSSID field of the frame shall be set to the wildcard BSSID ~~value~~.

**11.18 STAs communicating Data frames outside the context of a BSS**

d) The STA shall set the BSSID field in all Management and Data frames to the wildcard BSSID ~~value~~.

**11.22.3.2.6 GAS procedures interaction with multiple BSSID set**

When a Multiple BSSID (as defined in 11.10.14 (Multiple BSSID set)) set contains two or more members and dot11InterworkingServiceActivated is true and dot11GASAdvertisementID is present and a query to the advertisement server(#571) corresponding to dot11GASAdvertisementID is not dependent on the BSSID ~~value~~ used in the GAS frame exchange(#109) to post the query, then

**26.2.2 Intra-BSS and inter-BSS PPDU classification**

The Individual/Group bit in the TA field ~~value~~ is forced to 0 prior to comparison.

The Individual/Group bit in the TA field ~~value~~ is forced to ~~the value~~ 0 prior to the comparison.

**26.5.4.2 Eligible RA-RUs**

Number Of RA-RU~~s~~ subfield

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3522 in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3263  Mark RISON | Remove PSMP from the spec | As it says in the comment |

Discussion:

PSMP was marked obsolete in 802.11-2020.

There are 728 hits for PSMP in D2.1. I also searched for DTT, UTT and (service interval) granularity. Do any other terms need to be searched for?

Proposed changes:

In D2.1:

In Table 9-27—MFB subfield in the CMMG variant HT Control field, change 10.30.4 to 10.32.4 (3x).

In Table 9-168—Group Identity for a STA Statistics report row 13 at the end of the rightmost cell add a line “8 reserved octets” (note also deletion of the last 2 lines in the changes below).

In C.3 create a new dot11CountersGroup6 that supersedes dot11CountersGroup5 and is the same except for deleting dot11PSMPUTTGrantDuration and dot11PSMPUTTUsedDuration. Deprecate dot11CountersGroup5.

Change dot11CountersGroup3 to dot11CountersGroup6 in Table 9-144—Group Identity for a STA Statistics request (5x), Table 9-168—Group Identity for a STA Statistics report (5x), B.4.4.1 MAC protocol capabilities (1x), C.3 dot11RMRqstSTAStatRqstGroupID (5x), dot11STAStatisticsGroupID (5x). In the C.3 changes also change “Tablefor31” to “Subset1” etc.

Delete the following (entire subclause unless otherwise specified, only the highlighted portion where a yellow highlight is present):

Clause 3 definitions/abbreviations:

minimum downlink transmission time (DTT) to uplink transmission time (UTT)(#238) spacing:

power save multi-poll (PSMP):

power save multi-poll (PSMP) burst:

power save multi-poll downlink transmission time (PSMP-DTT):

power save multi-poll (PSMP) sequence:

power save multi-poll (PSMP) session:

power save multi-poll uplink transmission time (PSMP-UTT):

power save multi-poll uplink transmission time (PSMP-UTT) spacing:

PSMP [in 3.4]

PSMP-DTT [in 3.4]

PSMP-UTT [in 3.4]

4.3.13 High Throughput (HT) STA:

An HT STA has MAC features that include frame aggregation, some block ack features, power save multi-poll (PSMP) operation, reverse direction (RD), and protection mechanisms supporting coexistence with non-HT STAs.

4.3.24 DMG STA:

A DMG STA does not use any of the following: HCCA, power save multi-poll (PSMP), TDLS, GCR.

6.7.4.2 Semantics of the service primitive: aIUSTime and aDTT2UTTTime parameters of primitive, and rows of the table

Table 9-13—Ack policy: PSMP Ack row

9.2.5.2 Setting for single and multiple protection under enhanced distributed channel access (EDCA):

A STA always uses multiple protection in a TXOP that includes the following:

[…]

— PSMP frames

9.2.5.5 Settings within a PSMP sequence

9.2.5.6 Settings within a dual CTS sequence:

the Duration/ID field is set according to the rules in the following subclauses:

— 9.2.5.2 (Setting for single and multiple protection under enhanced distributed channel access (EDCA)) rule b) for multiple protection if Frame1 is not a QoS +CF-Poll frame and the TXOP holder is not operating under HCCA or PSMP

— 9.2.5.3 (Setting for QoS CF-Poll frames) if Frame1 is a QoS +CF-Poll frame and the TXOP holder is not operating under HCCA or PSMP

— 9.2.5.4 (Setting for frames sent by a TXOP holder under HCCA) if the TXOP holder is operating under HCCA

— 9.2.5.5 (Settings within a PSMP sequence). if the TXOP holder is operating under PSMP

9.4.1.24 PSMP Parameter Set field

9.4.1.25 PSMP STA Info field

Table 9-144—Group Identity for a STA Statistics request:

STA Counters from dot11CountersGroup3 (BlockAckReq, Channel Width, PSMP)

Table 9-168—Group Identity for a STA Statistics report:

STA Counters from dot11CountersGroup3 (BlockAckReq, Channel Width, PSMP):

dot11ImplicitBARFailureCount (Counter32),

dot11ExplicitBARFailureCount (Counter32),

dot11ChannelWidthSwitchCount (Counter32),

dot11TwentyMHzFrameTransmittedCount (Counter32),

dot11FortyMHzFrameTransmittedCount (Counter32),

dot11TwentyMHzFrameReceivedCount (Counter32),

dot11FortyMHzFrameReceivedCount (Counter32),

dot11PSMPUTTGrantDuration (Counter32),

dot11PSMPUTTUsedDuration (Counter32)

Table 9-190—Extended Capabilities field: PSMP Capability, S-PSMP Support, Service Interval Granularity rows (make the cells say Reserved and blank -- also notify ANA)

Table 9-198—Setting of Schedule subfield:

Scheduled PSMP or GCR-SP

Table 9-245—Power Save Mode definition: U-PSMP and S-PSMP rows (and Reserved row values updated to match)

Table 9-489—HT Action field values: PSMP row (and Reserved row values updated to match)

9.6.11.4 PSMP frame format

Table 9-629—A-MPDU contexts:

PSMP row

“outside a PSMP sequence” (2x)

Table 9-632—A-MPDU contents in the PSMP context

10.3.2.3.2 RIFS:

There are additional restrictions regarding when RIFS may be employed as defined in 10.29 (Reverse direction protocol) and 10.30 (PSMP operation).

10.3.2.3.4 PIFS:

— An HT AP during a PSMP sequence transmitting a PSMP recovery frame, as described in 10.30.2.3

(PSMP uplink transmission (PSMP-UTT))

10.6.5.1 Rate selection for non-STBC Beacon and non-STBC PSMP frames:

If the BSSBasicRateSet parameter is not empty, a non-STBC PSMP frame or a non-STBC Beacon frame that is not an ER beacon or HE beacon shall be transmitted in a non-HT PPDU using one of the rates included in the BSSBasicRateSet parameter.

10.6.5.3 Rate selection for other group addressed Data and Management frames:

This subclause describes the rate selection rules for group addressed Data and Management frames, excluding the following:

— Non-STBC Beacon and non-STBC PSMP frames

10.7 MSDU transmission restrictions:

For MSDUs or A-MSDUs belonging to the service class of QoSAck when the receiver is a QoS STA, the QoS Data frames that are used to send these MSDUs or A-MSDUs shall have Normal Ack, Implicit BAR, PSMP Ack or Block Ack ack policy.

10.23.2.8 Multiple frame exchange sequences in an EDCA TXOP:

In the case of PSMP, this AC transmission restriction does not apply to either the AP or the STAs participating in the PSMP sequence, but the specific restrictions on transmission during a PSMP sequence described in 10.30 (PSMP operation) do apply.

10.25.5 Selection of BlockAck and BlockAckReq variants:

(11ax)The Multi-TID BlockAck variant shall be used for all BlockAck frames related to an HT-immediate agreement transmitted inside a PSMP sequence and shall not be used otherwise. For non-HE STAs, the Multi-TID BlockAckReq variant shall be used for all BlockAckReq frames related to an HT-immediate agreement transmitted inside a PSMP sequence and shall not be used otherwise.

10.25.6.5 Generation and transmission of BlockAck frames by an HT STA, DMG STA, or S1G STA:

Except when operating within a PSMP exchange, [and change following a to A]

10.29.3 Rules for RD initiator:

An RDG shall not be present unless the MPDU carrying the grant, or every MPDU carrying the grant in an A-MPDU, matches one of the following conditions:

— (11ay)For a STA that is not an EDMG STA, a QoS Data frame with an ack policy other than PSMP Ack, (11ay)No explicit acknowledgment, or Scheduled Ack (i.e., including Implicit BAR), or

— (11ay)For an EDMG STA, a QoS Data frame with the Ack Policy field equal to any value except PSMP Ack or No explicit acknowledgment, or

— (11ay)For a non-DMG STA, a BlockAckReq frame related to an HT-immediate block ack agreement, or

— (11ay)For a non-DMG STA, an MPDU not needing an immediate response (e.g., block ack under an HT-immediate block ack agreement, or Action No Ack).

An RDG shall not be present within a PSMP sequence.

10.29.4 Rules for RD responder:

(11ay)The EDMG STA may aggregate in a multi-TID A-MPDU QoS Data frames with multiple TIDs as defined in Table 9-631 (A-MPDU contents in the data enabled no immediate response context) or Table 9-632 (A-MPDU contents in the PSMP context).

10.30 PSMP operation

10.70.1 General:

An EDMG STA may aggregate in a multi-TID A-MPDU QoS Data frames with multiple TIDs as defined in Table 9-631 (A-MPDU contents in the data enabled no immediate response context) or Table 9-632 (A-MPDU contents in the PSMP context).

11.2.3.11 PSMP power management

11.2.3.19 CMMG TXOP power save:

— In a received PSMP frame, the STA finds that the STA\_AID field in the PSMP STA Info field is not its AID nor does the PSMP Group Address ID subfield match its group address.

11.3.5.4 Non-AP and non-PCP STA reassociation initiation procedures:

If the reassociation is to the same AP (as described above), the following states, agreements, and allocations are not affected by the reassociation procedure:

1) PSMP sessions [and renumber following items, making sure cross-references to them are updated too]

11.4.6 PSMP management

14.2 Mesh STA dependencies:

An HT mesh STA does not support PSMP or STBC.

Table 19-25—HT PHY characteristics: aDTT2UTTTime and aIUStime rows

Table 23-41—S1G PHY characteristics: aDTT2UTTTime row

B.4.4.1 MAC protocol capabilities:

PC37 and all its children

HTM5.5 reference to 10.30.2.7 (PSMP acknowledgment rules)

C.3 deprecate the following:

dot11PSMPOptionImplemented

dot11STAStatisticsPSMPUTTGrantDuration

dot11STAStatisticsPSMPUTTUsedDuration

dot11RMNeighborReportExtCapPSMPSupport

dot11RMNeighborReportExtCapSPSMPSup

dot11RMNeighborReportExtCapServiceIntervalGranularity

dot11PSMPControlledAccess

dot11ServiceIntervalGranularity

dot11PSMPUTTGrantDuration

dot11PSMPUTTUsedDuration

C.3:

dot11WNMDiagConfigProfRprtPowerSaveMode syntax: delete upsmpMode(6), spsmpMode(7),

Table G-1—Attributes applicable to frame exchange sequence definition: more-psmp, no-more-psmp, psmp-ack rows

Appendix G:

Delete descriptions/definitions and uses of:

psmp-burst

non-last-psmp-sequence

last-psmp-sequence

downlink-phase

uplink-phase

psmp-allocated-time

psmp-ppdu

A frame-not-requiring-response may be included with any of the following sequences in any position, except the initial position when this contains a BlockAck frame or Multi-TID BlockAck frame: ppdu-bar, ppdu-ba-bar, ppdu-ba, ppdu-rd, ppdu-rd-bar, ppdu-ba-rd-bar, psmp-ppdu \*)

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3263 in <this document>, which delete all references to PSMP.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3697  Mark RISON  C.3 | There is no reference to dot11STACivicLocation in main body of the standard. The same thing apply to dot11STACivicLocationType.  Furthermore, it seems that dot11STACivicLocationConfigTable is poorly defined and probably does not pass MIB compilation. In description of "dot11RMCivicConfigured", there is a reference to dot11STACivicLocationEntry. However, dot11STACivicLocationEntry is not defined anywhere. | Delete dot11STACivicLocation |

Discussion:

dot11STACivicLocation does indeed not appear in the main body of the standard, but it influences dot11RMLCIConfigured, which “is written by the SME, which sets it to false when an external management entity configures dot11STACivicLocation and dot11STACivicLocationType” and does appear in the main body of the standard.

The MIB immediately prior to SA ballot of what became 802.11-2020 was validated by Yongho SEOK.

There are no instances of dot11STACivicLocationEntry in D2.0.

Proposed resolution:

REJECTED

Setting dot11STACivicLocation or dot11STACivicLocationType can change dot11RMLCIConfigured and dot11RMCivicConfigured, so dot11STACivicLocation and dot11STACivicLocationType are indirectly referred to in the main body of the standard.

The MIB is believed to compile (the MIB immediately prior to SA ballot of what became 802.11-2020 was validated).

dot11STACivicLocationEntry does not appear anywhere in D2.0.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3694  Mark RISON  C.3 | Why is there a MIB variable dot11VHTNumberSoundingDimensions but not dot11VHTBeamformeeSTSCapability | Add a MIB attribute dot11VHTBeamformeeSTSCapability |

Discussion:

This is the set of MIB attributes mentioned under dot11VHTTransmitBeamformingConfigTable in Table 21-27—VHT PHY MIB attributes:

dot11VHTSUBeamformeeOptionImplemented

dot11VHTSUBeamformerOptionImplemented

dot11VHTMUBeamformeeOptionImplemented

dot11VHTMUBeamformerOptionImplemented

dot11VHTNumberSoundingDimensions

dot11VHTBeamformeeNTxSupport

dot11VHTNumberSoundingDimensions is described as:

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the number of antennas used by the beamformer

when sending beamformed transmissions."

dot11VHTBeamformeeNTxSupport is described as:

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the maximum number of space-time streams that the

STA can receive in a VHT NDP, the maximum value for NSTS, total that can

be sent to the STA in a VHT MU PPDU if the STA is MU beamformee capable and

the maximum value of Nr that the STA transmits in a VHT Compressed

Beamforming frame."

These map to the following fields in Table 9-311—Subfields of the VHT Capabilities Information field respectively:

Number of Sounding Dimensions: Beamformer’s capability indicating the maximum value of the TXVECTOR parameter NUM\_STS for a VHT NDP.

Beamformee STS Capability: Indicates the maximum number of space-time streams that the STA can receive in a VHT NDP and the maximum value of Nr that the STA transmits in a VHT Compressed Beamforming frame.

So there is a MIB attribute for beamformee STS capability, it’s just called something different.

I think “number of antennas used by the beamformer” is equivalent to “value of the TXVECTOR parameter NUM\_STS for a VHT NDP”, though dot11VHTNumberSoundingDimensions is missing “maximum”.

I note dot11VHTBeamformeeNTxSupport has “the maximum value for NSTS, total that can be sent to the STA in a VHT MU PPDU if the STA is MU beamformee capable” but the capability field doesn’t.

However, Table 9-313—Supported VHT-MCS and NSS Set subfields has a field Maximum NSTS,total defined as “If MU beamformee capable and different from 0, indicates the maximum value for NSTS,total minus 1 that can be sent to the STA in a VHT MU PPDU.

NOTE—This value is greater than or equal to the value in the Beamformee STS Capability subfield of the VHT Capabilities Information field.

If MU Beamformee capable and equal to 0, indicates that the maximum value for NSTS,total is equal to the value in the Beamformee STS Capability subfield of the VHT Capabilities Information field.”

So the Beamformee STS Capability field sometimes indicates the MU STS capability (but note the minus 1, missed by the Maximum NSTS,total field description).

But what if the Maximum NSTS,total field is non-zero and not equal to the Beamformee STS Capability field? How can dot11VHTBeamformeeNTxSupport cover this case?

Proposed resolution:

REVISED

In D2.1:

At 5342.26 change “This attribute indicates the number of antennas used by the beamformer when sending beamformed transmissions” to “This attribute indicates the maximum number of antennas used by the beamformer when sending beamformed transmissions”.

At 1226.24 change “Indicates the maximum number of space-time streams that the STA can receive in a VHT NDP and the maximum value of Nr that the STA transmits in a VHT Compressed Beamforming frame.” to “Indicates the maximum number of space-time streams that the STA can receive in a VHT NDP, the maximum value for NSTS,total that can be sent to the STA in a VHT MU PPDU if the STA is MU beamformee capable (subject to the Maximum NSTS,total field in the Supported VHT-MCS and NSS Set field) and the maximum value of Nr that the STA transmits in a VHT Compressed Beamforming frame.” with the first NSTS,total italicised and with all but the N subscript.

At 1230.15 change “If MU Beamformee capable” to “If MU beamformee capable”.

At 1230.17 change “is equal to the value in the Beamformee STS Capability subfield of the VHT Capabilities Information field.” to “is indicated by the Beamformee STS Capability subfield of the VHT Capabilities Information field.”

Note to the commenter: dot11VHTBeamformeeNTxSupport contains the beamformee STS capability.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3538  Mark RISON  C.3 | It is not clear whether dot11RSNAStatsCMACReplays includes Management replays, i.e. includes the number in dot11RSNAStatsRobustMgmtCCMPReplays | State in the description of the latter that it does not include the former |

Discussion:

There is a zoo of MIB attributes, including:

dot11RSNAStatsCMACReplays

dot11RSNAStatsRobustMgmtCCMPReplays

dot11RSNAStatsCCMPReplays

dot11RSNAStatsRobustMgmtGCMPReplays

dot11RSNAStatsGCMPReplays

Note the GCMP ones are not in STA Statistics reports (see Table 9-168—Group Identity for a STA Statistics report), and they are in dot11DMGCountersTable, even though they (can) apply to non-DMG STAs too.

Note also there is no dot11RSNAStatsGMACReplays (or dot11RSNAStatsGCMPDecryptErrors).

We have:

[CCMP general] When discarding a frame, the receiver shall increment by 1 dot11RSNAStatsCCMPReplays for Data frames or dot11RSNAStatsRobustMgmtCCMPReplays for robust Management frames.

[BIP] If the value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this IGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

[GCMP general] When discarding a frame, the receiver shall increment by 1 dot11RSNAStatsGCMPReplays for Data frames or dot11RSNAStatsRobustMgmtGCMPReplays for robust Management frames.

So the same MIB attribute is used for groupcasts, but not for unicasts.

Proposed changes:

Change in C.3 as follows:

dot11RSNAStatsCCMPReplays OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the MAC when the condition described below occurs.

~~The number of received CCMP MPDUs discarded by the replay mechanism.~~

The number of received Data frames discarded due to CCMP replay errors."

::= { dot11RSNAStatsEntry 8 }

dot11RSNAStatsCMACReplays OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the MAC when the condition described below occurs.

The number of received ~~MPDUs~~ group addressed robust Management and protected Beacon frames discarded (#1401)due to ~~CMAC~~BIP replay errors."

::= { dot11RSNAStatsEntry 12 }

dot11RSNAStatsRobustMgmtCCMPReplays OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the MAC when the condition described below occurs.

The number of received individually addressed robust Management frames discarded due to CCMP replay errors."

::= {dot11RSNAStatsEntry 13}

dot11RSNAStatsGCMPReplays OBJECT-TYPE

SYNTAX Unsigned32 (0..4294967295)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the ~~SME or an external management entity~~ MAC when the condition described below occurs.

~~Counter for the number of times an MPDU with the Type subfield equal to Data is discarded due to PN violation.~~

The number of received Data frames discarded due to GCMP replay errors."

DEFVAL { 0 }

::= { dot11DMGCountersEntry 1 }

dot11RSNAStatsRobustMgmtGCMPReplays OBJECT-TYPE

SYNTAX Unsigned32 (0..4294967295)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the ~~SME or an external management entity~~ MAC when the condition described below occurs.

~~Counter for the number of times a Management frame is discarded due to PN violation.~~

The number of received individually addressed robust Management frames discarded due to GCMP replay errors."

DEFVAL { 0 }

::= { dot11DMGCountersEntry 2 }

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3538 in <this document>. Note to the commenter: dot11RSNAStatsCMACReplays is for groupcasts, while dot11RSNAStatsRobustMgmtCCMPReplays is for unicasts. Also, dot11RSNAStatsCMACReplays also counts GMAC replays and protected Beacon replays.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3526  Mark RISON  6.5.4.2 | aCMMGPPMinListeningTime and other PHY characteristics are missing from 6.5.4.2 | At the end of 6.5.4.2 add "NOTE---There are other PHY characteristics, described in the corresponding clauses." |

Discussion:

Subclause is wrong: should be 6.7.4.2.

CID 3276 was resolved as:

REVISED (GEN: 2022-12-05 19:23:16Z) at p540.40 change "provides the PHY" to "provides PHY" (delete "the").

So the same approach can be taken here. But the wording should be consistent.

Proposed resolution:

REVISED

In D2.1:

In 6.7.3.1 change "provide the PHY operational characteristics" to "provide PHY operational characteristics"

In 6.7.4.1 change "provides (#3276)PHY operational parameters" to "provides PHY operational characteristics"

In 6.7.4.4 change "provides the operational characteristics of the PHY entity" to "provides PHY operational characteristics"

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3504  Mark RISON  C.3 | A STA acting as a TDLS STA shares its MIB attributes with when it's acting as a STA of its AP. Some MIB attributes that would not apply (e.g. group frame counts) or would need doubling (e.g. unicast frame counts) or might differ (e.g. dot11RSNAProtectedManagementFramesActivated) | Have MIB attributes for TDLS separate from the non-TDLS STA |

Discussion:

Some settings can certainly differ between the link to the AP and the link to a peer TDLS STA (e.g. for security). There is no clear way to identify these, however, nor is there a way to handle the settings that can differ on the link to the peer TDLS STA.

Proposed resolution:

In C.3 rename NOTE to NOTE 1 and after it add:

“NOTE 2—Certain MIB attributes for a TDLS STA only apply to the link with the AP.”

Note to the commenter: there is no easy way to identify the attributes that only apply to the AP link, nor is there any way to access the corresponding settings for the TDLS link(s).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3271  Mark RISON  C.3 | dot11NonAPStationBroadcastCipherSuite -- don't we also need one for the AP? | Add a dot11APBroadcastCipherSuite |

Discussion:

We have dot11NonAPStationUnicastCipherSuite and dot11NonAPStationBroadcastCipherSuite in the MIB, but no AP equivalents.

The former is mentioned in R.4.2.5 Link Layer Encryption Method (in R.4.2 SSPN interface parameters), though it is not immediately clear exactly how it is used:

**R.4.2.5 Link Layer Encryption Method**

This parameter indicates the link layer encryption method selected during the RSNA establishment process for protecting the pairwise communication between the non-AP STA and the AP. The cipher suite format of this parameter is drawn from the RSNE defined in 9.4.2.24 (RSNE). The AP obtains this information about the STA via the MLME SAP.

In the interworking service, the SSPN also participates in the selection of the cipher suite selection, as described in 11.22.5. Therefore, the link layer encryption method selected will meet or exceed the security requirement of the SSPN.

NOTE—In interworking, the SSPN can require visibility and configurability of the STA access.

With this information available to the SSPN, the operator would be able to have better control, e.g., barring access to IEEE 802.11 networks if null encryption is used. This is also related to the operator network’s configuration, e.g., if preauthentication should be supported.

The following is used:

— dot11NonAPStationUnicastCipherSuite

So the argument could be that we need the interworking MIB attributes from Dot11InterworkingEntry that are referred to somewhere (other than just C.3). But then there is no justification for having dot11NonAPStationBroadcastCipherSuite and dot11NonAPStationAssociatedSSID, which are not used anywhere.

Proposed resolution:

REVISED

Deprecate dot11NonAPStationBroadcastCipherSuite and dot11NonAPStationAssociatedSSID with reason “This is not required for interworking.”

Note to the commenter: a dot11APBroadcastCipherSuite is not needed for interworking.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3508  Mark RISON  11.52 | Given beacon protection, we also need broadcast probe response protection in FILS, or at least a statement that thou shalt not trust unprotected broadcast probe responses. Note that a broadcast probe response might be issued as a result of a probe request used to fetch updated EDCA parameters with a BSS | At the end of the third para of the referenced subclause add "If dot11BeaconProtectionEnabled is true, a non-AP STA shall discard broadcast Probe Response frames." |

Discussion:

The resolution of CID 1528 said:

Beacon protection only provides protection to associated STAs. It does not apply to unassociated STAs. Unassociated STAs can use broadcast Probe Response frames and FILS discovery frames to discover APs however, the information received in such frames cannot be trusted. The proposed change would limit the STAs ability to discover APs.

Proposed resolution:

REVISED

At the end of the third para of the referenced subclause add "If dot11BeaconProtectionEnabled is true, a non-AP STA shall discard broadcast Probe Response frames received from an associated AP."

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3181  Mark RISON  6  408.51 | "The operating class of the advertised BSS." -- I'm not sure BSSes have OCs; channel numbers have them. Also "operating class of the transmitting AP" in 22/0115 | Clarify |

Discussion:

There are about 20 hits for “operating class[es] of” in D2.1:

* … the BSS
* … the advertised BSS
* … the STA [also “the STA’s operating class”]
* … the AP or PCP
* … those 6 GHz APs
* … the channel
* … the BSS channel width trigger event

9.4.2.8 Country element says “An operating class is an index into a set of values for radio equipment sets of rules.”

E.1 Country information and operating classes says “The operating class value is an index into sets of values for radio operation in a regulatory domain.”

So not very clearly defined. However, ultimately an operating class allows you to understand what a channel index/number refers to, and any constraints (“behavior limits”), so I think it pertains to a channel.

Proposed resolution:

REVISED

In D2.1:

At 1485.56 in “the Channel Number is a channel from the STA’s operating class as defined in E.1” change “STA’s operating class” to “operating class of the STA”.

At 2554.59 in “If a Supported Operating Classes element is present in the received Beacon frame, the operating class of the BSS channel width trigger event is set to the value of the Current Operating Class field of the Supported Operating Classes element of the received Beacon frame;” delete “set to”.

At the end of 1.4 add a para:

References to the operating class of a BSS or STA are to be understood as being to the operating class pertaining to the channel on which the BSS or STA operates.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3370  Mark RISON | An "Ethernet 89-0d frame" is not a frame, it's an MSDU | Change to "Ethernet 89-0d payload" throughout |

Discussion:

The actual spec wording is “EtherType 89-0d frame”. However, in any case it’s not a frame = MPDU, it’s an MSDU.

The relevant occurrences of 89-0d in D2.1 are:

**3.2 Definitions specific to IEEE Std 802.11**

(#237)tunneled direct link setup (TDLS) frame (TDLS frame): A Data frame carrying all or part of the encapsulation of a TDLS Action field, using (#2186)EtherType 89-0d.(#1356)

**11.20.2 TDLS payload**

(#196)TDLS uses (#2186)EtherType 89-0d frames, as defined in Annex H, for TDLS signaling. The Payload field of the (#2186)EtherType 89-0d frame contains one of the TDLS Action fields specified in 9.6.12 (TDLS Action field formats) followed by zero or more Vendor Specific elements.(#1680)

**11.22.3.4 Registered location query protocol (RLQP) procedures**

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

When security is required by regulation, the (#2186)EtherType 89-0d frame body may employ corresponding security features.

**11.31.6 FST payload**

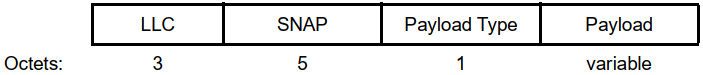
When FST Action frames are forwarded by an AP, FST uses (#2186)EtherType 89-0d frames as defined in Annex H. In this case, the FST payload contains an FST Action frame body as is specified in 9.6.20 (FST Action frame details).

**13.10.3 Remote Request/Response frame definition**

The Remote Request frame is transmitted over the DS from the current AP to the target AP. The Payload for the Remote Request/Response frame is given in Table 13-2 (Remote Request/Response Payload format). Remote Request/Response frames shall use an (#2186)EtherType of 89-0d, as specified in Annex H. The Remote Request/Response frame contains Version, Type, and Length fields, along with the AP Address.

**Annex H, Usage of EtherType 89-0d(#2186)**

The (#2186)EtherType 89-0d frame body is specified in Figure H-1 ((#2186)EtherType 89-0d frame body), omitting any possible security header and trailer.



**Figure H-1—(#2186)EtherType 89-0d frame body**

LLC is defined in ISO/IEC 8802-2:1998.

SNAP is defined in IEEE Std 802. The formatting of the SNAP header is according to IETF RFC 1042. The EtherType(#2186) is set to 89-0d.

The approach chosen here is to consistently refer to an “MSDU with EtherType xx-yy”.

Proposed changes:

In D2.1 change as follows:

**3.2 Definitions specific to IEEE Std 802.11**

(#237)tunneled direct link setup (TDLS) frame (TDLS frame): A Data frame carrying all or part of the

encapsulation of a TDLS Action field~~, using~~ in an MSDU with (#2186)EtherType 89-0d.(#1356)

**11.20.2 TDLS payload**

(#196)TDLS uses MSDUs with (#2186)EtherType 89-0d ~~frames~~, as defined in Annex H, for TDLS signaling. The Payload field of the ~~(#2186)EtherType 89-0d frame~~MSDUs contains one of the TDLS Action fields specified in 9.6.12 (TDLS Action field formats) followed by zero or more Vendor Specific elements.(#1680)

**11.22.3.4 Registered location query protocol (RLQP) procedures**

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

When security is required by regulation, the Payload field of the MSDUs with (#2186)EtherType 89-0d ~~frame~~ body may employ corresponding security features.

**11.31.6 FST payload**

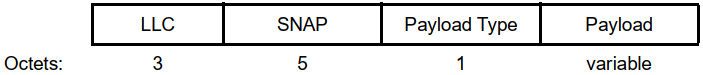
When FST Action frames are forwarded by an AP, FST uses MSDUs with (#2186)EtherType 89-0d ~~frames~~ as defined in Annex H. In this case, the ~~FST payload~~Payload field of the MSDUs contains an FST Action frame body as is specified in 9.6.20 (FST Action frame details).

**13.10.3 Remote Request/Response frame definition**

The Remote Request frame is transmitted over the DS from the current AP to the target AP. ~~The Payload for the Remote Request/Response frame is given in Table 13-2 (Remote Request/Response Payload format).~~ Remote Request/Response frames shall use an MSDU with (#2186)EtherType ~~of~~ 89-0d, as specified in Annex H. The Payload field of the MSDU for the Remote Request/Response frame is given in Table 13-2 (Remote Request/Response Payload format). The Remote Request/Response frame contains Version, Type, and Length fields, along with the AP Address.

**Annex H, Usage of EtherType 89-0d(#2186)**

The (#2186)MSDU with EtherType 89-0d ~~frame body~~ is specified in Figure H-1 ((#2186)EtherType 89-0d frame body)~~, omitting any possible security header and trailer~~.



**Figure H-1—MSDU with EtherType 89-0d ~~frame body~~**

LLC is defined in ISO/IEC 8802-2:1998.

SNAP is defined in IEEE Std 802. The formatting of the SNAP header is according to IETF RFC 1042. The EtherType(#2186) field is set to 89-0d.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3370 in <this document>, which refer to MSDUs with EtherType 89-0d instead.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3400  Mark RISON  9 | "The RSNE is present" -- sometimes it's "otherwise not present", sometimes not | Add "otherwise not present" where not present |

Discussion:

If a STA does not have RSNA support activated, it should not transmit an RSNE as this would be interpreted by the receiver as supporting RSNAs.

Note there are similar issues with e.g. FTE, but these are not dealt with below.

Proposed resolution:

REVISED

In D2.1:

Add “; otherwise not present” at the end of the following locations:

Table 9-60—Beacon frame body: The RSNE is present within Beacon frames generated by STAs that have dot11RSNAActivated equal to true [+change “within Beacon frames generated by STAs that have dot11RSNAActivated equal to” to “if dot11RSNAActivated is”]

Table 9-62—Association Request frame body: The RSNE is present if dot11RSNAActivated is true

Table 9-458—TDLS Discovery Response frame Action field format: The RSNE is present if security is required on the TDLS direct link (see 12.7.8.1 (General))

Table 9-483—FT Request frame body: A RSNE is present if dot11RSNAActivated is true [+change “A” to “The”]

Table 9-484—FT Response frame body: The RSNE is present if dot11RSNAActivated is true

Table 9-485—FT Confirm frame body: The RSNE is present if dot11RSNAActivated is true

Table 9-486—FT Ack frame body: The RSNE is present if dot11RSNAActivated is true

Table 9-498—Information for TDLS Setup Request Action field: The RSNE is present if security is required on the TDLS direct link (see 12.7.8.1 (General))

Table 13-1—FT authentication elements: The RSNE is present if dot11RSNAActivated is true

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3699  Mark RISON  9 | It is not clear that the requirements in the NOTEs in the table Setting of the Supported Channel Width Set subfield and Extended NSS BW Support subfield at a STA transmitting the VHT Capabilities Information field are normatively stated or implied elsewhere | Delete the "NOTE---"s so that the statements are normative |

Discussion:

The NOTEs in question are as follows.

NOTE 1—Max VHT NSS is defined per MCS in 9.4.2.157.3 (Supported VHT-MCS and NSS Set field).

This is indeed normatively specified in the referenced location, so OK.

NOTE 2—CCFS1 refers to the Channel Center Frequency Segment 1 field of the most recently transmitted VHT Operation element.

NOTE 3—CCFS2 refers to the Channel Center Frequency Segment 2 field of the most recently transmitted HT Operation element.

These clarify how CCFS1/2 are to be understood in the table. But they should be referred to explicitly in the column headings.

NOTE 4—CCFS1 is nonzero when the current BSS bandwidth is 160 MHz or 80+80 MHz and the NSS support is at least Max VHT NSS. CCFS2 is zero in this case.See NOTE 7.

NOTE 5—CCFS2 is nonzero when the current BSS bandwidth is 160 MHz or 80+80 MHz and the NSS support is less than Max VHT NSS. CCFS1 is zero in this case. See NOTE 7.

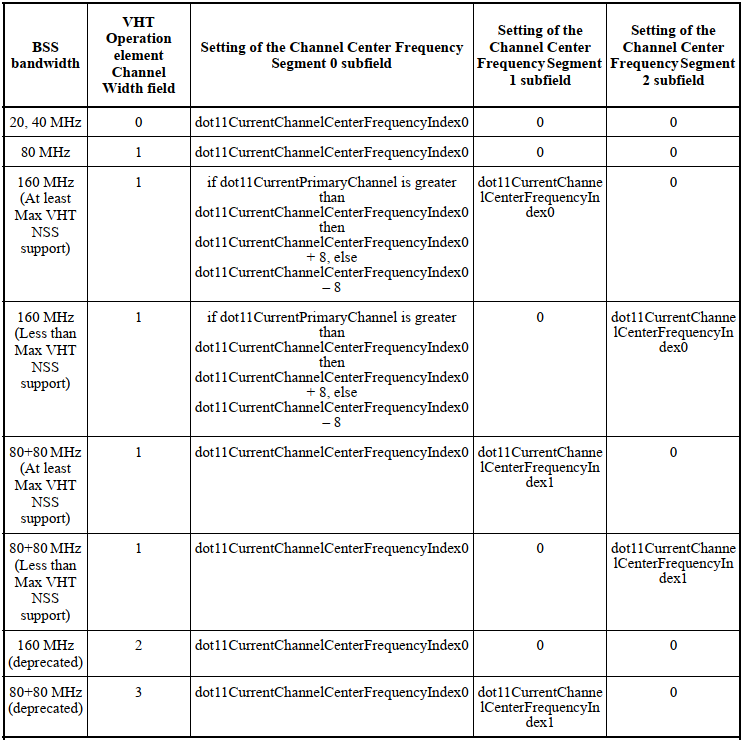
NOTE 6—At most one of CCFS1 and CCFS2 is nonzero when the current BSS bandwidth is 160 MHz or 80+80 MHz. See NOTE 7.

All these are making informative statements of fact, which need to be supported by normative text. So the question is whether NOTE 7 helps.

[Missing space before the See in NOTE 4.]

NOTE 7—See Table 11-27 (Setting of Channel Center Frequency Segment 0, Channel Center Frequency Segment 1, and Channel Center Frequency Segment 2 subfields).

Here is what the table says:



So NOTEs 4 and 5 are true except for the deprecated 160 signalling, and ambiguous for the deprecated 80+80 signalling (is the NSS support less than Max VHT NSS?). We should avoid incorrect statements.

NOTE 6 is indeed normatively specified in the table, so OK. It’s true for all BSS bandwidths, in fact.

NOTE 8—A receiving STA in which dot11VHTExtendedNSSBWCapable is false will ignore the Extended NSS BW Support subfield and effectively evaluate this table only at the entries where Extended NSS BW Support is 0.

I think this is indeed normatively specified in 10.6.13.1 Rx Supported VHT-MCS and NSS Set and 10.6.13.2 Tx Supported VHT-MCS and NSS Set, so OK.

NOTE 9—See also 11.38 (VHT BSS operation).

Not sure what this is in reference to, but clearly not normative, so OK.

Proposed changes:

In D2.1:

At the bottom of the rightmost 2 cells at the top of the table add “(see NOTEs 2 and 3)”.

In NOTE 4, add a space before “See”.

In NOTE 6, delete “when the current BSS bandwidth is 160 MHz or 80+80 MHz”.

At the start of NOTEs 4 and 5 add “When the VHT Operation element Channel Width field is not 2 or 3, ”

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3699 in <this document>. Note to the commenter: some of the NOTEs clarify interpretation of the table, and the others are supported by normative text elsewhere. However, some small clarifications have been made.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3466  Mark RISON  12.7.2  2902.63 | "It may contain 0 if a nonce is not required to be sent." is confusing | Change to "It shall contain 0 if a nonce is not required to be sent." |

Discussion:

I think it’s trying to say that in those cases where a nonce is not required, it is set to 0. However, Jouni MALINEN has suggested that some implementations set a non-zero value in M4.

Proposed changes:

In D2.1:

Change at 2907.56 as follows:

e) **Key Nonce**. This field conveys the ANonce from the Authenticator and the SNonce from the

Supplicant. It ~~may~~should contain 0 if a nonce is not required to be sent.

NOTE 9—Some deployed Supplicant implementations set the Key Nonce field in message 4 of the 4-way handshake to the same value as in message 2.

and renumber subsequent NOTEs.

Change at 2923.45 as follows:

Key Nonce = 0 (but see 12.7.2)

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3466 in <this document>, which clarify that although the Key Nonce field should be 0 if not needed, it might be set to a non-zero value in M4 by some implementations.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3385  Mark RISON  20  3368.40 | Terminology like "RS(224,208)+Block-Code(16,8)" does not appear to be defined (appears in C20, C24 and I) | Add definitions of RS(), SPC() and Block-Code() |

Discussion:

Assaf KASHER helpfully drew my attention to the fact that these are used in low-power SC modes, which are specified to be obsolete. So the only issue is in Annex I, which he thinks should be made obsolete too.

Proposed resolution:

REVISED

At the end of the para in I.7.3.1 add “The DMG low-power SC mode is obsolete.”

At the end of the first para in I.7.4.1 add “The DMG low-power SC mode is obsolete.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3175  Mark RISON | The way Action frames are described is very confusing. An Action frame contains an Action field, which always starts with a Category subfield, and it's that Category field that is referred to when we talk of a Blah Action frame (as the set of frames; individual frames are just called Foo frames, not Foo Action frames) | Describe how Action frames are identified and referred to in the spec |

Discussion:

There is in fact a description in 9.4.1.11 Action field (not in 9.6 Action frame format details):

Action frames of a given category are referred to as <category name> Action frames. For example, frames in the QoS category are called QoS Action frames. Action frames of a given category and further identified by a subfield in the Action Details field are referred to as <subfield name> frames. For example, frames in the QoS category with a QoS Action subfield of ADDTS Request are called ADDTS Request frames.

The bit on the subfield in the Action Details field is unnecessarily vague: except for Vendor Specific Action frames, it’s specifically the first octet in that field, which is a <blah> Action field.

Proposed changes:

In D2.1:

Delete the following text from 9.4.1.11 Action field (not in 9.6 Action frame format details):

Action frames of a given category are referred to as <category name> Action frames. For example, frames in the QoS category are called QoS Action frames. Action frames of a given category and further identified by a subfield in the Action Details field are referred to as <subfield name> frames. For example, frames in the QoS category with a QoS Action subfield of ADDTS Request are called ADDTS Request frames.

Add the following para above the para that starts “References in this standard to a “<name> frame”” in 1.4:

References in this standard to “<name> Action frames”, where <name> corresponds to a category identified in Table 9-79 (Category values), are to be understood as being to “Action frames whose Category field indicates <name>”, and references in this standard to a “<name> Action frame”, where <name> corresponds to an Action frame subtype identified by the octet immediately after the Category field (the <something> Action field identified in the subclauses of Subclause 9.6 (Action frame format details), are to be understood as being to “an Action frame with that <something> Action field (and the corresponding Category field)”. For example, frames in the QoS category are called QoS Action frames, and frames in the QoS category with a QoS Action subfield of ADDTS Request are called ADDTS Request frames. Vendor Specific frames are a special case in that they are identified from the Category field and do not have a <something> Action field.

Change “9.6.5 Vendor-specific Action frame details” to “9.6.5 Vendor-specific frame details”.

Change “9.6.27 Control Response MCS Negotiation frame details” to “9.6.27 Control Response MCS Negotiation Action frame details”.

Change “9.6.33 WUR Action details” to “9.6.33 WUR Action frame details”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 3175 in <this document>, which move the clarification of the Action frame terminology from 9.4.1.11 to 1.4 and use the formulation from there. Some editorial inconsistencies are also addressed.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3057  Graham SMITH  16  3136.1 | Is it time to look at removing Clause 16 HR/DSSS aka CCK from the standard? 5.5 and 11Mbps are better served by 6 and 12 Mbps OFDM. Fallback tends to go 12, 6, 2, 1 and 11 and 5.5 ar not used. Furthermore having to support the CCK modem in addition to OFDM is a waste. Going forward there is no technical reason to keep CCK as a chipset supporting only 11b still needs two modems and it is easier to replace the CCK with OFDM even if only for 6 and 12 Mbps. | Let's have a discussion and get input to see if chipsets are really using CCK or whether, as I suspect, they skip over it using 6 and 12Mbbs OFDM rather than 5.5 and 11. (Or if not, they should be). |

Discussion:

See <https://mentor.ieee.org/802.11/dcn/22/11-22-1868-01-000m-cck-deprecation-discussion.pptx> .

Proposed resolution:

REJECTED

This proposal was extensively discussed in the task group, but consensus could not be found to make this change at present. The reasons given for this included:

- There are still 11b-only implementations, which have value in certain use cases

- The benefit of removing CCK from the standard would be small

- CCK is not burdensome to implement

- Certain external standards allow for operation above 2 Mbps without use of OFDM

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3329  Mark RISON  4.5.4.9  314.45 | "Management frame protection protocols in an MBSS apply to the following frames:  -- Individually addressed robust Management frames, after establishment of the MTK,  -- Group addressed Action frame " -- also Action No Ack frames? Ditto other locations identified under CID 1980 in 22/0353r1 | Change "Action frame" to "Action and Action No Ack frames" |

Discussion:

MFP applies to Action No Ack frames just as it does to Action frames.

Proposed changes:

In 4.5.4.9 Management frame protection, "Action frame" needs to become "Action or Action No Ack frame":

Management frame protection protocols in an MBSS apply to the following frames:

— Individually addressed robust Management frames, after establishment of the MTK,

— Group addressed Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values), after establishment of the MGTK, and

— Group addressed robust Management frames that are not Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values), after establishment of the IGTK.

The MME is present when management frame protection is enabled at the AP and the frame is a group addressed robust Action frame not of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values).

Proposed resolution:

REVISED

Change "Action frame"[s] to "Action or Action No Ack frame"[s] in 4.5.4.9 (3x).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3361  Mark RISON | Per CID 1630, "time priority Management frame:" etc. needs to become "time priority management frame:" | As it says in the comment |

Discussion:

Subclauses 3.1 and 3.2 are an exception to the rule that frame types/names are capitalised. However abbreviations like EAP, EAPOL and TVHT remain capitalised.

Also, elements/frames have one name and this remains capitalised.

Proposed resolution:

REVISED

Lowercase the following terms before the colon in Subclauses 3.1 and 3.2:

mesh Data frame:

robust Action frame:

robust Management frame:

time priority Management frame:

Change the following to use the actual element name (locations in D2.1):

traffic indication map (TIM) element -> TIM element [188.28]

traffic classification (TCLAS) elements -> TCLAS elements [193.61]

high throughput (HT) and very high throughput (VHT) Operation elements -> HT and VHT Operation elements [205.14]

management message integrity code (MIC) element (MME) -> MME [217.8]

multiple MAC sublayers (MMS) element -> MMS element [218.40]

RAW parameter set (RPS) element -> RPS element [227.37]

RSN element (RSNE) -> RSNE [227.57]

robust security network element (RSNE) -> RSNE (2x) [229.44, 234.6]

Change the following to use the actual frame name (locations in D2.1):

broadcast wake-up radio (WUR) wake-up frame: -> broadcast WUR Wake-up frame [206.1]

group addressed wake-up radio (WUR) wake-up frame: -> group addressed WUR Wake-up frame [212.63]

VHT null data PPDU (NDP) Announcement frame -> VHT NDP Announcement frame [218.49]

TBD:

DONE (separate) 3233 Tue AM1: 22/0305-mgr

3238: 218r2 re “power” v “power level”

DONE 3185: remove (optional) in F5-1 etc. and say some blocks not apply in some contexts

DONE 3224: locref

3225: what exactly is a locref?

3273: new column for inheritance

DONE 3653-3656 propose to make the changes shown under "Proposed changes:" for CIDs 1985, 1986, 1535, 1419, 1536 in 22/0353r10 (posted to reflector) [no responses]

DONE 3796: tagged v untagged -- ACCEPT

3632: null -> not present in C6 (else null/otherwise, null/otherwise null -> else not present)

3566: “is recommended to”

3535: always/never

DONE 3175: action frame terminology

3457: “implements” in 3.1/3.2

DONE 3370: “89-0d”

DONE 3057: graham CCK deprecation, make up rejected reason, say not the right time, refer to 22/1868 and reflector

DONE 3699: NOTEs in the extended NSS BW table

DONE 3400 “RSNE is present” -- otherwise not present

DONE 3466 “nonce may be 0” -- actually allow Key Nonce = 0 or SNonce in M4

3693: provide “subfield” locations -- just in the subclause identified

3726: “MIB attribute” in C.3 (see also 11-15/355r13)

DONE ~3174 how does modifying BA agreement work (11.5.2 v 10.25.2 last para)

3289\* add dot11BSSColorCollisionMaxReports

DONE 3485: In Table 27-53--HE PHY MIB attributes why do we have both dot11VHTChannelWidthOptionImplemented and dot11HEChannelWidthOptionImplemented

3629: Follow-up to CID 164: make the changes shown in <https://www.ieee802.org/11/email/stds-802-11-tgm/msg02488.html>

DONE 3522: RA/TA/SA/DA “values”

DONE (by Youhan) 3291: xreffing to earlier PHYs

DONE 3480 CCA.ind delay

DONE 3181: operating class of the advertised BSS’s channel (channel has attributes OC and index); or maybe make 1.4/1.5 comment about OC of BSS/AP means OC of channel on which BSS/AP operates

DONE 3697 delete dot11STACivicLocation

DONE ~3694 Why is there a MIB variable dot11VHTNumberSoundingDimensions but not dot11VHTBeamformeeSTSCapability Add a MIB attribute dot11VHTBeamformeeSTSCapability

3408\* CID 2123: we \*do\* have "dynamic PHY characteristics" -- see e.g. Table 27-53--HE PHY MIB attributes rightmost column; Clarify that "static" means "constant for a given PHY instantiation", and make the following sentence in each case consistent

DONE 3504 different MIB attributes for TDLS, at least security

3499/3500/3501 Table 9-218--Subelement IDs says that when the subelement ID is 2 the Data field contains the GTK, but this is misleading as it contains other stuff

3512 missing “otherwise not present” (generic, not RSNE-specific)

?3570 "A QoS STA shall use the EDCA Parameter Set Update Count subfield(11ax)

in the QoS Capability element of Beacon frames, when present, to determine whether the STA is using the

current EDCA parameters. If the EDCA Parameter Set Update Count subfield in the QoS Capability element is

different from the value that has been stored, the QoS STA shall query the updated EDCA parameters by

sending a Probe Request frame to the AP." -- what about DMG STAs? Note no QoS Cap in Announce frames so not clear how a DMG STA finds out

?3607 It is not clear whether it is OK to have a Classifier Mask field (where it is not reserved) that is all-0, and if so whether that is an "always matches" or a "never matches"

?3537 A DMG SME has suggested that DMG relay should be deprecated. (And if it isn't the addressing rules need to be clarified)

Send updated Figure 9-875—PPE Thresholds Info field format to Editors

3551 require AP to stop using old GTK as soon as it has used the new GTK

3375/3514: “Its value is determined by device capabilities” (also post to reflector) [no responses]

3544: "header field[s]" in Clause 20 and children clauses should be "Header field"

3659: Sometimes fields described as "(optional)" in their defining figure don't say ", if present," in their description

3667: Don't use hyphens for minuses

3668: Figures should not have xrefs unless they will automatically be updated when the xref number changes, otherwise there will be spec rot

3677: Some of the PICS selectors have unnecessary outside parens

3679: Things like "See 11.22.2.4 (Peer-to-peer link" should not be in DESCRIPTIONs unless there is a REFERENCE line to give the revision. Actually should be entirely in the REFERENCE line

3681: "vendor-specific element" (case-insensitively) should be "Vendor Specific element" and otherwise "vendor-specific" should be "vendor specific" (case-preservingly)

3700: The use of "or both" (~77x) implies that uses of "or" without and "or both" are exclusive, but this is not the case

3701: Should not have a comma before a modal verb (when not the end of a subclause or list)

3705: There are many editorial issues with the description of subelements (19/0856)

3723: "Key ID" should be "key ID" when not at the start of a sentence etc. and not followed by "field" etc.

3733: Delete "(bit <n>)" when it just duplicates info already in a figure or table

3735: "Classifier Parameter" is sometimes spuriously capitalised. Also "the Classifier.". Also "Classifier Type" and words after it inconsistent too

DONE ~3361: locations for uppercase frame in 3.1/3.2

3362: PN -> packet number?!

DONE 3379: Vendor Specific field specification

DONE ~3404: TIME\_OF\_DEPARTURE definition consistency

3298: on “the WM”/”the wireless medium”/”the medium”

DONE 3683: “drop” -> “discard”

3725: ccfs say it’s actually an index (as a NOTE)

DONE 3488 ask reflector what “contents of the RSNE” means

DONE provide F10-147 update for DTIM beacon

DONE provide F12-23 based on F12-29

3343: CID 1851 changes to change "PTKSA" to "any PTKSA(s)" (because you could be doing EKIDs) should be done throughout

3433: In ranges expressed as x-y the hyphen should be a minus or en dash (in some places hyphens or em dashes are used

3543: "counter value" should just be "counter"

3545: "any STA" is the same as "a STA" and the latter would be more consistent so should be used

3586: "is an unsigned integer" is not needed in Clause 9 since covered by 9.2.2

3623: Identifiers should not have spaces in them

3625: "Vendor-Specific" should have a space, not a hyphen. Also case sometimes wrong ("Vendor-specific" or "vendor-specific" or "Vendor specific" or "vendor specific")

3370: missing/variable VS field descriptions

3627: The list of AANs in 9.4.1.1 Authentication Algorithm Number field should be a table

3645: CID 238 follow-up. I expect folding in new amendments will have added abbreviations that are not expanded on first use in each definition.

3706: "The structure of this/the blah field/element" is a bit odd

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

Discussion:

Proposed changes:

Proposed resolution:

REVISED

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

**References:**

802.11me/D2.0 except where otherwise specified