IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Some editorial CIDs | | | | |
| Date: 2019-09-02 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry | Cisco |  |  | jerhenry@cisco.com |

Abstract

This document presents resolutions to Clause 9 CIDs: 1789, 1790, 1942, 1958, 1966, 1967, 1969, 1974, 1993, 1999.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1789 | 35.04 | 4 | 9.4.2.21.10 | This approximation is only valid at the equator (at 45 deg it would be 1.57 cm) | change to "corresponds to approximatievly two cm at the equator). | **Revised** . |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1790 | 35.07 | 7 | 9.4.2.21.10 | This approximation is only valid at the equator (at 45 deg it would be 1.57 cm) | change to "corresponds to approximatievly two cm at the equator). | **Revised** |

Discussion:

The Relative Latitude and Longitude subfields provide an offset meauremenet in degrees (which is valid identically on any point of the earth considered as a sphere). An indication of the translation of the unit into cm is provided for clarity. However, 360 degrees at the equator represent about 40,075 km. At 45 degress latitude north for example, 360 degres represent 28361 km. Therefore, the 2 cm scale for the longitude is only valid at the equator. Additionally, the earth is an oblate spheroid, 134.397 km wider at the equator than at the poles. Therefore, one degree of latitude represents 110.57 km at the equator but 111.69 km at the pole. Making 2 cm an absolute reference generates confusion instead of helping the designer.

***TGaz Editor: Replace the two paragraphs in P35L2-10 as follows***

The Relative Latitude subfield contains a signed integer in two’s complement format indicating the latitude offset of the reported location in relation to the specified reference location, in units of 1.8e-07 deg. (Corresponds to approximately two cm at the equator (#1789).)

The Relative Longitude subfield contains a signed integer in two’s complement format indicating the longitude offset of the reported location in relation to the specified reference location, in units of 1.8e-07 deg. (Corresponds to approximately two cm at the equator (#1790).)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1942 | 137 | 12 | 12.2.11 | "The Info field is a fixed string unique to this protocol: For example: "IEEE 802.11az ranging"" -- it shouldn't be an example, and it should have sexy quotes on both sides | Change to "The Info field is "IEEE 802.11az ranging" without a trailing null" with both the double quotes being sexy | **Revised** |

Discussion:

RFC 5869 section 2 describes how the HMAC-based key is derived. In the ‘expand’ phase, the optional info field can be used. As per RC 5869 3.2:

“While the 'info' value is optional in the definition of HKDF, it is

often of great importance in applications. Its main objective is to

bind the derived key material to application- and context-specific

information. For example, 'info' may contain a protocol number,

algorithm identifiers, user identities, etc. In particular, it may

prevent the derivation of the same keying material for different

contexts (when the same input key material (IKM) is used in such

different contexts). It may also accommodate additional inputs to

the key expansion part, if so desired (e.g., an application may want

to bind the key material to its length L, thus making L part of the

'info' field). There is one technical requirement from 'info': it

should be independent of the input key material value IKM.

As such, if the info field is used, it has to contain information that is clearly identified as representing 802.11az. Thus the value we design here should not be an example, but a fixed value that implementers will use to recognize 802.11az (on both sides).

CID 1455 made a comment in that direction, however D1.2 implements the following change:

*The Info field is a fixed string unique to this protocolin order to guard against accidental key re-use in a different subsystem. Key reuse across different subsystems must be avoided through careful system architecture, Secret Key must not be visible outside of the subsystem. See RFC5869, Section 2.3 for Info field.*

Such change is only partly satisfactory, as it resolves the problem by hiding it, thus leaving to implementers (or other organisations like WFA) the task of choosing the info value. As we define the other elements of the protocol, it might be valuable to also define the value of this field. There is no repository of RFC 5869 info fields, however it is reasonable to assess that no one has used any value yet within the PEDMG Secure ranging exchange.

***TGaz Editor: Modify the text in the second pargraph of 12.2.11 P137L13-16 as follows:***

The Info field is “IEEE 802.11az ranging” in order to guard against accidental key re-use in a different subsystem. Key reuse across different subsystems must be avoided through careful system architecture, Secret Key must not be visible outside of the subsystem. See RFC5869, Section 2.3 for Info field.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1958 |  | 45 |  | It is not clear whether the things after "Note:" are normative or not | If they are informative (i.e. do not express normative behaviour that is not normatively stated elsewhere) change them to start "NOTE---". If they are in fact normative delete the "Note:" | Revised |

***TGaz Editor: Modify the text in P28L19:***

Note— for non-secure ranging, the UL Rep is set to a value no larger than the RSTA Assigned UL Rep (See 11.22.6.3 Fine Timing Measurement procedure negotiation).

***TGaz Editor: Modify the text in P29L6:***

Note— For secure ranging, the UL Rep is set to the RSTA Assigned UL Rep (See 11.22.6.3 Fine Timing Measurement procedure negotiation.)

***TGaz Editor: Modify the text in P126L2:***

Note— A device should discard ranging measurements when it detects that its ranging peer’s clock drift considering its local clock, exceeds the allowed tolerance from the values specified in subclause 20.3.3.2.1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1966 | 96 | 22 | 11.22.6.4.3.3 | No such thing as an "NDP-A frame" | Change to "NDP Announcement frame". Also at 96.23/26. In F11-36i, 101.26 change "NDP-A" to "NDPA" | Revised |
| 1967 |  |  |  | No such thing as an "NDP-A frame" | Change to "NDP Announcement frame" and change "NDP-A" where it is an abbreviation in a figure to "NDPA" | Revised |

***TGaz Editor: Insert acronym in P6L9:***

NDPA NDP Announcement

***TGaz Editor: Modify the text in P72L16to27:***

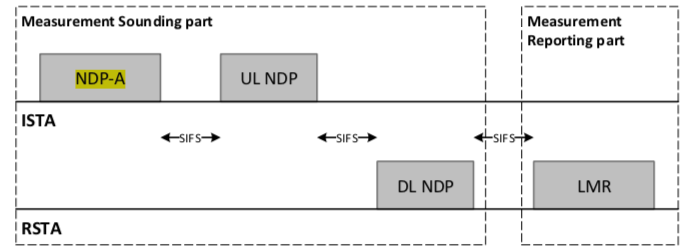
The ToD field contains a timestamp that represents the time, with respect to a time base, at which the first HE-LTF symbol of the corresponding NDP frame appeared at the transmit antenna connector. The corresponding NDP frame in an RSTA-to-ISTA Location Measurement Report (LMR) frame is a DL NDP, while in an ISTA-to-RSTA LMR frame it is an UL NDP. In both cases the corresponding NDP frame refers to a measurement exchange that included an NDPA which carried the matching dialog token that is also included in this LMR.

The ToA field contains a timestamp that represents the time, with respect to a time base, at which the first HE-LTF symbol of the corresponding NDP frame arrived at the receive antenna connector. The corresponding NDP frame in an RSTA-to-ISTA LMR frame is an UL NDP, while in an ISTA-to-RSTA LMR frame it is a DL NDP. In both cases the corresponding NDP frame refers to a measurement exchange that included an NDPA which carried the matching dialog token that is also included in this LMR.

***TGaz Editor: Modify the text in P101L1to7:***

The format (#2161) of the UL NDP is an HE TB Ranging NDP (see subclause 27.3.17b HE Ranging NDP ). SIFS time after receiving the last UL NDP, the RSTA shall transmit an NDP Announcement frame followed by a DL NDP (#2161); the NDPA is a Ranging NDP Announcement frame, see subclause 9.3.1.19 and the DL NDP is an HE Ranging NDP, see subclause 27.3.17a. Figure 11-36e shows an availability window with an RSTA and two ISTAs (ISTA 1 and ISTA 4) responding to the poll. The TF Ranging Sounding allocates a separate spatial stream to each ISTA. The NDPA is addressed to and the DL NDP is used by all ISTA taking part in the exchange.

***TGaz Editor: Modify the figure 11-36i P106L6:***



***TGaz Editor: Modify the text in P106L11:***

The measurement sounding phase of the measurement exchange sequence in non-TB Ranging shall follow the sequence illustrated in Figure 11-36I. The NDPA and UL/DL NDP frames refer to a Ranging NDP Announcement frame and HE Ranging NDPs respectively, whose frame formats are defined in 9.3.1.20 and 27.3.17a, respectively. The measurement reporting phase consists of an LMR frame, which is a Location Measurement Report as defined in 9.6.7.37.

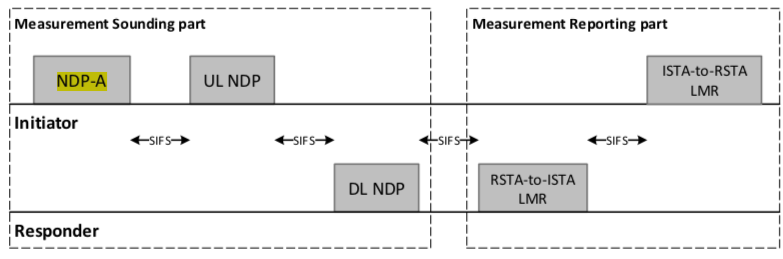
***TGaz Editor: Modify the text in P107L8-32:***

In the non-TB measurement exchange sequence, the ISTA shall transmit the NDPA frame with the same bandwidth as the UL NDP to reserve the medium (#1829) and set UL Rep, DL Rep subfields of the STA Info field to a value in the range of 0 to RSTA assigned UL rep, 0 to RSTA assigned DL rep respectively; the RSTA shall transmit the DL NDP with the same bandwidth as the NDPA and UL NDP, while the LMR can be transmitted at a different bandwidth, according to the rules of multiple frame transmission in an EDCA TXOP (see 10.22.2.7), i.e., not exceeding the bandwidth of the NDPA, UL NDP and DL NDP. The allowed bandwidths for the NDPA and UL/DL NDP frames are specified in the Format and Bandwidth subfield of the Ranging Parameters field (see 9.4.2.279).

Accordingly:

* An ISTA transmitting a Ranging NDP Announcement frame shall not use a bandwidth wider than that indicated by an RSTA in the Ranging Parameters element, in the initial Fine Timing Measurement frame. The TA field of the Ranging NDP Announcement frame is a bandwidth signaling TA when the Ranging NDP Announcement frame is sent in a non-HT duplicate PPDU (see 10.7.6.6)
* An ISTA transmitting an UL NDP shall set the TXVECTOR parameter CH\_BANDWIDTH to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging NDP Announcement frame.
* An RSTA transmitting a DL NDP shall set the TXVECTOR parameter CH\_BANDWIDTH to the bandwidth of the Ranging NDP Announcement frame and/or the UL NDP frame; which are obtained from the RXVECTOR parameter CH\_BANDWIDTH of the Ranging NDP Announcement frame or UL NDP frame respectively. For the NDPA frame, when not received in an HE/VHT/HT PPDU: from the RXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT when the Ranging NDP Announcement frame is received in a non-HT duplicate PPDU and is 20 MHz when the Ranging NDP Announcement frame is received in a non-HT PPDU.

***TGaz Editor: Modify the figure 11-36i P110L8:***



***TGaz Editor: Modify the text in P106L16:***

The data rate or MCS used for transmitting the LMR frame is solely decided by the transmitter of the corresponding LMR frame. The bandwidth used to transmit the LMR frame shall not be wider than the bandwidth of the soliciting NDPA.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1969 | 102 | 6 |  | "nominally" is unclear | Change to "normally" | Revised |

***TGaz Editor: Modify the text in P98L8to13:***

Each availability window normally contains a single poll, which should poll all ISTAs assigned to the availability window. If the available bandwidth is insufficient to allow for the polling of all ISTAs assigned to the availability window with one poll, the RSTA shall indicate that one or more extra polling/sounding/reporting triplets can be expected within the availability window (see example in Figure 11-36b and Figure 11-36c). All instances of polling/sounding/reporting triplets must be completed before the end of the availability window

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1974 |  |  |  | There are references to "device"s but these are not defined | Change "device" to "STA" throughout (6.20, 63.13/19, 65.8/14, 109.1, 127.1) | Revised |

Discussion:

“Device” appears more than 400 times in 802.11Revmd2.3. It is often used as a generic term. However, there are advantages in clarifying the device nature when the identification is clear. There nare cases where the ‘device’ can be either the RSTA or the ISTA, and changing to STA does not bring a clear advantage, for example p 101 (D1.2):

*In the secured mode of TB Ranging, it is recommended that a* ***device*** *discards ranging measurements when it detects that the transmit center frequency offset (CFO) between the ISTA and the RSTA exceeds the allowed tolerance from the values specified in 28.3.18.3 and 28.3.14.3.*

Or p 117 (D1.2):

*Note: It is recommended that a* ***device*** *discards ranging measurements when it detects that its ranging peer’s clock drift considering its local clock, exceeds the allowed tolerance from the values specified in section 20.3.3.2.1.”*

***TGaz Editor: Modify the text in P55L9to19:***

The AOA Azimuth subfield contains the Angle of Arrival (AOA) azimuth result in degree/4 resolution. This subfield is an unsigned two’s complement number taking values between 0 and 1439. When the AOA Reference subfield is set to 1, the AOA Azimuth subfield is in earth coordinates (i.e. direction 0 is north). When the AOA Reference subfield is set to 0, the AOA Azimuth subfield is in coordinates relative to the ISTA.

The AOA Elevation subfield contains the AOA elevation result in degree/4 resolution. This subfield is a signed two’s complement number taking values between -360 and 360.

When the AOA Reference subfield is set to 1, the AOA Elevation subfield is in earth coordinates (i.e. elevation 0 is horizon). When the AOA Reference subfield is set to 0, the AOA Elevation is in coordinates relative to the ISTA.

***TGaz Editor: Modify the text in P57L4to14:***

The AOD Azimuth subfield contains the Angle of Departure (AOD) azimuth result in degree/4 resolution. This subfield is an unsigned two’s complement number taking values between 0 and 1439. When the AOD Reference field is set to 1, the AOD Azimuth is in earth coordinates (i.e. direction 0 is north). When the AOD Reference subfield is set to 0, the AOD Azimuth subfield is in coordinates relative to the transmitting STA.

The AOD Elevation subfield contains the AOD elevation result in degree/4 resolution. This subfield is a signed two’s complement number taking values between -360 and 360.

When the AOD Reference field is set to 1, the AOD is in earth coordinates (i.e. elevation 0 is horizon). When the AOD Reference subfield is set to 0, the AOD Elevation subfield is in coordinates relative to the transmitting STA.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1993 | 59 |  |  | Duplication is bad, m'kay? | Delete "is one octet wide and " at 59.4/8 (and change "indicate" to "indicates") and "is four Bits wide and " at 59.15 | Revised |

Discussion:

The field size is described in the figure above. We do not usually tell the size of a field when it is already known.

***TGaz Editor: Modify the text in P51L11to24:***

The MinTimeBetweenMeasurements field indicates the minimum time between subsequent range measurements initiated by an ISTA, in units of 100 microseconds. The MinTimeBetweenMeasurements field is set the same value as the MinToAReady field if the MinToAReady field value is nonzero.

The MinToAReady field indicates the minimum time the responder requires to compute the ToA value, in units of 100 microseconds. When set to a nonzero value, MinToAReady indicates a delayed response, in which case the ToD and ToA values in the corresponding LMR frame are from the previous range measurement. The MinToAReady field value 0 indicates an immediate response, in which case the ToD and ToA values included in the corresponding Location Measurement Report (LMR) frame are from the current range measurement. The MinToAReady field is reserved in an initial FTM Request frame.

The MaxToAAvailableExp field indicates the maximum time duration for which the responder retains the computed ToA value. The MaxToAAvailableExp field is reserved in an initial FTM Request frame.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1999 | 59 | 19 |  | "The range of valid values for MaxToAAvailableExp 19 is 0 to 15 with corresponding maximum time duration values ranging from 256 msec to 140 20 minutes. " -- since it's a 4-bit field this sentence adds nothing of value | Delete the cited text | Revised |

Discussion:

MaxToAAvailableExp is defined just the paragraph before, therefore repeating the size is not useful. However, the formula may look unusual (with an unusual exponent format), as such clarifying the expected retention range might be useful.

***TGaz Editor: Modify the text in P51L25to18:***

Maximum time duration for which the responder retains the computed ToA value = 2^(MaxToAAvailableExp+8) millisecondswith corresponding maximum time duration values ranging from 256 msec to 140 minutes.

**References:**

[1] Draft P802.11azD1.0

[2] Draft P802.11ayD3.0

[3] Draft P802.11RevMD\_2.1