IEEE P802.11
Wireless LANs

|  |
| --- |
| Telecon Minutes for REVme - December 6, 13 and 20 |
| Date: 2021-12-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jon Rosdahl | Qualcomm, Technologies, Inc. | 10871 N 5750 WHighland, UT 84003 | +1-801-492-4023 | jrosdahl @ ieee . org |
|  |  |  |  |  |

Abstract

This file has the Telecon Minutes for REVme for December 6, 13 and 20.

R0: Dec 6th Telcon Minutes – Thanks to Mark HAMILTON for taking the majority of the notes.

R1: add Dec 13 Telecon Minutes

1. **TGme (REVme) Telecon – 2021 December 06 Monday 10-12pm ET.**
	1. **Called to order** 10:04am ET by the TG Chair, Michael MONTEMURRO (Huawei).
		1. IMAT Reported attendance

|  |  |  |
| --- | --- | --- |
|  | Name | Affiliation |
| 1 | Andersdotter, Amelia | Sky UK Group |
| 2 | Au, Kwok Shum | Huawei Technologies Co., Ltd |
| 3 | Coffey, John | Realtek Semiconductor Corp. |
| 4 | Halasz, David | Morse Micro |
| 5 | Hamilton, Mark | Ruckus/CommScope |
| 6 | Kim, Youhan | Qualcomm Incorporated |
| 7 | Kneckt, Jarkko | Apple, Inc. |
| 8 | Liu, Der-Zheng | Realtek Semiconductor Corp. |
| 9 | Patwardhan, Gaurav | Hewlett Packard Enterprise |
| 10 | Petrick, Albert | InterDigital, Inc. |
| 11 | RISON, Mark | Samsung Cambridge Solution Centre |
| 12 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| 13 | Smith, Graham | SR Technologies |
| 14 | Torab Jahromi, Payam | Facebook |

* 1. **Introductions of Officers.**
		1. TG Chair - Michael MONTEMURRO (Huawei).
		2. Vice Chair – Mark Hamilton (CommScope/Ruckus)
		3. Vice Chair – Mark RISON (Samsung)
		4. Editor - Emily QI (Intel)
		5. Editor – Edward AU (Huawei)
		6. Secretary - Jon ROSDAHL (Qualcomm)
	2. **Review Patent Policy, Copyright Policy and 802 Policies**
		1. Patent, Participation, and policy related slides: See slides 4-19 in <https://mentor.ieee.org/802.11/dcn/21/11-21-1642-00-0000-2nd-vice-chair-report-november-2021.pptx>
		2. No response to call for Patents.
	3. **Review and Approve Agenda – 11-21/1885r3**:
		1. <https://mentor.ieee.org/802.11/dcn/21/11-21-1885-03-000m-nov-jan-teleconference-agendas.docx>
		2. Change order to address those present.
		3. No objection to the agenda as presented.
	4. **Editor Report**
		1. WG Letter Ballot has started Dec 1 for 40 days.
	5. **Discuss the future Telecon**
		1. Move Jan 10 to Jan 14
			1. Mark HAMILTON may not be available.
			2. Discussion on if it is feasible.
			3. Discuss if we move to 9-11am ET or 12-2pm ET
			4. Editor needs more time to prepare the comment database.
			5. Move to Jan 14 and keep the time at 10-12pm ET.
	6. **Review doc 11-21/11821r4 - GEN CIDs.**  – Jon Rosdahl (Qualcomm)
		1. <https://mentor.ieee.org/802.11/dcn/21/11-21-1821-04-000m-cc35-13-gen-cids.docx>)
		2. CID 497 (GEN):
			1. We talked about a very similar CID (CID 230) in the last meeting.
			2. This proposes a similar rejection.
			3. C: Disagree that a DEFVAL indicates a minimum capability. Deleted the last sentence, that talks about minimum capability.
			4. Proposed Resolution: Rejected. RFC 2578, section 7.9 gives a pretty good description. It pretty clearly says DEFVAL is appropriate for anything that's read-only. And it is optional for anything that is read-write.
			5. Mark Ready for motion, on a separate tab, along with CID 230.
			6. Comment Group = “Gen Motion CID 230 and 497”
		3. CID 372 (GEN):
			1. Reviewed prior discussions on this CID/topic.
			2. C: Can’t be insufficient details – it says to change “transmitter address” to “TA” which is explicit.
			3. C: This seems very related to CID 422, in 11-21/829r9 (<https://mentor.ieee.org/802.11/dcn/21/11-21-0829-09-000m-resolutions-for-some-comments-on-11me-d0-0-cc35.docx>).
			4. C: CID 422 was withdrawn, however.
			5. C: Subclause 9.3.3.1 (Format of PV0 Management frames) shows that Beacon frames call this field the “Address 2” field.
			6. C: This definition is about the BSSID field. We should not try to change this definition.
			7. C: “transmitter address field” does appear in the Frame report. R: But that is a unique context, and that is the name of the field there.
			8. C: But, the definition does say the MAC header “transmit address field”, and there is no such field. We need to fix this.
			9. Considered clause 11.1.3.8 (Multiple BSSID procedure). This subclause uses the terms derived from transmitted and nontransmitted
			10. C: But the definition does talk about the “TA” field, as part of how the transmitted Beacon is identified. That could be re-written to talk about the transmitted Beacon, instead, but that’s a lot of work to be sure it is correct. Suggest we can just replace the refence to the MAC header’s transmitter address to be the MAC header’s Address 2 field, to make it correct, even if not entirely helpful.
			11. Proposed Resolution: Revised. Change the definition from “The BSSID included in the medium access control (MAC) header transmitter address field of a Beacon frame when the multiple BSSID capability is supported.” To “The BSSID included in the medium access control (MAC) header Address 2 field of a Beacon frame when the multiple BSSID capability is supported.”
			12. Mark Ready for motion. – Comment Group = “Gen Motion - Dec A”
		4. CID 111 (GEN):
			1. C: This is actually the instances of “that intends”.
			2. Reviewed the proposed changes.
			3. Noted that “S-Aps” should be “S-APs”
			4. The change in P1424.8 seems to be adding semantics. Modified the change to just remove the “that intends to join the centralized cluster”.
			5. For the change at P1808.58, use the “prior to” structure above. Otherwise, we just change “intends” to ”prepares”, which has the same original problem. Changed to:
			6. Prior to transmitting an 8 or 16 MHz PPDU, an S1G STA may also invoke a backoff procedure …
			7. Considered the same thing for the next change (P1813.11). But it needs a different structure. Needs more work, come back to this.
			8. P1966.3: More, similar discussion. Considered, “Prior to dynamically allocating… an AP or PCP shall”, or “In order to dynamically allocate…, an AP or PCP shall”, or “To dynamically allocate…, an AP or PCP shall”.
			9. No objection to the “In order to…” direction.
			10. Agreed to: “In order to dynamically allocate an SP within the DTI, an AP or PCP shall commence a GP at a time instant indicated by at least one of the following:”
			11. P1992.24: Also, similar. Suggested: change to, “In order to become a member AP or member PCP after receiving a DMG Beacon frame including cluster information transmitted by an S-AP, a centralized clustering enabled AP or PCP shall successfully perform the following steps in order:”
			12. C: This structure buries the event.
			13. Came up with three options. Will work further off-line.
			14. Chair noted that this comment is an example of one that would be better assigned back to the commenter, to get the specific changes. The Chair will do more to enforce that approach on future ballots.
	7. **Review Document: 11-21/1782r3** ) - Graham SMITH (SR Technologies)
		1. <https://mentor.ieee.org/802.11/dcn/21/11-21-1782-03-000m-annex-g-cids-resolution.docx>
		2. This is trying to wrap up the discussion about removing references to Annex G and “frame exchange sequence”, and to correct uses of “frame exchange” that should have “sequence” added.
		3. It was pointed out that “transmission” of a frame exchange sequence is not needed in many places (and is arguably wrong, since a FES involved both transmission and reception, usually). Changes are added to address these places.
		4. C: This seems to have more changes, that are not really related to the subject (Annex G). The “transmission of” corrections, went too far. Removed the ones not related. Cleaned up changes to remove any use of “transmission of frame exchange sequences” or similar wording.
		5. Didn’t finish review of the rest. Will bring this back on Jan 20.
	8. **Adjourned 12:00 ET**
1. **TGme (REVme) Telecon – 2021 December 13 Monday 10-12pm ET.**
	1. **Called to order** 10:01am ET by the TG Chair, Michael MONTEMURRO (Huawei).
		1. IMAT Reported attendance

|  |  |  |
| --- | --- | --- |
|  | Name | Affiliation |
| 1 | Au, Kwok Shum | Huawei Technologies Co., Ltd |
| 2 | Bhandaru, Nehru | Broadcom Corporation |
| 3 | Coffey, John | Realtek Semiconductor Corp. |
| 4 | Halasz, David | Morse Micro |
| 5 | Hamilton, Mark | Ruckus/CommScope |
| 6 | Harkins, Daniel | Aruba Networks, Inc. |
| 7 | Kim, Youhan | Qualcomm Incorporated |
| 8 | Levy, Joseph | InterDigital, Inc. |
| 9 | Lumbatis, Kurt | CommScope, Inc. |
| 10 | Malinen, Jouni | Qualcomm Incorporated |
| 11 | Montemurro, Michael | Huawei Technologies Co., Ltd |
| 12 | Petrick, Albert | InterDigital, Inc. |
| 13 | Qi, Emily | Intel Corporation |
| 14 | RISON, Mark | Samsung Cambridge Solution Centre |
| 15 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| 16 | Smith, Graham | SR Technologies |

* 1. **Introductions of Officers.**
		1. TG Chair - Michael MONTEMURRO (Huawei).
		2. Vice Chair – Mark Hamilton (CommScope/Ruckus)
		3. Vice Chair – Mark RISON (Samsung)
		4. Editor - Emily QI (Intel)
		5. Editor – Edward AU (Huawei)
		6. Secretary - Jon ROSDAHL (Qualcomm)
	2. **Review Patent Policy, Copyright Policy and 802 Policies**
		1. Patent, Participation, and policy related slides: See slides 4-19 in <https://mentor.ieee.org/802.11/dcn/21/11-21-1642-00-0000-2nd-vice-chair-report-november-2021.pptx>
		2. No response to call for Patents.
	3. **Review and Approve Agenda – 11-21/1885r4**:
		1. <https://mentor.ieee.org/802.11/dcn/21/11-21-1885-04-000m-nov-jan-teleconference-agendas.docx>
		2. Review Comment Resolution Specific Agenda for today:
1. **Monday December 13, 2021 – 10am – noon Eastern**
	1. Comment resolution – Focus on 9 Security CIDs
		1. CID 224 – Montemurro (Huawei)
		2. CID 344 (MAC) – Rison (Samsung)
		3. 11-21/829 - SEC CIDs – Rison (Samsung)
			1. No objection to the Agenda Plan.
	2. **Editor Report** – Emily QI (Intel)
		1. Nothing to report.
	3. **Review CID 224** – Michael Montemurro (Huawei)
		1. Review comment in Database.
		2. Prior discussion in May, and a proposal to reject was declined.
		3. Discussed again in November, and a plan for including in 11-21/829r9
		4. <https://mentor.ieee.org/802.11/dcn/21/11-21-0829-09-000m-resolutions-for-some-comments-on-11me-d0-0-cc35.docx>
		5. Review Discussion in submission in 11-21/829r9.
		6. Discussion on potential changes.
		7. Discussion on if wording should be more normative vs more informative.
		8. Discussion on how to articulate the intent of what “at least as strong”.
		9. Straw poll -- Do you support adding guidance on how to select a cipher for TDLS Link? yes/no/abstain
			1. Results: 3-5-2
			2. Will mark this CID as Rejected. No consensus.
	4. **Review doc 11-21/829r9** – Mark RISON (Samsung)
		1. <https://mentor.ieee.org/802.11/dcn/21/11-21-0829-09-000m-resolutions-for-some-comments-on-11me-d0-0-cc35.docx>
		2. CID 344 (MAC)
			1. Review comment
			2. Review discussion in submission
			3. Review proposed changes
			4. Discussion on what is the problem being identified.
			5. Discussion on How to make things easier to find.
			6. Straw Poll: Do you support resolution for CID 344 in 11-21/829r9?
				1. Results: 7 -2-5
				2. Slight Indication of consensus
			7. Proposed Resolution: CID 344 (MAC): REVISED (MAC: 2021-12-13 15:31:03Z): Change “direct hashing” to “the hash-to-element method” in Table 9-50—Status codes.

Change “the direct hashing to element technique” to “the hash-to-element method” in Table 9-93—BSS membership selector value encoding.

Change “directly hashing” to “the hash-to-element method” in Table 9-321—Extended RSN Capabilities field.

Change “the direct hashing technique” to “the hash-to-element method” in 12.4.2 Assumptions on SAE.

Change “support for direct hashing” to “support for the hash-to-element method”; “The direct hashing technique” to “The hash-to-element method” in 12.4.4.2.3 Hash-to-curve generation of the password element with ECC groups.

Change “for direct hashing” to “for the hash-to-element method”; “he direct hashing technique” to “he hash-to-element method” (3x) in 12.4.4.3.3 Direct generation of the password element with FFC groups.

Change “directly hashing to a group element” to “the hash-to-element method” in 12.4.5.2 PWE and secret generation.

Change “the direct hashing technique” to “the hash-to-element method” in 12.4.5.4 Processing of a peer’s SAE Commit message (2x).

Change “technique” to “method” in 12.4.2 Assumptions on SAE (first instance), 12.4.4.2.3 Hash-to-curve generation of the password element with ECC groups (first 3 instances), 12.4.4.3.3 Direct generation of the password element with FFC groups (2nd, 3rd and 4th instances).

* + - 1. No objection – Mark Ready for Motion
		1. CID 507 (SEC)
			1. Review comment
			2. Review proposed changes
			3. Discussion on the changes – first change and 3rd change seem contradictory.
			4. Discussion on how to clarify the text changes.
			5. Request to see the context.
			6. Editor input that prefers page/line number on a particular draft version. The search in the subclause is extra work for the Editor. Documenting Context does help in the discussion and making the changes.
			7. While this maybe the minimum requirements, it would be better to help with the context.
			8. Discussion on what does “=” mean in this sentence.
			9. Proposed Resolution: CID 507 (SEC): REVISED

In 12.7.6.2 change “Key Data = PMKID for the PMK being used during PTK generation” to “Key Data = <newline> — PMKID KDE containing the PMKID for the PMK being used during PTK generation”.

In 12.7.6.5 4-way handshake message 4 change “Key Data = none required” to “Key Data = <newline> — none required”.

In 12.7.7.3 Group key handshake message 2 change “Key Data = OCI KDE” to “Key Data = <newline> — OCI KDE”.

At the end of the bullet list in 12.7.6.1 General and 12.7.7.1 General add a bullet “One or more vendor specific KDEs and/or Vendor Specific elements may appear in the {Key Data}.”

* + - 1. Concern with not being able to see the context of the changes.
				1. This fixed PMKID -> PMKID KDE and adds a note on allowing vendor specific KDEs/IEs in all EAPOL-Key Frames.
			2. Updated Proposed Resolution: Rejected – No Consensus
			3. Mark Ready for Motion
		1. CID 432 (SEC)
			1. Review Comment
			2. Review proposed changes
			3. Discussion on if we can add Deprecated TKIP in new text.
			4. Removal of TKIP in general is not the scope of this CID.
			5. Remove RSNA and put in Cryptographic mechanism.
			6. Remove TKIP in 4.5.4.1 as well (two locations TKIP was moved).
			7. Proposed resolution: CID 432 (SEC): Revised. Incorporate the changes shown in 11-21/0829r10 for CID 432.
			8. Request to remove the “Comments” from the document. The submitter noted that viewing the document in final form removes the comments from view.
			9. Mark Ready for Motion
		2. CID 462 (SEC)
			1. Review Comment
			2. Review discussion in submission.
			3. See doc 11-21-816r3
				1. <https://mentor.ieee.org/802.11/dcn/21/11-21-0816-03-000m-on-a-msdu-addressing.docx>
			4. This new doc is scheduled for January 7 Telecon.
			5. Move on to next CID.
		3. CID 186 and 188 (SEC)
			1. Were pulled from a motion previously.
			2. Review Comments
			3. Review Discussion in submission.
			4. Review proposed changes.
			5. Discussion on some suggested text changes may not be needed.
			6. Discuss the possibility to have the changes moved to separate topical comments in a future ballot.
			7. Need to revisit this CID again.
		4. CID 193 (SEC)
			1. Review comment
			2. Reviewed Discussion material
			3. Reviewed proposed changes
			4. C: Is the number of counters necessarily the same as the number of TIDs? A: That is current text. C: But is it correct (and all these changes are aligning to it)? Discussion, considering a RXr with 2 counters, that RXs 3 TIDs, for example. C: Not convinced the current text is clear/correct. Will think about it off-line.
			5. Proposed Resolution: CID 193 (SEC): Revised. Make the changes shown under “Proposed changes” for CID 193 in 11-21/829r10 <<https://mentor.ieee.org/802.11/dcn/21/11-21-0829-10-000m-resolutions-for-some-comments-on-11me-d0-0-cc35.docx>>, which address the issues raised by the commenter. Note to the commenter: there is no PN in PV1 MPDUs; instead, the PN is generated locally.
			6. Discussion on how the replay counters and ordering and which replay counter is used for which TID.
			7. Mark Ready for motion
		5. CID 179, 180 (SEC)
			1. Review comments
			2. Reviewed Discussion material
			3. Reviewed proposed changes
			4. Discussion on when the secure bit should be set.
			5. There may be many implantation details, but we should clearly put in text that is what “should” be done.
			6. No objection to suggested changes.
			7. Yellow highlighted notation has a comment that was withdrawn to be posted in LB for D1.0
		6. Out of time.
	1. **Adjourn 12:01pm**

**References:**

**Dec 6th:**

1. <https://mentor.ieee.org/802.11/dcn/21/11-21-1642-00-0000-2nd-vice-chair-report-november-2021.pptx>
2. <https://mentor.ieee.org/802.11/dcn/21/11-21-1885-03-000m-nov-jan-teleconference-agendas.docx>
3. <https://mentor.ieee.org/802.11/dcn/21/11-21-1821-04-000m-cc35-13-gen-cids.docx>
4. <https://mentor.ieee.org/802.11/dcn/21/11-21-0829-09-000m-resolutions-for-some-comments-on-11me-d0-0-cc35.docx>
5. <https://mentor.ieee.org/802.11/dcn/21/11-21-1782-03-000m-annex-g-cids-resolution.docx>

**Dec 13th:**

1. <https://mentor.ieee.org/802.11/dcn/21/11-21-1642-00-0000-2nd-vice-chair-report-november-2021.pptx>
2. <https://mentor.ieee.org/802.11/dcn/21/11-21-1885-04-000m-nov-jan-teleconference-agendas.docx>
3. <https://mentor.ieee.org/802.11/dcn/21/11-21-0829-09-000m-resolutions-for-some-comments-on-11me-d0-0-cc35.docx>
4. <https://mentor.ieee.org/802.11/dcn/21/11-21-0816-03-000m-on-a-msdu-addressing.docx>
5. <https://mentor.ieee.org/802.11/dcn/21/11-21-0829-10-000m-resolutions-for-some-comments-on-11me-d0-0-cc35.docx>