IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S1G SB1 Miscellaneous Comment Resolutions | | | | |
| Date: 2016-03-17 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Menzo Wentink | Qualcomm | Straatweg 66, Breukelen, The Netherlands |  | mwentink@qti.qualcomm.com |
| Jouni Malinen | Qualcomm | Finland |  |  |

Abstract

This submission proposes resolutions for multiple comments related to TGah D6.0.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **IDs** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 9028 | 4.3.13a.2  10.36 | Due to previous comment resolutoin this subclause now has 3 sentences which description is not complete. At least add a sentence to describe what the relay does. | Insert a sentence as follows: "The relay forwards frames between the root AP and other STAs that are part of the relay network (see 5.1.5.6 (S1G relay) and 10.51 (S1G Relay operation))." | Revised - At the cited location, add "An S1G relay forwards frames between STAs associated to its S1G relay AP and the AP to which its S1G relay STA is associated.". |
| 9030 | 6.3.2.2  16.17 | 8504 removed some relay related elements from some MLME related parameter (related to Probe Request. Similarly it removed in 9.3.3.10 and 9.3.3.11. However those elements (I believe also reachable address update is needed?) were needed to enable discovery and activation of relays. | Add the elements back. | Revised - in 6.3.3.3 (MLME-SCAN.confirm), to the BSSDescriptionSet table, add a new entry with "S1GRelay" at the Name column, "As defined in frame format" at the Type column, "As defined in 9.4.2.201 (S1G Relay element)" at the Valid range column, "The S1G Relay element is present in the S1G Beacon if dot11RelayAPOperationActivated is true or if dot11RelayAPImplemented is true; otherwise not present. The S1G Relay element is optionally present in (Short) Probe Response if dot11RelayAPImplemented is true. More description is provided in 10.51 (S1G Relay operation)." at the Description column, and "Do not adopt" at the IBSS adoption column.  In 9.3.3.11 (Probe Response frame body), in Table 9-34, add a new entry with "S1G Relay element" at the Information column and "The S1G Relay element is optionally present if dot11RelaySTAImplemented is true; otherwise not present." at the Notes column. |
| 9051 | 12.5.3.2a  381.63 | Seems the use of the SC field to build up the PN0||PN1 does not exclude the case when the Fragment Number field contains an offset of the winstart for NDP BlockAck (see 10.24.7.3). | Add this exemption. I.e., append the following text to this item "with the FN subfield masked to 0 when the PV1 MPDU is carried in an A-MPDU that is not an S-MPDU". | Accepted. |
| 9052 | 12.5.3.2a  381.63 | There is no need to have a PN per TID/ACI (note that PV1 frames contain this information in the Frame Control field). | Relax the requirement to have a PN per TID/ACI. | Revised - in 12.5.3.2a (Construction of the CCMP header for PV1 MPDUs), at 381.64, delete ", per TID/ACI". |
| 9049 | 10.55  343.58 | Since PV1 frames are designed to reduce overhead it is beneficial that MSDUs carried with PV1 frames use EPD headers (saves 6 bytes per MSDU). Refer to 11/15/1521r3 for details. | "Specify that PV1 frames carry MSDUs with EPD header. I.e., Insert the following sentence at the end fo this paragraph:  ""EPD as defined in IEEE Std 802-2014 (Overview and Architecture) shall be used for transmission of all MSDUs carried in PV1 frames.""" | Rejected - the comment fails to identify a technical issue in sufficient detail. |
| 9056 |  | Resolution to i-480 is incorrect. The comment identifies a specific technical problem (absence of test vectors) and a specific technical solution (add test vectors). If the sponsor WG can not generate test vectors from the specification in the standard, this is clear evidence the specification is not technically complete. | Withdraw the draft from sponsor ballot, and initiate a new ballot when the draft is technically complete. A | Revised - add test vectors as specified in 11-16/465r1. Please note that the presence or absence of test vectors is not related to the technical completeness of a specification. |
| 9050 |  | CCMP test vectors are missing for PV1 frames. | Add CCMP test vectors for PV1 frames. | Revised - add test vectors as specified in 11-16/465r1, at a suitable location. |

CCMP PV1 test vectors

BSSID: a2:ae:a5:b8:fc:ba

DA: 02:d2:e1:28:a5:7c

SA: 52:30:f1:84:44:08

Association ID: 7

Base PN: 123 (0x0000007b)

SC = 0x3380 (FragNum=0 SeqNum=824)

TID = 3

Key ID: 0

TK - hexdump(len=16): c9 7c 1f 67 ce 37 11 85 51 4a 8a 19 f2 bd d5 2f

PN = SC||BPN

PN (PN0..PN5) - hexdump(len=8): 80 33 7b 00 00 00 00 00

PV1 test vector #1:

Header compression used and A3 was previously stored at the receiver

FC=0x0061 (PV=1 Type=0 PTID/Subtype=3 From\_DS=0 More\_Fragments=0 Power\_Management=0 More\_Data=0 Protected\_Frame=0 End\_of\_SP=0 Relayed\_Frame=0 Ack\_Policy=0)

A1=a2:ae:a5:b8:fc:ba

A2=07 00 (SID: AID=7 A3\_Present=0 A4\_Present=0 A-MSDU=0)

Sequence Control: 80 33 (FN=0 SN=824)

A3 not present

A4 not present

Plaintext Frame Header - hexdump(len=12): 61 00 a2 ae a5 b8 fc ba 07 00 80 33

Plaintext Frame Body - hexdump(len=20): f8 ba 1a 55 d0 2f 85 ae 96 7b b6 2f b6 cd a8 eb 7e 78 a0 50

CCMP AAD - hexdump(len=12): 61 10 a2 ae a5 b8 fc ba 07 00 80 33

CCMP nonce - hexdump(len=13): 20 52 30 f1 84 44 08 00 00 00 7b 33 80

CCM B\_0 - hexdump(len=16): 59 20 52 30 f1 84 44 08 00 00 00 7b 33 80 00 14

CCM T - hexdump(len=8): 89 8c b6 37 00 99 8c f3

CCM U - hexdump(len=8): 5b 50 10 10 df eb 4b 0a

CCMP encrypted - hexdump(len=20): dd d7 40 e2 a5 86 e1 2b 06 0e 45 69 d0 a3 93 61 60 41 2e 45

Encrypted Frame Header - hexdump(len=12): 61 10 a2 ae a5 b8 fc ba 07 00 80 33

Encrypted Frame Frame Body - hexdump(len=28): dd d7 40 e2 a5 86 e1 2b 06 0e 45 69 d0 a3 93 61 60 41 2e 45 5b 50 10 10 df eb 4b 0a

Encrypted Frame FCS - hexdump(len=4): fc a4 f9 bd

PV1 test vector #2:

Header compression used and A3 was not previously stored at the receiver

FC=0x0061 (PV=1 Type=0 PTID/Subtype=3 From\_DS=0 More\_Fragments=0 Power\_Management=0 More\_Data=0 Protected\_Frame=0 End\_of\_SP=0 Relayed\_Frame=0 Ack\_Policy=0)

A1=a2:ae:a5:b8:fc:ba

A2=07 20 (SID: AID=7 A3\_Present=1 A4\_Present=0 A-MSDU=0)

Sequence Control: 80 33 (FN=0 SN=824)

A3=02:d2:e1:28:a5:7c

A4 not present

Plaintext Frame Header - hexdump(len=18): 61 00 a2 ae a5 b8 fc ba 07 20 80 33 02 d2 e1 28 a5 7c

Plaintext Frame Body - hexdump(len=20): f8 ba 1a 55 d0 2f 85 ae 96 7b b6 2f b6 cd a8 eb 7e 78 a0 50

CCMP AAD - hexdump(len=18): 61 10 a2 ae a5 b8 fc ba 07 20 80 33 02 d2 e1 28 a5 7c

CCMP nonce - hexdump(len=13): 20 52 30 f1 84 44 08 00 00 00 7b 33 80

CCM B\_0 - hexdump(len=16): 59 20 52 30 f1 84 44 08 00 00 00 7b 33 80 00 14

CCM T - hexdump(len=8): f3 65 0b 2d e5 12 92 6c

CCM U - hexdump(len=8): 21 b9 ad 0a 3a 60 55 95

CCMP encrypted - hexdump(len=20): dd d7 40 e2 a5 86 e1 2b 06 0e 45 69 d0 a3 93 61 60 41 2e 45

Encrypted Frame Header - hexdump(len=18): 61 10 a2 ae a5 b8 fc ba 07 20 80 33 02 d2 e1 28 a5 7c

Encrypted Frame Frame Body - hexdump(len=28): dd d7 40 e2 a5 86 e1 2b 06 0e 45 69 d0 a3 93 61 60 41 2e 45 21 b9 ad 0a 3a 60 55 95

Encrypted Frame FCS - hexdump(len=4): bd 8b 35 d4

PV1 test vector #3:

Type 3 frame from SA to DA(=BSSID) (i.e., no separate DA in this example)

FC=0x006d (PV=1 Type=3 PTID/Subtype=3 From\_DS=0 More\_Fragments=0 Power\_Management=0 More\_Data=0 Protected\_Frame=0 End\_of\_SP=0 Relayed\_Frame=0 Ack\_Policy=0)

A1=a2:ae:a5:b8:fc:ba

A2=52:30:f1:84:44:08

Sequence Control: 80 33 (FN=0 SN=824)

A3 not present

A4 not present

Plaintext Frame Header - hexdump(len=16): 6d 00 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 80 33

Plaintext Frame Body - hexdump(len=20): f8 ba 1a 55 d0 2f 85 ae 96 7b b6 2f b6 cd a8 eb 7e 78 a0 50

CCMP AAD - hexdump(len=16): 61 10 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 80 33

CCMP nonce - hexdump(len=13): 20 52 30 f1 84 44 08 00 00 00 7b 33 80

CCM B\_0 - hexdump(len=16): 59 20 52 30 f1 84 44 08 00 00 00 7b 33 80 00 14

CCM T - hexdump(len=8): 81 fa a4 65 f7 18 fa d6

CCM U - hexdump(len=8): 53 26 02 42 28 6a 3d 2f

CCMP encrypted - hexdump(len=20): dd d7 40 e2 a5 86 e1 2b 06 0e 45 69 d0 a3 93 61 60 41 2e 45

Encrypted Frame Header - hexdump(len=16): 6d 10 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 80 33

Encrypted Frame Frame Body - hexdump(len=28): dd d7 40 e2 a5 86 e1 2b 06 0e 45 69 d0 a3 93 61 60 41 2e 45 53 26 02 42 28 6a 3d 2f

Encrypted Frame FCS - hexdump(len=4): b4 0b 48 92