CONFIDENTIAL TRADE SECRET

FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS

– DO NOT COPY –

Wi-Fi CERTIFIED n System Interoperability Test Plan

Version 2.12

Wi-Fi Alliance

• 10900-B Stonelake Boulevard, Suite 126
• Austin, TX 78759
Phone: 512.498.9434 • Fax: 512.498.9435 • Email: certifications@wi-fi.org
www.wi-fi.org

Change History

Version	Date dd/mm/yy	Remarks
1.0	06/15/2007	Initial Release
1.1	06/22/2007	General – Changed STA Meetinghouse to CSSC General – Changed channel 11 for channel 6 General – Added channel number for Dual Band device 2.2.1 – Removed reference for multiple sniffers for PMK caching 3.10.9.4 – Cleaned up text concerning section 4 reference 4.2 Table 8 – Changed PMK caching to Mandatory 4.2.7 Table 25 – Identified STA as STA1 4.2.30 – Added sniffer to step 4 4.2.35 RIFS – Removed test 4.2.38 – Test procedure changed 5.2.12 &13 Tables 142 & 144 – Removed channel 36 reference 5.2.36 Table 129 Step 1 Expected Results – Removed entry 5.2.35 RIFS – Removed test 5.2.38 – Added sniffer to step 4 Appendix A – Updated contacts list Appendix E – Updated threshold tables
1.1.1	8/8/2007	4.2.3 & 5.2.3 – If running tests in 2.4 GHz, use B mode (not G). 4.2.25, Table 86 – IPTV10Mbps.scr changed to IPTV10Mbps-dn.scr 5.2.3 – For dual band devices, use 5 GHz Appendix E – Updated IBSS thresholds 5.2.37, 5.2.38, & 5.2.42 added 1 spatial stream thresholds General edits
1.2	9/25/2007	2.1 – List Adept software version instead of firmware version. 2.2 – Corrected Marvell STA driver version. 4.1.1 & 5.1.1 – Removed optional settings. 4.2.7 – Examine 4-way handshake with STA2 instead of STA1. 4.2.14, 4.2.15, 4.2.28, 5.2.19, 5.2.20, 5.2.21 – Changed wording of pass criteria. 4.2.36 – Use 5 GHz band. 5.2.1 – Replaced Atheros legacy AP with Atheros 11n AP. 5.2.22 & 5.2.23 – Noted that 802.11h tests are optional. Appendix A – Updated Marvell contact. Appendix E – Updated thresholds for NAV / PLCP tests. Moved equipment list to appendices. Changes to Testbed devices and supplicants. Added RIFS test to AP and STA sections Added Appendix H – RIFS transmitter set up instructions Updated Appendix A version numbers Added text to tests 5.2.36 & 5.2.45 to allow testing of single stream devices
1.2.1	9/27/2007 10/24/07	4.2.22 – Changed Testbed device. 4.2.26 & 5.2.35 – Made corrections. 4.2.38, 5.2.45, & Appendix H – Made corrections. Change copyright statement at beginning. Moved Channel Width Bit test for APUTs from 4.2.26 to 4.2.1. Added in explanatory material to emphasize OOB state for DUT. Put in notes on RIFS tests for both APUT and STAUT that these test shall collect data only and not be used to pass or fail the DUT. Updated all SW for Testbed equipment.

1.2.2	10/26/07	4.2.27 – clarified steps for 2.4 GHz only devices. 4.2.38, Table 112 – reduced Dual band tests from 4 to 2. 5.2.36 – clarified steps for 2.4 GHz only devices. 5.2.45, Table 237 – reduced Dual band tests from 4 to 2. Appendix A – Added OpenSUSE information and updated Cisco AP's product name. Appendix H – Made corrections. 5.2.36, Table 220, Step 2 – modified sniffer test for 1 SS or 2 SS
1.3	1/15/08	Replaced Conexant legacy AP with Marvell AP. Cleaned up based on Jeremy deVries' comments 4.2.1 and 5.2.1 – Moved check for supported features from 4.2.26 and 5.2.35 to here. Appendix A – Added information on legacy devices. Updated 11n model numbers. Appendix H – Clarified instructions.
1.3.1	2/1/08 4/22/08 5/30/08	Replaced Conexant legacy STA. Replaced Meetinghouse server. Table 190 – Corrected caption. 4.2.26 and 5.2.35 – Moved check for supported features back 4.2.28 – Corrected pass/fail criteria. 5.2.37 – Ensure A-MSDU is disabled. Appendix A – Updated contact for Intel. Clarified aggregation settings. Adjust throughput criteria for 5.2.5 and 5.2.6 to use the Marvell 11n station in place of the Conexant station. Added note that Cisco ACS server uses 32 characters (octets) for the shared secret. Added notes to APUT h+d testing that each test may be performed separately depending on whether the APUT supports only one of the two functions. Update version of Juniper client.
1.4	7/8/08	Change Marvell 11n station to Broadcom 11n station in test 4.2.22 Change Marvell 11n station SW to version 3.0.4.9 . Change 4.2.24 and 5.2.34 No Ack tests scripts to reduce send buffer size to 1456 bytes.
1.5	7/30/08 8/28/08 9/4/08 9/23/08 10/22/08 11/05/2008 12/01/08	Removed notices stating that the RIFS tests are for data collection only. Change from Intel 3945 station to the Marvell 11n station in test 4.2.24, NoAck test. Changed "and" to "or" in test 5.2.31 to match the WMM test plan. This was a typographical error. Updated FTP information. Modified 5.2.26 for stations that only support one band. Update the SW version on the ADEPT box in table 256. ECN 135, remove Intel station from test 4.2.24.
1.5.4	1/29/09	Add in Extended EAP methods AKA and FAST.
1.6.0	03/02/2009	Accepted all changes.
1.6.1	03/02/2009	Corrected Copyright year. Updated reference to TGn Marketing MRD. Added AP STBC Tx test case Added STA STBC Rx test case.

		Added AP A-MPDU Tx test case. Added STA A-MPDU Tx test case. Minor editorial and formatting.
1.6.2	03/04/2009	Modified copyright date to 2008 – CID 3 Modified document title – CID 4 Modified phase 2 feature from mandatory to optional Testbed – CID 10 Removed disable aggregation from test case 4.2.39 – CID 11 Removed disable aggregation from test case 5.2.46 – CID 12 Removed "Phase 2" from the test plan – CID 13 Fixed Tested to Testbed typo – CID 17 Addressed CIDs related to compatibility with IEEE 802.11n IEEE 802.11-2012 (18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, and 37). Corrected table number – CID 16 Addressed CID on AP STBC testing – CID 9 Minor editorial comments.
1.6.3	03/06/2009	Corrected APUT and STAUT table for 802.11d+h testing. This should be only done in 5 GHz and is optional. Added 40 MHz Intolerance AP Test cases. Added 40 MHz Intolerance STA Test cases.
1.6.4	03/10/2009	Formatting and Editing fixes. Added test cases to Table 8. Corrected 20/40 MHz interoperability test cases for both AP and STA. Modified 4.2.23 and 5.2.30. Set 11n testbed devices to legacy mode. Set all streams to the same data rate. Add Intel 4965AGNMM2WB as alternative to …GN as the latter is no longer available.
1.6.5	03/23/2009	Accepted all changes. Minor editorial and formatting fixes. Added 3 Spatial Streams for AP and STA. Added MCS Index/PHY Data rate table for 3 SS. Made corrections to the 20/40 MHz Coexistence tests.
1.6.6	03/24/2009	Accepted all changes. Minor editorial and formatting fixes. Minor fix on test case 5.2.42, fixed pass criteria. Added Channel Width Set in 4.2.40. Made changes to 4.2.43 based on plugfest contribution. Made changes to 5.2.50 based on plugfest contribution. Modified procedure for test case 4.2.41 per contribution. Modified procedure for test case 5.2.48 per contribution.
1.6.7	03/30/2009	Accepted all changes. Replaced WFA logo with the new one. Replaced Broadcom AP with Ralink AP in test 5.2.41. Made some updates to section 2.2.

		Updated RADIUS server information in 2.3. Updated device information in 3.3.3.3 and 3.3.4. Updated Supplicant and Server information in relevant AP and STA test cases. Added priority for new EAP Types (FAST and AKA). NOTE: All Extended EAP tests for AKA and FAST are currently not performed. Merged changes from WFA Staff's test plan 1.5.6 and 1.5.7. Minor editorial and formatting fixes.
1.6.8	05/20/2009	Accepted all changes. Modified 4.2.41 20/40 MHz coexistence test, step 2 and step 4. Removed content from Appendix since there will be new testbed devices and new performance thresholds. Added Channel Width configuration for testbed APs in 5.2.20. Corrected channel list pass/fail criteria in test case 5.2.48. Defined loop variable I in test case 4.2.42. Minor editorial and formatting fixes.
1.6.9	6/25/2009	Accepted all changes. 4.2.40 Removed step 1 and added expected results 4.2.44 Added negative test for HT rates and WPA. 5.2.51 Added negative test for HT rates and WPA. 4.2.31 and 4.2.32 Updated purpose and description 4.2.33 and 4.2.34 Fixed STA2 HT-Greenfield value 4.2.39 Added configuration parameter MCS Rate for STA1 and STA2 4.2.40 Modified equipment, configuration, and procedure. 4.2.41 Removed testbed 802.11g STA, not required. Added note for intermittent ping timeouts. 4.2.43 Modified steps and expected results. Update table on test cases. 5.2.27 and 5.2.28 Modified Chariot scripts 5.2.29 Modified Chariot scripts 5.2.34 Updated configuration of Ralink .11n AP 5.2.39 Updated purpose and description 5.2.40 Updated purpose and description 5.2.46 Added usage of STBC to step 1 5.2.47 Modified test environment, configuration, and procedure 5.2.48 Modified expected results. 5.2.50 Modified test procedure. Minor editorial and formatting fixes.
Lab 01	07/08/2009	Accepted all changes. 4.2.40 & 5.2.47 Typos, Front page legal boilerplate changes, Added MCS rates in Appendix F.
Lab 02	07/14/2009	Updated document cross references,, updated parameter names, fixed "Tested" for Testbed. Added ECN 164, Formatted tables, added Servers and Supplicant tables
Lab 03	7/23/2009	4.2.39 step 5 added detail to ping (request). 4.2.35 added Vendor row to table 108. 4.2.17 tables 64, 65, 66, 67, & 68. 4.2.18 table 74. Fixed table numbering error in test plan. 4.2.43 & 5.2.50 lengthened ping from 32 bytes to 1000 bytes
Lab 04	7/30/2009	Modified tests 4.2.33 & 5.2.41& 4.2.34 & 5.2.42
Lab 05	8/11/2009	Fixed typos in 4.2.1 &9. 5.2.4, 9, 10, 12, 18, 21, 31, 34, & 36 Dual band devices test in both bands 4.2.42 & 49

		Modified tests 4.2.38 & 5.2.45 (RIFS)
Lab 06	8/13/2009	Modified test 5.2.9&5.2.1, updated testbed schematics
Lab 07	8/18/2009	Removed old testbed equipment allocations for each test. Added new test bed schematics, Added testbed equipment
Lab 08	8/18/2009	Accepted all changes
Lab 09	8/20/2009	Modified Ping criteria. Added requirement to test spatial streams in both bands for dual band devices. Added Sigma Software description. Fixed broken links. Updated TOC.
Lab 10	8/21/2009	Allow 40 MHz testing in 2.4 GHz band.
1.7	8/21/2009	Accepted all changes. Released for BoD approval and initiation of IPR period.
1.7.1	9/16/2009	Selected test bed devices. Changed 3.2.11.4 to allow for 20/40 MHz in 2.4 GHz and 1SS stations. Changed 4.2 and 5.2 so that coexistence is only tested in 2.4 GHz. Changed 4.2.26 so that features are checked by examining beacons. Changed 4.2.27 and 5.2.36 to allow 2.4 GHz devices to be tested in 20/40 MHz. Clarified 4.2.44 and 5.2.51 so that the DUT fails if it sends HT packets to or acks HT packets from a test bed device using TKIP. Removed Appendices F and H. Cleanup.
1.7.2	9/25/2009	Changed 4.2.44. Changed all ping tests for better pass/fail metric Scrubbed document for errors. 4.2.1 placed check for OOB in 20 MHz only. Combined 5.3.1 & 5.3.2 into one test. Combined 5.3.3 & 5.3.4 into one test. All IBSS test run in Legacy mode. Added test bed products to Appendix A
1.7.3	9/28/2009	Selected test bed devices.
1.7.4	9/29/2009	Added edits from Technical Director's review
1.7.5	9/29/2009	Selected test bed devices. Added threshold values.
2.0	9/29/2009	Initial Release
2.0.1	10/01/2009	Modified 4.2.44 & 5.2.51 to reflect changes to TGn DRAFT 2.0 Test Plan
2.0.2	10/19/2009	Juniper reference removed from 5.3. Updated Ralink AP software revision. 4.2.1 Replaced Marvell supplicant with Intel supplicant. Updated threshold numbers (added Chariot numbers). 4.2.1 Modified steps 1 &3 to reflect correct OOB requirements. 5.2.51 removed reference to Ralink Draft 2.0 AP. 5.2.1 Modified step 2 to reflect correct OOB requirements. 5.2.35 Replaced Atheros AP with Ralink AP. 5.2.26 Replaced WPA-TKIP with WPA2-AES. 4.2.41 Cleaned up text in steps 4, 6, 7, & 10. 5.2.44 Modified step numbering to clean up typo. 5.2.42 Modified channel width settings for AP1.4.2.34 Modified channel width settings for 20/40 MHz operation. 5.2.38 step 4 Removed reference to Marvell AP. Appendix A, tables 278 & 279 added contact information to test bed products. 4.2.44, table 132 Cleaned up text and steps. 2.1.2 Added ping test duration note. 4.2.30 Changed Broadcom STA for Ralink STA. 5.2.38 Changed Broadcom AP for Ralink AP.
2.0.3	11/25/2009	5.2.2, table 270 removed Draft 2.0 reference from Ralink device. 4.2.42, step 2 sniffer check moved to step 1. Section 6, Appendix A updated testbed distribution information. Section 2.1.1 updated version number of Omnipeek sniffer. Page 231, table 282 updated Omnipeek

		version and contact information. Page 230, table 230 corrected Intel part number. 4.2.26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 40, 41, 43, & 44 added note to allow 1x1 AP testing. 4.2.27, 39, and 42 added note to prohibit 1x1 AP testing. 5.2.50, step 4 – added text to allow 1x1 STA testing. 4.2.24 – removed reference to Marvell STA. 5.2.16 – changed text to read mandatory for Enterprise devices. 4.1.1removed item 2 – ability to set beacon Interval.
2.0.4	12/23/2009	Change history (11/25/2009) 4.2.44 changed to 4.2.42. 4.2.38, table 124, step 1 – removed reference to Appendix H. 5.2.45, table 260, step 1 – removed reference to Appendix H and changed MCS rate from 7 to 4. Page 232, table 279 – Broadcom AP software version changed from 5.10.128.05 to 5.22.69.2. Page 116, table 106 – changed Dual band channel to use 6. Page 116, section 1 – modified last sentence. Page 25, section 1.2.1 added reference to Supplicant Testing Policy. Page 25, section 1.2.2–- modified Class 1 text. Page 30, section 2.1.3 added a last sentence. Page 30, section 3.1, item #5 – modified text. Page 34, section 3.2.6, Item 6 – changed text. Second paragraph – added text. PS Poll changed text in first sentence. Page 35, section 3.2.11 – added sentence. Page 39, section 3.2.17, 5th bullet modified text. Page 51, sections 3.6 & 3.7 – added text. Page 137, table 132, step 7 added Filesndl.scr. Page 226, 5.3.1 – added more text for Test Configuration. Page 229, table 275 – added REALAUD.scr reference. Page 118, table 108 – added information for 1SS. Page 119, table 110–- added information for 1SS. Page 120, table 112 – changed dual band to use channel 1. Page 123, table 116–- added information for 1SS. Page 134, section 4.2.42, Test Configuration – added text.
2.0.5	03/08/2010	Section 3.5.4 – updated first paragraph. Section 1.2.4.3 added note on 20/40 MHz Coexistence. Swapped Broadcom AP & STA software versions in Appendix A. Section 4.2.39 – steps 5 & 6 added Ping Request & updated Table caption for 125 & 126. Section 4.2.19, Table 77 applied bold format to heading. Section 4.2.42, Table 131 applied bold format to heading. Appendix A, updated Ralink STA and AP part numbers and software versions. Section 5.2.5, Table 150 replaced Ralink AP with Marvell AP5.2.43, Table 258 replace Atheros AP1 with Marvell AP. 5.2.1, AP1 is an 11n device. 5.2.15, Table 171 – changed STAUT supplicant to WPA_Supplicant. 5.2.25 – removed note for EAP tests for FAST and AKA. 5.2.46 – added note for 1x1 STAs. 5.2.2, Table 142 – Replaced Marvell AP with Atheros AP. 5.2.11 – Replaced Marvell AP with Atheros AP. 4.2.9 – Removed note about WPA-PSK. 5.2.45 – Replaced Broadcom Draft 2.0 11n AP with Broadcom 11n CERTIFIED AP. 4.2.38 – Replaced Broadcom Draft 2.0 11n STA with Broadcom 11n CERTIFIED STA. Appendix A – Removed Broadcom Draft 2.0 11n AP & STA. 4.2.26 Table 99 – Removed reference to IEEE 11n IEEE 802.11-2012 & inserted RTS/CTS or CTS to self note. 5.2.24 , Table 205 – Added second AP as per test requirements. 5.3.2, Table 178 – replaced Intel STA with Atheros STA. 3.2.11.4 – Added note about 1x1, 2x2, and 3x3 device capabilities. 5.2.24 – added note about STA disconnection before each test. 5.2.26 – changed name of test to Roaming Test for Single & Dual Band STAs with WPA-PSK. Updated Appendix E with revised threshold numbers. 5.2.24, Table 193 (ExS5) – replaced Marvell AP with Broadcom AP. 5.2.24, Table 199 (ExS11) – replaced Marvell AP with Atheros AP. 5.2.24, Table 207 – replaced Marvell AP with Broadcom AP. 5.2.47, Table 267–-

		replace Atheros AP1 with Ralink AP, replace Ralink AP2 with Atheros AP.
2.0.6	05/27/2010	Corrected Change History for 2.0.5–- 5.2.5, now reads Ralink AP and Marvell AP. Appendix A–- corrected Atheros STA to AR5BXB. 4.2.16 - changed notes between tables 48 & 49 and swapped steps 4 & 5 in table 49. 5.2.23, table 188–- changed step 4 Expected Results. 4.2.11, table 34–- changed STA 1 supplicant from CSSC to Microsoft. 4.2.42, table 131 – replaced Intel STA with Ralink STA. 5.2.1, table 141, step 2 – now reads Association Request. 5.2.24, tables 198 & 200 – removed footnotes. 4.2.17 tables 50 through 62 and 64 through 69 – specified dual band channel for each test.4.2.18, tables 71 through 75 – specified dual band channel for each test. 5.2.24, tables 189 through 201 and 203 through 208 – specified dual band channel for each test. 5.2.25, tables 210 through 214 – specified dual band channel for each test. 4.2.25, table 96 – changed script to IPTV20Mbps-dn.scr. 4.2.43, table 134, step 7 – ping length changed to 1000. Appendix A, table 282 Broadcom driver changed to 5.10.112.3. 4.2, table 10 & 5.2, table 139 – added footnote concerning 20/40 MHz Coexistence becomes mandatory if 20/40 MHz is supported. 5.2, table 139 – item 5.2.50 changed to mandatory. 4.2.17, 4.2.18, 5.2.24, & 5.2.25 – removed note "All Extended EAP tests for FAST and AKA are currently not performed". Appendix A – Marvell AP firmware changed to 5.0.6.2B. 4.2.6, 4.2.8, & 4.2.10 – added footnotes "Atheros STA can only go into Power Save mode when operating off the battery. Remove power cord for this test". 5.2.13, table 167 – removed mixed mode parenthetical comments. 4.2.9, table 30 – remove "Note 1" from table and remove actual note below table 31. 4.2.xx & 5.2.yy–- added new tests for negative WEP for AP and STA. Sections 4.1.3 & 5.1.3–- Removed. 5.2.10, 5.2.13, 5.2.15, 5.2.16, 5.2.19, & 5.2.21 – Added missing table.
2.0.7	8/4/2010 8/11/2010	Test 4.2.1, changed to allow either station 1 or station 4 to associate and ping with the APUT. 4.2.45–- APUTs that prohibit the configuration of WEP and HT rates pass in step 1. Allow for multiple models of the Intel STA.
2.0.8	9/16/2010	5.2.37 – Use Broadcom AP.
2.0.9	10/12/210	Table 9, test 4.2.43 changed to mandatory. 4.2.11, table 33 – changed STA 1 supplicant from Microsoft to WPA Supplicant. 5.2.9, 5.2.10, 5.2.11 – removed step 0. 4.2.31, 4.2.32, 4.2.35, 5.2.38 – Remove references to Downlink x.y. 5.2.29, table 230 – STA2 channel width entry deleted. 4.2.20, table 80 – changed script data rates to 18/14/14 Mbps. 4.2.20, table 81 – changed pass rate in step 7 to 67%. 4.2.26, table 97 – Removed 5 GHz from 20/40 MHz options. 5.2.33, table 244, steps 4, & 6 % ratios changed. 5.2.30, Table 234, changed traffic streams from 10, 10, 10 to 18, 14, 14 Mbps. 4.2.23, Table 89 changed traffic streams from 10, 10, 10 to 18, 14, 14 Mbps. 4.2.26, step 1 added note (If 20/40 MHz supported in 2.4 GHz then 20/40 MHz Coexistence support is required). 5.2.35, step 3 – added note (If 20/40 MHz supported in 2.4 GHz then 20/40 MHz Coexistence support is required).
2.0.10	1/11/11	Changed contact for Broadcom per Broadcom's request.

	2/9/11	4.2.23 – changed 1st sentence of Purpose and Description. 1.1, table 1 – corrected ISM acronym. 4.2.16, table 47 – changed channel 56 to channel 44. 4.2, table 9 – added note about optional and tested. 5.2 table 139 – added note about optional and tested. 4.2.38 – corrected table reference numbers. 4.2.38 & 5.2.45 – added note to use MCS 4 for 1x1 devices. 5.2.8 Swapped out Atheros STA for Broadcom STA. 5.2.22, table 191 – changed channel 56 to channel 44. 5.2.23, table 193 – changed channel 56 to channel 44.
2.0.11	2/21/11	5.2.28 and 5.2.29, remove Atheros station and replace with Broadcom BCM943224HMS station.
	3/14/11	Allow Chariot version to be 6.4 or higher. Update Chariot contact information.
	4/6/11	4.2.19 – Clarified that this test is skipped for single radio or single band APUTs. Changed from “Mandatory” to “Optional and Tested”. 4.2.43 – Clarified that this test is run twice for dual band APUTs.
	4/8/11	4.2.1 – Added two legacy APs – one on channel 1 and another on channel 11 – to force 20/40 MHz capable APUTs to 20 MHz. 5.2.1 – Moved AP1 to channel 1 and AP2 to channel 11 to force 20/40 MHz capable STAUTs to 20 MHz.
2.0.12	4/18/11	4.2.22 – Changed data rates of Chariot scripts for 1x1 APUTs.
	4/25/11	Appendix A – Changed Intel’s technical support contact.
	5/3/11	5.2.46 – Removed 1x1 requirement.
	5/26/11	4.2.7 – Corrected a typo.
	6/7/11	Appendix A – Changed Atheros’ technical support contact.
	6/9/11	1.2.3 – Added text for WPA2-Personal only DUTs.
	7/13/11	4.2.33 – Corrected step 6. STA2 pings APUT instead of APUT pings APUT.
	7/19/11	4.2.1 – Corrected step 1. Examine the secondary channel offset field instead of the supported channel width field.
	7/22/11	4.2.44 – Corrected step 2. Removed “and probe response” since the probe response is not checked in step 2 results.
	7/25/11	4.2.7 and 4.2.8 – Added note to skip these tests if the APUT supports only WPA2 and not WPA.
	8/2/11	Table 9 – 4.2.36 can be run in 2.4 GHz as well.
	8/17/11	5.2.27 – Added note to check for saturation.

	9/27/11	5.2.31 – Added statement that no packets are allowed to be sent with QoS level AC_VI. Appendix A – Changed Ralink's technical support contact.
	9/30/11	4.2.16 – Changed starting channel to 56. 5.2.22 – Changed starting channel to 56 and ending channel to any non DFS channel.
2.0.13	10/7/11	5.2.44 – Added channel for 2.4 GHz devices.
	10/12/11	5.2.23 – Changed channels to match 5.2.22.
	11/7/11	3.1 – Corrected WMM specification version number to latest released version. 3.3.3 – Added references to table 8 for EAP types.
	11/10/11	4.2.10, 4.2.13, 4.2.22, 4.2.44 – Added notes for WPA2 only devices.
	11/11/11	Appendix A – Changed Marvell AP's firmware from 5.0.6.2.B to 5.0.6.2C
	11/29/11	4.2.38 – Added note for MCS rates used by various APs.
	12/1/11	4.2.3 and 5.2.3 – Removed PLCP tests. Appendix A – Replaced Intel 5300 with Intel 6300. Appendix A – Replaced Cisco CSSC supplicant with Cisco AnyConnect supplicant. Appendix A – Added WFA-EMT as new test tool.
2.0.14	12/13/11	4.2.38 – Corrected typo. Appendix A – Specified that Intel station uses Windows 7.
	12/16/11	4.2.10 – Added check for TIB bit. Until April 17, 2012, the TIB check is for data collection purposes only. The APUT will not be failed due to this check. [issue #6, CMG]
2.0.15	1/13/12	The Cisco, Open1x, and WPA supplicants cannot be used with Windows 7. In the Extended EAP test cases (4.2.17 and 4.2.18), replace the Intel station with another station if the test requires the Cisco, Open1x, or WPA supplicant. In all other test cases, when using the Intel station, only use the Microsoft supplicant.
2.0.16	2/10/12	Fixed typos.
	2/16/12	Appendix A – Added version number for EMT.
	3/6/12	4.2.10 – Fixed typo. 5.2.41 – Added note that 1T1R stations cannot use GF and Short GI together per 802.11n IEEE standard.
	3/15/12	5.2.41 – Added sniffer checks.
	3/22/12	Removed categories 1 and 2 APUTs. Removed categories 2 and 3 STAUTs.
2.0.17	4/3/12	5.2.41 – Modified sniffer checks.
	4/3/12	

	4/16/12	Changed 5.2.2 to put STAUT into power save mode if STAUT supports power save. 4.2.10 – Check for TIB is now mandatory.
2.0.18	4/25/12 4/26/12 5/1/12 5/2/12 5/9/12 5/15/12	4.2.3 – Added TSF test. Updated MediaTek/Ralink station driver to 1.4.13.1617 and reduced threshold for 4.2.37T7DT2. Updated Atheros/Qualcomm station driver to 9.2.0.499. 5.1.1 – Removed static IP requirement, 5.1.2 – Removed WPA security requirement. Tables 9 and 111 – Changed some tests from mandatory to optional due to some devices not supporting WPA or enterprise security. 4.2.34 – Swapped Broadcom and Intel stations. Added more ASCII characters to SSIDs.
2.0.19	5/23/12 5/31/12	Added support for AKA' 5.2.8, 5.2.20 – Removed pairing of Atheros/Broadcom station and WPA supplicant. 5.2.17, 5.2.18 – Reverted to previous SSID for EMT. Removed ASCII characters used by Sigma.
2.0.20	6/6/12 6/25/12 7/09/12 7/11/12	4.2.41 – Added 200 second wait time. Replace IEEE 802.11 Draft 5.0 with IEEE 802.11-2012 standard. 4.2.11 – Fixed typos. Removed additional ASCII characters used by Sigma.
2.0.21	7/30/12 8/6/12 9/28/12	Appendix A – Updated Hostapd to version b80eb89 Appendix A – Added Atheros station for AKA' testing ExA26 – Use the newly added Atheros station as the test bed device. 4.2.41 – Allow the APUT to select the secondary channel above or below the primary channel.
2.0.22	10/3/12	5.2.14 – For steps 3 and 4, set the pass criteria to "This test passes if 50% or more of the sent packets are successfully received."
2.0.23	11/8/12 12/3/12 12/4/12 12/19/12 12/20/12	Added section 3.8 Allowed Security Combinations. Added test 5.2.53 "Support for AES if TKIP is supported". Removed prerequisites for WPA only mode. Updated headings for test 5.2.26 to reflect the intended security method. Grammar and spelling corrections. Appendix A – Updated Microsoft's email. ExS21 – Changed WPA2 to WPA1 in the table to match the test procedure.

	1/3/13	4.2.1 – Clarified that the APUT should use default security. 4.2.10 – Added group traffic testing. Appendix B – Added sample sniffer captures for group traffic testing. 5.2.1 – Removed check for supported features. Allow the STAUT to connect to either AP1 or AP4. 5.2.35 – Enabled supported features on the test bed AP for those STAUTs that do not enable supported features unless the AP advertises them. 5.2.36 – Made it clearer on which steps to run for 1SS and 2SS STAUTs.
	1/11/13	5.2.53 – Use the Ralink AP as the test bed AP.
2.0.24	1/16/13	4.2.7A5DT2WPA2 – Reduced threshold value.
	1/18/13	4.2.44, 4.2.45, 5.2.51, 5.2.52 – Clarified test steps.
	1/22/13	4.2.10 – Revised group traffic test. 5.2.18 – Added step 9.
2.0.25	1/23/13	4.2.11 – Made step 5 generic so that any supplicant could be used. 4.2.16 – Fixed a typo.
	1/29/13	3.8 – Clarified that WPA-TKIP is still allowed until January 2014.
	1/31/13	4.2.10 – Revised group traffic test to include check on more data bit in all group packets.
2.0.26	2/1/2013	3.8 - separated security combinations into APUTs and STAUTs per the Security Roadmap. Changing Broadcast/Multicast to Group Traffic and Unicast to Directed Traffic
	2/15/13	4.2.10 – Removed note about Atheros station in power save mode. 4.2.16 – Allow any non-DFS channel to be used after channel switch
	2/20/13	Corrected the usage of the words simultaneous and concurrent.
2.0.27	3/5/13	5.3.1 – The test bed devices are no longer set to actively or passively scan. Run the test only once.
	3/20/13	Added note to 5.2.53 that it is for data collection only until January 1, 2014. Added purpose statement.
	4/3/13	Added tests 4.2.46 and 5.2.54 “Traffic sharing on the same access category”. These tests are for data collection only until July 3. 2013.
2.0.28	4/18/13	4.2.1 – 4.2.19 Removed reference to “Wi-Fi 802.11 with WPA2, WPA, and WEP System Interoperability Test Plan for IEEE 802.11a, b & g Devices”, 4.2.20 – 4.2.25 Removed reference to” WMM System Interoperability Test Plan” 5.2.1 – 5.2.26 Removed reference to “Wi-Fi 802.11 with WPA2, WPA, and WEP System Interoperability Test Plan for IEEE

		802.11a, b & g Devices", 5.2.27 – 5.2.34 Removed reference to" WMM System Interoperability Test Plan" Appendix F - Added List of Test Cases for WPA2 System Interoperability Testing Appendix G - Added List of Test Cases for WMM System Interoperability Testing
	5/2/13	Added test 4.2.47 "Power Save". This test is for data collection only until July 31, 2013. Appendix A – Added Ralink RT2800PD2 for Power Save test.
2.0.29	5/10/13	4.2.46 – The test bed stations are set to disable aggregation instead of the access points. The DTIM values are set to OOB. The TXOP limits are set to default. Clean up. 5.2.54 – Clean up.
2.0.30	5/20/13	4.2.1 – Removed 11n sniffer check for non-11n DUTs. 4.2.16 – Noted non-DFS channel in step 6. 4.2.46 and 5.2.54 – Clarified settings for 1, 2, and 3SS DUTs.
2.0.31	6/20/13	Table 114 – Corrected the test case titles for 5.2.19, 5.2.20, and 5.2.21 5.2.6, 5.2.8 – Corrected the test case titles. 4.2.46 and 5.2.54 – Changed the data collection dates to indefinitely.
2.0.32	7/8/13 7/16/13 7/18/13	5.2.41 – Removed unnecessary check in step 4. 4.2.47 – Use the Ralink 3800 instead of the Ralink 2800. 4.2.27 – Clarified security setting. 4.2.29 – Skip steps 1 to 4 if the APUT doesn't support Open security. 4.2.47 – Pushed data collection date to 1/1/14. Modified and clarified several checks.
2.0.33	7/22/13 7/29/13 8/12/13	4.2.47 – Clarified that retries do not count as multiple packets. Apendix A – Removed ADEPT. Clean up the usage of the words conformance and compliance. 4.1.2 and 5.1.2 – Added security checks.
2.0.34	8/29/13	4.2.9, 4.2.22, 4.2.24, 4.2.34, 4.2.36, 4.2.40, 4.2.34, 5.2.4, 5.2.11, ExS23, 5.2.26, 5.2.35, 5.2.37, 5.2.49 – Changed the SSID 4.2.46 and 5.2.54 – Modified the tests to measures the back off slot distribution for APUT and STAUT Appendix I – Added sniffer information for test cases 4.2.46 and 5.2.54 5.2.28 and 5.2.29 – Replaced the Broadcom station with the Intel station.

	9/5/13	5.2.14 – Specified that the test bed AP should be using a DTIM count of 1. 5.2.41 – Added a sniffer check to ensure that the test bed AP is transmitting Greenfield.
2.0.35	9/9/13 9/25/13 10/14/13	4.1, 4.2.1, and 5.1 – If a DUT only supports WPA2, it does not have to turn WPA2 on or off. 4.2.46 and 5.2.54 – Removed confusing text. Fixed typos. 5.2.53 – Clarified that the DUT should disconnect from the AP before changing the security settings on the AP. Added step 4.1 allowing the station to be disconnected and reconnected to the AP.
2.0.36	10/16/13 10/29/13 10/31/13 11/13/13 11/19/13 11/26/13 12/4/13 1/6/14	4.2.42 – Clarified that steps 5 and 6 are only skipped if the APUT does not support 40 MHz. 5.2 – Changed test case 5.2.19 to optional and tested. 5.2.53 – Allow the station 65 seconds to change from TKIP to AES. 5.2.2 – Highlighted in red the sections that are for data collection purposed only. Table 9, table 114, and test case 4.2.12 – Clarified that PMK is mandatory for Enterprise devices. 4.2.47 – Clarified that step 7 only applies to the initial transition. 4.2.40 – Removed confusing notes about burst and AMSDU. Cleaned up for removal of WPA only. 3.8 – Removed WPA only as an allowed combination. 5.2.53 – Test is now mandatory.
2.0.37	1/15/14 1/28/14 1/29/14 2/10/14 3/5/14 3/19/14	5.2.53 – Removed unnecessary disconnect from steps 3 and 6. 4.2.44 – Deleted table 108 procedure as WPA alone not allowed anymore on DUT. 3.5.8 – Clean up and clarifications. 3.8.2 – Added “mixed mode WPA2/WPA, open” as an allowed security combination. 5.2.51 – Clarified that the STAUT should be in mixed mode WPA2/WPA. Skip this test if the STAUT doesn’t support mixed mode WPA2/WPA. 3.5.9.1 – Removed line about having to turn on security since some devices have it on by default. Added test cases 5.2.55 and 5.2.56. For now, these will be used for data collection only.

	4/17/14	Added test cases 4.2.48, 4.2.49, 4.2.50, 5.2.57, 5.2.58, and 5.2.59. For now, these will be used for data collection only. Added Appendix J. 4.2.10 – Clarified that the group and directed traffic that is being monitored is from the APUT. Renamed Ralink to MediaTek.
2.0.38	5/5/14 5/7/14 5/22/14 6/3/14 6/18/14 6/26/14 07/10/14 7/22/14 7/23/14 7/30/14	5.2.55 and 5.2.56 – These tests are mandatory. Updated MediaTek's contact info. 3.8.1 and 3.8.2 – Added WPA2, WEP, and open as an allowed security combination. Appendix A – Allow the option to use the Qualcomm AR5BXB-00114A as the sniffer. 5.2.1 – Allow stations to use WPA2/WPA mixed mode OOB. Note that these stations should associate to the WPA2 AP. Appendix C – Removed tables and refer to Annex E of IEEE 802.11 standard. 4.2.16d – Added APUT OOB beacon country code check. Removed the reference to Wi-Fi allinance country code list and pointed to the list mentioned in the tech-ops manual 5.2.37 – Removed AMPDU aggregation needing to be in manual mode. 4.2 and 5.2 tables – Corrected the names of the WMM Back Off tests. Corrected a few test case names.
2.1	8/11/14 9/5/14 9/17/14 10/6/14 12/31/14 1/5/15	Updated Mediatek AP's firmware Appendix E – Corrected the ordering of some test cases. 3.1 – Refer to the latest released version of the WPA2 test plan. 5.2.57 – Corrected reference to WMM table. 4.2.46 and 5.2.54 – Modified the pass critera. Removed no-aggregation and TXOPs parameters from the text. 5.2.55 – no longer in data collection phase. 5.2.56 – removed.
2.2	8/21/14	4.2.1, 4.2.3, 4.2.6, 4.2.9, 4.2.10, 4.2.16, 4.2.20, 4.2.22, 4.2.23, 4.2.24, 4.2.25, 4.2.27, 4.2.28, 4.2.29, 4.2.30, 4.2.31, 4.2.32, 4.2.33, 4.2.34, 4.2.35, 4.2.36, 4.2.37, 4.2.38, 4.2.39, 4.2.40, 4.2.41, 4.2.42, 4.2.43,

		4.2.47 - Added missing passphrases and/or added ASCII characters to passphrases. 5.2.1, 5.2.3, 5.2.6, 5.2.7, 5.2.9, 5.2.14, 5.2.17, 5.2.18, 5.2.20, 5.2.21, 5.2.26, 5.2.27, 5.2.35, 5.2.37, 5.2.53, 5.2.55, 5.2.56 - Added missing passphrases and/or added ASCII characters to passphrases. 3.3.3.1 – Added requirements for ASCII passphrases.
	10/2/14	5.2.30 – Replaced the Atheros AP with the Broadcom AP. The Atheros AP has an issue with some STAUTs that have power save enabled.
	1/7/15	5.2.53 – the AP should be in non-11n mode.
	3/20/15	4.2.8 and 4.2.13 – Clarified that these tests are only skipped if the APUT doesn't support mixed mode.
	3/26/15	2.1.3 – Clarified that Chariot will use TCP or UDP while Sigma will only use UDP.
2.3	5/7/15	ExS9 – Replaced Devicescape server with Radiator server. ExS10 – Replaced Devicescape server with HostAPD server. ExS11 and ExS12 – Removed. Appendix A – Removed Devicescape server. Updated HostAPD, Radiator, and Windows Server.
	5/18/15	Appendix A – Updated Ixia and WFA's support email addresses.
	5/22/15	4.2.46, 4.2.48, 4.2.49, 4.2.50, 5.2.54, 5.2.57, 5.2.58, 5.2.59 – Removed due to the closure of CMG 19 and 21.
2.4	3/31/15	4.2.26 – Allow the APUT to use non-HT mixed-mode.
	6/19/15	Replaced the Broadcom station with the Broadcom BCM94360MC from the CERTIFIED ac test bed. 4.2.1, 4.2.5, 4.2.9, 4.2.10, ExA24, 5.2.8, 5.2.14 – the BCM94360MC station only supports WPA Supplicant. Replaced the MediaTek station with the Marvell RD-88W-8897-WIFI-S0 or another existing station. 4.2.1, 4.2.13, 4.2.14, 4.2.15 – the Marvell RD-88W-8897-WIFI-S0 use the integrated Fedora supplicant or the WPA Supplicant. 4.2.1, 4.2.31, 4.2.32, 4.2.33, 4.2.35, 4.2.37, 4.2.39, 4.2.40, 5.3.1, 5.3.2, 5.3.3 – test bed device changes. 4.2.10, 5.2.14 – use 224.0.0.5 as the multicast IP. Removed references to Chariot and corrected typos.

2.5	6/23/15 7/7/15 7/16/15	4.2.3 – Clarified that the test bed station should be in b mode, not the APUT. 1.2.3 – Clarified how to handle test cases if the DUT doesn't support open security, 5.2.46 – Clarified that the AP should be in 2 SS.
2.6	7/23/15 8/11/15	4.2.1 – Corrected the SSID for the APUT. 5.2.60 – Added new test case for CMG issue 34. Appendix A – Added Cisco AP for test case 5.2.60.
2.7	8/11/15 8/21/15 9/11/15	Section 3.9 – Added text regarding MAPUTs that do not support 1 and 2 Mbps in the basic rate sets. 4.2.47 – Removed MediaTek specific command 1.1, 3.2.11, 4.2.3 – Added text regarding MAPs.
2.8	8/11/15 4/15/15 8/10/15 10/6/15 10/12/15	4.2.40 – Replaced the Intel station with the Broadcom station. 4.2.40 – Enabled WMM Power Save on one test bed station to make sure that the APUT aggregates packets transmitted to WMM Power Save enabled stations. ExA26 – Replaced the Qualcomm station with the Broadcom station. Appendix A – Removed the Qualcomm Linux station. Appendix A – Clean up. 3.9 – Revised text to make it more clear. Sigma is now known as Wi-Fi Test Suite. Appendix A – Updated the Marvell station's driver. Appendix E – Added thresholds for Mobile APs, Handsets, TVs, Printers, and Set Top Boxes.
2.9	11/16/15 12/7/15 1/8/16 1/20/16 2/4/16 2/19/16	Changed some mandatory test cases to optional and tested. 4.2.29 – Clarified the passphrase to use. 5.2.37 and 5.2.38 – Removed confusing text about Appendix E. Appendix A – Removed OmniPeek sniffer. 5.2.60 – Removed Appendix A – Removed Cisco AP since it was only used in test case 5.2.60. 4.2.31 and 4.2.32 – Allow the APUT to start in mixed mode. Appendix A – Updated the Broadcom station's Wi-Fi Test Suite version. Fixes LDPC and mixed mode security issues.

2.10	2/2916	5.2.35 – Removed the sniffer checks for protection. Appendix A – Updated the Marvell station's software. Fixes LDPC issue.
	4/20/16	5.2.53 – Allow for reassociation requests.
	5/3/16	5.2.14 – Clarified that WPA2 only STAUTs run the test with WPA2 only 5.2.17, 5.2.18 – Clarified that WPA2 only STAUTs skip these test cases.
	5/11/16	3.2.11 – Corrected section numbering
	5/27/16	Undid the changes in version 2.4 that removed Chariot
2.11	6/2/16	Appendices F and G – Refer to sections 4.1 and 5.1
	7/5/16	Appendix A – Updated the Broadcom station's software. Fixes LDPC Tx issue.
	7/18/16	4.2.10 – Clarified that steps 1 to 4 require WPA2/WPA mixed-mode and steps 5 to 8 require WPA2 mode. 4.2.29 – Changed SSID to match Wi-Fi Test Suite scripts. 5.2.46 – STAUT must be in 1x1. Skip if the STAUT cannot be configured to 1x1. Appendix – Added an example of a WMM test run.
	8/19/16	5.2.15 – Removed incorrect check in step 5. Removed "APUT" from step 6.
	8/31/16	Appendix E – Thresholds updated. Added 3 more categories.
	9/9/16	4.2.7 – Clarified when test is skipped.
2.12	10/11/16	Table 6 – Corrected.
	12/21/16	Lowered throughput threshold for 5.2.4S2DT3 Audio devices from 0.7 to 0.3 Mbps
	1/5/17	Appendix A – Replaced the Qualcomm/Atheros XP station with the Realtek station or another test bed station. Affects test cases 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.6, 4.2.7, 4.2.8, 4.2.10, 4.2.11, 4.2.16, ExA14, 4.2.19, 4.2.26, 4.2.31, 4.2.32, 4.2.33, 4.2.35, 4.2.41, 5.2.5, 5.2.6, 5.2.7, 5.2.20, 5.2.33, 5.2.39, 5.2.40, 5.2.41, and 5.2.43. Appendix A – Removed the Cisco supplicant as it is no longer used in any test cases.

		Appendix B – Removed reference to Windows XP as it is no longer used by any test bed devices. Test case 4.2.1 step 5 – Clarified that the APUT should ping the connected station.
	1/18/17	Removed consecutive ping checks.
	2/20/17	Appendix A – Replaced the Qualcomm AP with a new Qualcomm AP or another test bed AP. Affects test cases 4.2.9, 4.2.32, 4.2.35, 4.2.41, 5.2.1, 5.2.2, 5.2.6, 5.2.10, 5.2.11, 5.2.14, ExS1, ExS4, ExS7, ExS18, ExS20, ExS24, 5.2.26, 5.2.29, 5.2.33, 5.2.39, 5.2.40, 5.2.43, 5.2.46, 5.2.47, 5.2.48, 5.2.50

Table of Contents

List of Tables

List of Figures

1. Overview

The goal of the Wi-Fi Alliance (WFA) is to ensure interoperability among IEEE 802.11a, b, g, and n products that support the extended security features of Wi-Fi Protected Access 2 (WPA2) from multiple manufacturers, and to promote this technology within both the business and consumer markets. To this end, the WFA has developed the following interoperability test suite. Working in conjunction with an authorized test lab, these tests are performed on vendor products.

This test plan exercises various combinations of PHY layer, MAC layer, and security features. With the advent of 802.11n, numerous mandatory and optional PHY and MAC features have been added. The TGn MRD has defined baseline mandatory and optional tested features. Section 4.10 of the TGn MRD (ref. 3) defines the mandatory and optional tested features.

The TGn MRD has defined an updated certification plan, which adds new features and functions. In order to validate these new features and functions, new test cases have been added to the AP DUT and STA DUT. Not all the device profile features defined in the TGn MRD will be tested and certified during the 802.11n program. The additional optional features for the 802.11n certification program launched in September, 2009 are:

- A-MPDU Aggregation when the AP is the Transmitter
- A-MPDU Aggregation when the STA is the Transmitter
- AP STBC Transmit (2x1) Test
- STA STBC Receive Test
- AP 20/40 MHz Coexistence Test
- STA 20/40 MHz Coexistence Test
- AP 3 Spatial Streams Test
- STA 3 Spatial Streams Test

1.1 Terms and Definitions

Acronyms presented throughout the document are defined in the following table. Some acronyms are commonly used in publication and standards defining the operation of wireless LAN. Others have been generated by WFA.

Acronym	Definition
AC	Access Category
AC_BE	Access Category Best Effort
AC_BK	Access Category Background
AC_VI	Access Category Video
AC_VO	Access Category Voice
ACK	Acknowledgement
ACM	Admission Control Mandatory
ADDBA	Add Block ACK
AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
AIFSN	Arbitration Interframe Space Number
AM	Active Mode
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
AP	Access Point
APUT	Access Point Under Test
AS	Authentication Server
ASCII	American Standard Code for Information Interchange
AV	Audio/Video
BSS	Basic Service Set
CCK	Complementary Code Keying
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CE	Consumer Electronics

CEPT	European Conference of Postal and Telecommunications Administrations
CHAP	Challenge-Handshake Authentication Protocol
CIE	Country Information Element
CSI	Channel State Information
CTS	Clear to Send
CW	Contention Window
DA	Destination Address
DELBA	Delete Block ACK
DS	Design Specification
DSCP	Differentiated Service Code Point
DSSS	Direct Sequence Spread Spectrum
DTIM	Delivery Traffic Indication Map
DUT	Device Under Test
DVD	Digital Versatile Disc
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ERP	Extended Rate PHY
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Committee
GF	Greenfield
GHz	Gigahertz
GI	Guard Interval
GTC	Generic Token Card
GUI	Graphical User Interface
HDD	Hard Disk Drive
HEX	Hexadecimal
HH	Hand Held
HT	High-throughput
HT-GF	High-throughput Greenfield
IBSS	Independent Basic Service Set
IE	Information Element
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineering
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical
KB	Kilobyte (1024 bytes)
Kbps	Kilobits per second (1000 bits)
LAN	Local Area Network
MAC	Medium Access Control
MAP	moble access point Note: “AP” stands for a non-mobile AP, so there is a strict distinction between “AP” and “MAP”.
Mbps	Megabits per second
MCS	Modulation Coding Scheme
MHz	Megahertz
MIC	Message Integrity Check
MIMO	Multiple InputMultiple Output
MPDU	MAC Protocol Data Unit
MRD	Marketing Requirements Document
MSCHAP	Microsoft CHAP
MSDU	MAC Service Data Unit
NA or N/A	Not Applicable
NAV	Network Allocation Vector
NIC	Network Interface Card
NOS	Network Operating System
OOB	Out of Box
OS	Operating System
OSI	Open Systems Interconnection
OUI	Organization Unique Identifier
PC	Personal Computer
PCF	Point Coordination Function
PCI	Peripheral Component Inter
PCMCIA	Personal Computer Memory Card International Association

PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PEAP	Protected EAP
PHY	Physical (Layer)
PID	Protocol Identifier
PLCP	Physical Layer Convergence Protocol
PMK	Pairwise Master Key
PMKID	PMK Identifier
PN	Packet Number
PSK	Pre-shared Key
PSMP	Power Save Multi-poll
PTK	Pairwise Transient Key
QoS	Quality of Service
RADUIS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RIFS	Reduced Interframe Spacing
RSN	Robust Secure Network
RTOS	Real Time Operating System
RTP	Real time Protocol
RTS	Request to Send
SA	Source Address
SGI	Short Guard Interval
SIM	Subscriber Identity Module
SM	Spatial Multiplexing
SNAP	Subnetwork Access Protocol
SS	Spatial Stream
SSID	Service Set Identifier
STA	Station
STAUT	Station Under Test
STB	Set Top Box
STBC	Space Time Block Coding
TCP	Transmit Control Protocol
TELEC	Japanese Telecom Engineering Center
TG	Task Group
TID	Traffic Identifier
TIM	Traffic Indication Map
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TP	Test Plan
TSN	Transient Secure Networks
TSpec	Traffic Specification
TTLS	Tunneled TLS
TxBF	Transmit Beamforming
TXOP	Transmission Opportunity
UDP	User Datagram Protocol
U-NII	Unlicensed National Information Infrastructure
USB	Universal Serial Bus
WEP	Wired Equivalent Protection
WiFi or Wi-Fi	Wireless Fidelity
WMAC	Wireless Medium Access Control
WMM	Wireless Multimedia
WNIC	Wireless Network Interface Card
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2

Table 1: Acronyms and Definitions

1.2 Definition of Devices Under Test (DUT)

1.2.1 Access Points Under Test (APUTs)

Generally, APs may be Personal APs or Enterprise APs. Personal APs do not support 802.1X remote authentication with an authentication server (AS). Personal APs support the use of preshared keys (PSK) only. Enterprise APs support 802.1X remote authentication using an AS.

1.2.2 Stations Under Test (STAUTs)

In addition to the categories defined in the supplicant testing policy, there are 3 STA device classes.

Class 1. Handheld (HH) Devices
Handheld devices are those categorized by a small form factor, small screen size, and battery powered with a range of throughput capability. HH devices include:

- Mobile/Wi-Fi phones
- PDAs supporting mobile services.
- Portable media players

The main application for these devices is power management and real-time support to manage latency and QoS. These devices also require improved range given constrained antenna configurations. These devices support a minimum of one spatial stream.

Class 2. Consumer Electronics (CE) Devices
Consumer electronics devices are those primarily used in the home and entertainment environments. These devices require high and reliable throughput and coverage area (range). These devices include:

- TV displays
- DVD/HDD players
- Home theater systems
- Media servers
- STBs
- Tuners
- Audio devices
- Video phones
- Portable AV players (battery powered device)
- Digital still cameras and camcorders (battery powered device)

Typical applications for CE devices are AV streaming, large file transfers, and general wireless communication.

Class 3. Personal Computer (PC) Devices
The PC segment is typically home and enterprise computer network devices. These devices include:

- Desktop computers
- Laptop/Notebook computers
- Table PCs
- Media centers
- Entertainment PCs
- USB adapters
- PC Cards
- PCI adapters

These devices can be wall or batter powered. The main application for PC devices is high throughput and coverage in a home or enterprise environment.

1.2.3 Applicability of Tests

Section 4 defines the tests for submitted AP devices.

Section 5 defines the tests for submitted STA devices.

In each section reference is made to Legacy Mode. Legacy Mode is defined as devices operating in any of 802.11a/b/g mode. All tests are performed using 1, 2, or 3 Spatial Streams as stated in each test case.

If the submitted device is a WPA2-Personal AP, all tests that specify WPA2-Enterprise shall be replaced with WPA2-Personal, and the ASCII string 12345678 shall be used for the key.

If the submitted device is a WPA2-Personal STA, all tests that specify WPA2-Enterprise shall be replaced with WPA2-Personal.

If the submitted device doesn't support open security and a test case specifies open security, then run the test with WPA2-Personal with the ASCII string 12345678 as the key.

If a test specifies WPA2-Personal, but no key is specified, then any key may be used (ex. 12345678).

1.2.4 Testing Scenarios

This section defines the various testing scenarios in order to achieve complete interoperability verification.

1.2.4.1 AP Testing Scenarios

- Coexistence between STAs having different MIMO Power Save Modes
- AP will advertise the "non-GF" STA exists when there is "non-GF" device associated

1.2.4.2 STA Testing Scenarios

- Roaming
  - Roaming from 20 MHz to 20 MHz in 2.4 GHz and 5 GHz all devices.
  - Roaming from 20/40 MHz to 20/40 MHz in 5 GHz only, this is NOT performed for 2.4 GHz 11n devices only
  - Roaming from 20/40 MHz to 20 MHz and vice versa in 5 GHz only, this is NOT performed for 2.4 GHz 11n devices only
  - Roaming from legacy 802.11a/b/g to 802.11n AP and vice versa.
- IBSS Operation

1.2.4.3 AP and STA Testing Scenarios

- Correct behavior of Operating Mode and AP indication to STAs
  - 2.4 GHz and 5 GHz
    - 20 MHz only Capable AP
      - 11n 20 MHz capable AP and all associated STA are 20 MHz working in 20 MHz
      - 11n 20 MHz capable AP in Mixed environment where both HT and non-HT STAs are associated
  - 5 GHz only; these test shall NOT be performed in 2.4 GHz band.
    - 20/40 MHz Capable AP configured for 40 MHz operation 11n APs only.

- 11n 20/40 capable AP and all associated STA are 20/40 MHz capable working in 40 MHz
- 11n 20/40 capable AP and all associated STA are 20/40 MHz capable working in 20 MHz
  - 11n 20/40 MHz capable AP, no non-HT STAs associated but at least one 20 MHz 802.11n STA is associated. Transmissions in 40MHz channel shall be protected in this 20/40 MHz capable BSS
  - 11n 20/40 MHz capable AP in Mixed environment where both 802.11n and non-HT STAs are associated
  - 11n 20/40 MHz AP with the existence of legacy non-AP STA devices in both the control and extension channel, protection is optional in BSS

- 20/40 MHz Coexistence, 11n devices only. A device that supports 20/40 MHz operation in the 2.4 GHz band shall implement 20/40 MHz Coexistence mechanism. The 20/40 MHz Coexistence tests are mandatory if a device supports 20/40 MHz operation in the 2.4 GHz band.
- Overlapping BSS in 5 GHz band only; these test shall NOT be performed in 2.4 GHz band, 11n devices only.
  - 20/40 MHz BSS running in 40 MHz channel width and another legacy 802.11a/b/g or 20 MHz BSS exists in the extension channel
  - 20/40 MHz BSS having its control channel on another 20/40 MHz BSS extension channel
- AP and STA adherence to the Recommended Transmission Channel Width Management Action Frame 11n devices only.
- Another two modes taken into consideration is the position of the extension channel (i.e. Extension Channel Offset Field 2), the two modes are (11n devices only):
  - Control channel center frequency is higher than extension channel center frequency.
  - Control channel center frequency is lower than extension channel center frequency.
- Block ACK Mechanism (11n devices only)
  - Recipient ADDBA Mechanism
  - Recipient DELBA Mechanism
  - Adherence to the Block ACK timeout
  - Receiver Buffer Size
- 802.11n A-MPDU Aggregation (11n devices only)
  - Adherence to
    - Maximum A-MPDU Factor
    - MPDU Density
- 802.11n A-MSDU Aggregations (11n devices only)
- 802.11n Spatial Multiplexing (SM) Power Save (11n devices only)
  - Initial settings of the DUT
    - Static SM power save mode (mode 00)
    - Dynamic SM power save mode (mode 01)
    - No Limitation (mode 11)
  - RTS before any MIMO sequence while the Recipient is in Dynamic SM Power Save Mode.
  - Ability to receive SM sequences while in Dynamic SM Power Save Mode
  - No MIMO sequences are transmitted when the recipient is in Static SM Power Save Mode
  - Adherence to SM Power Save Management Action Frame
- Group traffic and mixed group and directed traffic
- Coexistence of Different Spatial Streams Configurations (11n devices only)
- HT-Greenfield (Optional tested feature, 11n devices only)
  - Receiving HT-Greenfield frames when HT-Greenfield Capability is Advertised

  - The use of protection when “non-GF HT STAs Present” device are associated in the BSS
  - DUT will not transmit HT-GF frames to devices that do not support HT-GF
- Short Guard Interval (Optional tested feature, 11n devices only
  - DUT will not transmit short GI frames to devices that do not support short GI
- HT Duplicate (Optional tested feature, 11n devices only)
- AP and STA STBC (Optional tested feature, 11n devices only)
- AP and STA A-MPDU Aggregation when the DUT is a Transmitter (Optional tested feature, 11n devices only)
- AP and STA 20/40 MHz BSS Operation (Optional tested feature, 11n devices only)
- AP and STA 3 Spatial Stream (Optional tested feature, 11n devices only)

2 Test Tools, Methodology, and Approach

This section defines the tools, methodology, and approach for testing and certifying 802.11n devices.

2.1.1 Sniffers

Two sniffers are required to be used simultaneously on some tests (e.g. pre-Authentication).

1. A wireless sniffer capable of capturing and decoding 802.11a, b, g, i, and n frames and WMM required.
2. A wired sniffer capable of capturing and decoding EAPOL frames is required.

Note: Wildpackets Omnipeek version 6.0 supports the required decoding for both wired and wireless networks. A single laptop can be used, running two instances of Omnipeek.

Note: The wireless sniffer might need to support 802.11d and 802.11h frame capturing and decoding for the optional 802.11d and 802.11h testing.

2.1.2 IxChariot Software

IxChariot software from IXIA may be used. IxChariot includes a large set of standard, editable scripts, which can be used to define a particular traffic flow between two “endpoints”. The script definition, test configuration, test execution, and results reporting are managed through the IxChariot “console”, which in our case will be separate machine from the units under test.
Unless otherwise specified, default parameters are used. Throughput tests shall be run for 1.5 minutes. Ping tests may run between 10 and 90 seconds.

Note: Unlike IxChariot, Wi-Fi Test Suite uses UDP only.

2.1.3 Chariot Scripts

Test cases refer to the following Chariot scripts. Ignore these when using Wi-Fi Test Suite.

FILESNDL (“File Send Long”)
This emulates a large file transfer between endpoints.
The Ixia Chariot default values will be used for file size and receive and transmit buffer sizes. Depending on the test case, TCP or UDP traffic will be used.

FILESNDL-HT (“File Send Long HT”) (FILESNDL modified).
For 802.11n testing for UDP throughput traffic. This script has been modified for 640 Kbyte file size and 64KByte receive and transmit buffer sizes.

HIGH_PERFORMANCE_THROUGHPUT

INQUIRYL (“Inquiry Long”)
This emulates a series of client/server transactions.

REALAUD (Real Audio)
This emulates a group traffic Real Audio stream.

INQUIRYL-Replay (“Inquiry Long Replay test”)

This transmits enough packets to make sure the replay counters can correctly pass the 16-bit boundary.

Note: FILESNDL, INQUIRYL, AND REALAUD are run for a fixed duration of 1 minute 30 seconds set in the “Run Options” pull down menu. INQUIRYL-Replay is run setting the run “until all endpoints finish” in the “Run Options”. These scripts can be found in the Chariot library section.

2.1.4 Wi-Fi Test Suite Software

As an alternative to IxChariot, the Wi-Fi Test Suite may be used. This tool suite provides configuration, test control, traffic generation, and results analysis services. The test plan, in its entirety, can be executed in a fully automated manner through the WFA distributed Wi-Fi Test Suite Command Scripts and the Wi-Fi Test Suite Unified CAPI Console. Additional information is available through the test tools page on the member website.

2.2 Authentication Server

All Authentication servers are PC based. These servers perform the 802.1X port based authentication server function; they check the credential of the supplicant (STA) on behalf of the authenticating agent (AP). The authentication server then responds to the authenticating agent indicating whether or not the supplicant is authorized to access the authenticator’s services.

The shared secret between all the APs and the Authentication servers must use 64 characters (octets). The following 64-character string shall be used for the secret:

1234567890…12345678901234

The sequence is repeated until 64 characters are reached.

2.3 Basic System Test Configuration

The basic test configuration for infrastructure tests is depicted in the following figure and is a physical connection diagram (note there are two logical networks to separate chariot traffic from configuration traffic for STAs only).
:

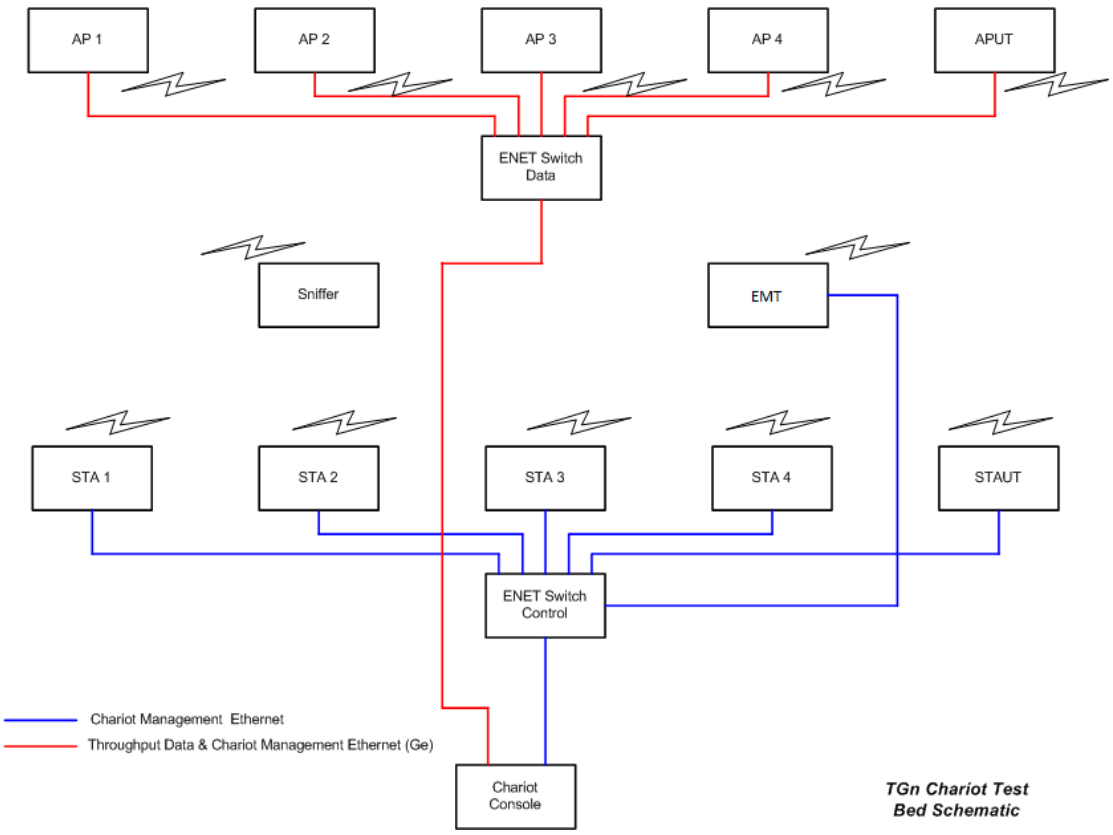


Figure 1: Basic System Test Configuration

The stations and the IxChariot Server operate as IxChariot endpoints, with the tests configured and controlled from the IxChariot Console.

When a STA is being tested, only one station is typically present, namely the station under test (STAUT). When an AP is being tested, only one AP is typically present, namely the AP under test (APUT). The specific test bed products used in these testing configurations are listed in Appendix B.

With tthe Wi-Fi Test Suite approach, full automation of the certification tests can be accomplished.

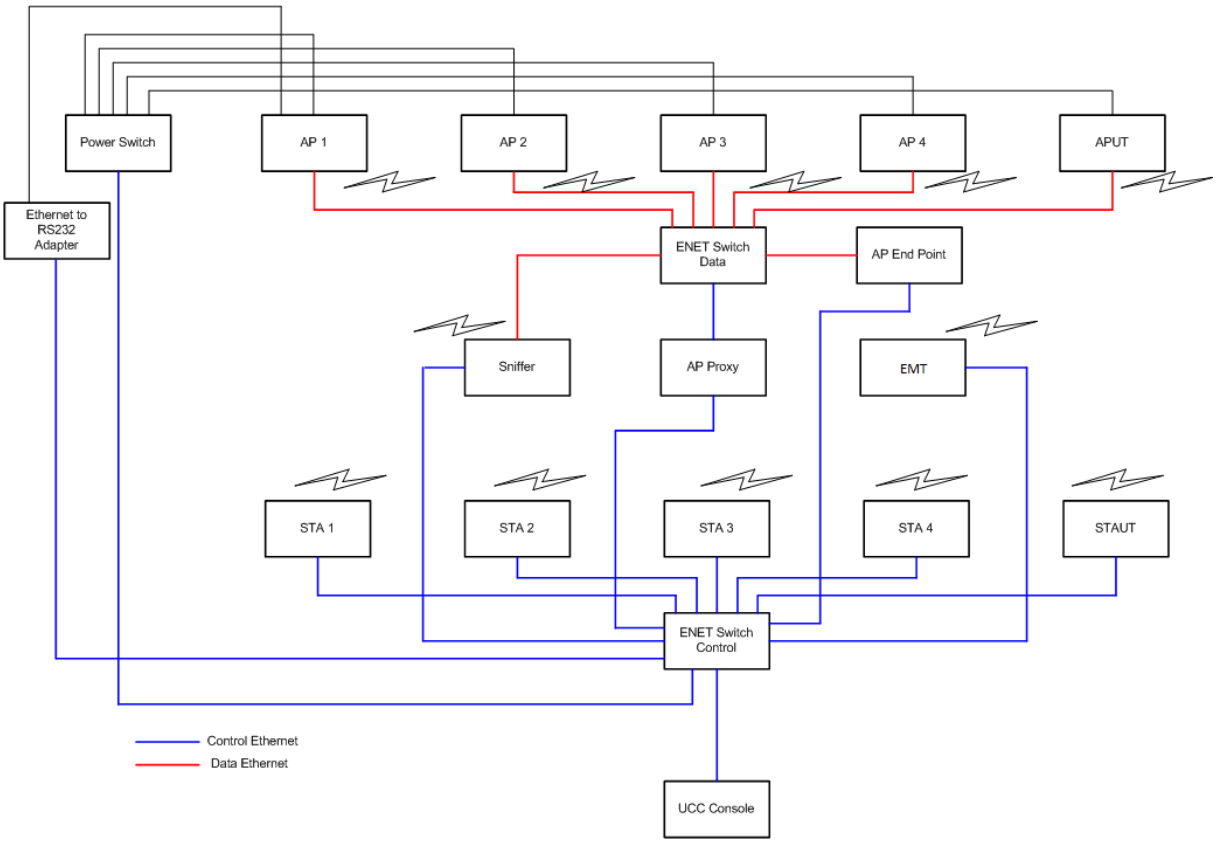


Figure 2:Wi-Fi Test Suite System Test Configuration

3 Implementation Requirements for WFA Certification

The following items describe the necessary features that are required for an implementation to pass Wi-Fi 802.11n interoperability testing. This is intended to provide guidance to vendors as they prepare their product for Wi-Fi certification testing.

Throughout this document ALL WPA2 configurations use CCMP (AES) for directed traffic. In mixed mode operation (WPA and WPA2 are allowed simultaneously) for APs, all WPA2 directed frames shall use CCMP, all WPA directed frames shall use TKIP, and all group traffic packets shall use TKIP.

3.1 Compliance Standard

1. The product shall comply with the Wi-Fi Alliance WPA protocol as defined by Wi-Fi document "Wi-Fi Protected Access (WPA) – Enhanced Security Implementation Based on IEEE 802.11
2. The product shall comply with the Wi-Fi Alliance WPA2 protocol as defined by Wi-Fi document "Wi-Fi 802.11 with WPA2, WPA, and WEP System Interoperability Test Plan for IEEE 802.11a, b, and g Devices, latest released version.
3. The product shall comply with TGn Marketing MRD – Version 1.994 (11n devices only)
4. The product shall comply with the Wi-Fi Alliance WMM protocol as defined by the Wi-Fi document "WMM (including) WMM Power Save) Specification" latest released version.

3.2 General Requirements

The following requirements are independent of any security method used and applicable to all APs and STA device classes.

3.2.1 General Handling for Reserved Bits

- Ignore on receive.
- Set to zero on transmit.

3.2.2 ESSID Element

- Support for ASCII printable characters as a minimum.
- ACSII character from code 32-126 can be used to represent an ESSID string
- ASCII character 32(space) shall not be used to begin and terminate an ESSID character strings
- ESSID character strings shall not be terminated by ASCII null

3.2.3 AP must respond to broadcast ESSID probe requests. Beacon Interval

- Stations must be able to support any beacon interval within the range 20 ms - 1000 ms.
- AP must support at least one beacon/DTIM interval of within the range 20 ms - 1000 ms.

3.2.4 TIM Element

- AP must be capable of generating correct TIM for clients that use power save protocol.
- Stations in PSP must interpret TIM correctly.

3.2.5 Data Payload

- Encrypted and unencrypted support is required.
- Data payload size is limited to Ethernet payload size.
- Payload formats are defined in 802.1H, which specifies the use of RFC1042.
- General rule: if a specific Ethertype in the table, then 802.1H bridge tunnel encapsulation format shall be used, otherwise RFC1042 applies.
- Ethertypes 80F3 and 8137 shall be in the table.

3.2.6 802.11 Power Save

- Client (Station) power save mode is not required.
- AP support of power save stations is required. An APUT must buffer the traffic for a time no less than the Listen Interval it accepted when sending a successful association response.
- APs must be capable of generating DTIMs at a DTIM interval between 1 and 5.
- APs must support the dynamic switching of a station between power save and Continuously Active/Awake mode (CAM) states as indicated by the power save bit in frames generated by the station.
- APs shall ignore the power save bit in any received group traffic Probe Request.
- APs shall ignore the power save bit in any received Authenticate and (Re) Associate packet, and should assume the station is awake for the response.

Power save may be implemented within a client (station) in one of two ways (or both ways) and testing is performed according to Out Of Box (OOB) default settings:

1. **PSnonPoll:** A client may dynamically move between Awake and Doze states. In this case, the associated Access Point shall be capable of monitoring the “Power Management” field transmitted by the client (defined in the 802.11 standard) and only transmits during Active Mode (AM) as defined in the 802.11 standard.

2. **PSPoll:** Station remains in a doze state and retrieves each packet from the Access point using PSPoll. In this case the Access Point must also accurately monitor for the PSPoll frames and respond accordingly to the procedure defined by the 802.11 standard.

3.2.7 RTS/CTS

- APs and STAs must correctly support reception of RTS (NAV update) and generation of CTS.
- APs and STAs must correctly support reception of CTS-to-self (NAV update).
- Protection Mechanism generation of both RTS and CTS-to-self is not required.
- The STAUT must generate Protection Mechanism of either RTS or CTS-to-self if the Use_Protection (b1) bit is set in AP.

3.2.8 Fragmentation

- Both APs and Clients (Stations) must support reception of fragmented packets.
- Fragmented transmission is not required for any device.

3.2.9 PCF (Point Coordination Function)

- PCF support is not required.

3.2.10 Packet Response Times

- Probe response must occur within 5 ms (assuming clear channel).
- Stations must wait for a minimum of 5 ms for a probe response.
- In case of open system authentication, the authenticate response must occur within 100 ms when AP is idle.
- The (re)associate response must occur with 100 ms when AP is idle.
- Stations must be capable of associating to APs that respond at the maximum times allowed.

3.2.11 Data Rates

802.11 a, b, g, n single and dual band devices are tested.

3.2.11.1 APs

3.2.11.1.1 802.11a

- Must be capable of operating at each data rate (6, 12, 24, and 54 Mbps).
- Must be capable of operating within a BSS with 6, 12, and 24 Mbps considered the basic rates, and 54 Mbps, which is a supported rate.

3.2.11.1.2 802.11g

- Must be capable of operating at each data rate (1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps)
- Basic Rate Set #1: Must be capable of operating within a BSS with all of 1, 2, 5.5 and 11 Mbps considered basic rates as defined in 802.11 and 6, 9, 12, 18, 24, 36, 48 and 54 Mbps as supported rates
- Basic Rate Set #2: Must be capable of operating within a BSS with all of 1, 2, 5.5, 11, 6, 12 and 24 Mbps considered basic rates as defined in 802.11 and 9, 18, 36, 48 and 54 Mbps as supported rates
- The Out Of Box Basic Rates setting shall be Rate Set #1

3.2.11.1.3 802.11b

- Must be capable of operating at each data rate (1, 2, 5.5, and 11 Mbps)
- Must be capable of operating within a BSS with all of 1, 2, 5.5 and 11 Mbps considered basic rates as defined in 802.11
- Must be capable of operating within a BSS with 1 and 2 Mbps considered the basic rates and 5.5 and 11 as supported rates

3.2.11.1.4 802.11n (11n devices only)

- Must be capable of operating within a BSS with Basic Rate #1.
- Must be capable of operating within a BSS with Basic Rate #2.
- The Out of the Box Basic Rates settings shall be Basic Rate Set #1.

3.2.11.2 Stations

3.2.11.2.1 802.11a

- Must be capable of operating at each data rate (6, 12, 24, and 54 Mbps).

- Must be capable of operating within a BSS with 6, 12, and 24 Mbps considered the basic rates, and 54 Mbps, which is a supported rate.

3.2.11.2.2 802.11g

- Must be capable of operating at each data rate (1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps)
- Basic Rate Set #1: Must be capable of operating within a BSS with all of 1, 2, 5.5 and 11 Mbps considered basic rates as defined in 802.11 and 6, 9, 12, 18, 24, 36, 48 and 54 Mbps as supported rates
- Basic Rate Set #2: Must be capable of operating within a BSS with all of 1, 2, 5.5, 11, 6, 12 and 24 Mbps considered basic rates as defined in 802.11 and 9, 18, 36, 48 and 54 Mbps as supported rates
- The Out Of Box Basic Rates setting shall be Rate Set #1

3.2.11.2.3 802.11b

- Must be capable of operating at each data rate (1, 2, 5.5, and 11 Mbps)
- Must be capable of operating within a BSS with all of 1, 2, 5.5 and 11 Mbps considered basic rates as defined in 802.11
- Must be capable of operating within a BSS with 1 and 2 Mbps considered the basic rates and 5.5 and 11 as supported rates

3.2.11.2.4 802.11n (11n devices only)

- Must be capable of operating within a BSS with Basic Rate #1.
- Must be capable of operating within a BSS with Basic Rate #2.
- The Out of the Box Basic Rates settings shall be Basic Rate Set #1.

3.2.11.3 Mobile APs (that do not support 1 and 2 Mbps)

Mobile APs that support 1 and 2 Mbps refer to section 3.2.11.1 and ignore section 3.2.11.3.

3.2.11.3.1 802.11a

- Must be capable of operating at each data rate (6, 12, 24, and 54 Mbps).
- Must be capable of operating within a BSS with 6, 12, and 24 Mbps considered the basic rates, and 54 Mbps, which is a supported rate.

3.2.11.3.2 802.11g

- Rate Set #3: Must be capable of operating within a BSS with all of 5.5 and 11 Mbps considered basic rates and 6, 9, 12, 18, 24, 36, 48 and 54 Mbps as supported rates
- The Out Of Box Basic Rates setting shall be Rate Set #3

3.2.11.3.3 802.11b

- Must be capable of operating at each data rate (1, 2, 5.5, and 11 Mbps)
- Must be capable of operating within a BSS with all of 1, 2, 5.5 and 11 Mbps considered basic rates as defined in 802.11
- Must be capable of operating within a BSS with 1 and 2 Mbps considered the basic rates and 5.5 and 11 as supported rates

3.2.11.3.4 802.11n (11n devices only)

- The Out Of Box Basic Rates setting shall be #3

For 802.11n APs and STAs, the data rates are defined based on the modulation coding scheme (MCS) index. The data rates are also a function of the following parameters that are used in the following tables.

- N_{SS}: Number of Spatial Streams
- R: Code Rate
- N_{BPSC}: Number of coded bit per single carrier
- N_{SD}: Number of data subcarriers
- N_{SP}: Number of pilot subcarriers
- N_{CBPS}: Number of coded bits per symbol
- N_{DBPS}: Number of data bits per symbol
- N_{ES}: Number of FEC encoders

There are specific data rate requirements for the different AP types and STA device types depending on device capabilities (1x1, 2x2, or 3x3):. These are presented below (note: SGI rates are optional and must be supported if implemented).

- Baseline 802.11n AP shall support data rates for receive and transmit as follows
  - 20 MHz APs in 2.4 GHz and 5 GHz
    - Data Rates defined in Table 2
    - Data Rates defined in Table 3
  - 20/40 MHz APs in 2,4 GHz and 5 GHz
    - Data Rates defined in Table 2
    - Data Rates defined in Table 3
    - Data Rates defined in Table 5
    - Data Rates defined in Table 6
- Optional 802.11n AP devices shall support data rates for transmit and receive as follows:
  - 20 MHz APs in 2.4 GHz and 5 GHz
    - Data Rates defined in Table 4
  - 20/40 MHz APs in 2.4 GHz and 5 GHz
    - Data Rates defined in Table 4
    - Data Rates defined in Table 7

- Baseline 802.11n STA device shall support data rates for receive as follows:
  - 20 MHz STAs in 2.4 GHz and 5 GHz
    - Data Rates defined in Table 2
  - 20/40 MHz STAs in 2.4 GHz and 5 GHz
    - Data Rates defined in Table 2
    - Data Rates defined in Table 5
- Optional 802.11n STA devices shall support data rates for transmit and receive as follows:
  - 20 MHz STAs in 2.4 GHz and 5 GHz
    - Data Rates defined in Table 3
    - Data Rates defined in Table 4
  - 20/40 MHz STAs in 2.4 GHz and 5 GHz
    - Data Rates defined in Table 3
    - Data Rates defined in Table 4
    - Data Rates defined in Table 6
    - Data Rates defined in Table 7

▪

MCS Index	Modulation	R	N_{BPSC}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data Rates (Mbps)	
								800ns GI	400ns GI
0	BPSK	1/2	1	52	4	52	26	6.5	7.2
1	QPSK	1/2	2	52	4	104	52	13.0	14.4
2	QPSK	3/4	2	52	4	104	78	19.5	21.7
3	16-QAM	1/2	4	52	4	208	104	26.0	28.9
4	16-QAM	3/4	4	52	4	208	156	39.0	43.3
5	64-QAM	2/3	6	52	4	312	208	52.0	57.8
6	64-QAM	3/4	6	52	4	312	234	58.5	65.0
7	64-QAM	5/6	6	52	4	312	260	65.0	72.2

Table 2: Mandatory 20 MHz, N_{SS} = 1, N_{ES}= 1

MCS Index	Modulation	R	N_{BPSC}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data Rates (Mbps)	
								800ns GI	400ns GI
8	BPSK	1/2	1	52	4	104	52	13.0	14.444
9	QPSK	1/2	2	52	4	208	104	26.0	28.889
10	QPSK	3/4	2	52	4	208	156	39.0	43.333
11	16-QAM	1/2	4	52	4	416	208	52.0	57.778
12	16-QAM	3/4	4	52	4	416	312	78.0	86.667
13	64-QAM	2/3	6	52	4	624	416	104.0	115.556
14	64-QAM	3/4	6	52	4	624	468	117.0	130.0
15	64-QAM	5/6	6	52	4	624	520	130.0	144.444

Table 3: Mandatory 20 MHz, N_{SS} = 2, N_{ES}= 1

MCS Index	Modulation	R	N_{BPSC}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data Rates (Mbps)	
								800ns GI	400ns GI
16	BPSK	1/2	1	52	4	156	78	19.5	21.7
17	QPSK	1/2	2	52	4	312	156	39.0	43.4
18	QPSK	3/4	2	52	4	312	234	58.5	65.0
19	16-QAM	1/2	4	52	4	624	312	78.0	86.7
20	16-QAM	3/4	4	52	4	624	468	117.0	130.0
21	64-QAM	2/3	6	52	4	936	624	156.0	173.3
22	64-QAM	3/4	6	52	4	936	624	175.0	195.0
23	64-QAM	5/6	6	52	4	936	780	195.0	216.7

Table 4: Optional 20 MHz, NSS = 3, NES= 1

MCS Index	Modulation	R	N_{BPSC}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data Rates (Mbps)	
								800ns GI	400ns GI
0	BPSK	1/2	1	108	6	108	54	13.5	15.0
1	QPSK	1/2	2	108	6	216	108	27.0	30.0
2	QPSK	3/4	2	108	6	216	162	40.5	45.0
3	16-QAM	1/2	4	108	6	432	216	54.0	60.0
4	16-QAM	3/4	4	108	6	432	324	81.0	90.0
5	64-QAM	2/3	6	108	6	648	432	108.0	120.0
6	64-QAM	3/4	6	108	6	648	486	121.5	135.0
7	64-QAM	5/6	6	108	6	648	540	135.0	150.0

Table 5: Optional 40 MHz, N_{SS} = 1, N_{ES}= 1

MCS Index	Modulation	R	N_{BPSC}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data Rates (Mbps)	
								800ns GI	400ns GI
8	BPSK	1/2	1	108	6	216	108	27.0	30.0
9	QPSK	1/2	2	108	6	432	216	54.0	60.0
10	QPSK	3/4	2	108	6	432	324	81.0	90.0
11	16-QAM	1/2	4	108	6	864	432	108.0	120.0
12	16-QAM	3/4	4	108	6	864	648	162.0	180.0
13	64-QAM	2/3	6	108	6	1296	864	216.0	240.0
14	64-QAM	3/4	6	108	6	1296	972	243.0	270.0
15	64-QAM	5/6	6	108	6	1296	1080	270.0	300.0

Table 6: Optional 40 MHz, N_{SS} = 2, N_{ES}= 1

MCS Index	Modulation	R	N_{BPSC}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data Rates (Mbps)	
								800ns GI	400ns GI
16	BPSK	1/2	1	108	6	324	162	40.5	45.0
17	QPSK	1/2	2	108	6	648	324	81.0	90.0
18	QPSK	3/4	2	108	6	648	486	121.5	135.0
19	16-QAM	1/2	4	108	6	1296	648	162.0	180.0
20	16-QAM	3/4	4	108	6	1296	972	243.0	270.0
21	64-QAM	2/3	6	108	6	1944	1296	324.0	360.0
22	64-QAM	3/4	6	108	6	1944	1458	364.5	405.0
23	64-QAM	5/6	6	108	6	1944	1620	405.0	450.0

Table 7: Optional 40 MHz, NSS = 3, NES= 1

3.2.12 Handling Unexpected Frames

- Ability to ignore unknown information elements.
- APs and stations must be capable of operating properly upon receipt of unknown information elements (i.e. they must ignore them).
- Any AP or station that generates an information element not specified by 802.11 must include the vendor's OUI as the first three bytes of the information field within the element.

3.2.13 Ability to Handle Null Frames

- APs and stations must be capable of operating properly upon receipt of null frames.
- Control bits within null frames are to be acted upon (e.g. power save bits).
- Null frames received from a non-authenticated or non-associated station shall elicit a De-authenticate/Disassociate response from the AP.

3.2.14 Ability to Handle Proprietary Messages

- Stations and APs must be able to operate properly upon receipt of any proprietary message that is formatted in accordance with SNAP with the manufacturer OUI.

3.2.15 Ability to handle unsolicited PS-Poll

- If poller is not associated, response is ACK followed by De-authenticate or Disassociate.
- If poller is associated, allowable responses include: 1) ACK 2) data 3) null data or empty data, or 3) ACK followed by data or null data or empty data.

3.2.16 AP Notification of Bridges Upon Station Roaming

- When a station roams from an old AP to a new AP, the new AP is responsible for ensuring that any bridges between the two APs are properly notified of the station's new location.
- The manner in which this is accomplished is not specified. The only requirement is that some method is implemented which ensures that packets will flow properly to the station's new AP.

3.2.17 Ad Hoc Support – Independent Basic Service Set (IBSS) Requirements

- IBSS support is optional but must be tested if the station supports it.
- Station must:
  - Be able to create an IBSS network with a specified SSID
  - Be able to handle ESSIDs can be up to 32 characters
  - Not null terminate ESSID
  - Be able to select the channel to be used
  - Be able to create an unencrypted IBSS; an encrypted IBSS (with 40 bit WEP key) is optional but will be tested if implemented. WPA and WPA2 are not required to be supported and will not be tested if implemented.
  - Select BSSID randomly
  - Allow stations doing active scanning and passive scanning to join
  - Be able to join an IBSS network with specified SSID
  - Be able to join an IBSS that has been started on an arbitrary channel
  - Be able to join an unencrypted IBSS; if WEP is implemented then the station must be able to join an IBSS with encrypted IBSS (40 bit WEP key).
  - Not adopt WEP keys; again tested only if WEP is implemented.
- Stations may either active or passive scan for the network
- Authentication is not required in an IBSS
- Communication test between multiple IBSS stations:
  - Support of clear text operation is required.
  - Support of a totally encrypted cell using a single 40-bit WEP key is optional but tested if WEP is implemented.
  - 802.11a stations must be capable of operating at the maximum data rates: 54 Mbps,
  - 802.11g and 802.11b stations must be capable of 11 Mbps
  - 802.11n stations are required to support 802.11a and 802.11g rates.
  - Station must receive data packets sent using RTS/CTS
  - Station must receive fragmented data packets
  - Threshold requirements are based on 802.11b values.
- Group traffic must be supported
  - Station must support transmission of group traffic
  - Station must support reception of group traffic
- The station must change to a new BSSID if it encounters an existing cell with the same SSID and a greater TSF on the same channel
- IBSS distributed beaconing
  - Station must continue beaconing when the station that created the IBSS is turned off.
  - Station must implement distributed beaconing algorithm
- IBSS Power management support is not required
- The station, while a member of on IBSS, shall not receive packets from another IBSS (with different SSID) on the same channel

3.2.18 Preamble

- Stations and APs by default must allow communication using long preamble. Stations and APs must support short preamble. Protection Mechanisms use short or long preamble based on the Barker_Preamble_Mode indication in the ERP IE. (§7.3.2.13)

3.2.19 Overlapping Legacy BSS Condition (OLBC) (2.4 GHz band only)

- APs must be capable of detecting an overlapping legacy BSS condition (OLBC).
- An OLBC exists when an AP receives a Beacon from a neighboring BSS in which no ERP rates are supported. Or an AP receives a Beacon, which contains an ERP IE in which the NonERP_Present (b0) bit is set.
- An AP is the state of OLBC shall set the Use_Protection (b1) bit and shall not set NonERP_Present (b0) bit unless a clause 15 or a clause 18 STA is associated.

3.2.20 Short Slot Time (2.4 GHz band only)

- Stations and APs must support the short slot time option. In a BSS containing only ERP devices, short slot time is required. Short slot time is allowed in ERP only BSSs with an Overlapping Legacy BSS Condition (as currently defined in Section 3.2.19).
- Short slot is not allowed in IBSS mode.

3.2.21 Network Allocation Vector (NAV)

- APs and Stations must honor the duration field in valid received frames not addressed to the STA (i.e. it must update its NAV and defer transmission while the NAV is non-zero).
- **Honoring NAV Background:** An AP must honor the duration field of valid received frames not addressed to the AP by updating its NAV and deferring contending for them medium while the NAV is non-zero (must treat the medium as busy during this time).
    - A test device with special test code is required for this test.
    - Upon successfully competing for medium, the test device will generate a CTS-to-self with a large duration field.
    - Upon transmitting the CTS-to-self, the test device waits the large duration before competing for the medium again.

3.3 WPA & WPA2 General Requirements

The following sections describe requirements that are common to both WPA and WPA2.

3.3.1 General Test Requirements

WPA2 and WPA interoperability testing will be confined to the BSS mode only. A device (Access Point or Station) must be either WPA2-Enterprise/WPA-Enterprise (WPA 802.1X/EAP plus PSK) or WPA2-Personal/WPA-Personal (PSK-only). When using Client Certificates for EAP method TLS, the certificates are defined in RFC 3280.

A fully interoperable WPA2 system consists of the Access Point (AP), the station (STA), and an 802.1X compliant supplicant. If the 802.1X port based authentication server mode (WPA2-Enterprise) is used, then this also becomes a component of the interoperable system. All components must interoperate together in

order to provide WPA2 service. To ensure the correct operation of TKIP & CCMP, fragmentation will also be verified with WPA2 turned on.

This figure illustrates the WPA2 interfaces that must interoperate properly in order to provide WPA2 service.

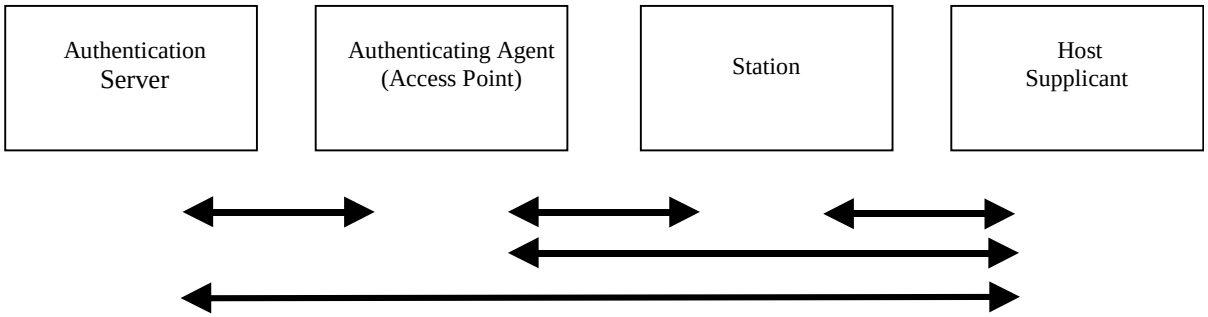


Figure 3: WPA2 Interoperability Interfaces

The test bed specifies a combination of each of these components. All components have been fully tested for interoperability with each other. Conceptually, this test plan may be used to test any of these components by replacing a component of the test bed with the component under test and executing the tests specified herein. However, the focus of this test plan is on testing stations and Access Points.

3.3.2 Key Provisioning

A product must be one of these two classes:

a) WPA2-Enterprise/WPA-Enterprise: the device supports obtaining keys from both a Pre-Shared key (PSK) pass phrase utility and via an 802.1X authentication server.

b) WPA2-Personal/WPA-Personal: a pre-shared key only product (PSK-Only). The device only supports obtaining keys from a Pre-Shared key (PSK) pass phrase utility. The device does not support obtaining keys via an 802.1X authentication server.

Recommendations for Wi-Fi® Protected Access Certification for Consumer Electronics Devices, shall apply. That is, PC-Centric devices as defined by that policy, which seek WPA2 Certification, shall be required to seek WPA2-Enteprise certification. Non-PC-Centric devices, as defined by that policy, that seek WPA2 Certification, shall be required to seek only WPA2-Personal certification, but may seek WPA2-Enterprise certification at the vendor's option. For clarity, Access Points are regarded as being Non-PC-Centric and may certification as either WPA2-Personal or WPA-Enterprise.

Station devices that provide wireless networking capabilities directly to a PC must be WPA2-Enterprise. Example devices include:

- Laptop PC's with Wi-Fi embedded
- PC Cards (PCMCIA)
- CardBus cards
- Compact Flash adapters
- Mini PCI cards

- USB-dongles

3.3.3 Key Management

This test plan requires support for at least one Extensible Authentication Protocol (EAP) for STAUTs and support eight EAP methods for APUTs. The following table gives the EAP methods full names and short names. The short names will be used throughout this test plan.

EAP Method Full Name	EAP Method Short Name	References
EAP-TLS	TLS	RFC 2716 (http://www.ietf.org/rfc/rfc2716.txt)
EAP-TTLS/MSCHAPv2	TTLS	RFC 5281(http://www.ietf.org/rfc/rfc5281.txt)
PEAPv0/EAP-MSCHAPv2	PEAP0	Internet Draft: Microsoft's PEAP version 0 (Implementation in Windows XP SP1) ‹ Draft 0, Kamath, et. al., October 2002.
PEAPv1/EAP-GTC	PEAP1	Internet Draft: Protected EAP Protocol (PEAP) Draft 5, Andersson, et. al., September 2002. **
EAP-SIM	SIM	RFC 4186 (http://www.ietf.org/rfc/rfc4186.txt)
EAP-AKA	AKA	RFC 4187 (http://www.ietf.org/rfc/rfc4187.txt)
EAP-AKA'	AKA'	RFC 5448 (http://www.ietf.org/rfc/rfc5448.txt)
EAP-FAST	FAST	RFC 4851 (http://www.ietf.org/rfc/rfc4851.txt), RFC 5421 (http://www.ietf.org/rfc/rfc5421.txt), RFC 5422 (http://www.ietf.org/rfc/rfc5422.txt). ***

Table 8: EAP Methods

**EAP-PEAPv1 implementations have a number of small variations due to more than one Internet draft version having been used to describe this EAP method. Wi-Fi interoperability testing requires a variation that is one of the most commonly used in current implementations. This is based on draft-josefsson-pppext-eap-tls-eap-05.txt with "client PEAP encryption" replaced with the old label for PRF, i.e., "client EAP encryption" in section 2.8 (Key derivation).

***EAP-FAST is tested only with authenticated in-band provisioning. Both EAP-FAST-GTC and EAP-FAST-MSCHAPv2 are used inside the tunnel in Phase 2.

The use of these EAP methods does not preclude the implementation of other Authentication Protocols.

3.3.3.1 ASCII Pass Phrase

To enable WPA2 capable products to be used in a BSS which does not utilize an authentication server, a key management utility based upon the reference algorithm, as defined in the 802.11i standard document, is to be supported by both Stations and Access Point WPA2 capable products. This key management utility is to be used for the generation a 256-bit Master WPA2 key from an ASCII based pass phrase.

Access Points are required to incorporate this ASCII pass phrase utility and are explicitly tested. Supplicants likewise incorporate this utility.

WPA2 utilizes the IEEE 802.1X standard for port based network access control. The 802.1X standard is used as a basis for access control, authentication and key management.

The *WPA for 802.11 Specification – Version 3.1, August 2004* specifies a method of using 802.1X authentication in co-operation with WEP only. The testing of 802.1X with WEP is excluded from this test plan. However, where the WPA IE defines the capability to be WPA, the authentication mechanism used between an AP and a STA will be based upon the 802.1X authentication.

This test plan requires support for at least one Extensible Authentication Protocols (EAP). The use of these EAP methods does not preclude the implementation of other Authentication Protocols.

ASCII pass phrase requirements

- Support for ASCII printable characters as a minimum.
- ACSII character from code 32-126 can be used to represent a string
- ASCII character 32(space) shall not be used to begin and terminate a character string
- Character strings shall not be terminated by ASCII null

3.3.3.2 Group Key only Support in Access Points

The WPA specification allows for case where an Access Point may optionally support group keys only, and as a consequence uses group keys to encrypt and decrypt directed traffic. This level of functionality is weaker than an Access Point that can support both group and Pairwise keys, and not currently supported. This test plan does not test group key only operation and Access Points are required to support pair-wise key.

3.3.3.3 Authentication Support

802.1X port based authentication servers (AS) are typically supported by Authentication servers (Remote Access Dial-In User Service). These servers may run on separate PCs (desktop or laptop PCs), mainframes, etc. or may run on an AP itself.

This test plan requires that the APUT and STAUT interoperate with the four different 802.1X port based servers in the testbed. The four servers used here are Radiator, Microsoft IAS, Hostapd, and Devicescape. These servers are identified in

Appendix A: Test Bed Products of this document.

3.3.4 Supplicant

The supplicant is the user end (or STA) peer entity that requests 802.1X authentication from the 802.1X authentication server or from the authenticator within an AP when Pre-Shared Keys (PSK) are used.

This test plan specifies third party supplicants to be used by the reference Stations. Please see the Appendix for the current list of supplicants.

STAUTs must be supplied with a vendor supplicant and documentation for the technician to enable installation (if required), enabling/disabling, configuration, and any relevant logging or status information. For these category of devices, a SIM card must be supplied for the SIM test and a uSIM card for the AKA and AKA' tests by the STAUT owner. In the AKA and AKA' test cases, the supplicant must support the Milenage algorithm. For devices which cannot install supplicants, a uSIM card supporting the Milenage algorithm must be used (e.g. Gemalto GemXplore 3G test card, part number SCAM000628, used as purchased, no modification needed).

A detailed description of the applicable device classes for STAUTs may be found in the Supplicant Testing Policy.

3.4 WPA

3.4.1 WPA Cipher Suite Support

Both Access Points and Stations must be capable of interoperating with non-WPA capable Access Points and Stations. The following configurations or modes are to be verified by this test plan.

a) Where the WPA IE defines the BSS capability to be WEP only, all directed and group traffic packets use legacy based WEP functionality, interoperating only at a 40-bit capability.
b) Any other encryption schemes supported by the product (e.g., CCMP or RSN) under test will not be tested since they are NOT part of WPA.
c) Neither will this test plan confirm any additional encryption schemes are active or inactive.

3.4.2 WPA Countermeasures

Both the Access Point and the Station must be capable of supporting countermeasures as defined by the WPA requirements document.

The test plan requires that countermeasures to detect and handle MIC failures be implemented in both the Supplicant (STA) and the Authenticator (within the AP).

3.4.2.1 Within a Supplicant

A MIC failure event can be due to a directed traffic or group traffic Michael MIC failure:

1. Increments the MIC failures counter.
2. Send a Michael MIC failure report frame to the AP.
3. If this is the first MIC failure, initialize the countermeasures timer. If the failure was in a directed traffic or group traffic, discard the offending frame.
4. If less than 60 seconds have passed since a previous Michael MIC failure, delete the PTK (and GTK). Disassociate from the AP and wait for 60 seconds before (re) associating.

3.4.2.2 Within an Authenticator

The countermeasures used by an Authenticator that detects a MIC failure event are described below:

1. Increments the MIC failure counter
2. If this is the first MIC failure, initialize the countermeasures timer. If the failure was in a directed frame, discard the offending frame.
3. If less than 60 seconds have passed since a previous Michael MIC failure, transition every STA in the BSS to State 2 in the 802.11 state diagrams. The Authenticator shall disallow associations for the duration of 60 seconds. At the end of the 60 seconds, the MIC failure counter and timer may be reset and new associations resume.

If the Authenticator is using EAP, transition the state of the Authenticator state machine to State INITIALIZE. This will restart the EAP state machine. If the Authenticator is using PSKs, this step is omitted.

3.4.3 WPA User Interface

3.4.3.1 WPA 'ON' mode

When WPA is enabled, this test plan shall ensure:

a) WPA in not allowed to be used alone; it shall only be used in mixed security mode with WPA2.
b) Interoperation with other products which have WPA enabled
c) Ensure that the two modes of operation WPA-Enterprise and WPA-Personal are not active at the SAME time

3.4.3.2 Station & AP Configuration Tests

The STA or AP device under-test will be examined to verify that certain parameters can be configured. These parameters include the following:

a) When WPA is ON, select authentication mode: Enterprise or Personal.
b) When PSK mode is selected, a pass phrase, as defined above, can be entered.

Optionally, a device may support an interface to enable a WPA key to be entered manually using its HEX derivative.

3.4.4 WPA Information Elements (WPA IE)

The Access Point must be capable of broadcasting its capability in the WPA Information Element (IE) contained within the Access Points beacon or probe response frame. Where a Station does not detect the WPA IE, the Station will follow the association process as defined with the IEEE 802.11 standard. Both the Access Point and Station must be capable of being configured for either WPA or Non-WPA (where Non-WPA implies either WEP based security or, no security) operation. Furthermore, in WPA mode, the Access Point and Station must be capable of being configured to use a WPA key provided by either a Pre-Shared key (PSK) pass phrase utility or obtain keys via an 802.1X authentication server. An Access Point/Station combination must be configured in the same manner. Thus mismatched combinations must explicitly not be supported. WPA STA must properly process a received WPA IE in any combination orders with RSN IE, WMM IE or any other IE's from an AP.

3.5 WPA2

3.5.1 General Requirements

These sections describe the necessary features that will be required for an implementation to pass WPA2 interoperability testing. Note: They are in *addition* to the WPA requirements defined previously.

The IEEE 802.11 standard defines two classes of secure networks, Pre-RSNA and RSNA:

- Pre-RSNA security is comprised of the following algorithms:
  1. WEP
  2. IEEE 802.11 entity authentication
- RSNA security is comprised of the following algorithms:
  1. TKIP
  2. CCMP

WPA2 introduces an AES based encryption protocol, CCMP, modifications to the 4-Way Handshake, and Pre-Authentication for WPA2-Enterprise capable equipment.

WPA2 interoperability testing will be confined to the BSS mode only. A device (Access Point or Station) must either be WPA2-Enterprise (WPA2 802.1X/EAP plus PSK) or WPA2-Personal (PSK-only).

TLS Client Certificates (which are used by all the EAP methods except for SIM) are defined in RFC 3280.

3.5.2 CCMP Overview

CCMP employs the AES encryption algorithm using the CCM mode of operation. The CCM mode combines ***CounterMode*** (CTR) for confidentiality and ***Cipher Block Chaining Message Authentication Code*** (CBC-MAC) for authentication and integrity. CCM protects the integrity of both the MPDU data field and selected portions of the IEEE 802.11 MAC header.

The Advanced Encryption Algorithm (AES) algorithm is defined in FIPS PUB 197. All AES processing used within CCMP uses AES with a 128-bit key and a 128-bit block size.

The CCM encryption is defined in RFC 3610. CCM is a generic mode that can be used with any block oriented encryption algorithm. CCM has two parameters (M and L), and CCMP uses the following values for the CCM parameters:

- M = 8; indicating that the MIC is 8 octets.
- L = 2; indicating that the length field is 2 octets, which is sufficient to hold the length of the largest possible IEEE 802.11 frame in octets.

CCM requires a fresh temporal key (TK) for every session. CCM also requires a unique nonce value for each frame protected by a given TK, and CCMP uses a 48-bit packet number (PN) for this purpose. Reuse of a packet number (PN) with the same TK voids all security guarantees.

To ensure the correct operation of CCMP, fragmentation will also be verified with WPA2 turned on.

3.5.3 RSNA Selection

A WPA2 Access Point must be capable of broadcasting its capability in the RSN Information Element (IE) contained within the Access Points beacon or probe response frame.

The included RSN IE shall specify all the authentication and cipher suites enabled by the STA's policy. A STA shall not advertise any authentication or cipher suite that is not enabled.

Both the Access Point and Station must be capable of being configured for WPA2, WPA or legacy operation. An AP must support a configuration option allowing both WPA and WPA2 stations yet specifically exclude STA's supporting only legacy security.

The AP shall advertise all the pairwise cipher suits it is configured to support. STA shall select the most secure cipher suit that it is configured to support from the list advertised by the AP. The AP/STA shall ignore cipher suit selectors, which contain an OUI value that is not recognized.

Furthermore, in WPA2 mode, the Access Point and Station must be capable of being configured to use a WPA2 pairwise key provided by either a Pre-Shared key (PSK) pass phrase utility or obtain keys via an 802.1X authentication server.

3.5.4 WPA2 Selection Policy within an RSN

In an RSN, WPA2 security is selected during the normal IEEE 802.11 association procedure between the STA and AP.WPA2 policy selection is performed by the associating STA. The STA does this by including an RSN IE in its (Re)Association Requests.
In an RSN an AP shall not associate with pre-RSNA STA's, i.e., with STA's that fail to include a valid RSN IE in the Association or Re-association Request frame.

A WPA2-configured STA initiating an association shall insert an RSN IE into its (Re) association Request whenever the targeted AP indicates RSNA support. The initiating STA's RSN IE shall include one authentication and pairwise cipher suite from among those advertised by the targeted AP in its Beacons and Probe Responses. An AP may advertise an RSN IE, which takes on default values for fields that are not explicitly given. However, a STA associating to such an AP must fully specify all fields of the RSN IE when forming its (Re-) association Request frame.

A WPA2-configured STA shall also specify the group key cipher suite specified by the targeted AP. If at least one RSN IE field from the AP's RSN IE fails to overlap with any value the STA supports, the STA shall decline to associate with that AP. It is invalid in an RSN to specify "Use Group Key" as the pair wise cipher.

3.5.5 WPA2 Selection Policy with legacy security networks

In a legacy security network,
RSN STAs shall include the RSN IE in its (Re) association requests.

An RSNA-capable AP configured to operate in a Transient Security Network (TSN) shall include the RSN IE, and may associate with both RSNA and pre-RSNA STA's. This means that an RSNA-capable AP shall respond to an associating STA that includes the RSN IE just as in an RSN.

If an AP operating within a TSN receives a (Re) association request without an RSN IE, it shall allow communications only if a WEP or WPA key has been configured or if the key will be provisioned by IEEE802.1X to secure communication. If a WEP or WPA key is not installed, and if IEEE 802.1X authentication and key management is not enabled, the AP shall reject the association request; if a WEP or WPA key is configured or if the AP is configured to provide IEEE 802.1X authenticated key management, the AP may accept the request.

An AP cannot support multiple group key cipher suites concurrently. In particular, a TSN must use the weakest directed traffic cipher suite as the group key cipher suite

In order to accommodate local security policy, a STA may choose not to associate with an AP that does not support any pair wise key cipher suites.

3.5.6 Pre-Authentication and Key management

Pre-Authentication support is optional. Where a device supports the Pre-Authentication mechanism, this capability shall be validated by this test plan.

In the case of WPA2-Enterprise product, Pre-authentication shall not be used unless the 'new' Access Points have advertised their pre-authentication capability in the RSN IE.

The OUI and Pre-authentication Ethertypes assigned by the IEEE 802.11i document are: OUI = 00-0F-AC, Pre-authentication Ethertype= 88-C7.

The descriptor type in the EAPOL-key Protocol version field value shall be = 2, as specified in IEEE 802.1X. These values shall be used by this test plan.

3.5.7 Cached PMKs and Key Management

A WPA2 STA can retain, in its cache the PMKs it established as a result of a successful IEEE 802.1X authentication. This PMK can be used with the 4-Way Handshake to establish new PTKs.

The 802.11i standard does not define a maximum number for cached PMKs. This test plan will validate that at least one cached PMK is supported.

3.5.8 Cipher Suite Support

a) APUTs must have the ability to configure WPA2-only mode. WPA2 only mode must use AES encryption for both directed and group traffic.
b) Access Points may be configured for WPA2 only and accept only WPA2 clients.
c) Clients are not required to be able to be configured for WPA2 only; clients are allowed to have a WPA2 only mode, optionally.
d) Clients may support a mode where they can associate with an AP which uses WPA2 only or WPA only. This is named the compatibility mode. When associating to an AP which uses mixed mode, the client must use WPA2.
e) Similar to WPA/WEP mixed mode, WPA2/WEP mixed mode is not allowed due to security concerns associated with WEP. There shall be a negative test to ensure this mode is not supported in a product's default Wi-Fi configuration.

3.5.9 WPA2 User Interface

3.5.9.1 Default configuration

The default out-of-box (OOB) configuration shall be set to security and encryption off or WPA2 (personal or enterprise) for APs. For stations, out-of-box (OOB) configuration shall be set to security and encryption off or WPA2 (personal or enterprise), or WPA2/WPA mixed security mode (personal or enterprise).

3.5.9.2 WPA2 only mode

When WPA2 only mode is enabled, this test plan shall ensure:

a) Interoperation with other products which have WPA2 only enabled

b) Ensure that WEP is NOT supported when WPA2 only is enabled in either the directed traffic or group traffic cipher suit.
c) Ensure that WPA is NOT supported when WPA2 only is enabled in either the directed traffic or group traffic cipher suit.

3.5.9.3 WPA2 Mixed mode APs only

Applicable only to Access Point products and when WPA2 mixed mode is enabled, this test plan shall ensure that the Access Point is capable of being configured to simultaneously support both WPA and WPA2 clients only. Consequently, for WPA2/WPA mixed mode this test plan requires that for interoperability:

- WPA2 STAs use WPA2 (AES) for directed traffic and WPA (TKIP) for group traffic.
- WPA STAs use WPA (TKIP) for directed traffic and WPA (TKIP) for group traffic.

3.5.9.4 WPA compatibility mode Clients only

IF a client supports WPA, the client is not allowed to use WPA alone. WPA must only be used in conjuction with WPA2. In this mode, the client can associate in either WPA2 or WPA security modes. If both modes are present, then the client must use WPA2 preferentially over WPA.

3.5.9.5 Station & AP Configuration Tests

The STA or AP device under-test will be examined to verify that certain parameters can be configured. These parameters include the following:

a) Turn WPA2 security On or Off for APUTs,
b) Turn WPA2/WPA mixed security On or Off for APUTs,
c) Turn compatibility mode on or off for STAUTs,
d) If supported, WEP security On or Off for both APUTs and STAUTs
e) When WPA2 or WPA2/WPA (mixed security mode and compatibility mode) are ON, select authentication mode: Enterprise (802.1X) or Personal (PSK) for those devices that are enterprise devices,
f) When PSK mode is selected, a pass phrase, as defined by the IEEE 802.11istandard, can be entered. Optionally, a device may support an interface to enable a WPA2 or WPA2/WPA key to be entered manually using its HEX derivative.

3.6 IEEE 802.11d Testing

IEEE 802.11d tests apply only to APUT and are optional. There are no IEEE 802.11d tests for STA. If testing is required then this capability is declared at time of application. This test is not mandatory tested if implemented.

3.6.1 Country Information Element (CIE)

The *Country Information element* contains the information corresponding to the regulatory domain in which the AP operates. This information is required to allow a STA to identify the regulatory domain in which it is located and to configure its PHY for operation according to regulations applicable to that regulatory domain.

An AP shall include the *Country Information element* in Beacons and Probe Response frames, and an AP shall be tested to verify that it generates Beacon and Probe Response frames, including all the fields in the *Country Information element.*

A list of the countries supported by ISO can be found at the following link:

http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html#sz.

The latest version of the h+d Tech Ops manual, entitled *Wi-Fi h+d Testing Manual,* has a list of the countries, but may not be up to date with the ISO website.

This test requires sniffer functionality for verification. These tests apply to the APUT only. There are no 802.11d tests for stations. This test is optional.

3.7 IEEE 802.11h Testing

IEEE 802.11h tests apply to both APUT and STAUT, but are optional. If testing is required then this capability is declared at time of application. This test is not mandatory tested if implemented.

3.7.1 Power Constraint Information Element

This test applies to APUT only. The Power Constraint element contains the information necessary to allow a STA to determine the local maximum transmit power in the current channel.

An APUT shall include the *Power Constraint element* in Beacons and Probe Response frames, and an APUT shall be tested to verify that it generates Beacon and Probe Response frames that include a valid value in the Local Power Constraint field in the Power Constraint element.

3.7.2 Channel Switch Announcement Element

This test applies to both the APUT and STAUT. The ***Channel Switch Announcement element*** is used by an APUT to advertise when it is changing to a new channel. This IE is sent when the APUT detects radar signals on the current operating channel, and operation of a BSS on this channel may interfere with the operation of the radar.

An AP shall support the generation of *Channel Switch Announcement element* within the Beacon frame. The ***Channel Switch Announcement element*** shall include within itself a New Channel number field indicating a channel that it may switch to, although this channel may not be the one the AP eventually uses. An AP shall be tested to verify that it supports the generation of a ***Channel Switch Announcement element***.

APs are required to provide a command to force a channel switch. The operation of this command is vendor-specific, and a method to simulate RF events that may initiate an involuntary channel switch and broadcast of this element shall be provided. This method may be in the AP's
GUI, command line interface, or other comparable means, and must be documented for the purposes of interoperability testing.

Stations that utilize 802.11h are required to observe Channel Switch Announcements issued by an AP. When an appropriate channel switch announcement is received, the STAUT must stop all frame transmissions on that BSS in order to not interfere with radar.

3.8 Allowed Security Combinations

3.8.1 APUT Security Combinations

APUTs must support one and only one of the following security combinations.

1. WPA2 only (no WPA, no WEP, no open)
2. WPA2 only and open (no WPA, no WEP)
3. WPA2 only, WEP, and open (no WPA)
4. WPA2 only, mixed mode WPA2/WPA (no WPA alone, no WEP, no open)

5. WPA2 only, mixed mode WPA2/WPA, WEP (no WPA alone, no open)
6. WPA2 only, mixed mode WPA2/WPA, open (no WPA alone, no WEP)
7. WPA2 only, mixed mode WPA2/WPA, WEP and open (no WPA alone)

3.8.2 STAUT Security Combinations.

STAUTs must support one and only one of the following security combinations.

1. WPA2 only (no WPA, no WEP, no open)
2. WPA2 only and open (no WPA, no WEP)
3. WPA2 only, WEP, and open (no WPA)
4. WPA2 only, mixed mode WPA2/WPA (no WPA alone, no WEP, no open)
5. WPA2 only, mixed mode WPA2/WPA, WEP (no WPA alone, no open)
6. WPA2 only, mixed mode WPA2/WPA, open (no WPA alone, no WEP)
7. WPA2 only, mixed mode WPA2/WPA, WEP and open (no WPA alone)
8. mixed mode WPA2/WPA (no WPA alone, no WEP, no open)
9. mixed mode WPA2/WPA, WEP (no WPA alone, no open)
10. mixed mode WPA2/WPA, WEP and open (no WPA alone)
11. mixed mode WPA2/WPA, open (no WPA alone, no WEP)

3.9 MAPUTs

1. If a MAPUT does not support STA mode, it shall be certified as an AP and must support 1 and 2 Mbps in its basic rates.
2. If a MAPUT does not support 1 and 2 Mbps in it basic rates, it shall support STA also and shall certify as a MAP and a STA (section 5 of this test plan).
3. A MAP that is also a STA shall be able to receive 1 & 2 Mbps, and transmission at 1 & 2 Mbps is optional.

4 Access Point Testing

This section defines all the test cases for an APUT.

4.1 Configurability Tests

4.1.1 General Configurability Tests

All APUT must be capable of configuring the following general parameters:

1. SSID
2. Wireless Operational Mode, a/b/g/n
3. Channel
4. Static IP Address and Netmask

The APUT fails if any item above cannot be configured through the user interface. If the device fails, no further testing will be performed until the vendor addresses the problems and has updated the device.

4.1.2 Security Configurability Tests

The APUT must be capable of configuring the following security parameters:

1. The DUT must follow one of the security combinations described in section 3.8.
2. Turn WPA2 on or off. Skip this step if the APUT only supports WPA2.
3. When WPA2 is turned on, verify that WPA2-Personal or WPA2-Enterprise running EAP method modes can be selected (for those APs supporting Enterprise).
4. Specify the default pass phrase (“12345678”) for WPA2-PSK can be entered.
5. The shared secret between the AP and the RADIUS server must be capable of using 64 characters (octets). To test, type in the following 64 character string for the secret and verify that it is accepted:

   1234567890…12345678901234

   This is a repeating sequence until 64 characters are reached. This test will have assumed to pass if the AP can accomplish an authentication between a client and the RADIUS server.

6. The AP cannot configure WPA alone; only WPA2/WPA mixed security mode is allowed when WPA is used.

The APUT fails if any item above cannot be configured through the user interface. If the device fails, no further testing will be performed until the vendor addresses the problems and has updated the device.

The interoperability tests assure that the APUT can operate with a variety of ESSIDs, can handle fragmentation, security, Power Save, different channels, different basic rates, and different 802.11n modes and features.

4.2 APUT Test Cases

This section provides a comprehensive list of AP test cases. It defines all the mandatory , Optional and Tested test cases for an APUT and when these tests should be conducted in the 2.4 GHz or 5 GHz frequency bands using 20 MHz or 20/40 MHz channel width respectively. 5 GHz only devices all testing done in 5 GHz band. 2.4 GHz only devices all testing done in 2.4 GHz band, observe b and g settings in each tests. Dual band devices observe test cases. **For non-11n APUT device, tests shall be conducted using 20MHz channel width**.

Test Case	Frequency Band (GHz)	Channel Width (MHz)	Mandatory / Optional and Tested[1]	Test Section
WPA2 Test Cases				
AP Out of the Box (OOB)	2.4 5	20 20/40	Mandatory	4.2.1
AP WPA2 Initial Ping Interoperability Test	2.4 5	20 20/40	Mandatory	4.2.2
AP & STA Association & Throughput, Honoring NAV	2.4 5	20 20/40	Mandatory	4.2.3
AP & STA Association & Throughput using WPA2-Enterprise with TLS	2.4 5	20 20/40	Mandatory	4.2.4
AP & STA Association & Throughput using WPA2-PSK	2.4 5	20 20/40	Mandatory	4.2.5
AP & STA Association & Throughput Replay Counter Processing	2.4 5	20 20/40	Mandatory	4.2.6
AP & STA Association & Throughput using Mixed Mode WPA/WPA2 Enterprise with TLS	2.4 5	20 20/40	Optional and Tested	4.2.7
AP & STA Association & Throughput using Mixed Mode WPA/WPA2 PSK	2.4 5	20 20/40	Optional and Tested	4.2.8
Re-association/Bridging Tests	2.4 5	20 20/40	Mandatory	4.2.9
Group Traffic with WPA/WPA2-PSK Mode	2.4 5	20 20/40	Mandatory	4.2.10
Pre-authentication	2.4 5	20 20/40	Optional and Tested	4.2.11
PMK Caching	2.4 5	20	Mandatory for Enterprise devices	4.2.12
WPA Specific Countermeasures	2.4 5	20	Optional and Tested	4.2.13
WPA2 Negative Tests – No Association with a WEP or No Encryption STA	2.4 5	20	Mandatory	4.2.14
WPA2 Negative Tests – No Association with a WPA2-Enterprise with TLS Configured Access Point	2.5 5	20	Mandatory	4.2.15
802.11d and 802.11h Testing	5	20	Optional and Tested	4.2.16
Extended EAP Tests (Enterprise APs Only)	2.4 5	20	Optional and Tested	4.2.18
Dual Band APs	2.4 5	20	Optional and Tested	4.2.19
Power Save	2.4 5	20	Mandatory	4.2.47
WMM Test Cases				
Basic WMM Association and Transmission	2.4 5	20	Mandatory	4.2.20
Traffic Differentiation in Single BSS with 2 802.11n STAs	2.4 5	20	Mandatory	4.2.21
Traffic Differentiation in Single BSS with WMM STA	2.4 5	20	Mandatory	4.2.22

[1]Optional and tested means that it is optional to implement the feature, and if implemented, it is mandatory to test.

Traffic Differentiation in Single BSS with Legacy Non-WMM STA	2.4 5	20	Mandatory	4.2.23
APUT "No Acknowledgement" Test	2.4 5	20	Mandatory	4.2.24
Traffic Forwarding in Single BSS	2.4 5	20	Mandatory	4.2.25
11n Test Cases				
Basic Association in 802.11n Environment	2.4 5	20 20/40	Mandatory	4.2.26
Ability to Receive 1 and 2 Spatial Streams	2.4 5	20 20/40	Mandatory	4.2.27
SM Power Save Operation	2.4 5	20	Mandatory	4.2.28
A-MDPU Aggregation when the AP is the Recipient with and without WPA2-PSK	2.4 5	20 20/40	Mandatory	4.2.29
A-MSDU Aggregation when the AP is the Recipient	2.4 5	20	Mandatory	4.2.30
Overlapping BSS – 2.4 GHz	2.4	20	Optional and Tested	4.2.31
Overlapping BSS – 5 GHz	5	20	Optional and Tested	4.2.32
HT-Greenfield Operation	2.4 5	20	Optional and Tested	4.2.33
Short GI Operation	2.4 5	20 20/40	Optional and Tested	4.2.34
Overlapping BSS on the Extension Channel	5	20/40	Optional and Tested	4.2.35
HT Duplicate Mode (MCS = 32)	2.4 5	20/40	Optional and Tested	4.2.36
AP Concurrent Operation in 2.4 and 5 GHz Frequency Band	2.4 5	20 20/40	Optional and Tested	4.2.37
AP RIFS Test	2.4 5	20 20/40	Mandatory Receive	4.2.38
AP STBC Transmit Test	2.4 5	20 20/40	Optional and Tested	4.2.39
A-MPDU Aggregation when the AP is the Transmitter	2.4 5	20 20/40	Optional and Tested	4.2.40
AP 20/40 MHz Coexistence	2.4	20/40	Optional[2] and Tested	4.2.41
Ability to Receive 3 Spatial Streams	2.4 5	20 20/40	Optional and Tested	4.2.42
AP Transmitting to STA using Supported Number of Spatial Streams	2.4 5	20 20/40	Mandatory	4.2.43
Disallow TKIP with HT Rates	2.4 5	20 20/40	Optional and Tested	4.2.44
AP Negative tests to ensure WEP is not used with HT associations in 11n devices	2.4 5	20 20/40	Optional and Tested	4.2.45

Table 9: APUT Test Cases

[2] 20/40 MHz Coexistence is a mandatory tests if APUT supports 20/40 MHz

4.2.1 AP Out of the Box (OOB)

Purpose and Description

The APUT is set to its Out of Box (OOB) 'default configuration' to simulate using the device for the first time at initial power on.

Test Environment

APUT
STA1: Testbed 802.11a/b/g (5GHz band) or testbed 802.11a/b/g STA1 (2.4 GHz band)
STA2: Testbed 802.11a/b/g
STA3: Testbed 802.11a/b/g
STA4: Testbed 802.11a/b/g
STAs 1 – 4 are 11n devices operating in legacy mode
AP1: Testbed 802.11a/b/g
AP2: Testbed 802.11a/b/g

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	STA3 Values	STA4 Values	AP1 Values	AP2 Values	APUT Values
Vendor	**Marvell**	**Broadcom**	**Intel**	**Realtek**	**Marvell**	**MediaTek**	-
SSID	wi-fiwi-	wi-fiwi-	wi-fiwi-	wi-fiwi-	ignore	ignore	wi-fiwi-
Security	OFF	WEP	WPA-PSK	WPA2-PSK	OFF	OFF	Default
Encryption Key	-	0x9876543210	wi-fiwi-	wi-fiwi-	-	-	-
Supplicant/ Server	Fedora supplicant	WPA Supplicant	Microsoft	Microsoft	-	-	-
AP Control Channel	-	-	-	-	1 (only needed for 2.4 GHz testing)	11 (only needed for 2.4 GHz testing)	6 or 36 Dual band test both bands.

Table 10: AP Out of the Box Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.
AP1 and AP2 are used to force 20/40 MHz capable APUTs to 20 MHz.

Steps	Testbed 802.11a/b/g Legacy STA1	Testbed 802.11a/b/g Legacy STA2	Testbed 802.11a/b/g Legacy STA3	Testbed 802.11a/b/g Legacy STA4	Testbed 802.11a/b/g Legacy AP1	Testbed 802.11a/b/g Legacy AP2	APUT	Expected Results
All APUT must be capable of being configured in the following ways: 1. ESSID 2. Channel 3. Fixed IP address and sub-net mask 4. Shared Secret The APUT fails if any item above cannot be configured through the user interface. If the device fails, no further testing will be performed until the vendor addresses the problems and has updated the device. If the APUT Beacon does not have the above configuration (Table 9) then fail. The APUT must be capable of being configured in the following ways: 1. Turn WPA2, WPA2/WPA mixed mode, or WEP (if supported) on or off. Skip this step if the APUT only supports WPA2. 2. When WPA2 is turned on, further verify that a WPA2-only mode or, a mixed mode that allows either WPA2/WPA STAs only to associate mixed modes can be selected. 3. When WPA2 is turned on, WEP cannot be turned on, 4. When WPA2 is turned on, verify that WPA2-PSK or WPA2-Enterprise running an EAP method modes can be selected for those APs supporting Enterprise, 5. Verify that WPA alone cannot be turned on. 6. Specify the default pass phrase (“12345678”) for WPA2-PSK can be entered, 7. The shared secret between the AP and the RADIUS server must be capable of using 64 characters (octets). To test, type in the following 64 character string for the secret and verify that it is accepted: 1234567890…12345678901234 This is a repeating sequence until 64 characters are reached. This test will have assumed to pass if the AP can accomplish an authentication between a client and the RADIUS server. The APUT fails this test if any item cannot be configured through the user interface.								
0							Configure for WPA2/WPA mixed mode	Verify that the beacon contains BOTH the RSN IE and WPA IE
0.5							Reset APUT to OOB configuration	
1					Beacon (only needed for 2.4 GHz testing)	Beacon (only needed for 2.4 GHz testing)	Beacon	11n APUT only: Look at the HT Operation element and if the secondary channel offset field is zero then pass for 2.4 GHz. For 5 GHz band this bit may be either 1 or 0.
2	Association Request			Association Request				

3							Association Response	If STA1 or STA4 connects but not both connect, then PASS
4		Association Request	Association Request					if STA2 connects then fail if STA3 connects then fail
5							Ping <connected STA IP>	If pings timeout then fail

Table 11: AP Out of the Box Procedure and Results

4.2.2 AP WPA2 Initial Ping Interoperability Test

Purpose and Description
Verifies that the APUT can authenticate, associate and support pings to a wired authentication server on a subnet connected to the test configuration.

Test Environment
APUT
STA1: Testbed 802.11a/b/g
STA2: Testbed 802.11a/b/g
STA3: Testbed 802.11a/b/g
STA4: Testbed 802.11a/b/g
STAs 1 – 4 are 11n devices operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	STA3 Values	STA4 Values	APUT Values
Vendor	**Realtek**	**Broadcom**	**Intel**	**Marvell**	**-**
ESSID	123%(04	123%(04	123%(04	123%(04	123%(04
Security	WPA2-Enterprise	WPA2-Enterprise	WPA2-Enterprise	WPA2-Enterprise	WPA2-Enterprise
Supplicant/Server	Microsoft	WPA Supplicant	Microsoft	WPA Supplicant	Hostapd
EAP Method (see note)	TLS	TLS	TLS	TLS	TLS
AP Control Channel	-	-	-	-	6 or 36 Dual band use 6

Table 12: AP WPA2 Initial Ping Test Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	Testbed 802.11a/b/g Legacy STA2	Testbed 802.11a/b/g Legacy STA3	Testbed 802.11a/b/g Legacy STA4	APUT	Expected Results
1					Beacon	
2	Association Request					
3					Association Response	
4	Ping test network through APUT for 90 seconds					If the ping fail to continue for the whole 90 seconds then fail
5	Disassociate					
6		Association Request				
7					Association Response	
8		Ping test network through APUT for 90 seconds				If the ping fail to continue for the whole 90 seconds then fail
9		Disassociate				
10			Association Request			
11					Association Response	
12			Ping test network through APUT for 90 seconds			If the ping fail to continue for the whole 90 seconds then fail
13			Disassociate			
14				Association Request		
15					Association Response	
16				Ping test network through APUT for 90 seconds		If the ping fail to continue for the whole 90 seconds then fail
17				Disassociate		

Table 13: AP WPA2 Initial Ping Test Procedure and Results

4.2.3 AP & STA Association & Throughput, Honoring NAV

Purpose and Description
Test different data transfer types.
Test Honoring NAV Background.
Test that the APUT correctly updates its Timing Synchronization Function (TSF) keeping it within the error limit of ±0.01%.

Note: For MAP devices this test case checks for deference to 1Mbps frames.

Test Environment
APUT
STA1: Testbed 802.11a/b/g
Testbed WFA-EMT
STA 1 is an 11n device operating in legacy mode (if running in 2.4 GHz, set STA 1 to B mode, not G)

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	APUT Values
Vendor	**Realtek**	-
AP Control Channel	-	6 (use B mode) or 36, Dual band use 36
Beacon Interval (milliseconds)	-	100
Security		Open if supported, otherwise WPA2-PSK 12345678

Table 14: AP & STA Association & Throughput, Honoring NAV Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	Testbed WFA-EMT	APUT	Expected Results
1	.		Beacon	
2	Association Request		Association Response	
3			Start TCP FILESNDL to STA1	If recorded throughput is less than 4.2.3A1DT1 then fail Set up Wireshark sniffer to capture DT1 run. Filter out everything except for the beacons. Run the PERL analysis script to check the TSF accuracy. The TSF test passes if the PERL script says PASS. Otherwise the APUT fails the test.
4	Start TCP FILESNDL to APUT			If recorded throughput is less than 4.2.3A1DT2 then fail
5			Start INQUIRYL to STA1	If recorded throughput is less than 4.2.3A1DT3 then fail
6		Configure WFA-EMT for NAV test and start NAV test		
7		Configure the testbed WFA-EMT to generate a CTS-to-self with a 25,000 µs large duration field. Upon transmitting the CTS-to-self, the test device waits 30,000 µs before competing for the medium again.	Start TCP FILESNDL to STA1	If throughput is greater than 80% of the throughput in step 3 then fail

Table 15: AP & STA Association & Throughput, Honoring NAV Procedure and Results

4.2.4 AP & STA Association and Throughput using WPA2-Enterprise with TLS

Purpose and Description
Test different data transfer types with WPA2-enterprise.
Testing De-fragmentation.

Test Environment
APUT
STA1: Testbed 802.11a/b/g
STA 1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	APUT Values

Vendor	**Realtek**	-
Security	WPA2-Enterprise TLS	WPA2-Enterprise TLS
Supplicant/Server	Microsoft	Microsoft
EAP Method (see note)	TLS	TLS
AP Control Channel	-	6 or 36, Dual band use 6
Fragmentation	430 Byte	-

Table 16: AP & STA Association and Throughput using WPA2-Enterprise with TLS Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	APUT	Expected Results
1		Beacon	
2	Association Request	Association Response	
3		Start TCP FILESNDL to STA1	If recorded throughput is less than 4.2.4A2DT1 then fail
4	Start TCP FILESNDL to APUT		If recorded throughput is less than 4.2.4A2DT2 then fail
5		Start TCP INQUIRYL to STA1	If recorded throughput is less than 4.2.4A2DT3 then fail

Table 17: AP & STA Association and Throughput using WPA2-Enterprise with TLS Procedure and Results

4.2.5 AP & STA Association and Throughput using WPA2-PSK

Purpose and Description
Test different data transfer types with WPA2-PSK.
Testing Honoring of PS-Poll.

Test Environment
APUT
STA1: Testbed 802.11a/b/g
STA 1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
Power Save	PS-Poll (enable)	-
Security	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678
Supplicant/Server	WPA Supplicant	
AP Control Channel	-	6 or 36, Dual band use 36

Table 18: AP & STA Association and Throughput using WPA2-PSK Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	APUT	Expected Results
1		Beacon	
2	Association Request	Association Response	If association fail then fail
3		Start TCP FILESNDL to STA1	If test runs to completion without error, then pass
4	Start TCP FILESNDL to APUT		If test runs to completion without error, then pass
5		Start INQUIRYL to STA1	If test runs to completion without error, then pass

Note: because APUTs can have DTIMs set between 1 and 5 by default, the throughputs seen will vary widely from APUT to APUT depending on their default DTIM value.

Table 19: AP & STA Association and Throughput using WPA2-PSK Procedure and Results

4.2.6 AP & STA Association and Throughput using Replay Counter Processing

Purpose and Description

Ensure correct replay counter processing. The APUT will need to send/receive at least 70K packets (cross 16-bit boundary of 65K packets).

Test Environment

APUT
STA1: Testbed 802.11a/b/g
STA 1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Note: For this test only, if Chariot is being used, under Chariot run options use ***run until all pairs end*** instead of run for 1 minute 30 seconds. The Chariot script Inquiryl-Replay.scr is executed with the test server running Endpoint 1, and the test is examined to confirm whether the APUT was able to pass data successfully, to completion of the script.

Parameter	STA1 Values	APUT Values
Vendor	**Realtek**	-
ESSID	?>867@?>	?>867@?>
Security	WPA2-PSK	WPA2-PSK
Encryption Key	?>867@?>	?>867@?>
Supplicant/Server	Microsoft	
AP Control Channel	-	6 or 36, Dual band use 6
Power Save	PS-Non-Poll	Default on AP

Table 20: AP & STA Association and Throughput using Replay Counter Processing Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g STA1	APUT	Expected Results
1	Configure the Testbed STA to switch off all the optional features.	Beacon	
2	Association Request	Association Response	
3		Start INQUIRYL-REPLAY to STA1	If test runs to completion without error and the number of bytes received by E1 (endpoint 1 – test server) exceeds 6.6 Megabytes, then pass

Table 21: AP & STA Association and Throughput using Replay Counter Processing Procedure and Results

4.2.7 AP & STA Association and Throughput using Mixed Mode WPA/WPA2 Enterprise with TLS and Message 3 Validation

Purpose and Description

Test APUT ability to work and pass traffic with two security modes WPA and WPA2 Enterprise.
Note: If the APUT does not support WPA/WPA2-Enterprise mixed mode security, this test is skipped.

Validates that the AP sends only a WPA Information Element and no other IE's in the third message of the 4-way association handshake when a WPA station associates with an AP in WPA2/WPA mixed mode operation.

Test Environment
APUT
STA1: Testbed 802.11a/b/g
STA2: Testbed 802.11a/b/g
Wireless Legacy Sniffer
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Realtek**	**Intel**	-
Security	WPA2-Enterprise	WPA-Enterprise	WPA2/WPA mixed mode Enterprise
Supplicant/Server	Microsoft	Microsoft	Microsoft
EAP Method (see note)	TLS	TLS	TLS
AP Control Channel	-	-	6 or 36, Dual band use 36

Table 22: AP&STA Association and Throughput using Mixed Mode WPA/WPA2 Enterprise with TLS and Message 3 Validation Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g STA1	Testbed 802.11a/b/g STA2	APUT	Expected Results
1			Beacon	
2	Association Request	Association Request	Association Response to STA1 Association Response to STA2	If any stations fail to associate then fail
3	SN: Capture the 4 way handshake			Locate message 3 from the mixed mode WPA2 AP to STA2 association. The pass criteria for this test will be that the APUT has only a WPA IE (Tag #221) and no other IEs in the third message. If any other IE is present or the WPA IE is not present, the test fails.
4			Start TCP FILESNDL to STA1 Start TCP FILESNDL to STA2	If recorded throughput is less than 4.2.7A5DT1WPA2 then fail If recorded throughput is less than 4.2.7A5DT1WPA then fail
5	Start TCP FILESNDL to APUT	Start TCP FILESNDL to APUT		If recorded throughput is less than 4.2.7A5DT2WPA2 then fail If recorded throughput is less than 4.2.7A5DT2WPA then fail
6			Start TCP INQUIRYL to STA1 Start TCP INQUIRYL to STA2	If recorded throughput is less than 4.2.7A5DT3WPA2 then fail If recorded throughput is less than 4.2.7A5DT3WPA then fail

Table 23: AP & STA Association and Throughput using Mixed Mode WPA/WPA2 Enterprise with TLS and Message 3 Validation Procedure and Results

Note that the two stations are associated to the AP simultaneously, and the tests for the stations are run simultaneously. For example, the DT1 test shall be set up so that there are 2 streams from the console to each of the 2 stations. For DT2, the setup is the same as DT1 with the streams reversed so that the streams are from the stations to the console. DT3 is set up so that the console is the source of the stream and the stations are the sinks.

4.2.8 AP & STA Association and Throughput using Mixed Mode WPA/WPA2-PSK

Purpose and Description

Test APUT ability to work and pass traffic with two security modes WPA and WPA2-PSK. Note: If the APUT does not support mixed mode WPA2/WPA, this test is skipped.

Test Environment

APUT
STA1: Testbed 802.11a/b/g
STA2: Testbed 802.11a/b/g
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Intel**	**Broadcom**	-
Power Save	-	On – Fast Mode	-
Security	WPA2-PSK	WPA-PSK	WPA2/WPA mixed mode PSK
Encryption Key	12345678	12345678	12345678
Supplicant/Server	Microsoft	WPA Supplicant	-
AP Control Channel			6 or 36, Dual band use 6

Table 24: AP & STA Association and Throughput using Mixed Mode WPA/WPA2-PSK Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g STA1	Testbed 802.11a/b/g STA2	APUT	Expected Results
1			Beacon	
2	Association Request	Association Request	Association Response to STA 1 Association Response to STA2	If any stations fail to associate then fail
3			Start TCP FILESNDL to STA1 Start TCP FILESNDL to STA2	If recorded throughput is less than 4.2.8A6DT1WPA2 then fail If recorded throughput is less than 4.2.8A6DT1WPA then fail
4	Start TCP FILESNDL to APUT	Start TCP FILESNDL to APUT		If recorded throughput is less than4.2.8 A6DT2WPA2 then fail If recorded throughput is less than 4.2.8A6DT2WPA then fail
5			Start TCP INQUIRYL to STA1 Start TCP INQUIRYL to STA2	If recorded throughput is less than 4.2.8A6DT3WPA2 then fail If recorded throughput is less than 4.2.8A6DT3WPA then fail

Table 25: AP & STA Association and Throughput using Mixed Mode WPA/WPA2-PSK Procedure and Results

4.2.9 Re-association/Bridging Tests

Purpose and Description
To verify the APUT's ability to handle re-association and re-authentication of roaming stations from multiple vendors. This includes the notification of any intervening bridges that a station has roamed (so that bridge ARP caches are properly updated).

Test Environment
APUT
STA1: Testbed 802.11a/b/g
AP2: Testbed 802.11a/b/g
STA 1 is an 11n device operating in legacy mode
AP2 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	Testbed AP2	APUT Values
Vendor	**Broadcom**	**Qualcomm**	-
ESSID	MSK*^~/M	MSK*^~/M	MSK*^~/M
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	MSK*^~/M	MSK*^~/M	MSK*^~/M
Supplicant/Server	WPA Supplicant	Microsoft	-
AP Control Channel	-	Same as APUT	6 or 36, Dual band use 36

Table 26: Re-association/Bridging Tests Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g STA1	Testbed 802.11a/b/g AP	APUT	Expected Results
1			Beacon	
2	Association Request		Association Response to STA 1	If any stations fail to associate then fail
3			Ping STA1 (ping STA IP) 90 seconds	If more that 10% ping failures, then fail.
4		Start tested AP to beacon	Stop APUT when testbed AP starts to beacon	
5	Association request to testbed AP	Association response to STA1		
6		Ping STA1 (ping STA IP –t) 90 seconds		If more that 10% ping failures, then fail.
7		When APUT start beacon stop tested AP	Start APUT to beacon	
8	Association Request		Association Response to STA 1	
9			Reattempt to ping (ping STA IP -t)	If more that 10% ping failures, then fail.

Table 27: Re-association/Bridging Tests Procedure and Results

4.2.10 Group traffic with WPA2-PSK Only Mode and WPA/WPA2-PSK Mixed Mode

Purpose and Description

- To check APUT's ability to handle correctly the reception and transmission of group traffic in WPA2 Only Mode and WPA/WPA2 Mixed Mode
- To verify that DTIM count decreases monotonically and linearly.
- To verify APUT's ability to correctly set the Traffic Indicator Bit (TIB) (Bit 0 of the Bitmap Control octet) when group traffic is buffered and the DTIM counter is zero
- To verify APUT's ability to send Group traffic when TIB bit is set and DTIM count=0
- To verify that APUT shall transmit buffered group addressed Buffer able units (Bus), before transmitting any individually addressed frames

Note: If the APUT supports only WPA2 and not WPA, then run both portions using WPA2.

When group traffic is originated by a test bed STA, the traffic is transmitted as directed packets to the APUT. The APUT will re-transmit the packets as group traffic. The APUT is tested to ensure the correct directed traffic key/group key is used for the reception and transmission of group traffic.

Test Environment
APUT
STA1: Testbed 802.11a/b/g
STA2: Testbed 802.11a/b/g
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration

Note: If Chariot is being used, “Validate Data upon Receipt” is selected on the Chariot Run Options tab of the Run Options dialog.

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Broadcom**	**Marvell**	-
SSID	Multicast	Multicast	Multicast
Security	Steps 1 to 8: WPA2-PSK	Steps 1 to 4: WPA-PSK Steps 5 to 8: WPA2-PSK	Steps 1 to 4: WPA2/WPA mixed mode PSK Steps 5 to 8: WPA2-PSK
Beacon Interval			100
DTIM Interval			OOB
Encryption Key	Multicast	Multicast	Multicast
Supplicant/Server	WPA Supplicant	-	-
Power Save	PS-Poll (enabled)	-	
AP Control Channel	-	-	6 or 36, Dual band 6

Table 28: Group traffic with WPA2-PSK Only Mode and WPA2/WPA-PSK Mixed Mode Configuration

Test Procedure
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g STA1	Testbed 802.11a/b/g STA2	APUT	Expected Results
1			Beacon	
2	Association Request	Association Request	Association Response to STA 1 Association Response to STA2 Set up the sniffer to capture beacons	If any stations fail to associate then fail Check for DTIM value of Beacons. The value of DTIM count value shall decrease to zero monotonically, and linearly (Ex: If DTIM count =3, then sequence of DTIM count would be 2,1,0) See Note 1.
3	The two group traffic Test Stations are set up with IP Multicast Address 224.0.0.5. Each station’s unique IP address must also be configured into the test to be able to configure the IP Multicast Address on those stations. UDP is selected as the underlying protocol. REALAUD is selected as the script.			
4			Start traffic with STA1 as Endpoint 1, and the console and STA2 as Endpoint 2	If the test can run to completion without stopping, the test passes. If Chariot posts warning messages, these are not failures to complete the test.

5		Change security to WPA2-PSK only mode	Change security to WPA2-PSK only mode	
6	Association Request	Association Request	Association Response to STA 1	If STA1 does not associate, then fail
7				
8			Start traffic with pair 1 and pair 2: Pair 1 (group traffic pair): the console as Endpoint 1, and STA1 and STA2 as Endpoint 2 Pair 2 (directed traffic pair): the console as Endpoint 1 and STA2 as Endpoint 2. Use TCP FILESNDL. Capture packets in sniffer for at least 30 seconds	Pass/Fail Criteria: 1) If the test fails to run to completion without Errors , the test FAILS. 2) Check for the DTIM counter value of the beacons. After DTIM count=0 and TIB=1 (a DTIM beacon): a) APUT shall deliver group traffic. If APUT does not deliver group traffic then FAIL. b) From sniffer, verify that the APUT delivers Group traffic before the APUT delivers any directed traffic. If the APUT delivers any group traffic after the APUT delivers any directed traffic, then FAIL. c) *Ignoring the last group data packet,* verify that the More Data Bit is 1 in all the group traffic packets in this DTIM beacon. *The last data packet is examined in #3 and #4 below.* 3) If more data bit is zero in the last group addressed packet in the DTIM beacon interval in #2, then verify that no group traffic is sent following beacons with DTIM counter ≠0. If group traffic is sent in these beacons, then FAIL. See note 1. 4) If more data bit is 1 in the last group addressed packet in the DTIM beacon interval in #2, then verify that TIB=1 in the TIM element of following beacon. IF the TIB=0, then FAIL. See note 2. If Chariot posts warning messages, these are not failures to complete the test.

				If all the above criteria are not FAIL, then the test is a PASS. Refer Appendix B for sample sniffer captures

Table 29: Group Traffic with WPA2/WPA-PSK Mixed Mode and WPA2-PSK Only Procedure and Results

Note 1: If the APUT uses a DTIM interval of 1, then every beacon will be a DTIM beacon with the DTIM counter equal to zero. For these APUTs, every beacon is able to have group traffic, and this criterion does not apply to this APUT.

Note 2: In this case, the AP is allowed to send group traffic in beacons where the DTIM counter ≠0. In this case, the APUT does not fail criterion #3.

4.2.11 Pre-authentication

Purpose and Description

This test is optional.

Only if an APUT contains this capability will the ability of the APUT to perform WPA2 pre-authentication be tested. If the APUT does not support pre-authentication completion of this section is not required.

Test Environment

APUT
STA1: Testbed 802.11a/b/g
AP2: Testbed 802.11a/b/g
A wireless sniffer
A wired sniffer
STA 1 is an 11n device operating in legacy mode
AP2 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	Testbed AP2	802.11n APUT Values
Vendor	**Realtek**	**MediaTek**	-
Security	WPA2-Enterprise	WPA2-Enterprise	WPA2-Enterprise
Supplicant/Server	Microsoft	Microsoft	Microsoft
EAP Method (see note)	TLS	TLS	TLS
AP Control Channel	-	Same as APUT	6 or 36, Dual band use 36

Table 30: Pre-authentication Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	Testbed 802.11a/b/g AP	APUT	Expected Results
0				Connect the wired AP to the Backbone between the APs

1	Flush any previously cached authentication data on the station (e.g. by disabling and re-enabling BOTH the supplicant and the wireless device on laptop containing the station.	Beacon	Powered off	
2	Association Request	Association Response to STA 1		If any stations fail to associate then fail
3	Initiate a continuous ping to the console (ping <console IP> -t)			Insure that the ping pass SN: start both the wired and the wireless sniffers
4			Power on and wait it to beacon	
5	Start a scan for available networks on the test bed station.			Allow up to 180 seconds to elapse for the STA1 to receive an EAP-Success frame with an Ethertype of "pre-authentication" (0x88c7); this will be seen on the wired side sniffer. If STA1 does not receive the pre-authentication Ethertype within 180 seconds, the test is considered to have failed.
6		Power off		Verify that the ping resumes within 90 seconds between STA1 and the console. SN: Verify that neither an EAPOL_START nor an EAPOL_IDENTITY_REQUEST message is seen in the wired side sniffer after the STA roams to the APUT and resumes ping.
7	Inspect the wireless sniffer capture and verify: 1. That a PMKID is included in the association or re-association request from STA1 to APUT after AP2 is powered off, 2. The same PMKID is included in message 1 of the 4-way handshake sent by the APUT (This is the first EAPOL message after the re-association response message) after STA1 has received an EAPSuccess frame (0x88c7) as seen on the wired side sniffer, and 3. No EAP frames (full 802.1X exchange) are sent from STA1 to APUT or from APUT to STA1 after the AP2 is powered off Note: Do not rely on RADIUS logs as they may incorrectly indicate a failure, use sniffer. PASS/FAIL Criteria: The test will have deemed to have passed when the required EAPSuccess has been captured by the wired sniffer, and when the PMKIDs in the associate message and 4-way message 1 match, and a full EAP authentication does not occur over the air between STA and APUT. Note: A full EAP authentication request can be recognized on the wireless sniffer by an EAPOL_START from the STAUT or EAPOL_IDENTITY_REQUEST message from the AP			

Table 31: Pre-authentication Procedure and Results

4.2.12 PMK Caching

Purpose and Description

This test is mandatory for Enterprise devices.
If the pre-authentication test was performed and passed, then this test must have passed simultaneously. If so, this test need not be done here.

Unlike pre-authentication the PMK Cache test is required. There is no upper limit for the number of PMK that a station can cache, however this test plan verifies that at least one PMK can be cached and used within the BSS.

Methodology: STA1 within the test bed is first associated and authenticated with an APUT. Ping test is used to demonstrate application level connectivity.

A wireless sniffer is configured to capture all frames to and from the APUT.
STA1 is forced to re-associate with the APUT. The sniffer capture is examined to verify that a cached PMK was used.

Test Environment

APUT
STA1: Testbed 802.11a/b/g
Sniffer
STA 1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Supplicant/Server	WPA Supplicant	Microsoft
AP Control Channel	-	6 or 36, Dual band 6

Table 32: PMK Caching Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	APUT	Expected Results
1		Beacon/Probe Response	
2	Association Request		
3		Association Response	If the STA1 did not connect successfully then fail.
4	Configure a wireless sniffer to capture all traffic with from and to the APUT		
5	Ping <Wired IP>		If more that 10% ping failures, then fail.
6	Force a re-association event for the station to the APUT using the WC command "wc reassoc <macaddr_of_APUT>" to force the STA to (re)associate with the appropriate AP.		If the ping does not resume within 15 seconds then fail
7	1. Inspect the sniffer capture and verify that a PMKID is included in the association or re-association request from the STA to APUT. 2. The same PMKID is included in message 1 of the 4-way handshake sent by the APUT (This is the first EAPOL message after the re-association response message.), and 3. No EAP frames (full 802.1X exchange) are sent from the STA station to APUT or from APUT to the STA. Note: Do not rely on RADIUS logs as they may incorrectly indicate a failure, user sniffer. The test will have deemed to have passed when the PMKIDs in the (re)associate message and 4-way message 1 match, and a full EAP authentication does not occur. Note: A full EAP authentication request can be recognized on the wireless sniffer by an EAPOL_START from the STAUT or EAPOL_IDENTITY_REQUEST message from the AP		

Table 33: PMK Caching Procedure and Results

4.2.13 WPA Specific Countermeasures

Purpose and Description
The purpose of the following test is to ensure that WPA countermeasures are implemented correctly within the APUT and that the products within the test bed can recover from a MIC failure. Note: If the APUT does not support mixed mode WPA2/WPA, this test is skipped.

For an APUT the configuration considered by this test is two test bed STAs, one operating with WPA2-Personal (802.11a/b/g STA) and the other operating in WPA-personal (802.11a/b/g STA) – a mixed mode. Both are associated with the APUT. With this configuration all group traffic will use TKIP. A third station, the WFA-EMT operating as a station using WPA-Personal, is introduced into this configuration; this is the MIC attacker and is capable of generating a Michael MIC failure data frame.

Test Environment
APUT
STA1: Testbed 802.11a/b/g
STA2: Testbed 802.11a/b/g
Testbed WFA-EMT
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	WFA-EMT	APUT Values
Vendor	**Intel**	**Marvell**		-
Security	WPA2-PSK	WPA-PSK	-	WPA2/WPA mixed mode PSK
Encryption Key	12345678	12345678	-	12345678
Supplicant/Server	Microsoft	Fedora supplicant	-	-
AP Control Channel	-	-	-	6 or 36, Dual band 36

Table 34: WPA Specific Countermeasures Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	Testbed 802.11a/b/g STA2	WFA-EMT	APUT	Expected Results
1				Beacon/Probe Response	
2	Association Request	Association Request		Association Responses to STA1 and STA2	
3	Ping APUT	Ping APUT	WFA-EMT: No ping check is required.		If the ping does not pass then fail
4			Generate a single bad frame		If for the next 70 seconds both test bed stations continue with their 'ping' sessions then pass
5			After 70 seconds generate another bad frame		If for the next 50 seconds both test bed stations continue with the 'ping' sessions then pass
6			After 50 seconds generate a third bad frame		This part of the test is considered to have passed if the APUT de-authenticates both of the test bed STAs (WPA and WPA2). Both 'ping' sessions will stop.
7	After a period of 60 seconds both test bed stations are able to associate again with the APUT. The 'ping' sessions are re-established. This re-establishment of the association may require manual intervention. This is acceptable. The aim of the test here is to ensure that re-establishment can only occur after 60 seconds.				

Table 35: WPA Specific Countermeasures Procedure and Results

4.2.14 WPA2 Negative Tests – No Association with a WEP or No Encryption STA

Purpose and Description

Testbed STA1 is configured to use a 40-bit WEP key as its method of encryption. The APUT is powered on in and WPA2 only is selected (with WPA2-Enterprise running TLS). While the STA attempts to associate with the APUT, the STA pings the IP address of the authentication server. This test is deemed to have failed if the STA ever receives a ping response; however if no ping response is received within 90 seconds, the test will have assumed to pass.

Testbed STA2 is configured so as not to use Security (e.g., WPA, WPA2 or WEP off). The APUT is powered on in its defined configuration (see table below). While STA2 attempts to associate with the APUT, STA2 pings the IP address of the authentication server. This test is deemed to have failed if STA2 receives a ping response with 90 seconds.

Where the following test requires the entry of a 256-bit WPA or WPA2 key, the test is equally valid if the method of inputting the key is via a key generation utility or directly as a HEX based equivalent key.

Test Environment

APUT
STA1: Testbed 802.11a/b/g
STA2: Testbed 802.11a/b/g
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	802.11n APUT Values
Vendor	**Intel**	**Marvell**	-
Security	WEP	None	WPA2-Enterprise running TLS
Encryption Key	0x9876543210	None	-
Supplicant/Server	Microsoft	Fedora supplicant	Microsoft
AP Control Channel	-	-	6 or 36, Dual band 6

Table 36: No Association with WEP or No Encryption STA Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	Testbed 802.11a/b/g STA2	APUT	Expected Results
1			Beacon/Probe Response	
2	Start a continuous ping to the authentication server	Start a continuous ping to the authentication server		
3	Try to associate by applying the profile above for at least 90 seconds	Try to associate by applying the profile above for at least 90 seconds		If either station can ping the authentication server within the 90 seconds then fail

Table 37: No Association with WEP or No Encryption STA Procedure and Results

4.2.15 WPA2 Negative Test Cases – No Association with a WPA2-Enterprise with TLS and WPA2-PSK Configured Access Point

Purpose and Description

Test Environment
APUT
STA1: Testbed 802.11a/b/g
STA2: Testbed 802.11a/b/g
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed. The test is run twice (WPA2 Enterprise TLS and WPA2-PSK).

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Intel**	**Marvell**	-
Security	WPA2-Enterprise running TLS	WPA2-PSK	WPA2-Enterprise running TLS WPA2-PSK
Encryption Key	-	12345678	"12345678" for WPA2-PSK
Supplicant/Server	Microsoft	Fedora supplicant	Microsoft
AP Control Channel	-	-	6 or 36, Dual band 36

Table 38: No Association with a WPA2-Enterprise with TLS Configured AP Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	Testbed 802.11a/b/g STA2	APUT	Expected Results
1			Beacon/Probe Response	
2	Start a continuous ping to the authentication server	Start a continuous ping to the authentication server		
3	Associate by applying the profile above	Try to associate by applying the profile above for at least 90 seconds		If STA1 succeed to connect and pass ping for 90 seconds then PASS. If STA2 can ping the authentication server within the 90 seconds then FAIL.

4			Enable WPA2-PSK security mode	
5	Try to associate by applying the profile above for at least 90 seconds	Associate by applying the profile above		If STA2 succeed to connect and pass ping for 90 seconds then PASS. If STA1 can ping the authentication server within the 90 seconds then FAIL.

Table 39: No Association with a WPA2-Enterprise with TLS Configured AP Procedure and Results

4.2.16 802.11d and 802.11h Testing

Purpose and Description

These tests are mandatory for APUTs that implement the Country Element Information.
This test is to verify the 802.11d country information element (CIE).
This test is to verify the 802.11h power constraint information element.
Note: an AP may support one without the other functionality. 802.11d and 802.11h are separate tests.

The Channel Switch Announcement test applies to 802.11n 5GHz APs only. APs that utilize 802.11h are required to advertise when they are changing to a new channel, with a Channel Switch Announcement Element (Information Element ID (IE=37)).

Test Environment
APUT
STA1: Testbed 802.11h+d capable
Wireless Legacy Sniffer
STA 1 is an 11n device operating in legacy mode
Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	802.11n APUT Values
Vendor	**Realtek**	-
Supplicant/Server	-	Open if supportred, otherwise WPA2-PSK 12345678
AP Control Channel	-	56
New Channel	-	36 (or any non-DFS channel)

Table 40: 802.11d and 802.11h Testing Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

For APs supporting only 802.11d, perform steps 1 through 5.
For APs supporting only 802.11h, perform steps 5 through 9.

Steps	Testbed 802.11d Capable STA1	APUT	Expected Results
1		Configure the APUT to OOB	SN: Check the country code advertised in the AP Beacon. If it matches with the ISO standard country code name then continue else fail the test. Note: Refer to the tech-ops manual section 13 for the list of country codes.
2	Repeat the process for 4 additional countries for those APs that support 5 or more countries. For those that support fewer than 5 countries, repeat the procedure for all the countries supported.		
3		Select one country from the list supplied by the APUT vendor.	
4		Beacon/Probe Response	SN: Look for Information Element #7 in the beacon and the probe response. If The Country Information Element (country name field) is identical in both the beacon and probe response, and both codes correspond to the code specified for the configured country in the list then continue. Note: Refer to the tech-ops manual section 13 for the list of country codes.
5	Association request	Association response	If the station connects then continue.
6		Beacon/Probe Response	SN: Look for the Power Constraint Information Element #32 in the beacon and the probe response, if the beacon and probe response messages contain a Power Constraint Element then continue.
7		Use the APUT supplied command to force a channel switch.	Watch the sniffer until no more beacons are seen from the APUT, or 15 seconds elapses from the issuance of the command to change the channel of the APUT to a non-DFS channel. If the AP fails to stop beaconing on this channel within 15 seconds, assume the test has failed.
8	1. Find the last beacon sent by the APUT and verify that it contains the CSA IE. Assume the test has failed if last beacon does not hold CSA IE. 2. Find at least four earlier beacons from the APUT and verify they all carry the CSA IE. 3. If a total of five beacons with correct CSA IEs cannot be found, assume the test has failed.		
9	This test passes if the Channel Switch Announcement Element (#37) is repeated in the last 5 beacons that are captured after the channel switch command is given and before the channel switch occurs, and the AP stops beaconing on the channel within 15 seconds after issuing the channel switch command.		

Table 41: 802.11d and 802.11h Testing Procedure and Results

4.2.17 removed

4.2.18 Extended EAP Tests (Enterprise APs Only)

Purpose and Description

Extended EAP testing applies to APs tested as WPA2-enterprise devices only; APs that are WPA2-personal devices are not tested in this section. These tests are to test the APs ability to use EAP methods beyond TLS: TTLS, PEAP0, PEAP1, and SIMs. All tests are performed using “Ping” tests; there are no throughput tests.

Test Environment

APUT
STA1: Testbed 802.11a/b/g
STA 1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

The Testbed’s Servers and Supplicants support all EAP methods, and the APUT must be tested with all combinations. Some TLS tests have already been performed in previous sections, and they will not be repeated here.

Parameter	STA1 Values	APUT Values
Vendor	**Marvell**	-
AP Channel	-	11 or 36, dual band use channel 11
Security	WPA2-ENTERPRISE RUNNING TTLS	WPA2-ENTERPRISE RUNNING TTLS
Supplicant/Server	WPA Supplicant	Radiator

Table 42: Extended EAP Tests Configuration #ExA14

Parameter	STA1 Values	APUT Values
Vendor	**Intel**	-
AP Channel	-	11 or 40, dual band use channel 11
Security	WPA2-ENTERPRISE RUNNING PEAP0	WPA2-ENTERPRISE RUNNING PEAP0
Supplicant/Server	Microsoft	Microsoft

Table 43: Extended EAP Tests Configuration #ExA15

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
AP Channel	-	6 or 48, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING PEAP1	WPA2-ENTERPRISE RUNNING PEAP1
Supplicant/Server	WPA Supplicant	Hostapd

Table 44: Extended EAP Tests Configuration #ExA16

Parameter	STA1 Values	APUT Values
Vendor	**Marvell**	-
AP Channel	-	11 or 44, dual band use channel 11
Security	WPA2-ENTERPRISE RUNNING SIM	WPA2-ENTERPRISE RUNNING SIM
Supplicant/Server	WPA Supplicant	Hostapd

Table 45: Extended EAP Tests Configuration #ExA17

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
AP Channel	-	11 or 44, dual band use channel 11
Security	WPA2-ENTERPRISE RUNNING FAST	WPA2-ENTERPRISE RUNNING FAST
Supplicant/Server	WPA Supplicant	Hostapd

Table 46Extended EAP Tests Configuration #ExA24

Parameter	STA1 Values	APUT Values
Vendor	**Marvell**	-
AP Channel	-	11 or 44, dual band use channel 11
Security	WPA2-ENTERPRISE RUNNING AKA	WPA2-ENTERPRISE RUNNING AKA
Supplicant/Server	WPA Supplicant	Hostapd

Table 47Extended EAP Tests Configuration #ExA25

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
AP Channel	-	11 or 44, dual band use channel 11
Security	WPA2-ENTERPRISE RUNNING AKA’	WPA2-ENTERPRISE RUNNING AKA’
Supplicant/Server	WPA Supplicant	Hostapd

Table 48 Extended EAP Tests Configuration #ExA26

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g Legacy STA1	APUT	Expected Results
1		Beacon/Probe Response	
Association Positive Test			
2	Both the Station and AP have valid authentication certificates installed. The appropriate EAP method is set up on both the APUT and the Station. The Station is associated to the APUT.	Both the Station and AP have valid authentication certificates installed. The appropriate EAP method is set up on both the APUT and the Station. A ping test is started to validate the association.	If the ping test does not successfully start within 90 seconds, the APUT fails the test, and all testing is stopped.

Table 49: Extended EAP Tests Procedure and Results

4.2.19 Dual Band APs

Purpose and Description

Test Environment
APUT
STA1: Testbed 802.11a STA
STA2: Testbed 802.11g STA
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed. Note single band and single radio devices skip this test.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Realtek**	**Intel**	-
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Supplicant/Server	Microsoft	Microsoft	Microsoft
AP Control Channel	36	6	6 and 36

Table 50: Dual Band AP Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11a STA1	Testbed 802.1g STA2	APUT	Expected Results
1			Beacon/Probe Response	If both STA1 and STA2 associate, then pass
2	Start TCP FILESNDL to STA2	Receive TCP FILESNDL		If STA1 -> STA2 throughput is greater than 4.2.19DBA1DT1 then pass
3	Receive FILESNDL	Start TCP FILESNDL to STA1		If STA2 -> STA1 throughput is greater than 4.2.19DBA1DT2 then pass

Table 51: Dual Band AP Procedure and Results

4.2.20 Basic WMM Association and Transmission

Purpose and Description

Test WMM capability negotiation.
Internal and distributed traffic differentiation between different traffic classes and various PHY rates between a single pair.

This test is performed between a single AP and a single STA to show that a device under test correctly differentiates packets. Two streams with different AC are transmitted from a DUT and the throughputs are compared in the same manner as the above differentiation tests.

Test Environment

APUT
STA1: Testbed 802.11n 20 MHz
Wireless Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed. Run tests for 20 seconds.

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
ESSID	LJHG50_=+’	LJHG50_=+’
Security	WPA2-PSK	WPA2-PSK
Encryption Key	LJHG50_=+’	LJHG50_=+’
AP Control Channel	-	6 or 36, Dual band use 36
AIFS	Default (see Appendix D)	Default (see Appendix D)
Cwmin	Default (see Appendix D)	Default (see Appendix D)
Cwmax	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	0
ACM: AC_VI	-	0
ACM: AC_BE	-	0
ACM: AC_BK	-	0
AC Tagging	DSCP	Default for AP
Channel Width	0 (20 MHz)	

Table 52: Basic WMM Association and Transmission Configuration

The following table defines the script that will be used for 11n APUT this test case.

Scripts	Script Names
RTP1	IPTV18Mbps.scr
RTP2	IPTV14Mbps.scr
RTP3	IPTV14MbpsDelay10sec.scr

Table 53: Basic WMM Association and Transmission Test Scripts

Note: The following table defines the scripts used for Non 11n APUT

Scripts	Script Names	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr(with delay)

Details of the script and parameters in Appendix H

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	APUT	Expected Results
0	Configure the STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
1		Beacon	SN: If Beacons contains WMM parameter element or WMM information element, PASS. If the WMM Parameter element is present, if ACI, ACM, AIFS, Cwmin, Cwmax and TXOP are set according to configuration above, PASS. Record ParamCount value.
2	Probe request	Probe response	SN: If a Probe Request occurs and Probe Response contains WMM parameter element with ParamCount matching the ParamCount in the beacon (step 1) and ACI, ACM, AIFS, Cwmin, Cwmax and TXOP set according to configuration above, Pass
3	Association Request	Association Response	SN: If Association Response contains WMM parameter element with ParamCount matching the ParamCount in the beacon/probe response (step 1) and ACI, ACM, AIFS, Cwmin, Cwmax and TXOP set according to test configuration above AND STA Associated, PASS
4	Receive RTP1_BE, RTP2_VI, RTP3_BE	Transmit RTP1_BE RTP2_VI RTP3_BE	SN: In a RTP1_BE QoS Data frame, if QoS Control Field UP=000_2, EOSP=0_2, ACKPOLICY=00 and the frame type=10_2, subtype=1000_2, PASS. SN: In a RTP2_VI QoS Data frame, if QoS Control Field UP=101_2 or 100_2, EOSP=0_2, ACKPOLICY=00_2 and the frame type=102, subtype=1000_2, PASS. SN: In a RTP3_BE QoS Data frame, if QoS Control Field UP=000_2, EOSP=0_2, ACKPOLICY=00_2 and the frame type=10_2, subtype=1000_2, PASS. CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
5	Receive RTP1_BE, RTP2_VI Transmit RTP3_BE	Transmit RTP1_BE RTP2_VI Receive RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BE,	Receive RTP1_BE	CH: Receive Data RTP1, RTP2, RTP3

	RTP2_VI Receive RTP3_BE	RTP2_VI Transmit RTP3_BE	If RTP2 in second phase (11~19s) is 79% or more than RTP2 in first phase (1~9s), PASS
7	Transmit RTP1_VI, RTP2_VO Receive RTP3_VI	Receive RTP1_VI RTP2_VO Transmit RTP3_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 67% or more than RTP2 in first phase (1~9s), PASS
8	Transmit RTP1_BK, RTP2_BE Receive RTP3_BK	Receive RTP1_BK RTP2_BE Transmit RTP3_BK	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS

Table 54: Basic WMM Association and Transmission Procedure and Results

4.2.21 Traffic Differentiation in Single BSS with 2 802.11n STAs

Purpose and Description

Internal and distributed traffic differentiation between different traffic classes at various PHY rates involving an AP and two STAs with downstream/ upstream traffic.

The general approach is to run traffic streams using only two different priorities for any one test. Several of the tests use two streams of the lower priority to clearly show the differentiation. The intended load (load – for definition see Section 3.5.1 of RFC 2285) of the higher priority stream does not exceed the link capacity. The background traffic stream provides enough additional traffic to saturate the wireless link. This is true regardless of whether the priority of the background traffic is higher or lower than the DUT's traffic. Thus the total intended load of the two streams exceeds the link capacity. In this situation, it is simple to compare the backoff algorithms of two devices – the higher priority stream should always get the bandwidth it needs to achieve its intended load, while the lower priority stream gets whatever is left over. The PHY rates of the DUT and the test bed source do not matter.

Test Environment

APUT
STA1: Testbed 802.11n 20 MHz
STA2: Testbed 802.11n 20 MHz
Wireless Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Broadcom**	**Intel**	-
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678
AP Control Channel	-	-	6 or 36, Dual band use 6
AIFS	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
Cwmin	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
Cwmax	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	DSCP	DSCP	Default for AP
Channel Width	0 (20 MHz)	0 (20 MHz)	

Table 55: Traffic Differentiation in Single BSS with 2 802.11n STA Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV22Mbps.scr
RTP2	IPTV18Mbps.scr
RTP3	IPTV18MbpsDelay10sec.scr

Table 56: Traffic Differentiation in Single BSS with 2 802.11n STA Test Scripts

Note: The following table defines the scripts used for Non 11n APUT

Scripts	Script Names	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	Testbed 802.11n 20 MHz Capable STA2	APUT	Expected Results
0	Configure the STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Configure the STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
1	-	-	Beacon	
2	Probe Request	Probe Request	Probe Response	SN: If a Probe Request occurs and Probe Response contains WMM parameter element, Pass
3	Association Request	Association Request	Association Response	SN: If Association Response contains WMM parameter

				element AND STA Associated, PASS
4	Receive RTP1_BE, RTP2_VI	Receive RTP3_BE	Transmit RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
5	Receive RTP1_BE, RTP2_VI	Transmit RTP3_BE	Transmit RTP1_BE RTP2_VI Receive RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BE, RTP2_VI	Receive RTP3_BE	Receive RTP1_BE RTP2_VI Transmit RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
7	Receive RTP1_VI, RTP2_VO	Receive RTP3_VI	Transmit RTP1_VI RTP2_VO RTP3_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
8	Receive RTP1_VI, RTP2_VO	Transmit RTP3_VI	Transmit RTP1_VI RTP2_VO Receive RTP3_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
9	Receive RTP1_BK, RTP2_BE	Receive RTP3_BK	Transmit RTP1_BK RTP2_BE RTP3_BK	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
10	Receive RTP1_BK, RTP2_BE	Transmit RTP3_BK	Transmit RTP1_BK RTP2_BE Receive RTP3_BK	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS

Table 57: Traffic Differentiation in Single BSS with 2 802.11n STA Procedure and Results

4.2.22 Traffic Differentiation in Single BSS with WMM STA

Purpose and Description

Internal and distributed traffic differentiation between different traffic classes at various PHY rates involving an AP and two STAs with downstream/upstream traffic. Note: If the APUT supports only WPA2 and not WPA, run this test in WPA2 only mode.

The general approach is to run traffic streams using only two different priorities for any one test. Several of the tests use two streams of the lower priority to clearly show the differentiation. The intended load (load – for definition see Section 3.5.1 of RFC 2285) of the higher priority stream does not exceed the link capacity. The background traffic stream provides enough additional traffic to saturate the wireless link. This is true regardless of whether the priority of the background traffic is higher or lower than the DUT's traffic. Thus the total intended load of the two streams exceeds the link capacity. In this situation, it is simple to compare the backoff algorithms of two devices – the higher priority stream should always get the bandwidth it needs

to achieve its intended load, while the lower priority stream gets whatever is left over. The PHY rates of the DUT and the test bed source do not matter.

Test Environment
APUT
STA1: Testbed 802.11n 20 MHz
STA2: Testbed 802.11a/b/g WMM Capable
Wireless Sniffer
STA 2 is an 11n device operating in legacy mode
Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Broadcom**	**Intel**	-
ESSID	NVCX@7.N	NVCX@7.N	NVCX@7.N
Security	WPA2-PSK	WPA-PSK	WPA/WPA2-PSK
Encryption Key	NVCX@7.N	NVCX@7.N	NVCX@7.N
AP Control Channel	-	-	6 or 36, Dual band use 36
AIFS	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
Cwmin	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
Cwmax	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	DSCP	DSCP	Default for AP
Channel Width	0 (20 MHz)		

Table 58: Traffic Differentiation in Single BSS with WMM STA Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names for 1x1 APUTs	Script Names for non-1x1 APUTs
RTP1	IPTV13Mbps.scr	IPTV22Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV18Mbps.scr
RTP3	IPTV8MbpsDelay10sec.scr (with delay)	IPTV14MbpsDelay10sec.scr (with delay)

Table 59: Traffic Differentiation in Single BSS with WMM STA Test Scripts

Note: The following table defines the scripts used for Non 11n APUT**Script**

	Script Names	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	Testbed 802.11a/b/g WMM Capable STA2	APUT	Expected Results
0	Configure the STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	-		
1			Beacon	
2	Probe Request	Probe request	Probe Response	SN: If a Probe Request occurs and Probe Response contains WMM parameter element, Pass
3	Association Request	Association request	Association Response	SN: If Association Response contains WMM parameter element AND STA Associated, PASS
4	Receive RTP1_BE, RTP2_VI	Receive RTP3_BE	Transmit RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
5	Receive RTP1_BE, RTP2_VI	Transmit RTP3_BE	Transmit RTP1_BE RTP2_VI Receive RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BE, RTP2_VI	Receive RTP3_BE	Receive RTP1_BE RTP2_VI Transmit RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
7	Receive RTP1_VI, RTP2_VO	Receive RTP3_VI	Transmit RTP1_VI RTP2_VO RTP3_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
8	Receive RTP1_VI, RTP2_VO	Transmit RTP3_VI	Transmit RTP1_VI RTP2_VO Receive RTP3_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
9	Receive RTP1_BK, RTP2_BE	Receive RTP3_BK	Transmit RTP1_BK RTP2_BE RTP3_BK	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
10	Receive RTP1_BK, RTP2_BE	Transmit RTP3_BK	Transmit RTP1_BK RTP2_BE Receive	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more

			RTP3_BK	than RTP2 in first phase (1~9s), PASS

Table 60: Traffic Differentiation in Single BSS with WMM STA Procedure and Results

4.2.23 Traffic Differentiation in Single BSS with Legacy Non-WMM STA

Purpose and Description

WMM capability negotiation should indicate one802.11n STA, in legacy mode, and one legacy Non-WMM STA.

The fairness tests address the remaining four of the 20 possible DUT-background traffic pairings.
The test procedure differs from the differentiation tests only in the method by which the link is saturated with traffic. The fairness tests require two sources (one from the DUT and the other from the tested) of equal AC traffic with the total intended load to exceed the channel capabilities. The two equal-AC traffic come from sources with identical characteristics (e.g., two identical RTP streams), because it is much easier to observe the equal change in frame rate of the streams when the link is saturated.

Test Environment

APUT
STA1: Testbed 802.11n in legacy mode WMM on
STA2: Testbed 802.11a/b/g (legacy) WMM off
Wireless Sniffer
STAs 1 & 2 are 11n devices operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Broadcom**	**Intel**	-
AP Control Channel	-	-	6 or 36, Dual band use 6
AIFS	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
Cwmin	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
Cwmax	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	DSCP	N/A	Default for AP
Channel Width	-	-	-
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678

Table 61: Traffic Differentiation in Single BSS with Legacy Non-WMM STA Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV18Mbps.scr
RTP2	IPTV14Mbps.scr
RTP3	IPTV14MbpsDelay10sec.scr

Table 62: Traffic Differentiation in Single BSS with Legacy Non-WMM STA Test Scripts

Note: The following table defines the scripts used for Non 11n APUT**Script**

	Script Name	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Tested 802.11n in legacy mode with WMM STA1	Testbed 802.11a/b/g STA2	APUT	Expected Results
1	-	-	Beacon	
2	Probe Request	Probe Request	Probe Response	SN: If a Probe Request occurs and Probe Response contains WMM parameter element, PASS
3	Association Request	Association Request	Association Response	SN: If Association Response to STA1 contains WMM parameter element AND STA1 Associated, PASS
4	Receive RTP1_BE, RTP2_VI	Receive RTP3_BE	Transmit RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
5	Receive RTP1_BE, RTP2_VI	Transmit RTP3_BE	Transmit RTP1_BE RTP2_VI Receive RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BE, RTP2_VI	Receive RTP3_BE	Receive RTP1_BE RTP2_VI Transmit RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
7	Receive RTP1_BE, Transmit RTP2_VI	Transmit RTP3_BE	Transmit RTP1_BE Receive RTP3_BE, RTP2_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP1 in second phase (11~19s) is 130% or less than RTP3 in second phase (11~19s), PASS (fairness with legacy test)

Table 63: Traffic Differentiation in Single BSS with Legacy Non-WMM STA Procedure and Results

4.2.24 APUT "No Acknowledgement" Test

Purpose and Description
Verify APUT operates correctly when it receives QoS packets with "No Acknowledgement".

The tested transmitter is configured to set the ACK policy to "No Acknowledgement" in the QoS control field of a traffic stream. A sniffer is used to verify that Acknowledgement packets are not being sent by the DUT. The throughput with the ACK policy set to "No Acknowledgement" is compared with the ACK Policy set to Acknowledgement. The test passes if the throughput is the same or higher.

Test Environment
APUT
STA1: Testbed 802.11a/b/g WMM Capable
Sniffer 11n
STA 1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	APUT Values
Vendor	**Marvell**	-
ESSID	alvhy%@_	alvhy%@_
AP Control Channel	-	6 or 36, Dual band use 36
AIFS	Default (see Appendix D)	Default (see Appendix D)
CWmin	Default (see Appendix D)	Default (see Appendix D)
CWmax	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	0
ACM: AC_VI	-	0
ACM: AC_BE	-	0
ACM: AC_BK	-	0
AC Tagging	DSCP	Default for AP
Security	WPA2-PSK	WPA2-PSK
Encryption Key	alvhy%@_	alvhy%@_

Table 64: APUT "No Acknowledgement" Test Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV14MbpsNoAck.scr
RTP2	IPTV10MbpsNoAck.scr

Table 65: APUT "No Acknowledgement" Test Scripts

Note: The following table defines the scripts used for Non 11n APUT

Script	Script Names	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14MbpsNoAck.scr	IPTV3.5MbpsNoAck.scr
RTP2	IPTV10MbpsNoAck.scr	IPTV2.8MbpsNoAck.scr
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results
The following table defines the test procedures and expected results. STA1 is put in its 11n mode for this test with 11n optional features disabled.

Steps	Testbed 802.11a/b/g WMM Capable STA1	APUT	Expected Results
1	-	Beacon	
2	Probe request	Probe Response	SN: If a Probe Request occurs and Probe Response contains WMM parameter element, Pass
3	Association Request	Association Response	SN: If Association Response contains WMM parameter element AND STA Associated, PASS
4	Transmit RTP1_BE RTP2_VI	Receive RTP1_BE, RTP2_VI	SN: QoS Data frame Verify ACK policy bits are set to “Acknowledge” in packets from STA. If APUT generates ACK packets, PASS. CH: Receive Data RTP1 and RTP2 Record values of RTP1 and RTP2 throughput
5	Configure the tested STA to set the “ACK policy” field to “01_2” (no acknowledgement) in QoS Control frames		
6	Transmit RTP1_BE RTP2_VI	Receive RTP1_BE, RTP2_VI	SN: QoS Data frame Verify ACK policy bits are set to “No Acknowledge” in packets from STA. If APUT does not generate ACK packets, PASS. CH: Receive Data RTP1 and RTP2 If RTP1-T06 and RTP2-T06 are 73% or more than RTP1-T04 and RTP2-T04 respectively, PASS

Table 66: APUT “No Acknowledgement” Test Procedure and Results

4.2.25 Traffic Forwarding in Single BSS

Purpose and Description
Traffic sent by the legacy STA to the WMM STA is transmitted as AC_BE (best effort) traffic from the APUT. Traffic sent in any QoS category from the WMM STA to the legacy STA is transmitted as legacy traffic.

In a given BSS with both 11n and legacy (non 11n/WMM) associated STAs, it is imperative that traffic between those two types of stations is forwarded correctly through the AP. A first Endpoint is setup on an 802.11n STA and a second Endpoint is setup on a legacy (non-WMM) STA. Traffic between the two endpoints must pass through the AP. The test passes if the packets are correctly formatted to the two STA and if throughput is suitable.

Test Environment
APUT
STA1: Testbed 802.11n 20 MHz
STA2: Testbed 802.11a/b/g (legacy)
Wireless Sniffer
STA 2 is an 11n device operating in legacy mode – WMM off
Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Broadcom**	**Intel**	-
AP Control Channel	-	-	6 or 36, Dual band use 6
AIFS	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmin	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmax	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	DSCP	DSCP	Default for AP
Channel Width	0 (20 MHz)		
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12354678	12345678	12345678

Table 67: Traffic Forwarding in Single BSS Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP2_BE	IPTV20Mbps-dn.scr
RTP1_BE, RTP2_VI , RPT2_BK	IPTV10Mbps-dn.scr

Table 68: Traffic Forwarding in Single BSS Test Scripts

Note: The following table defines the scripts used for Non 11n APUT

Script	Script Names	
	802.11g, 802.11a Equipment	802.11b Equipment
all RTP streams	IPTV10Mbps.scr	IPTV2.8Mbps.scr
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	Testbed 802.11a/b/g STA2	APUT	Expected Results
0	Configure STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.			
1	Transmit and receive Ping to STA2	-	-	If at least one ping reply is received then pass
2	-	Transmit and receive Ping to STA1	-	If at least one ping reply is received then pass
3	Receive RTP2_BE	Transmit: RTP2_BE	-	SN: In a RTP2_BE QoS Data frame with STA1 as the destination, if QoS Control Field UP=000_2 or 011_2, EOSP=0_2, ACKPOLICY=00_2 and the frame type=10_2, subtype 10002, PASS Traffic to/from a legacy STA shall not have QoS framing; if it has QoS framing, FAIL. CH: If Receive Data RTP2, PASS
4	Transmit RTP2_BK	Receive: RTP2_BK	-	SN: In a RTP2 Data frame with STA2 as the destination, if QoS Data Framing is not being used, PASS CH: If Receive Data RTP2, PASS
5	Transmit RTP2_BE	Receive RTP2_BE	-	SN: In a RTP2 Data frame with STA2 as the destination, if QoS Data Framing is not being used, PASS CH: If Receive Data RTP2, PASS
6	Transmit RTP1_BE RTP2_VI	Receive RTP1_BE RTP2_VI	-	CH: Receive Data RTP1_BE, RTP2_VI If RTP2 is 75% or more than RTP1, PASS

Table 69: Traffic Forwarding in Single BSS Procedure and Results

4.2.26 Basic Association in 802.11n Environment

Purpose and Description

Test Beacon/Probe Response, and Association response format and the existence of the appropriate information elements.
Testing association of 802.11n stations in pure 11n network as well as legacy station in mixed network and the ability to have basic connection and pass traffic to all station type.
Verifying HT Protection Mode Operating Mode settings as advertised by AP.

Test Environment

(Use a screen room)
802.11n APUT
STA1: Testbed 802.11n 20/40MHz Capable STA
STA2: Testbed 802.11n 20 MHz only Capable STA
STA3: Testbed 802.11ag STA
Wireless 802.11n Sniffer
STA 3 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	STA2 Values	STA3 Values	APUT Values
Vendor	**Realtek**	**Broadcom**	**Intel**	-
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678	12345678
AP Control Channel	-	-	-	1 or 36, dual band use 1 and 36 (one test run in each channel)
Supported channel width set	1 (20/40 MHz)	0 (20 MHz)	-	0 – For 20MHz Capable APUT 1 – For 20/40MHz Capable APUT

Table 70: Basic Association in 802.11n Environment Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1	Testbed 802.11n 20 MHz Capable STA2	Testbed 802.11ag Legacy STA3	802.11n APUT	Expected Results
1	Force STA1 to 20/40 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Force STA2 to 20 MHz only Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	-	Beacon	Look at the HT Capability IE and record the Supported Features [HT Capabilities Info Field] a. Supported Channel Width (20MHz, or 20/40MHz)* b. HT-Greenfield c. SGI 20 d. SGI 40 e. MCS Set (1 SS, 2 SS, or 3 SS) f. MCS 32 g. Tx STBC h. Rx STBC If the supported list does not match the submission then fail. *If 20/40 MHz supported in 2.4 GHz then 20/40 MHz Coexistence support is required
2	Association Request			Association Response to STA1	If the Association Response does not contain a SUCCESS status then fail. Look at the HT Information Element If the HT Protection Field is not 0 (no protection mode) or 3 (non-HT mixed mode) then fail.
3				Start a continuous Ping to STA1 (ping <STA1-IPaddress> -l 10000 -t)	If more that 10% ping failures, then fail.
4		(After 30 seconds) Association Request		Association Response to STA2	
5				Start a continuous Ping to STA2 (ping <STA2-IP address> -l 10000 -t)	If more that 10% ping failures, then fail. If the ping for STA1 is stopped then fail
6			(After 30 seconds) Association Request	Association Response to STA3	
7				Start a continuous Ping to STA3 (ping <STA3-IPaddress> -l 10000 -t)	1. If Association Response does not contain a SUCCESS status then fail. 2. Look at the HT Information Element

					If the HT Protection Field is not 3 (non-HT Mixed mode) then fail.
8	(after 30 seconds) Disassociate			Stop pings to STA 1	Nothing should change
9			(after 30 seconds) Disassociate	Stop pings to STA3	If the APUT HT Protection Field is not changed to 0 (no protection mode) or 2 (20MHz protection mode) or 3 (non-HT mixed mode), then fail
10		(After 30 seconds) Disassociate		Stop pings to STA2	If the APUT HT Protection Field is not changed to 0 (no protection mode) or 3 (non-HT mixed mode), then fail.

Table 71: Basic Association in 802.11n Environment Procedure and Results

4.2.27 Ability to Receive 1 and 2 Spatial Streams

Purpose & Description
Confirm that the APUT supports 1 and 2 SS on Rx side.

Test Environment
802.11n APUT
STA1: Testbed 802.11n 20/40 MHZ Capable

Test Configuration
The following table defines the parameter values for the devices in the test bed. Devices being certified under the 1x1 AP program are not required to execute the 2SS portion of this test.

Parameter	STA1 Values	APUT Values
Vendor	**Intel**	-
Security	**-**	Open if supported, otherwise WPA2-PSK 12345678
AP Control Channel	-	1 or 36, dual band use 1 and 36 (steps 1-2 should be run in each channel)

Table 72: Ability to Receive 1 and 2 Spatial Streams Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1	802.11n APUT	Expected Results
For i = 7,and i = 15 execute the following steps			
1	Set the testbed STA fixed TX rate to MCS[i] (20MHz only) Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2	Ping <IP> -t –l 10000		If more that 10% ping failures, then fail.
If the APUT is a 20/40MHz capable AP, then execute steps 3 and 4: For i = 7,and i = 15 execute the following steps			
3	Set the tested STA fixed TX rate to MCS[i] (40MHz) Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
4	Ping <IP> -t –l 10000		If more that 10% ping failures, then fail.

Table 73: Ability to Receive 1 and 2 Spatial Stream Procedure and Results

4.2.28 Spatial Multiplexing Power Save Operation

Purpose and Description

Check that APUT sends out RTS before transmitting MIMO sequences to a STA when it associates in Dynamic SM Power Save Mode.
Verify the association of STAs in Different SM Power Save Modes and the ability to pass traffic.
Check that APUT does not transmit MIMO sequences to a STA when it is in Static SM Power Save Mode.
Validate AP's Adherence to the STA SM Power Save Management Action Frame.
Test Coexistence of other STAs in different SM Power Save Mode.

Test Environment

802.11n APUT
STA1: Testbed 802.11n 20/40MHZ Capable STA
STA2: Testbed 802.11n 20/40MHZ Capable STA
Wireless 802.11n Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Broadcom**	**Marvell**	-
AP Control Channel			1 or 36, Dual band 36
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678

Table 74: Spatial Multiplexing Power Save Operation Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1	Testbed 802.11n 20/40 MHz Capable STA2	802.11n APUT	Expected Results
1	Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Switch off all the optional features. Disable AMPDU and AMSDU aggregation and configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2			Beacon	
3	Association Request with Dynamic SM Power Save Mode	Association Request with Static SM Power Save Mode	Association Response to STA1 And STA2	
4			ping <IP of STA 1> -t –l 10000 ping <IP of STA 2> -t –l 10000	If more that 10% ping failures, then fail. STA1: If the rate of the ping requests to STA1 is MCS7 or less then pass. If the rate of the ping requests to STA1 is greater than MCS7 and the APUT uses RTS/CTS before each frame send then pass STA2: If the rate of the ping requests to STA2 is less MCS7 or less then pass
5	After 30 seconds Send SM Power save mode action frame to the APUT to switch from Dynamic SM Power Save Mode to Static SM Power Save Mode i.e. Enable Field = 1 and Mode Field is 0			Each STA: If more that 10% ping failures, then fail. STA1: If the rate of the ping requests to STA1 is MCS7 or less then pass
6	After 30 seconds Send SM Power save mode action frame to the APUT to switch from Static SM < Power Save Mode to No Limitation i.e. Enable Field = 0 and Mode Field is “don’t care”			Each STA: If more that 10% ping failures, then fail.
7	After 30 Seconds Send SM Power save mode action frame to the APUT to switch from No Limitation into Dynamic SM Power Save Mode i.e. Enable Field = 1 and Mode Field is 1			Each STA: If more that 10% ping failures, then fail. STA1: If the rate of the ping requests to STA1 is MCS7 or less then pass. If the rate of the ping requests to STA1 is greater than MCS7 and the APUT uses RTS/CTS before each frame send then pass

Table 75: Spatial Multiplexing Power Save Operation Procedure and Results

4.2.29 A-MPDU Aggregation when the AP is the Recipient with and without WPA2-PSK

Purpose and Description
Test Block ACK stream and A-MPDU aggregation traffic in receive side.
Test Single and Multiple Block ACK streams.
Test A-MPDU aggregation with and without WPA2-PSK security mode.

Test Environment
802.11n APUT
STA1: Testbed 802.11n 20 MHz capable
11n Sniffer

Test Configuration and Procedure
The following table defines the parameter values for the devices in the test bed.
Run all tests in 20 MHz bandwidth.
Run all tests in batch mode.
1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
ESSID	Bdjfg^|tre	Bdjfg^|tre
Security	Open if supported & WPA2-PSK	Open if supported & WPA2-PSK
Encryption Key	bdjfg^|tre	bdjfg^|tre
AP Control Channel	-	1 or 36, Dual band use 36
Supported Channel Width Set	0 (20 MHz)	-

Table 76: A-MPDU Aggregation Single Stream when AP is the Recipient with and without WPA2-PSK Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	802.11n APUT	Expected Results
1	Set the testbed STA to operate in Manual Aggregation mode. Switch off all the optional features. Disable AMSDU aggregation.	No Security Beacon	Skip steps 1 to 4 if the APUT doesn't support Open security.
2	Association Request	Association Response to STA1	If the association response of STA 1 is with status different than success then fail
3	Send ADDBA request to APUT for TID 5	Send ADDBA Response to STA 1	
4	Start UDP Filesndl-HT on TID 5 for 30 seconds.		If Uplink throughput is less than 4.2.29T4DT2 then fail SN: Check that there are Block ACKs.
5	Set the testbed STA to operate in Manual Aggregation mode. Switch off all the optional features. Disable AMSDU aggregation.	Change security mode to WPA2-PSK Beacon	

6	Association Request	Association Response to STA1	If the association response of STA 1 is with status different than success then fail
7	Send ADDBA request to APUT for TID 5	Send ADDBA Response to STA 1	
8	Start UDP Filesndl-HT on TID 5 for 30 seconds.		If Uplink throughput is less than 4.2.29T8DT2 then fail SN: Check that there are Block ACKs

Table 77: A-MPDU Aggregation Single Stream when AP is the Recipient with and without WPA2-PSK Procedure and Results

4.2.30 A-MSDU Aggregation when AP is the Recipient

Purpose and Description

Test the mechanism of the A-MSDU Aggregation when the APUT is the recipient.

Test Environment

802.11n 20 MHz capable APUT
Testbed 802.11n 20/40 MHz capable STA That support both 3839 bytes and 7935 bytes Maximum A-MSDU Size in transmission
11n Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed.
1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
AP Control Channel	-	1 or 36, Dual band use 1
Security	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678

Table 78: A-MSDU Aggregation when AP is the Recipient Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1	802.11n APUT	Expected Results
1	Enable A-MSDU Aggregation. Switch off all the optional features. Disable A-MPDU Aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2	-	Beacon	
3	Association Request	Association Response	
4	Start UDP Filesndl-HT s from STA1 to APUT for 1.5 minutes Uplink 1		If Uplink1 throughput is less than 4.2.30T4DT2 then fail Note: Use sniffer to check that the STA1 packets are > 2346, if not then fail

Table 79: A-MSDU Aggregation when AP is the Recipient Procedures and Results

4.2.31 Overlapping BSS – 2.4 GHz

Purpose and Description
APUT will appropriately indicate the existence of and interoperate with the Overlapping BSS.

Test Environment
802.11n APUT
STA1: Testbed 802.11n 20 MHz Capable
AP2: Testbed 802.11g
STA2: Testbed 802.11g
Wireless Legacy Sniffer
STA 2 is an 11n device operating in legacy mode
AP2 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed. 5GHz only devices skip this test.1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	APUT Values	STA2 Values	AP2 Values
Vendor	**Realtek for 1 SS or 2SS APUT Broadcom for 3SS APUT**	**-**	**Broadcom for 1 SS or 2SS APUT Marvell for 3SS APUT**	**Broadcom for 1 SS or 2SS or 3 SS APUT**
AP Control Channel	-	6	-	6
Supported channel width set	0 (20 MHz)	0 (20 MHz)		-
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678	12345678

Table 80: Overlapping BSS – 2.4 GHz Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	802.11n APUT	Testbed 802.11g STA2	Testbed 802.11g AP2	Expected Results
1	Configure STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Set to channel 6		Set to channel 6	
2	-	Beacon/Probe responses		Beacon/Probe Responses	If the AP HT Protection Field is not 01 (non-member protection) or 03 (non-HT mixed mode) then fail
3	Association Request to APUT	Association response to STA1	Association Request to AP2	Association Response to STA2	
4		Start TCP High Performance Throughput from APUT to STA1 for 1 minute		Start TCP FileSndL from AP2 to STA2 for 1 minute	If throughput is less than 4.2.31T4DT1A then fail

					If throughput is less than 4.2.31T4DT1B then fail

Table 81: Overlapping BSS – 2.4 GHz Procedure and Results

4.2.32 Overlapping BSS – 5 GHz

Purpose and Description
APUT will appropriately indicate the existence and interoperate with the Overlapping BSS.

Test Environment
802.11n APUT
STA1: Testbed 802.11n 20 MHZ Capable
AP2: Testbed 802.11a
STA2: Testbed 802.11a
Wireless Legacy Sniffer
STA 2 is an 11n device operating in legacy mode
AP2 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed. 2.4 GHz only devise skip this test. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	APUT Values	STA2 Values	AP2 Values
Vendor	**Realtek for 1 SS or 2SS APUT Intel for 3SS APUT**	-	**Broadcom for 1 SS or 2SS APUT Marvell for 3SS APUT**	**MediaTek for 1 SS or 2SS APUT Qualcomm for 3SS APUT**
AP Control Channel	-	36	-	36
Supported channel width set	0 (20 MHz)	0 (20 MHz)	-	-
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678	12345678

Table 82: Overlapping BSS – 5 GHz Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	802.11n APUT	Testbed STA2	Testbed 802.11a AP2	Expected Results
1	Configure STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Set to channel 36		Set to channel 36	
2	-	Beacon/Probe responses		Beacon/Probe Responses	If the AP HT Protection is not 01 (non-member protection) or 03 (non-HT mixed mode) then fail

3	Association Request to APUT	Association response to STA1	Association Request to AP2	Association Response to STA2	
4		Start TCP High Performance Throughput from APUT to STA1 for 1 minute		Start TCP FileSndL from AP2 to STA2 for 1 minute	If throughput is less than 4.2.32T4DT1A then fail If throughput is less than 4.2.32T4DT1B then fail

Table 83: Overlapping BSS – 5 GHz Procedure and Results

4.2.33 HT-Greenfield Operation

Purpose and Description

APUT is appropriately receiving HT-Greenfield packets.
APUT appropriately indicate the existence of Non- HT-Greenfield devices associated.
APUT will use protection before transmitting HT-Greenfield packets when non-HT-GF devices are associated.

Test Environment

802.11n APUT
STA1: Testbed 802.11n 20/40 MHz Capable (HT-GF enabled)
STA2: Testbed 802.11n 20/40 MHz Capable (HT-GF disabled)
Wireless 802.11n Sniffer
Run in a clean environment (Chamber)

Test Configuration

The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Marvell**	**Realtek**	-
ESSID	*BDAFEpzyc	*BDAFEpzyc	*BDAFEpzyc
AP Control Channel	-	-	1 or 36, Dual band use 1
Supported channel width set	0 (20 MHz)	0 (20 MHz)	-
HT-Greenfield	1	0	1
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	*BDAFEpzyc	*BDAFEpzyc	*BDAFEpzyc

Table 84: HT-Greenfield Operation Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	Testbed 802.11n 20 MHz Capable STA2	802.11n APUT	Expected Results
1	Enable HT-GF Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2	-		Beacon	

3	Association Request		Association Response to STA1	If the non-GF bit in Beacon is set then fail
4	Ping <APUT IP> -l 10000 -t			If more that 10% ping failures, then fail.
5		Association Request	Association Response to STA2	If the non-GF bit in Beacon is not set then fail
6	Ping <APUT IP> -l 10000 -t	Ping <APUT IP> -l 10000 -t		If more that 10% ping failures, then fail. Use sniffer to confirm that the APUT uses active protection or sends frames with mixed-mode preamble
		Disassociate		If the non-GF bit in Beacon is set, then fail

Table 85: Greenfield Operation Procedure and Results

4.2.34 Short GI Operation

Purpose and Description
APUT is appropriately receiving Short GI.
APUT can communicate with stations that do and do not support short GI simultaneously.

Test Environment
802.11n APUT
STA1: Testbed 802.11n 20/40 MHz Capable (Support SGI)
STA2: Testbed 802.11n 20/40 MHz Capable (Does NOT support SGI)

Test Configuration
The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Intel**	**Broadcom**	-
ESSID	/QIRPxwno	/QIRPxwno	/QIRPxwno
AP Control Channel	-	-	1 or 36, Dual band use 36
Supported Channel Width Set	0 if APUT supports SGI at 20 MHz, otherwise use 1	Same as STA1	-
SGI	1	0	1
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	/QIRPxwno	/QIRPxwno	/QIRPxwno

Table 86: Short GI Operation Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1 with SGI enabled	Testbed 802.11n 20Mhz Capable STA2 NOT SGI capable	802.11n APUT	Expected Results
1	Enable SGI Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2	-		Beacon/Probe responses	
3	Association Request		Association response to STA1	
4	Ping <APUT IP> -l 10000 -t			If more that 10% ping failures, then fail.
5		Association Request	Association response to STA2	
6	Ping <APUT IP> -l 10000 -t	Ping <APUT IP> -l 10000 -t		If more that 10% ping failures, then fail.

Table 87: Short GI Operation Procedure and Results

4.2.35 Overlapping BSS on Extension Channel

Purpose and Description
APUT appropriately sense the extension channel before any 20/40 MHz transmission.

Test Environment
802.11n 20/40 MHz capable APUT
STA1: Testbed 802.11n 20/40MHz Capable
AP2: Testbed 802.11a
STA2: Testbed 802.11a
STA 2 is an 11n device operating in legacy mode
AP2 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	APUT Values	STA2	AP2 Values
Vendor	Realtek for 1SS or 2SS APUT Intel for 3SS APUT	-	Intel for 1 SS or 2SS APUT Marvell for 3 SS APUT	MediaTek for 1 SS or 2SS APUT Qualcomm for 3SS APUT
AP Control Channel	-	36	-	40
Supported channel width set	1 (20/40 MHz)	1 (20/40 MHz)	-	-
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678	12345678

Table 88: Overlapping BSS on Extension Channel Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1	802.11n APUT	Testbed 802.11a STA2	Testbed 802.11a AP2	Expected Results
1	Set STA to 20/40 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Set to channels 36 and 40		Set to channel 40	
2	-	Beacon/Probe responses		Beacon/Probe responses	
3	Association Request to APUT	Association response to STA1	Association Request to the AP2	Association Response to the STA2	
4		Start TCP High Performance Throughput from APUT to STA1 for 1 minute		Start TCP FileSndL from AP2 to STA2 for 1 minute	If throughput is less than 4.2.35T4DT1A then fail If throughput is less than 4.2.35T4DT1B then fail

Table 89: Overlapping BSS on the Extension Channel Procedure and Results

4.2.36 HT Duplicate Mode (MCS Index = 32)

Purpose and Description
APUT is ability to receive HT-Duplicate Mode when it is advertised.

Test Environment
802.11n APUT
STA1: Testbed 802.11n 20/40MHZ Capable (Support MCS 32)

Test Configuration
The following table defines the parameter values for the devices in the test bed.
Run tests in 20/40 or 40 MHz bandwidth (AP & STA).1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
ESSID	ROQP96'us	ROQP96'us
AP Control Channel	-	1 or 36, dual band 36
Supported channel width set	1 (20/40 MHz)	1 (20/40 MHz)
MCS index 32	1	1
Security	WPA2-PSK	WPA2-PSK
Encryption Key	ROQP96'us	ROQP96'us

Table 90: HT Duplicate Mode (MCS Index = 32) Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1	802.11n APUT	Expected Results
1	-	Beacon/Probe responses	
2	Association Request	Association response	
3	Set the tested STA to send data with fixed MCS index 32 (20/40 MHz). Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
4	Ping <APUT IP> -l 10000 -t		If the ping does not go through for 1 minute then fail

Table 91: HT Duplicate Mode (MCS Index = 32) Procedure and Results

4.2.37 AP Concurrent Operation in 2.4 and 5 GHz Frequency Bands

Purpose and Description

APUT is concurrently operating at 2.4 and 5 GHz.
APUT is passing traffic in both 2.4 and 5 GHz.

Test Environment

802.11n APUT
STA1: Testbed 802.11n 20/40MHz capable operating at 2.4 GHz
STA2: Testbed 802.11n 20/40MHz capable operating at 5 GHz

Test Configuration
The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	STA2 Values	APUT Values
Vendor	**Broadcom**	**Marvell**	-
AP Control Channel	1	36	1 and 36 at the same time
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678

Table 92: AP Concurrent Operation in 2.4 and 5 GHz Frequency Bands Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA1	Testbed 802.11n 20/40 MHz Capable STA2	802.11n APUT	Expected Results
1	Force the Testbed STA to tune to 2.4 GHz band only Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Force the testbed STA to tune to 5 GHz band only Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2	-		Beacon	
3	Association Request		Association Response to STA1	
4		Association Request	Association Response to STA2	
5			Beacon/Probe Response	If both STA1 and STA2 associate, then pass
6	Start TCP Filesndl-HT to STA2 for 1 minute	Receive TCP Filesndl-HT		If STA1 -> STA2 throughput is greater than 4.2.37T6DT2 then pass
7	Receive Filesndl-HT	Start TCP Filesndl-HT to STA1 for 1 minute		If STA2 -> STA1 throughput is greater than 4.2.37T7DT2 then pass

Table 93: AP Concurrent Operation in 2.4 and 5 GHz Frequency Bands Procedure and Results

4.2.38 RIFS Test

Purpose and Description
APUT is appropriately receiving RIFS packets in 20 MHz.
APUT is appropriately receiving RIFS packets in 20/40 MHz.

Test Environment
802.11n APUT
Testbed 802.11n 20/40MHz Capable STA (RIFS enabled)
Sniffer 11n

Test Configuration
The following table defines the parameter values for the devices in the test bed.
Run test for 100 pings with length of 30,000 bytes

The test is run multiple times with the testbed RIFS transmitter as outlined in tables121, 122, and 123.2.4 GHz single band devices use row 1, 5 GHz single band devices use row 2, and dual band devices use row 3. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Device Capability	RIFS Transmit
Single band – 2.4 GHz, 20 MHz	Run test 20 MHz
Single band – 5 GHz, 20 MHz, 40 MHz, 20/40 MHz	Run test 20/40 MHz
Dual band – 2.4 GHz & 5 GHz, 20 MHz, 40 MHz, 20/ 40 MHz	Run test at 5 GHz, 20/40 MHz

Table 94: RIFS Test Configurations

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
ESSID	YWZUTikm	YWZUTikm
AP Control Channel	NA	1 or 36
Green Field	0	0
MCS rates	For 1x1 APs, use MCS4. For all other APs, use MCS12	NA
Security	WPA2-PSK	WPA2-PSK
Encryption Key	YWZUTikm	YWZUTikm

Table 95: RIFS Operation Configuration

Test Procedure and Expected Results[3]
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA	802.11n APUT	Expected Results
1	Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2	Association Request	Association Response to STA1	
3	Start a long packet ping to Endpoint 1. Ping xx.xx.xx.xx –l 30000 –v 160 –n 100		The number of lost pings should be less than 30% SN. Check that there are no ACKs during RIFS frame sequence

Table 96: RIFS Operation Procedure and Results

4.2.39 STBC Transmit (2x1) Test

Purpose and Description
APUT is appropriately supporting Tx 2x1 STBC.
APUT can simultaneously communicate with stations with and without STBC.

Test Environment
802.11n APUT
STA1: Testbed 802.11n 20 MHz Capable w/ STBC disabled
STA2: Testbed 802.11n 20/40 MHz Capable w/ STBC enabled

[3]For 1x1 devices use MCS 4

STBC capable wireless 802.11 Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed. 1x1 APs cannot be tested using this procedure.

Parameter	STA1 Values	STA2 Values	802.11n APUT Values
Vendor	Broadcom	Marvell	-
AP Control Channel	NA	NA	1 or 36
Supported Channel Width Set	1	1	0 – For 20 MHz Capable APUT 1 – For 20/40 MHz Capable APUT (5 GHz)
Supported MCS Set	0-7	0-7	NA
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678

Table 97 STBC Tx (2x1) Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1 Not STBC Capable	Testbed 802.11n 20/40Mhz Capable STA2 STBC Capable	802.11n APUT	Expected Results
1	Force the Testbed STA to disable STBC	Force the Testbed STA to enable STBC	Enable STBC capability	
2	-		Beacon/Probe responses	If Tx STBC bit of HT Capability Info field in the Beacon is not set then fail
3	Association Request		Association response	If STA1 association fails, then fail
4		Association Request	Association response	If STA2 association fails, then fail
5			Ping STA1 (ping STA1 IP –t)	If ping request is not successful within 90 seconds then fail. Ping Request - Verify STBC field of HT_SIGNAL is ‘00’ using wireless sniffer
6			Ping STA2 (ping STA2 IP –t)	If ping is not successful within 90 seconds then fail. Ping Request - Verify STBC field of HT_SIGNAL is non-zero using wireless sniffer

Table 98STBC Tx (2x1) Test Procedure and Results

4.2.40 A-MPDU Aggregation when the AP is the Transmitter

Purpose and Description
Test the mechanism of A-MPDU Aggregation when the APUT is the transmitter.

Reference
TBD

Test Environment

802.11n APUT
Testbed 802.11n STA that supports 1 Stream configuration
Testbed 802.11n STA that supports 2 Stream configuration
Testbed 802.11n STA that supports 3 Stream configuration
Wireless 802.11n Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	STA2 Values	STA3 Values	APUT Values
Vendor	**Marvell**	**Broadcom**	**Broadcom**	-
ESSID	Iq9865hfg|?	Iq9865hfg|?	Iq9865hfg|?	Iq9865hfg|?
Security	-	-	-	open if supported, otherwise WPA2-PSK Iq9865hfg|?
Spatial Stream Support	1	2	3	-
Channel width	0	0	0	-
Short GI	Disabled	Disabled	Disabled	-
Green Field	Disabled	Disabled	Disabled	-
AP Control Channel	NA	NA	NA	1 or 36
WMM Power Save	Enabled for all ACs	disabled	disabled	OOB

Table 99: A-MPDU Aggregation when the AP is the Transmitter Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	Testbed 802.11n 20 MHz Capable STA2	Testbed 802.11n 20 MHz Capable STA3	802.11n APUT	Expected Results
1	Association request			Association response	
2	Send ADDBA response to APUT			Send ADDBA request to STA1 on TID6	
3				Start UDP Filesndl-HT on TID6 to STA1 x 4 pairs (Downlink 1)	If the downlink 1 throughput is less than 4.2.40T3DT1 then fail If sniffer doesn't indicate downlink traffic is aggregated (A-MPDU) than fail
4		Association request		Association response	
5		Send ADDBA response to APUT		Send ADDBA request to STA2 on TID6	
6				Start UDP Filesndl-HT on TID6 to STA2 x 4 pairs (Downlink 2)	If the downlink 2 throughput is less than 4.2.40T6DT1 then fail If sniffer doesn't indicate downlink traffic is aggregated (A-MPDU) than fail
7					If APUT supports more than 2 Spatial streams transmission than continue, else stop test
8		Association request		Association response	
9			Send ADDBA response to APUT	Send ADDBA request to STA3 on TID6	

10				Start UDP Filesndl-HT on TID6 to STA3 x 4 pairs (Downlink 3)	If the downlink 3 throughput is less than 4.2.40T10DT1 then fail If sniffer doesn't indicate downlink traffic is aggregated (A-MPDU) than fail

Table 100: A-MPDU Aggregation when the AP is the Transmitter Procedure and Results

4.2.41 AP 20/40 MHz Coexistence

Purpose and Description

APUT is not starting a 40 MHz BSS in presence of an 802.11g BSS.
APUT is appropriately switching from 40 MHz to 20 MHz in presence of 40 MHz intolerant STA.
APUT is appropriately switching from 40 MHz to 20 MHz when receiving frames disallowing the use of 40 MHz channel width.

Test Environment

802.11n APUT
STA1: Testbed 802.11n 20/40 MHz Capable
AP2: Testbed 802.11g
Wireless 802.11n Sniffer
AP2 is an 11n device operating in legacy g mode

Test Configuration

The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	Testbed 11n STA1 Values	Testbed 11g AP2 Values	APUT Values
Vendor	**Realtek**	**Qualcomm**	-
Security	-	-	Open if supported, otherwise WPA2-PSK 12345678
Supplicant/Server	-	-	-
AP Primary Channel	-	7	5
Supported channel width set	1 (20/40 MHz)	-	1 (20/40 MHz)

Table 101: 20/40 MHz Coexistence Channel Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable STA	Testbed 11g AP	802.11n APUT	Expected Results
1		Power up testbed AP Association Response		
2			Power up APUT Attempt to set the APUT to use 20/40 MHz	If the “STA Channel Width” or “Secondary Channel Offset” field of HT Operation Element in the Beacon is not set to 0 then fail Wait up to 200 seconds after test bed AP starts beaconing

				for the HT Operation Element in the Beacon to be set to 0.
3		Power down testbed AP	Reset the APUT Set the APUT to 20/40MHz Set the primary channel to 5 Set the secondary channel to 1. If the secondary channel cannot be set to 1, set the secondary channel to 9.	If the "Supported Channel Width" Set field of HT Capability element in the Beacon is not set to 1 then fail Wait up to 200 seconds for BW to change. If the secondary channel is set to 1 and the "Secondary Channel Offset" field of HT Operation Element in the Beacon is not set to 3 then fail If the secondary channel is set to 9 and the "Secondary Channel Offset" field of HT Operation Element in the Beacon is not set to 1 then fail If the "STA Channel Width" field of HT Operation Element in the Beacon is not set to 1 then fail
4	Set the "40 MHz Intolerant" field of the HT Capability Info field to 1 Association Request		Association Response ping <STA_IP> -l 10000 –t	If STA cannot associate then fail If the "STA Channel Width" or "Secondary Channel Offset" fields of HT Operation Element in the Beacon is not set to 0 then fail Once associated, if more that 10% ping failures, then fail. If 20/40 supported coexistence bit in Extended Capabilities IE for Association Response from the AP is not set than fail
5	Disassociate Set the "40 MHz Intolerant" field of the HT Capability Info field to 0		Reset the APUT Set the APUT to 20/40MHz	
6	Association Request		Association Response ping <STA_IP> -l 10000 –t	If STA cannot associate then fail If the "STA Channel Width" field of HT Operation Element in the Beacon is not set to 1 then fail If the secondary channel is set to 1 and the "Secondary Channel Offset" field of HT Operation Element in the Beacon is not set to 3 then fail If the secondary channel is set to 9 and the "Secondary Channel Offset" field of HT

				Operation Element in the Beacon is not set to 1 then fail Once associated, if more that 10% ping failures, then fail.
7	Send a “20/40 BSS Coexistence” Management frame to AP that includes setting the “40 MHz Intolerant” field to 1			If the “STA Channel Width” or “Secondary Channel Offset” field of HT Operation Element in the Beacon is not set to 0 then fail Once associated, if more that 10% ping failures, then fail.
8	Disassociate Set the “40 MHz Intolerant” field of the HT Capability Info field to 0		Reset the APUT Set the APUT to 20/40MHz	
9	Association Request		Association Response ping <STA_IP> -l 10000 –t	If STA cannot associate then fail If the “STA Channel Width” field of HT Operation Element in the Beacon is not set to 1 then fail If the secondary channel is set to 1 and the “Secondary Channel Offset” field of HT Operation Element in the Beacon is not set to 3 then fail If the secondary channel is set to 9 and the “Secondary Channel Offset” field of HT Operation Element in the Beacon is not set to 1 then fail If there are no ping replies then fail.
10	Send a “20/40 BSS Coexistence” Management frame to AP that includes setting the “20 MHz BSS Width Request” to 1			If the “STA Channel Width” or “Secondary Channel Offset” field of HT Operation Element in the Beacon is not set to 0 then fail Once associated, if more that 10% ping failures, then fail.
11	Disassociate Set the “40 MHz Intolerant” field of the HT Capability Info field to 0		Reset the APUT Set the APUT to 20/40MHz	
12	Association Request		Association Response ping <STA_IP> -l 10000 –t	If STA cannot associate then fail If the “STA Channel Width” field of HT Operation Element in the Beacon is not set to 1 then fail

				If the secondary channel is set to 1 and the "Secondary Channel Offset" field of HT Operation Element in the Beacon is not set to 3 then fail If the secondary channel is set to 9 and the "Secondary Channel Offset" field of HT Operation Element in the Beacon is not set to 1 then fail If more that 10% ping failures, then fail.
13	Send a "20/40 BSS Coexistence" Management frame containing one "20/40 BSS Intolerant Channel Report" element to AP that includes channel 3 in its channel list			If the "STA Channel Width" or "Secondary Channel Offset" field of HT Operation Element in the Beacon is not set to 0 then fail If more that 10% ping failures, then fail.

Table 102: 20/40 Coexistence Operation Procedure and Results

4.2.42 Ability to Receive 3 Spatial Streams

Purpose and Description
Confirm that the APUT supports 3 SS on Rx side.

Test Environnent
802.11n APUT
STA1: Testbed 802.11n Capable (Support 3 streams)

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	APUT Values
Vendor	**Broadcom**	-
AP Control Channel	-	1 or 36, Dual Band use 1 &36
Supported Channel Width Set	0 (20 MHz)	-
Security	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678

Table 103: Ability to Receive 3 Spatial Streams Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results. Note: Dual band devices run test twice (channel 1 and then channel 36).

Steps	Testbed 802.11n 20/40 MHz Capable STA1	802.11n APUT	Expected Results
1	Switch off all the optional features. Disable A-MPDU and A-MSDU aggregation. Configure the STA to reject any ADDBA request by	Beacon/Probe responses	If the APUT supported MCS set field in the HT Capability IE does not contain 1 in the bitmap indexes 16-23 (3 SS) then fail

	sending ADDBA response with status DECLINE.		
2	Association Request	Association response	
For i = 23			
3	Set the testbed STA fixed TX rate to MCS[i] (20 MHz only)		
4	Ping <console IP> -t –l 10000		If more that 10% ping failures, then fail..
If the APUT does not support 40 MHz in 2.4 GHz, skip steps 5 and 6 for 2.4 GHz If the APUT does not support 40 MHz in 5 GHz, skip steps 5 and 6 for 5 GHz For i = 23			
5	Set the testbed STA fixed Tx Rate to MCS[i] (40MHz)		
6	Ping < console IP> -t –l 10000		If more that 10% ping failures, then fail.

Table 104: Ability to Receive 3 Spatial Stream Procedure and Results

4.2.43 AP Transmitting to STA using Supported Number of Spatial Streams

Purpose and Description

Test the APUT transmits using the correct number of spatial streams as advertised by the STA.

Reference

Test Environment

802.11n APUT
STA1: Testbed 802.11n STA that supports 1 Stream configuration
STA2: Testbed 802.11n STA that supports 2 Stream configuration
STA3: Testbed 802.11n STA that supports 3 Stream configuration
Wireless 802.11n Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	STA2 Values	STA3 Values	APUT Values
Vendor	**Marvell**	**Broadcom**	**Intel**	-
Security				Open if supporterd, otherwise WPA2-PSK ioPL98=2bv
ESSID	ioPL98=2bv	ioPL98=2bv	ioPL98=2bv	ioPL98=2bv
Spatial Stream Support	1	2	3	
AP Control Channel	NA	NA	NA	1 or 36, Dual Band use 1 and 36 (run test twice, once per channel)
Supported Channel Width Set	0 (20 MHz)	0 (20 MHz)	0 (20 MHz)	-

Table 105: AP Transmitting To STA using Supported Number of Spatial Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20 MHz Capable STA1	Testbed 802.11n 20 MHz Capable STA2	Testbed 802.11n 20 MHz Capable STA3	802.11n APUT	Expected Results
1	Switch off all the optional features.	Switch off all the optional features.	Switch off all the optional features.	Sends Beacon indicating	

	Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	supported MCS rate	
2	Association Request with MCS support are 0 to 7			Association Response	
3				ping <STA1_IP> -n 100 –l 1000	If more that 10% ping failures, then fail. Use the sniffer to check that the APUT transmitted at least 10 ping requests at data rates that are equal to or greater than 52 Mbps (MCS = 5) then pass If the APUT transmitted any ping request at MCS greater than 7 then fail.
If APUT's maximum supported MCS rate in step 1 equals 7 then end test. Otherwise proceed with steps 4 and 5					
4		Association Request with MCS support rates are 0 to 15		Association Response	
5				ping <STA2_IP> -n 100 –l 1000	If more that 10% ping failures, then fail. Use the sniffer to check that the APUT transmitted at least 10 ping requests at data rates that are equal to or greater than 104 Mbps (MCS = 13) then pass If the APUT transmitted any ping request at MCS greater than 15 then fail
If the APUT's maximum supported MCS rate in step 1 equals 15 then end test. Otherwise proceed with steps 6 and 7					
6			Association Request with MCS support rates are 0 to 23	Association Response	
7				ping <STA3_IP> -n 100 –l 1000	If more that 10% ping failures, then fail. Use the sniffer to check that the APUT transmitted at least 10 ping requests at data rates that are equal to or greater than 156 Mbps (MCS = 21) then pass

Table 106: AP Transmitting To STA using Supported Number of Spatial Procedure and Results

4.2.44 Disallow TKIP with HT Rates Test

Purpose and Description
Ensure that the APUT does not use HT rates when using TKIP as the encryption cipher. Note: If the APUT supports only WPA2 and not WPA, this test is skipped.

Test Environment
802.11n APUT
STA1 11n station
Wireless 802.11n sniffer
STA1 has the ability to set TKIP + HT

Test Configuration
The following table defines the parameter values for the devices in the test bed. 1x1, 2x2, & 3x3 APs can be tested using this procedure.

Parameter	STA1 Values	APUT Values
Vendor	**Marvell**	
ESSID	Sdfw(*%@12	Sdfw(*%@12
AP Channel	-	36 or 11

Table 107: Disallow TKIP with HT Rates Test Configuration

WPA2-PSK/WPA-PSK Mixed Mode Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Step	Action	Results
1	Set up the APUT with HT and mixed mode WPA-PSK/WPA2-PSK.	If the UI on the APUT prohibits the configuration of WPA-PSK/WPA2-PSK when HT is enabled, the APUT fails the test. Skip the remaining steps. (The APUT in mixed mode must allow the use of WPA-PSK with TKIP, but no HT rates are allowed in this case. HT rates are only allowed with WPA2-PSK using AES (CCMP)).
2	Associate the test bed STA to the APUT with the STA configured for HT and WPA-TKIP. Using the 11n sniffer, look at the Association Request from the test bed STA.	Verify that the Association Request from the test bed STA contains IE 45 and that the pairwise cipher suite requested is TKIP. If not, there is a test bed problem. Correct the configuration and restart test.
3	Using the 11n sniffer, look at the Association Response from the APUT.	If the Association Response from the APUT contains a non-zero status code, the APUT passes the test. Skip the remaining steps. If the Association Response from the APUT contains IE 45 and the status code is zero, the APUT fails the test. Skip the remaining steps. If the Association Response from the APUT does not contain IE 45 and the status code is zero, continue to the next step.

4	Run a test script that emulates a long file transfer from a PC on the wired Ethernet side of the APUT to the associated test bed STA for at least 10 seconds.	
5	Using the 11n sniffer, collect 10 seconds of data packets.	If any of the data packets from the APUT are sent at HT rates, the APUT fails the test. Skip the remaining steps. If all of the data packets from the APUT are sent at non-HT rates, the APUT passes the test.
6		

Table 108: Disallow TKIP with HT Rates, WPA2-PSK/WPA-PSK Test Procedure and Results

4.2.45 AP Negative tests to ensure WEP is not used with HT associations in 11n devices

Purpose and Description
The 11n test bed station must allow association using WEP with HT. Note that this is a special capability, and is for testing purposes only.

Mandatory test if WEP is implemented on the 11n APUT.

Test Environment
802.11n APUT
STA 11n test bed station
Wireless 802.11n sniffer
STA has the ability to set WEP + HT

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA values	APUT values
Vendor	Broadcom	-
ESSID	NGJ750@	NGJ750@
AP channel	-	36 or 11
Security	-	WEP
Encryption Key	-	0x9876543210

Table 109AP Negative WEP Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Step	Action	Results
1	Set up the APUT with HT and WEP.	If the UI on the APUT prohibits the configuration of WEP when HT is enabled, the APUT passes the test. Skip the remaining steps.
2	Using the 11n sniffer, look at the Beacons from the APUT.	If the Beacons from the APUT contain IE 45 or 61, the APUT fails the test. Skip the remaining steps.
3	Force the test bed STA to do an active scan.	
4	Using the 11n sniffer, look at the Probe Responses from the APUT.	If the Probe Responses from the APUT contain IE 45 or 61, the APUT fails the test. Skip the remaining steps.
5	Associate the test bed STA to the APUT with the STA configured for HT and WEP.	
6	Using the 11n sniffer, look at the Association Response from the APUT.	If Association Response from the APUT contains IE 45 and the status code is zero, the APUT fails the test. Skip the remaining steps.
7	Run a test script that emulates a long file transfer from a PC on the wired Ethernet side of the APUT to the associated test bed STA for at least 10 seconds.	

8	Using the 11n sniffer, collect 10 seconds of data packets.	If any of the data packets from the APUT are sent at HT rates, the APUT fails the test. Skip the remaining steps. If all of the data packets from the APUT are sent at non-HT rates, the APUT passes the test.
9		

Table 110AP Negative WEP Test Procedure and Results

4.2.46 removed

4.2.47 Power Save

Purpose and Description
Verifies that the APUT responds properly to a station that enters power save mode. Verifies that the APUT responds properly to power save polls sent by a station in power save mode.

Test Environment
802.11 APUT
STA1: Testbed 802.11a/b/g
802.11 sniffer
STA 1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STA1 Values	APUT Values
Vendor	**Marvell**	**-**
ESSID	ps	ps
Security		Open if supported, otherwise WPA2-PSK 12345678
AP Control Channel	-	6 or 36 Dual band use 6

Table 111: Power Save Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	Testbed 802.11a/b/g STA1	802.11 APUT	Expected Results
1		Beacon	Check that the PVB = 0. If not, correct the environment. If can't make the PVB=0, fail.
2	Association Request		
3		Association Response	
4	Make sure power save is DISABLED (i.e., power management bit=0)		PVB = 0. Else fail.
5		Start TCP filesndl to STA1. This script must run long enough to complete step 6 Start the sniffer	
6	Make sure power save is ENABLED (i.e., power management bit=1)	After the station has entered power save mode, continue to capture packets for at least 15 seconds	Using the sniffer check that the station has entered power save mode: 1. The station sends a data or a null data packet to the APUT with the power management bit set to 1 2. The APUT sends an ACK in response to this data or null data packet. 3. When the AP has data buffered for STA1, it must set PVB≠0, else fail.
7			Once the APUT has acknowledged the PMB=1 from the station, the APUT is expected to stop sending directed packets to the station unless the station sends a PS poll. Directly after the acknowledgement packet from the APUT to the station is sent and before any PS Polls is sent, the APUT shall send no more than 2 data or null packets to the station. If 3 or more packets are sent directly after the acknowledgement (do not count retries), the APUT fails. This check is applicable for when the station switches from non-power save to power save and not for when the station is in power save.
8			For each PS poll the station sends to the APUT, the APUT is expected to send only one directed data packet in response. If APUT sends more than one directed data packet in response to a single PS poll, the APUT fails. If the station sends more than 1 PSPoll that is acknowledged by the APUT before the APUT responds with a data or null packet, the APUT shall ignore these extra PSPoll packets.

9			If the APUT sends data or null packets without these being in response to a PS-Poll, then fail (unsolicited data or null packets are a failure)

Table 112: Power Save Procedure and Results

4.2.48 removed

4.2.49 removed

4.2.50 removed

5 Station Testing

This section defines all the test cases for a STAUT for infrastructure and IBSS modes.

5.1 Configurability of Tests

5.1.1 General Configurability Tests

All STAUT must be capable of configuring the following general parameters: ESSID

The STAUT fails if the above cannot be configured through the user interface. If the device fails, no further testing will be performed until the vendor addresses the problems and has updated the device.

5.1.2 Security Configurability Tests

The STAUT must be capable of configuring the following security parameters:

1. The DUT must follow one of the security combinations described in section 3.8.
2. Turn WPA2 on or off. Skipt this step if the STAUT only supports WPA2.
3. When WPA2 is turned on, verify that WPA2-Personal or WPA2-Enterprise running EAP method modes can be selected (for those STAs supporting Enterprise).
4. Specify the default pass phrase (“12345678”) for WPA2-PSK can be entered.
5. If WPA is supported it must also support WPA2 concurrently.

The STAUT fails if any item above cannot be configured through the user interface. If the device fails, no further testing will be performed until the vendor addresses the problems and has updated the device.

The interoperability tests assure that the STAUT can operate with a variety of ESSIDs, can handle fragmentation, security, Power Save, different channels, different basic rates, and different 802.11n modes and features.

5.2 Infrastructure STAUT Test Cases

This section provides a comprehensive list of infrastructure STA test cases. It defines all the mandatory and Optional and Tested test cases for an STAUT and these tests should be conducted in the 2.4 GHz or 5 GHz frequency bands and using 20 MHz or 20/40 MHz channel width. **For non-11n STAUT device, tests shall be conducted using 20MHz channel width**

This table also includes the STAUT IBSS test cases.

Test Case	Frequency Band (GHz)	Channel Width (MHz)	Mandatory / Optional and Tested[4]	Test Section
WPA2 STAUT Test Cases				
STA Out of the Box (OOB)	2.4 5	20 20/40	Mandatory	5.2.1
STA WPA2 Initial Ping Interoperability Test	2.4 5	20 20/40	Mandatory	5.2.2
AP & STA Association & Throughput, Honoring NAV	2.4 5	20 20/40	Mandatory	5.2.3
AP & STA Association & Throughput using Fragmentation	2.4	20	Optional and Tested	5.2.4
Mixed 802.11b/g Interoperability STA Testing	2.4	20	Optional and Tested	5.2.5
Mixed 802.11b/g Interoperability STA Testing with WPA2-PSK	2.4	20	Optional and Tested	5.2.6
Mixed 802.11b/g Interoperability STA Testing with WEP and PSK Security	2.4	20	Optional and Tested	5.2.7
Mixed 802.11b/g Interoperability STA Testing with WPA2-Enterprise	2.4	20	Optional and Tested	5.2.8
AP & STA Association and Throughput using WPA2-PSK	2.4 5	20 20/40	Mandatory	5.2.9
AP & STA Association and Throughput using WPA2-Enterprise	2.4 5	20 20/40	Mandatory	5.2.10
AP & STA Association and Throughput with Replay Counter Processing	2.4 5	20 20/40	Mandatory	5.2.11
AP & STA Association and Throughput using WEP	2.4	20	Optional and Tested	5.2.12
AP & STA Association and Throughput using WPA2 with Fragmentation	2.4	20	Optional and Tested	5.2.13
Group Traffic Transmission/Reception with WPA2-PSK only Mode and WPA/WPA2-PSK Mixed Mode	2.4 5	20	Mandatory	5.2.14
Pre-authentication	2.5 5	20 20/40	Optional	5.2.15
PMK Caching	2.4 5	20	Mandatory for Enterprise devices	5.2.16
WPA Specific Countermeasures – Legacy WPA Only Mode	2.4 5	20	Optional and Tested	5.2.17
WPA Specific Countermeasures – WPA2/WPA Mixed Mode	2.4 5	20	Optional and Tested	5.2.18
WPA2 Negative Tests – Non-association with an AP not using WPA2	2.4 5	20	Optional and Tested	5.2.19
WPA2 Negative Test – Non-association with PSK-Configured STA	2.4 5	20 20/40	Mandatory	5.2.20
WPA2 Negative Test – Non-association with TLS-Configured STA	2.4 5	20	Optional and Tested	5.2.21
802.11h Testing – Spectrum Management Bit	5	20	Optional and Tested	5.2.22

[4]Optional and tested means that it is optional to implement the feature, and if implemented, it is mandatory to test.

802.11h Testing – Channel Switch Test	5	20	Optional and Tested	5.2.23
Extended EAP Tests (Enterprise STAs Only)	2.4 5	20 20/40	Optional and Tested	5.2.24
Band Roaming Tests for Single & Dual Band STAs with WPA2-PSK	2.4 5	20	Mandatory	5.2.26
Support for AES if TKIP is supported	2.4 5	20 20/40	Optional and Tested	5.2.53
OOB-STAUT association (Testbed AP: PMF enabled, supports SHA-1 only)	2.4 5	20 20/40	Mandatory	5.2.55
WMM STAUT Test Cases				
Traffic Differentiation in Single BSS with 802.11n STA	2.4 5	20 20/40	Mandatory	5.2.27
Traffic Differentiation in Single BSS with 2 802.11n STAs	2.4 5	20	Mandatory	5.2.28
Traffic Differentiation in Single BSS with WMM STA	2.4 5	20 20/40	Mandatory	5.2.29
Traffic Differentiation in Single BSS with Legacy Non-WMM STA	2.4 5	20 20/40	Mandatory	5.2.30
Test ACM Bit Conformance	2.4 5	20	Mandatory	5.2.31
Test the AC Parameter Modification	2.4 5	20	Mandatory	5.2.32
TXOP Limit Test	2.4 5	20	Mandatory	5.2.33
STAUT “No Acknowledgement” Test	2.4 5	20	Mandatory	5.2.34
11n Test Case				
Basic Association in 802.11n Environment	2.4 5	20 20/40	Mandatory	5.2.35
Ability to Receive 1 and 2 Spatial Streams	2.4 5	20 20/40	Mandatory	5.2.36
A-MDPU Aggregation when the STA is the Recipient	2.4 5	20 20/40	Mandatory	5.2.37
A-MSDU Aggregation when the STA is the Recipient	2.4 5	20 20/40	Mandatory	5.2.38
Overlapping BSS – 2.4 GHz	2.4	20	Optional and Tested	5.2.39
Overlapping BSS – 5 GHz	5	20	Optional and Tested	5.2.40
Greenfield Operation	2.4 5	20 20/40	Optional and Tested	5.2.41
Short GI Operation	2.4 5	20 20/40	Optional and Tested	5.2.42
Overlapping BSS on the Extension Channel	5	20/40	Optional and Tested	5.2.43
HT Duplicate Mode (MCS = 32)	2.4 5	20/40	Optional and Tested	5.2.44
STA RIFS Test	2.4 5	20 20/40	Mandatory Receive	5.2.45
STBC Receive Test	2.4 5	20 20/40	Optional and Tested	5.2.46
A-MPDU Aggregation when the STA is the Transmitter	2.4 5	20 20/40	Optional and Tested	5.2.47
STA 20/40 MHz Coexistence	2.4	20/40	Optional and Tested	5.2.48
Ability to Receive 3 Spatial Streams	2.4 5	20 20/40	Optional and Tested	5.2.49
STAUT Transmitting to AP using Supported Number of Spatial Streams	2.4 5	20 20/40	Mandatory	5.2.50
Disallow TKIP with HT Rates	2.4 5	20 20/40	Optional and Tested	5.2.51
STA Negative tests to ensure WEP is not used with HT associations in 11n devices	2.4 5	20 20/40	Optional and Tested	5.2.52
IBSS Test Cases				

IBSS Active & Passive Scanning Test	2.4 5	20	Optional and Tested	5.3.1
IBSS WEP On& Off Tests	2.4 5	20	Optional and Tested	5.3.2
IBSS Rejoin Tests	2.4 5	20	Optional and Tested	5.3.3

Table 113: STAUT Test Cases

5.2.1 STA Out of Box (OOB)

Purpose and Description

The STAUT test is set to its Out of Box (OOB) 'default configuration' to simulate using the device for the first time at initial power on. OOB security must be Off/Open/None, or WPA2, or WPA2/WPA mixed mode.

Test Environment

The Station under test is set to its 'default configuration' to simulate using the device for the first time. Four test bed APs are configured as follows:

STAUT
AP1: Testbed 802.11a/b/g
AP2: Testbed 802.11a/b/g
AP3: Testbed 802.11a/b/g
AP4: Testbed 802.11a/b/g
Sniffer
APs 1- 4 are 11n devices operating in legacy mode

Test Configuration and Procedure

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	AP2 Values	AP3 Values	AP4 Values
Vendor	-	**Qualcomm**	**Broadcom**	**Marvell**	**MediaTek**
SSID	wi-fiwi-	wi-fiwi-	wi-fiwi-	wi-fiwi-	wi-fiwi-
Beacon Interval (ms)	-	100	100	100	100
Channel	-	1 or 36, Dual Band use 1	11 or 36, Dual Band use 11	6 or 36, Dual Band use 6	6 or 36, Dual Band use 6
Security	Default	Off	WEP	WPA-PSK	WPA2-PSK
Encryption Key			0x9876543210	wi-fiwi-	wi-fiwi-

Table 114: STA OOB Test Configuration

Test Procedure and Expected Results

Steps	STAUT	Testbed 802.11n AP1	Testbed 802.11a/b/g AP2	Testbed 802.11a/b/g AP3	Testbed 802.11a/b/g AP4	Expected Results
1		Beacon	Beacon	Beacon	Beacon	
2	Attempt to connect to AP1 or AP4	Association Response			Association Response	STAUT should connect to either AP1 or AP4 depending on its default security setting. If it connects to neither AP, then fail
3	Attempt to connect to AP2					If STAUT did connect to AP2 then fail
4	Attempt to connect to AP3					If STAUT did connect to AP3 then fail
6	Ping console					If ping fails then fail

Table 115: STA OOB Procedure and Expected Results

5.2.2 STA WPA2 Initial Ping Interoperability Test

Purpose and Description

The initial ping test verifies that the STAUT can authenticate, associate and support pings to a wired authentication server on a subnet connected to the test configuration. This test shall use the WPA2-Enterprise running TLS mode of authentication. The test also verifies that STAUTs that support using power save do not set the power management bit (PM=1) in any Probe Request or Association Request packets.

Test Environment

STAUT
Testbed 802.11a/b/g AP
AP1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	Testbed AP 1 Values
Vendor	-	**Qualcomm**
SSID	-	Wi-fi
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 36
Security (see note below)	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Supplicant/Server	-	Hostapd
Power Save	If power save supported, enable power save PSPoll or PsnonPoll.	NA

Table 116: STA WPA2 Initial Ping Interoperability Test Configuration

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0

Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 117: EAP Priority Order

Procedure and Expected Results
The following table defines the test procedures and expected results.

Until further notice, steps 1b and 2 expected results in red are for data collection only. Do not use for pass/fail criteria.

`	STAUT	Testbed 802.11a/b/g AP	Expected Results
1a	Enable PS	Beacon	Skip this step if STAUT does not support Legacy PS.
1b	Probe request		Sniffer: filter on probe request packets and PM=1. If there are no packets, pass; otherwise fail. Skip this step if STAUT does not support PS or if STAUT does not produce any probe requests.
2	Association Request	Association Response	Sniffer: filter on Association request packets and PM=1. If there are no packets, pass; otherwise fail. Skip this step if STAUT does not support PS. IF STAUT fails to associate and authenticate to the tested AP then fail
3	Ping <Server IP>		If the STAUT fails to receive ping responses from the associated tested AP within 90 seconds, no further testing will be performed until the vendor addresses the problems and has updated the device.

Table 118: STA WPA2 Initial Ping Interoperability Procedure and Expected Results

5.2.3 AP & STA Association and Throughput, Honoring NAV

Purpose and Description
Different data transfer types and basic throughput and interoperability.
Honoring NAV Background.

Test Environment
WFA-EMT
STAUT
Testbed 802.11n 20/40 MHz AP in legacy mode
AP1 is an 11n device operating in legacy mode
Test Configuration
The following table defines the parameter values for the devices in the test bed. If running the test in 2.4 GHz, use B mode (not G).

Parameters	STAUT Values	AP1 Values
Vendor	-	**Marvell**

SSID	-	wpa2wpa2
Beacon Interval (ms)	-	100
Channel	-	6 (use B mode) or 36, Dual Band use 36
Security	WPA2-PSK	WPA2-PSK
Encyption Key	wpa2wpa2	wpa2wpa2
Supplicant/Server	-	-

Table 119: AP & STA Association and Throughput, Honoring NAV Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g AP	WFA-EMT	Expected Results
1		Beacon		
2	Association Request	Association Response		If STAUT fail to connect then fail
3		Start TCP FILESNDL to STAUT		If recorded throughput is less than 5.2.3S1DT1 then fail
4	Start TCP FILESNDL to testbed AP			If recorded throughput is less than 5.2.3S1DT2 then fail
5		Start TCP INQUIRYL to STAUT		If recorded throughput is less than 5.2.3S1DT3 then fail
6	Start TCP FILESNDL to testbed AP		Configure the WFA-EMT to generate a CTS-to-self with a 25,000 µs large duration field. Upon transmitting the CTS-to-self, the test device waits 30,000 µs before competing for the medium again.	(NAV) If throughput is greater than 80% of the throughput in step 4 then fail

Table 120: AP & STA Association and Throughput, Honoring NAV Procedure and Results

5.2.4 AP & STA Association and Throughput using Fragmentation

Purpose and Description
The following tests apply to stations operating in 2.4 GHz mode; skip this section for stations that operate only in 5 GHz mode. Ability of the STAUT to receive fragments OOB.

Test Environment
STAUT
Testbed 802.11b AP
AP1 is an 11n device operating in legacy b mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
SSID	WKV(*+8210	WKV(*+8210
Beacon Interval (ms)	-	100
Channel	-	11
Fragmentation	-	500 Bytes
Security	WPA2-Enterprise Running TLS	WPA2-Enterprise Running TLS

Supplicant/Server	-	Hostapd

Table 121: AP & STA Association and Throughput using Fragmentation Configuration

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 122: EAP Priority Order

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11b	Expected Results
0		Beacon	
1	Association Request	Association Response	If STAUT fail to connect then fail
2		Start TCP FILESNDL to STAUT	If recorded throughput is less than 5.2.4S2DT1 then fail
3	Start TCP FILESNDL to testbed AP		If recorded throughput is less than 5.2.4S2DT2 then fail
4		Start TCP INQUIRYL to STAUT	If recorded throughput is less than 5.2.4S2DT3 then fail

Table 123: AP & STA Association and Throughput using Fragmentation Procedure and Results

5.2.5 Mixed 802.11b/g Interoperability STA Testing

Purpose and Description

The following tests apply to stations operating in 2.4 GHz mode; skip this section for stations that operate only in 5 GHz mode. These tests ensure that the 2.4 GHz mode station can function properly in a BSS with both G and B stations associated to one AP.

Test Environment

STAUT
AP1: Testbed 802.11g
STA2: Testbed 802.11b
STA 2 is an 11n device operating in legacy b mode
AP1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	STA2 Values
Vendor	-	**Marvell**	**Realtek**
SSID	-	Wfa80211g	-
Beacon Interval (ms)	-	50	-
Channel	-	6	-
RTS Threshold	-	-	256 bytes
Fragmentation	-	-	430 bytes
Preamble	-	-	Long

Table 124: Mixed 802.11b/g Interoperability STA Testing Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11b STA1	Testbed 802.11g AP1	Expected Results
1	Association Request	Association Request	Association Response to STAUT Association Response to STA 2	If any stations fail to associate then fail
2			Ping STAUT and STA 1 from console	If either ping did not run then fail
3			Start TCP FILESNDL from console to STAUT and STA1	If STAUT throughput is <5.2.5MS8GDT1 then fail If STA1 throughput is <5.2.5MS8BDT1then fail
4	Start TCP FILESNDL from STAUT and STA1 to console			If STAUT throughput is <5.2.5MS8GDT2 then fail If STA1 throughput is <5.2.5MS8BDT2 then fail
5			Start TCP INQUIRYL from console to STAUT and STA1	If STAUT throughput is <5.2.5MS8GDT3 then fail If STA1 throughput is <5.2.5MS8BDT3 then fail

Table 125: Mixed 802.11b/g Interoperability STA Testing Procedure and Results

5.2.6 Mixed 802.11b/g Interoperability STA Testing with WPA2-PSK

Purpose and Description
The following tests apply to stations operating in 2.4 GHz mode; skip this section for stations that operate only in 5 GHz mode. These tests ensure that the 2.4 GHz mode station can function properly in a BSS with both G and B stations associated to one AP.

Test Environment
STAUT
AP1: Testbed 802.11g
STA2: Testbed 802.11b
STA 2 is an 11n device operating in legacy b mode
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	STA2 Values
Vendor	-	**Qualcomm**	**Realtek**
SSID	-	abcdefghijklmnopqrstuvwxyz ABCDEF	-
Beacon Interval (ms)	-	100	-
Channel	N/A	6	-
Fragmentation	-	-	430 bytes
Preamble	-	-	Long
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	abcdefghijklmnopqrstuvwxyz ABCDEF	abcdefghijklmnopqrstuvwxyz ABCDEF	abcdefghijklmnopqrstuvwxyzA BCDEF

Table 126: Mixed 802.11b/g Interoperability STA Testing with WPA-PSK Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11b STA1	Testbed 802.11d AP1	Expected Results
1	Association Request	Association Request	Association Response to STAUT Association Response to STA 2	If any stations fail to associate then fail
2			Ping STAUT and STA 1 from console	If either ping did not run then fail
3			Start TCP FILESNDL from console to STAUT and STA1	If STAUT throughput is <5.2.6MS9GDT1then fail If STA1 throughput is <5.2.6MS9BDT1 then fail
4	Start TCP FILESNDL from STAUT and STA1 to console			If STAUT throughput is <5.2.6MS9GDT2 then fail If STA1 throughput is <5.2.6MS9BDT2 then fail
5			Start TCP INQUIRYL from console to STAUT and STA1	If STAUT throughput is <5.2.6MS9GDT3 then fail If STA1 throughput is <5.2.6MS9BDT3 then fail

Table 127: Mixed 802.11b/g Interoperability STA Testing with WPA-PSK Procedure and Results

5.2.7 Mixed 802.11b/g Interoperability STA Testing with WEP or PSK Security

Purpose and Description
The following tests apply to stations operating in 2.4 GHz mode; skip this section for stations that operate only in 5 GHz mode. These tests ensure that the 2.4 GHz mode station can function properly in a BSS with both G and B stations associated to one AP.

Test Environment
STAUT
AP1: Testbed 802.11g
STA2: Testbed 802.11b
STA 2 is an 11n device operating in legacy b mode
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	STA2 Values
Vendor	-	**MediaTek**	**Realtek**
SSID	GLKDAJ98~@	GLKDAJ98~@	GLKDAJ98~@
Beacon Interval (ms)	-	200	-
Channel	-	6	-
RTS Threshold	-	-	256 bytes
Preamble	-	-	Long
Security	WEP, key = 0x9876543210 If WEP not supported WPA2-PSK = GLKDAJ98~@	WEP, key = 0x9876543210 If WEP not supported in STAUT WPA2-PSK = GLKDAJ98~@	WEP, key = 0x9876543210 If WEP not supported in STAUT WPA2-PSK = GLKDAJ98~@
Supplicant/Server	-	-	Microsoft

Table 128: Mixed 802.11b/g Interoperability STA Testing with WEP or PSK Security Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11b STA1	Testbed 802.11g AP1	Expected Results
1	Association Request	Association Request	Association Response to STAUT Association Response to STA 2	If any stations fail to associate then fail
2			Ping STAUT and STA 1 from console	If either ping did not run then fail
3			Start TCP FILESNDL from console to STAUT and STA1	If STAUT throughput is <5.2.7MS10GDT1then fail If STA1 throughput is <5.2.7MS10BDT1 then fail
4	Start TCP FILESNDL from STAUT and STA1 to console			If STAUT throughput is <5.2.7MS10GDT2 then fail If STA1 throughput is <5.2.7MS10BDT2 then fail
5			Start TCP INQUIRYL from console to STAUT and STA1	If STAUT throughput is <5.2.7MS10GDT3 then fail If STA1 throughput is <5.2.7MS10BDT3 then fail

Table 129: Mixed 802.11b/g Interoperability STA Testing with WEP or PSK Security Procedure and Results

5.2.8 Mixed 802.11b/g Interoperability STA Testing with WPA2-Enterprise

Purpose and Description
The following tests apply to stations operating in 2.4 GHz mode; skip this section for stations that operate only in 5 GHz mode. These tests ensure that the 2.4 GHz mode station can function properly in a BSS with both G and B stations associated to one AP.

Test Environment
STAUT
AP1: Testbed 802.11g
STA2: Testbed 802.11b
STA 2 is an 11n device operating in legacy b mode

AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	STA2 Values
Vendor	-	**Broadcom**	**Broadcom**
SSID	-	a	-
Beacon Interval (ms)	-	500	-
Channel	-	6	-
Preamble	-	-	Long
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Supplicant/Server	-	Hostapd	WPA Supplicant

Table 130: Mixed 802.11b/g Interoperability STA Testing with WPA-Enterprise Configuration

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 131: Priority, EAP Types, Supplicant, and Servers

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11b STA1	Testbed 802.11d AP1	Expected Results
1	Association Request	Association Request	Association Response to STAUT Association Response to STA 2	If any stations fail to associate then fail
2			Ping STAUT and STA 1 from console	If either ping did not run then fail
3			Start TCP FILESNDL from console to STAUT and STA1	If STAUT throughput is <5.2.8MS11GDT1 then fail If STA1 throughput is <5.2.8MS11BDT1 then fail
4	Start TCP FILESNDL from STAUT and STA1 to console			If STAUT throughput is <5.2.8MS11GDT2 then fail If STA1 throughput is <5.2.8MS11GDT2 then fail

Table 132: Mixed 802.11b/g Interoperability STA Testing with WPA-Enterprise Procedure and Results

5.2.9 AP & STA Association & Throughput using WPA2-PSK

Purpose and Description
This test verifies that the STAUT can pass traffic using WPA2-PSK security mode.

Test Environment
STAUT
Testbed 802.11n 20/40 MHz AP1 in Legacy mode
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
SSID	-	wpa2wpa2
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 36
Security	WPA2-PSK	WPA2-PSK
Encryption Key	wpa2wpa2	wpa2wpa2
Supplicant/Server	-	-

Table 133: AP & STA Association and Throughput using WPA2-PSK Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n AP	Expected Results
1		Beacon	
2	Association Request	Association Response	If STAUT fail to connect then fail
3		Start UDP FILESNDL to STAUT	If recorded throughput is less than 5.2.9T3DT1then fail
4	Start UDP FILESNDL to testbed AP		If recorded throughput is less than 5.2.9T4DT2 then fail
5		Start UDP INQUIRYL to STAUT	If recorded throughput is less than 5.2.9T5DT3 then fail

Table 134: AP & STA Association and Throughput using WPA2-PSK Procedure and Results

5.2.10 AP & STA Association and Throughput using WPA2-Enterprise

Purpose and Description
This test verifies that the STAUT can pass traffic using WPA2 enterprise security mode.

Test Environment
STAUT
Testbed 802.11n 20/40 MHz AP
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	**Qualcomm**
SSID	KLer90.	KLer90.
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 6
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Supplicant/Server	-	Hostapd

Table 135: AP & STA Association & Throughput using WPA2-Enterprise Configuration

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 136: Priority, EAP Types, Supplicant, and Servers

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n AP	Expected Results
1		Beacon	
2	Association Request	Association Response	If STAUT fail to connect then fail
3		Start TCP FILESNDL to STAUT	If recorded throughput is less than 5.2.10T3DT1 then fail
4	Start TCP FILESNDL to testbed AP		If recorded throughput is less than 5.2.10T4DT2 then fail
5		Start TCP INQUIRYL to STAUT	If recorded throughput is less than 5.2.10T5DT3 then fail

Table 137: AP & STA Association & Throughput using WPA2-Enterprise Procedure and Results

5.2.11 AP & STA Association & Throughput with Replay Counter Processing

Purpose and Description

The test of Configuration #S5 is used to ensure correct replay counter processing. The STAUT will need to send/receive at least 70k packets (cross 16-bit boundary of 65k packets).

This test is configured with the STAUT associated with a test-bed AP, the INQUIRYL-Replay script is executed.

Test Environment

STAUT
Testbed 802.11n 20/40 MHz AP
AP1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	**Qualcomm**
SSID	OBEW23@?+	OBEW23@?+
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 36
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Supplicant/Server	-	Hostapd

Table 138: AP & STA Association and Throughput with Replay Counter Processing Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n AP	Expected Results
1		Beacon	
2	Association Request	Association Response	If STAUT fail to connect then fail
3		Start INQUIRYL-REPLAY to STAUT	If test runs to completion without error and the number of bytes received by E1 (endpoint 1 – test server) exceeds 6.6 Megabytes, then pass

Table 139: AP & STA Association and Throughput with Replay Counter Processing Procedure and Results

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table: Priority, EAP Types, Supplicant, and Servers

5.2.12 AP & STA Association and Throughput using WEP

Purpose and Description
This test run in B-only mode, the AP is set up to B-only and the STAUT is used in its OOB configuration. 5 GHz only devices skip this test case.

Test Environment
STAUT
Testbed 802.11b AP1
AP1 is an 11n device operating in legacy b mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
SSID	-	WEP
Beacon Interval (ms)	-	100
Channel	-	6
Security	WEP Key = 0x1234abcdef	WEP Key = 0x1234abcdef
Supplicant/Server	-	-

Note: If WEP is not supported, use WPA2-PSK with key 1234abcdef.

Table 140: AP & STA Association and Throughput using WEP Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11b AP	Expected Results
1		Beacon	
2	Association Request	Association Response	If STAUT fail to connect then fail
3		Start TCP FILESNDL to STAUT	If recorded throughput is less than 5.2.12T3DT1 then fail
4	Start TCP FILESNDL to testbed AP		If recorded throughput is less than 5.2.12T4DT2 then fail
5		Start TCP INQUIRYL to STAUT	If recorded throughput is less than 5.2.12T5DT3 then fail

Table 141: AP & STA Association and Throughput using WEP Procedure and Results

5.2.13 AP & STA Association and Throughput using WPA2 with Fragmentation

Purpose and Description
This test run in B-only mode, the AP is set up to B-only and the STAUT is used in its OOB configuration. 5 GHz only devices skip this test case.

This test verifies that a STAUT can pass traffic using the WPA2 security mode when the AP is using fragmented packets.

Test Environment
STAUT
Testbed 802.11b AP

Sniffer
AP1 is an 11n device operating in legacy b mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
SSID	-	WPA2
Beacon Interval (ms)	-	100
Channel	-	6
Fragmentation	-	500 Bytes
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Supplicant/Server	-	Hostapd

Table 142: AP & STA Association and Throughput using WPA2 with Fragmentation Configuration

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 143: Priority, EAP Types, Supplicant, and Servers

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11b AP	Expected Results
1		Beacon	
2	Association Request	Association Response	If STAUT fail to connect then fail
3		Start TCP FILESNDL to STAUT	If recorded throughput is less than 5.2.13T3DT1 then fail
4	Start TCP FILESNDL to Testbed AP		If recorded throughput is less than 5.2.13T4DT2 then fail If STAUT is fragmenting frames then fail
5		Start TCP INQUIRYL to STAUT	If recorded throughput is less than 5.2.13T5DT3 then fail If STAUT is fragmenting frames then fail

Table 144: AP & STA Association and Throughput using WPA2 with Fragmentation Procedure and Results

5.2.14 Group Traffic Transmission/Reception with WPA/WPA2-PSK Mixed Mode

Purpose and Description
This tests the STAUT ability to handle correctly the reception and transmission of group traffic. When group traffic is originated by the STAUT the traffic is to be transmitted as directed traffic with the AP in the test bed re-transmitting the packets as group traffic.
The STAUT will be tested to ensure the correct directed traffic key/group key is used for the transmission and reception of group traffic.

Note: If the STAUT does not support WPA, then run both portions using WPA2.

Test Environment
STAUT
AP1: Testbed 802.11ag
STA2: Testbed 802.11ag
STA 2 is an 11n device operating in legacy mode
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	STA2 Values
Vendor	-	**Qualcomm**	**Broadcom**
SSID	-	Multicast	-
Beacon Interval (ms)	-	100	-
DTIM	-	1	-
Channel	-	6 or 36, Dual Band use 36	-
Power Save	-	-	On, PSPoll
Security	WPA2-PSK	WPA-PSK WPA2-PSK Selecting WPA2 mixed mode	WPA-PSK
Encryption Key	Multicast	Multicast	Multicast
Supplicant/Server	-		WPA Supplicant

Table 145: Group Traffic Transmission/Reception with WPA2-PSK Mode Configuration

Group Traffic Test Configuration
The STAUT and the test station are set up with IP group traffic Address 224.0.0.5. Each station's unique IP address must also be configured into the test in order to be able to configure the IP group traffic Address on those stations.

UDP is selected as the underlying protocol.
REALAUD is selected as the script.

Note: If Chariot is being used, "Validate Data upon Receipt" is selected on the Chariot Run Options tab of the Run Options dialog.

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11ag STA1	Testbed 802.11ag AP1	Expected Results
1	Association Request	Association Request	Association Response to STAUT Association Response to STA1	If any stations fail to associate then fail
2			Ping STAUT and STA1 from console	If either ping did not run then fail
3			Set up Test Server to support group traffic as Endpoint 1 with the STAUT set up as Endpoint 2. STA1 is also configured as an Endpoint 2 (called the "group traffic test station"). The streaming REALAUD script is used to generate a fixed	This test passes if 50% or more of the sent packets are successfully received.

			length group traffic stream of data at an average rate of 80Kbps for 92 seconds.	
4			Test Server is reconfigured to support group traffic as a Endpoint 2, with the STAUT now set as a Endpoint 1. STA1 is configured as Endpoint 2. As in Test run #1, the REALAUD script is used to generate a fixed length group traffic stream of data at an average rate of 80Kbps for 92 seconds.	This test passes if 50% or more of the sent packets are successfully received.

Table 146: Group Traffic Transmission/Reception with WPA2-PSK Mode Procedure and Results

5.2.15 Pre-authentication

Purpose and Description

This test is optional. Only if the STA contains this capability will the ability of the STAUT to perform pre-authentication be tested. If the STAUT does not support pre-authentication, completion of this section is not required.

Methodology: Two APs (both of which support pre-authentication) from the tested are configured with the same SSID. The STAUT is configured to associate to the SSID and allowed to associate to either AP. Ping is used to verify application level connectivity. A sniffer attached to the wired network is used to verify the appropriate pre-authentication behavior. A wireless sniffer is used to verify the appropriate roaming behavior.

Test Environment

STAUT
AP1: Testbed 802.11a/b/g
AP2: Testbed 802.11a/b/g
Sniffer
APs 1 & 2 are 11n devices operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	AP2 Values
Vendor	-	**MediaTek**	**Broadcom**
SSID	-	Pcache	Pcache
Beacon Interval (ms)	-	100	100
Channel	-	6 or 36, Dual Band use 36	6 or 36, Dual Band use 36
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS (mixed mode)	WPA2-Enterprise running TLS (mixed mode)
Supplicant/Server	-	Hostapd	Hostapd

Table 147: Pre-authentication Configuration

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP

First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 148: Priority, EAP Types, Supplicant, and Servers

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g AP	Testbed 802.11a/b/g AP	Expected Results
0	Flush any previously cached authentication data on STAUT (e.g., by disabling and re-enabling the supplicant and the wireless device on STAUT, or by rebooting the STAUT).			SN: start the Wired Sniffer Connect a sniffer to the wired network so that it can capture traffic sent from the APs. Configure a wireless sniffer to capture all traffic to or from the STAUT.
1		Beacon	Beacon	Power-on both APs, and configure both testbed APs as detailed above. Ensure that both APs are connected to the wired network.
2	Associate STAUT with either AP; call this APX. The other AP will be referred to as APY.			
3	Initiate a continuous ping from STAUT to the console or the Test Manager, to ensure that STAUT can both receive and pass traffic.			If there is no pings established then fail
4				SN: Sniff the following steps on both the wired and wireless sniffers.
5	Allow up to 180 seconds for an EAP-Success frame with an Ethertype of “preauthentication” (0x88c7) to be sent from APY to the STAUT; if no pre-authentication occurs within 180 seconds, the test is assumed to have failed.			
6		If this is APX then Power it off, to which the STAUT is currently associated.	If this is APX then Power it off, to which the STAUT is currently associated.	Verify that the STAUT associates with the other AP (call this APY) and that pinging resumes within 90 seconds. Verify that neither an EAPOL_START nor an EAPOL_IDENTITY_REQUEST message occurs in the sniffer after the STA roams to APY and resumes pinging.
7	Inspect the wireless sniffer capture and verify that a PMKID is included in the association or re-association request from STAUT to APY after APX is powered off. Verify the following: • The same PMKID is included in message 1 of the 4-way handshake sent by APY (this is the first EAPOL message after the (re)association response message) after the STAUT is associated with APY. • No EAP frames (full 802.1X exchange) are sent from the STAUT to APY or from APY to the STAUT after APX is powered off. Note: RADIUS logs are not reliable; they may incorrectly indicate a failure. Use sniffer.			

	The test will be considered passed when the required EAP-Success has been captured by the wired sniffer, and when the PMKIDs in the (re) associate message and 4-way message 1 match, and a full EAP authentication does not occur over the air between STAUT and APY. Note: A full EAP authentication request can be recognized on the wireless sniffer by an EAPOL_START from the STAUT or EAPOL_IDENTITY_REQUEST message from the AP.)

Table 149: Pre-authentication Procedure and Results

5.2.16 PMK Caching

Purpose and Description

This test is mandatory for Enterprise devices.
Unlike the APUT testing of pre-authentication, PMK caching must be done in addition to pre-authentication. Running pre-authentication does not test PMK caching for the STAUT.
Unlike pre-authentication, the PMK Cache Test is required. There is no upper limit for the number of PMKs that a station can cache; however, this test plan verifies that at least one PMK can be cached and used within the BSS.

Methodology: The STAUT is first associated and authenticated with the Broadcom AP. A ping test is used to demonstrate connectivity.

A second AP, the other AP, from within the test bed, is configured as part of the BSS and allowed to broadcasts its identity. The STAUT is forced to associate with the second AP. In doing, so, the initial AP from within the test bed must still remain active. STAUT is forced to re-associate with the initial AP from the test bed. A wireless sniffer is used to confirm that PMK caching is used, and a full EAP authentication does ***not*** occur.

Test Environment

STAUT
AP1: Testbed 802.11a/b/g
AP2: Testbed 802.11a/b/g
Sniffer
APs 1 & 2 are 11n devices operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values	AP2 Values
Vendor	-	**Broadcom**	**MediaTek**
SSID	-	Pcache	Pcache
Beacon Interval (ms)	-	100	100
Channel	-	6 or 36, Dual Band use 36	6 or 36, Dual Band use 36
Security	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS (mixed mode)	WPA2-Enterprise running TLS (mixed mode)
Authentication	-	Pre-authentication Disabled	Pre-authentication disabled
Supplicant/Server	-	Hostapd	Hostapd

Table 150: PMK Caching Configuration

Note: For STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP

First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 151: Priority, EAP Types, Supplicant, and Servers

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g AP 1	Testbed 802.11a/b/g AP 2	Expected Results
0			Power off	
1		Beacon	-	
2	Association Request	Association Response		
3	Initiate a continuous ping from STAUT to the console or the Test Manager, to ensure that STAUT can both receive and pass traffic.			If there is no pings established then fail
4	Force a roaming event for STAUT from AP1 to AP2 without clearing the PMK cache on AP1, by disabling the radio on AP1.		Power On (Beacon)	
5	Association Request		Association Response	If the STAs did not succeed to connect to AP2 and pings did not resume within 90 seconds then fail
6				SN: Configure a wireless sniffer to capture all traffic to or from STAUT.
7		Enable APs Radio and wait for 180 seconds for the STAUT to authenticate with the AP1.	Power off AP2 in order to force a re-association event for STAUT from the AP2 back to the AP1	If the pinging did not resume within 90 seconds then fail
9	Inspect the sniffer capture, and verify the following: • A PMKID is included in the association or re-association request from STAUT to AP1. • The same PMKID is included in message 1 of the 4-way handshake sent by AP1 to the STAUT. (This is the first EAPOL message after the re-association response message.) • No EAP frames (full 802.1X exchange) are sent from STAUT to AP1 The test will be considered passed when the PMKIDs in the (re) associate message and 4-way message 1 match, and a full EAP authentication does not occur. Note: If the test must be repeated for any reason, all caches shall be flushed before rerunning the test..			

Table 152: PMK Caching Procedure and Results

5.2.17 WPA Specific Countermeasures – Legacy WPA Only Mode

Purpose and Description

The purpose of the following test is to ensure that WPA countermeasures are implemented correctly within the STAUT and that the products within the test bed can recover from a MIC failure when work with legacy WPA only access point. Note: If the STAUT does not support WPA, then skip this test.

Test Environment

STAUT
WFA-EMT

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	WFA-EMT Values
SSID	PcachePc	PcachePc
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 6
Security	Mixed mode WPA2/WPA-PSK	WPA-PSK
Encryption Key	PcachePc	PcachePc
Supplicant/Server	-	-

Table 153: WPA Specific Countermeasures – Legacy WPA Only Mode Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	WFA-EMT	Expected Results
0		Configure the WFA-EMT as an AP for pure WPA-PSK	
1	Association Request	Association Response	
2	WFA-EMT: Initiate a directed ping from the STAUT to the WFA-EMT IP address acting as an AP to ensure that STAUT can both receive and send application-level traffic.	Start the test on the WFA-EMT (STAUT MIC test). The WFA-EMT will generate a bad MIC frame on the next outgoing directed data frame.	The STAUT must detect the bad MIC and send a MIC failure report to the WFA-EMT. Verify that the WFA-EMT indicates receipt of the MIC failure report. **If a report is not received, the test fails.**
3		The WFA-EMT will allow 70 seconds to pass.	Verify that pings from STAUT continue uninterrupted during this interval. **If the pings stop, the test fails.**
4		The WFA-EMT will generate a bad MIC on the next outgoing directed data frame.	The STAUT must detect the bad MIC and send a MIC failure report to the WFA-EMT. Verify that the WFA-EMT indicates receipt of the MIC failure report. **If a report is not received, the test fails.**
5		The WFA-EMT will allow 50 seconds to pass.	Verify that pings from the STAUT continue uninterrupted during this interval. **If the pings stop, the test fails.**
6		The WFA-EMT will generate a bad MIC on the next outgoing directed data frame.	The STAUT must detect the bad MIC and send a MIC failure report to the WFA-EMT. Verify that the WFA-EMT indicates receipt of the MIC failure report. **If a report is not received, the test fails.**
7	De-authenticate from the WFA-EMT.		The STAUT must then deauthenticate itself from the WFA-EMT. Verify that pings from the STAUT are interrupted, indicating that the STAUT is no longer connected to WFA-EMT. **If the STAUT remains associated to the WFA-EMT, the test fails.**
8	After 60 Seconds: Association Request	Association Response	Verify that the STAUT is able to associate again with the WFA-EMT and that the pings from the STAUT resume. This re-establishment of association may require manual intervention. If the station can manually be associated to the WFA-EMT after this second 60 seconds is up, the test is considered a pass.

			The aim of the test here is to ensure that re-establishment can occur after 60 seconds, and does not occur automatically prior to 60 seconds. **If the station can associate to the WFA-EMT before 60 seconds, or if the station cannot associate after 60 seconds, the test fails.**

Table 154: WPA Specific Countermeasures – Legacy WPA Only Mode Procedure and Results

5.2.18 WPA Specific Countermeasures – WPA2/WPA Mixed Mode

Purpose & Description

The purpose of the following test is to ensure that WPA countermeasures are implemented correctly within the STAUT and that the products within the test bed can recover from a MIC failure when work in mixed WPA2/WPA mixed mode. Note: If the STAUT does not support WPA, then skip this test.

Test Environment

STAUT
WFA-EMT

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	WFA-EMT Values
SSID	PcachePc	PcachePc
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 36
Security	WPA2-PSK	Mixed mode WPA/WPA2-PSK
Encryption Key	PcachePc	PcachePc
Supplicant/Server	-	-

Table 155: WPA Specific Countermeasures – WPA2/WPA Mixed Mode Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	WFA-EMT	Expected Results
0		The Attacker, WFA-EMT instrument, is configured as an AP for mixed WPA2-PSK/WPA personal mode operation. Since the WFA-EMT is running in this configuration all group traffic will use TKIP. The STAUT is configured for WPA2-PSK.	
1	Association Request	Association Response	
2		WFA-EMT: You don't need to generate group traffic.	It is not necessary that a successful reply is returned to this group traffic ping from any devices, including the STAUT and the WFA-EMT
3	WFA-EMT: Initiate a directed ping from the STAUT to the WFA-EMT IP address acting as an AP to ensure that STAUT can both receive and send application level traffic.	Start the test on the WFA-EMT (STAUT MIC Mixed attack test); it will generate a bad TKIP MIC on the next outgoing group traffic data frame.	The STAUT must detect the bad MIC and send a MIC failure report to the WFA-EMT. Verify that the WFA-EMT indicates receipt of the MIC failure report. **If a report is not received, the test fails.**
4		The WFA-EMT will allow 70 seconds to pass	Verify that pings from STAUT continue uninterrupted during this interval. **If the pings stop, the test fails.**
5		The WFA-EMT will generate a bad TKIP MIC on the next outgoing group traffic data frame.	The STAUT must detect the bad MIC and send a MIC failure report to the WFA-EMT. Verify that the WFA-EMT indicates receipt of the MIC failure report. **If a report is not received, the test fails.**
6		The WFA-EMT will allow 50 seconds to pass.	Verify that pings from the STAUT continue uninterrupted during this interval. **If the pings stop, the test fails.**
7		The WFA-EMT will generate a bad TKIP MIC on the next outgoing group traffic data frame.	The STAUT must detect the bad MIC and send a MIC failure report to the WFA-EMT Verify that the WFA-EMT indicates receipt of the MIC failure report. **If a report is not received, the test fails.**
8	De-authenticate and disassociate from the WFA-EMT		If the STAUT did not de-authenticate itself and disassociate then fail Verify that pings from the STAUT are interrupted, indicating that the STAUT is no longer connected to the testbed attacker AP. **If the station does not dissociate from the WFA-EMT, the test fails.**
9	After 60 Seconds: Association Request	Association Response	Verify that the STAUT is able to associate again with the WFA-EMT

			and that the pings from the STAUT resume. This re-establishment of association may require manual intervention. If the station can manually be associated to the WFA-EMT after this second 60 seconds is up, the test is considered a pass. The aim of the test here is to ensure that re-establishment can occur after 60 seconds, and does not occur automatically prior to 60 seconds. **If the station can associate to the WFA-EMT before 60 seconds, or if the station cannot associate after 60 seconds, the test fails.**

Table 156: WPA Specific Countermeasures – WPA2/WPA Mixed Mode Procedure and Results

5.2.19 WPA2 Negative Tests – Non-association with an AP not using WPA2

Purpose & Description

This test is intended to validate the correct Out Of the Box (OOB) and, once WPA2 has been selected, that the STAUT does not interoperate in configurations that will compromise the security of WPA2.

Test Environment

STAUT
Testbed 802.11a/b/g AP1
AP1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	Testbed AP1
Vendor	-	**Marvell**
SSID	-	Negative
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 6
Security	WPA2-Enterprise running TLS (negative case)	Off
Supplicant/Server	-	-

Table 157: WPA2 Negative Tests – Non-association with an AP not using WPA2 Configuration

Note: for STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 158: Priority, EAP Types, Supplicant, and Servers

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g AP	Expected Results
1		Beacon/Probe Response	
2	Start a continuous ping to the authentication server		
3	Try to associate by applying the profile above for at least 90 seconds		If STAUT can ping the authentication server within the 90 seconds then fail

Table 159: WPA2 Negative Tests – Non-association with an AP not using WPA2 Procedure and Results

5.2.20 WPA2 Negative Tests – Non-association with PSK-Configured Station

Purpose & Description

This test is intended to validate the correct Out Of the Box (OOB) and, once WPA2 has been selected, that the STAUT does not interoperate in configurations that will compromise the security of WPA2.

WPA2 configured devices must interoperate ***only*** with other devices with the same authentication mode (WPA2-Personal or WPA2-Enterprise).

Test Environment

STAUT
STA2: Reference Testbed 802.11a/b/g
AP1 Testbed AP 802.11a/b/g
STA 2 is an 11n device operating in legacy mode
AP1 is an 11n device operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	TestbedSTA2	Testbed AP1
Vendor	-	**Realtek**	**Broadcom**
SSID	-	-	Negative
Beacon Interval (ms)	-	-	100
Channel	-	-	6 or 36, Dual Band use 36
Security	WPA2-PSK	WPA2-Enterprise running TLS	WPA2-Enterprise running TLS
Encryption Key	Negative		
Supplicant/Server	-	Microsoft	Microsoft

Table 160: WPA2 Negative Tests – Non-association with PSK-Configured STA Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Reference 802.11a/b/g Testbed STA1	Testbed 802.11a/b/g AP	Expected Results
1	Configure the STA with a valid WPA2-PSK profile using the device WPA-Personal interface		Beacon/Probe Response	
2	Start a continuous ping to the authentication server	Start a continuous ping to the authentication server		
3		Association Request	Association response to STA2	Confirm that the pings are passing on the reference STA
4	Try to associate to the Testbed AP by applying the profile above for at least 90 seconds			If STAUT can ping the authentication server within the 90 seconds then fail

Table 161: WPA2 Negative Tests – Non-association with PSK-Configured STA Procedure and Results

5.2.21 WPA2 Negative Tests – Non-association with a TLS-Configured Station

Purpose & Description
This test is omitted when the STAUT supports only WPA2-PSK mode

This test is intended to validate the correct Out Of the Box (OOB) and, once WPA2 has been selected, that the STAUT does not interoperate in configurations that will compromise the security of WPA2.

WPA2 configured devices must interoperate ***only*** with other devices with the same authentication mode (WPA2-PSK or WPA2-Enterprise).

Test Environment
STAUT
STA2: Reference testbed 802.11a/b/g
Testbed AP1802.11a/b/g
STA 2 is an 11n device operating in legacy mode
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	STA2 Values	Testbed AP1
Vendor	-	**Intel**	**MediaTek**
SSID	-	-	Negative
Beacon Interval (ms)	-	-	100
Channel	-	-	6 or 36, Dual Band use 6
Security	WPA2-Enterprise running TLS	WPA2-PSK	WPA2-PSK
Encryption key		Negative	Negative
Supplicant/Server	-	Microsoft	

Table 162: WPA2 Negative Tests – Non-association with a TLS-Configured STA Configuration

Note: for STAUTs that do not support TLS, use the following table to choose the EAP method in priority order.

Priority	EAP
First	TTLS
Second	PEAP0
Third	PEAP1
Fourth	SIM
Fifth	FAST
Sixth	AKA

Table 163: Priority, EAP Types, Supplicant, and Servers

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	STA1	Testbed 802.11a/b/g AP	Expected Results
1	Configure the STAUT with a valid WPA2-TLS profile using the devices 802.1X – EAP TLS interface.		Beacon/Probe Response	
2	Start a continuous ping to the authentication server	Start a continuous ping to the authentication server		
3		Association Request	Association response to STA2	Confirm that the pings are passing on the reference STA
4	Try to associate to the testbed AP by applying the profile above for at least 90 seconds			If STAUT can ping the authentication server within the 90 seconds then fail

Table 164: WPA2 Negative Tests – Non-association with a TLS-Configured STA Procedure and Results

5.2.22 802.11h Testing – Spectrum Management Bit

Purpose & Description
This test is optional.
Conduct 802.11h testing with AP configuration as indicated. 2.4 GHz only devices skip this test case.

Test Environment
STAUT
Testbed 802.11h AP1
Sniffer
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	Testbed AP1
Vendor	-	**Broadcom**
SSID	-	80211h
Beacon Interval (ms)	-	100
Channel	-	56
Minimum # Beacons with Switch Announcement element after Channel Switch command	-	10
New Channel Number (if needed)	-	36 (or any non DFS channel)
Channel Switch Mode	-	1 (silence STA)

Table 165: 802.11h Testing – Spectrum Management Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g AP	Expected Results
1		Beacon/Probe Response	Set up the wireless sniffer to capture the association request from the STAUT to the AP
2	Association Request	Association Response	Look in Capability Info section of the association request for the spectrum management bit. This test passes if the spectrum management bit is set to 1.

Table 166: 802.11h Testing – Spectrum Management Bit Procedure and Results

5.2.23 802.11h Testing – Channel Switch Test

Purpose & Description
This test is optional.
Conduct 802.11h testing with AP configuration as indicated. 2.4 GHz only devices skip this test case.

Test Environment
STAUT
Testbed 802.11h AP1
Sniffer
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	Testbed AP1
Vendor	-	**Broadcom**
SSID	-	80211h
Beacon Interval (ms)	-	100
Channel	-	56
Minimum # Beacons with Switch Announcement element after Channel Switch command	-	10
New Channel Number (if needed)	-	36 (or any non DFS channel)
Channel Switch Mode	-	1 (silence STA)

Table 167: 802.11h Testing – Channel Switch Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g AP	Expected Results
1		Beacon/Probe Response	
2	Association Request	Association Response	
3	Start a continuous ping from the STAUT to a host connected through the wired side of the AP.		SN: Set up the wireless sniffer to capture the traffic from the STAUT.
4		Use the h+d AP-supplied command to force a channel switch announcement.	Check the Beacon frames for the Channel Switch Announcement Element (#37) presence for 15 seconds.
5			Verify that the last 6 beacons as captured by the sniffer contain channel switch announcement IE. The test passes if the STAUT stops sending any frames, and no further frames are transmitted on this channel by the station when the AP has sent the last 6 beacons, with the channel switch information elements as seen with the sniffer.

Table 168: 802.11h Testing – Channel Switch Test Procedure and Results

5.2.24 Extended EAP Tests (Enterprise STAs Only)

Purpose and Description
Extended EAP testing applies to Stations tested as WPA-enterprise devices only; Stations that are WPA-personal devices are not tested in this section. All PC-centric Stations are considered enterprise devices and must be tested here.
These tests are to test the stations ability to use EAP methods beyond TLS: TTLS, PEAP0, PEAP1, and GTC SIMs. All tests are performed using “Ping” tests; there are no throughput tests.

- Test 1: Association Positive Test (applies to all EAP methods).

Both the STAUT and AP have valid authentication certificates installed (SIM, AKA& AKA' do not require certificates). The appropriate EAP method is set up on both the AP and the STAUT. The STAUT is associated to the AP. A ping test is started to validate the association. If the ping test does not successfully start within 90 seconds, the STAUT fails the test, and all testing is stopped.

- Test 2: Association Negative Test, Expired AS Certificate (applies to TLS, TTLS, PEAP, and FAST).

  The AS is set up to look like it has an expired certificate by setting the STAUT's clock forward to a date after the AS certificate expires. The STAUT's supplicant is set up with a valid certificate. The STAUT is associated to the AP. A ping test is started to validate the association does not occur. If the ping test does not successfully start within 45 seconds, the STAUT passes the test. If the ping test successfully starts, the STAUT has failed the test, and all further testing is stopped.

- Test 3: Association Negative Test, SIM IMSI Not Contained Within the AS Database (applies to SIM only).

  Remove the triplets that were installed in the AS for the STAUT's supplicant associating with the AP. The STAUT is associated to the AP. A ping test is started to validate that the association does not occur. If the ping test does not successfully start within 45 seconds, the STAUT passes the test. If the ping test successfully starts, the STAUT has failed the test, and all further testing is stopped.

- Test 4: Sequence number resynchronization test (applies to AKA only).

  The simulated AuC/HLR is restarted so the sequence number is reset to its initial value. The STAUT's supplicant shall attempt to authenticate to a test bed AS through a test bed AP. The EAP-AKA server will indicate that the USIM card's sequence number needs to be resynchronized. The simulated AuC/HLR will indicate that a resynchronization occurred, and the supplicant shall give some indication that 802.1X authentication has been successful.

- Test 5: No USIM record (negative test; applies to AKA only).

  This test uses a USIM card that is not contained in the AS. The STAUT's supplicant shall attempt to authenticate to a test bed AS through a test bed AP. The supplicant shall give some indication that 802.1X authentication has not been successful. An attempt to ping the test bed AS from the STAUT shall fail.

- Test 6: Roaming test to validate protected success indication and AKA fast reconnect (applies to AKA only).

  Two testbed APs are configured identically with a WPAv1 SSID. The STAUT's supplicant shall attempt to authenticate to a test bed AS through a first test bed AP. The supplicant shall give some indication that 802.1X authentication has been successful. The STAUT shall then be able to 'ping' the test bed AS. The first test bed AP will be switched off, causing the STAUT to roam to a second test bed AP. The STAUT shall give some indication that the 802.1X (re)authentication has been successful. EAP-AKA fast reauthentication will be used if enabled by the STAUT when the test bed AS is (to be determined).

- Test 7: Association positive test with authenticated provisioning and GTC inner authentication (applies to FAST only).

  Clear any PACs installed on the server and supplicant. Configure the EAP-FAST PAC lifetime on the server to be one minute. Restart the authentication process to provision a new PAC, and wait in excess of one minute to "time out" the PAC so that the supplicant has no valid PACs which may be used for authentication.

Configure a wireless network using WPA version 1. WPA version 1 is required for this test to disable PMK caching. Configure the EAP-FAST server to have a PAC lifetime of one minute, or the shortest time supported by the EAP-FAST server. EAP-FAST should use authenticated provisioning with GTC inner authentication. Within the test bed AS's PAC lifetime, authenticate the STAUT to the network. The supplicant shall give some indication that the 802.1X authentication has been successful, and should give an indication that a new PAC has been provisioned. Ping from the supplicant to the AS. This operation should succeed. Wait for a time period in excess of the testbed AS's PAC lifetime to "time out" the PAC so that it is no longer valid.

Attempt to reauthenticate from the supplicant to the AS. Depending on implementation, a new PAC may be generated (this is implementation specific, but all testbed servers generate new PACs). If authentication is successful, then a new ping test should succeed. If the ping test fails, the test fails.

- Test 8: Association positive test with authenticated provisioning and MSCHAPv2 inner authentication (applies to FAST only).

  Clear any PACs installed on the server and supplicant. Configure the EAP-FAST PAC lifetime on the server to be one minute. Restart the authentication process to provision a new PAC, and wait in excess of one minute to "time out" the PAC so that the supplicant has no valid PACs which may be used for authentication.

  Configure a wireless network using WPA version 1. WPA version 1 is required for this test to disable PMK caching. Configure the EAP-FAST server to have a PAC lifetime of one minute, or the shortest time supported by the EAP-FAST server. EAP-FAST should use authenticated provisioning with MSCHAPv2 inner authentication. Within the test bed AS's PAC lifetime, authenticate the STAUT to the network. The supplicant shall give some indication that the 802.1X authentication has been successful, and should give an indication that a new PAC has been provisioned. Ping from the supplicant to the AS. This operation should succeed. Wait for a time period in excess of the testbed AS's PAC lifetime to "time out" the PAC so that it is no longer valid.

  Attempt to reauthenticate from the supplicant to the AS. Depending on implementation, a new PAC may be generated (this is implementation specific, but all testbed servers generate new PACs). If authentication is successful, then a new ping test should succeed. If the ping test fails, the test fails.

- Test 9: Negative test, unknown certificate association failure (applies to FAST only).

  A server certificate signed by an unknown CA is required for this test, and must be installed on EAP-FAST test bed ASes prior to the execution of this test. The testbed STA's supplicant shall attempt to authenticate to the APUT AS through a test bed AP. The supplicant shall give some indication that 802.1X authentication has not been successful. An attempt to ping a testbed device from the testbed STA will fail.

- Test 10: Negative test, change username prefix from "6" to "0" (AKA' only).

  The prefix for the AKA' username is changed from its standard "6" to "0" which is used by AKA. An authentication attempt is made. The supplicant shall give some indication that 802.1X authentication has not been successful. An attempt to ping a testbed device from the testbed STA will fail.

  Note: Before starting each test make sure the STA is disconnected from each authentication server.

Test Environment
STAUT
Testbed AP1 802.11a/b/g
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.
The STAUT supplicant may not support all EAP methods. Perform only those tests that the STAUT's supplicant supports that EAP method. For example, if TLS is not supported, skip test A13.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Qualcomm**
ESSID	Iou09+%	Iou09+%
AP Channel	-	6 or 44, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING TTLS	WPA2-ENTERPRISE RUNNING TTLS
Supplicant/Server	-	Radiator

Table 169: Extended EAP Tests Configuration #ExS1 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
AP Channel	-	6 or 40, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING PEAP0	WPA2-ENTERPRISE RUNNING PEAP0
Supplicant/Server	-	Hostapd

Table 170: Extended EAP Tests Configuration #ExS2 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
ESSID	NBGhgd901	NBGhgd901
AP Channel	-	6 or 36, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING PEAP1	WPA2-ENTERPRISE RUNNING PEAP1
Supplicant/Server	-	Hostapd

Note: For this test run in B-only mode, the AP is set up to B-only and the STAUT is used in its out-of-box configuration.

Table 171: Extended EAP Tests Configuration #ExS3 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**Qualcomm**
AP Channel	-	6 or 40, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING PEAP0	WPA2-ENTERPRISE RUNNING PEAP0
Supplicant/Server	-	Microsoft

Table 172: Extended EAP Tests Configuration #ExS4 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
ESSID	ZXKNpla56+~	ZXKNpla56+~
AP Channel	-	6 or 36, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING TLS	WPA2-ENTERPRISE RUNNING TLS
Supplicant/Server	-	Hostapd

Note: For this test run in B-only mode, the AP is set up to B-only and the STAUT is used in its out-of-box configuration.

Table 173: Extended EAP Tests Configuration #ExS5 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
AP Channel	-	6 or 40, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING TLS	WPA2-ENTERPRISE RUNNING TLS
Supplicant/Server	-	Microsoft

Table 174: Extended EAP Tests Configuration #ExS6 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**Qualcomm**
AP Channel	-	6 or 44, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING PEAP0	WPA2-ENTERPRISE RUNNING PEAP0
Supplicant/Server	-	Radiator

Table 175: Extended EAP Tests Configuration #ExS7 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
AP Channel	-	6 or 44, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING Peap1	WPA2-ENTERPRISE RUNNING Peap1
Supplicant/Server	-	Radiator

Table 176: Extended EAP Tests Configuration #ExS8 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
AP Channel	-	6 or 40, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING TLS	WPA2-ENTERPRISE RUNNING TLS
Supplicant/Server	-	Radiator

Table 177: Extended EAP Tests Configuration #ExS9 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
AP Channel	-	6 or 48, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING TTLS	WPA2-ENTERPRISE RUNNING TTLS
Supplicant/Server	-	HostAPD

Table 178: Extended EAP Tests Configuration #ExS10 Configuration

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
AP Channel	-	6 or 36, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING SIM	WPA2-ENTERPRISE RUNNING SIM
Supplicant/Server	-	Hostapd

Table 179: Extended EAP Tests Configuration #ExS13 Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n 20/40 MHz Capable AP	Expected Results
1		Beacon/Probe Response	
Association Positive Test			
2	Both the Station (STAUT) and AP have valid authentication certificates installed. The appropriate EAP method is set up on both the AP and the STAUT. The STAUT is associated to the AP.	A ping test is started to validate the association.	If the ping test does not successfully start within 90 seconds, the STAUT fails the test, and all testing is stopped.
Association Negative Test, Expired AS Certificate			
3	The STAUT's supplicant is set up with a valid certificate. The STAUT is associated to the AP.	The AS is set up with an expired certificate. A ping test is started to validate the association does not occur.	If the ping test does not successfully start within 45 seconds, the STAUT passes the test. If the ping test successfully starts, the STAUT has failed the test, and all further testing is stopped.
Association Negative Test, SIM IMSI not contained within the AS database (applies to SIM only)			
4	The STAUT is associated to the AP, and A ping test is started to validate the association does not occur.	Remove the triplets that were installed in the AS for the STAUT's supplicant associating with the AP.	If the ping test does not successfully start within 45 seconds, the STAUT passes the test. If the ping test successfully starts, the STAUT has failed the test, and all further testing is stopped.

Table 180: Extended EAP Tests (Enterprise STAs Only) Procedure and Results

Parameter	STAUT Values	AP1 Values
Vendor	-	**Qualcomm**
AP Channel	-	6 or 36, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING AKA	WPA2-ENTERPRISE RUNNING AKA
Supplicant/Server	-	Hostapd

Table 181 Extended EAP Tests Configuration #ExS18 Configuration (re: WPA2 ExS20)

Procedure for Test 4: Sequence number resynchronization test. (AKA only)

12. The simulated AUC/HLR is restarted so the sequence number is reset to its initial value.
13. The STAUT's supplicant shall attempt to authenticate to a test bed AS through a test bed AP.
14. The EAP-AKA server will indicate that the USIM card's sequence number needs to be resynchronized.
15. The simulated AUC/HLR will indicate that a resynchronization occurred, and the supplicant shall give some indication that 802.1X authentication has been successful.
16. Ping from the STAUT to a PC on the wired Ethernet side of the test bed AP. If ping is not successful, then fail the test.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
AP Channel	-	6 or 36, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING AKA	WPA2-ENTERPRISE RUNNING AKA
Supplicant/Server	-	Hostapd

Table 182 Extended EAP Tests Configuration #ExS19 Configuration (re: WPA2 ExS21)

Procedure for Test 5: No USIM record (negative test; AKA only)

1. This test uses a USIM card (supplied by STAUT vendor) that is not contained in the AS.
2. The STAUT's supplicant shall attempt to authenticate to a test bed AS through a test bed AP.
3. The supplicant shall give some indication that 802.1X authentication has not been successful.
4. An attempt to ping the test bed AS from the STAUT shall fail.

Parameter	STAUT Values	AP1 Values	AP2 Values
Vendor	-	**Broadcom**	**Qualcomm**
AP Channel	-	6 or 36	6 or 36, dual band use channel 6
Security	Mixed Mode WPA2/WPA-ENTERPRISE RUNNING AKA	WPA-ENTERPRISE RUNNING AKA	WPA-ENTERPRISE RUNNING AKA
Supplicant/Server	-	Radiator	Radiator

Table 183 Extended EAP Tests Configuration #ExS20 Configuration (re: WPA2 ExS22)

Procedure for Test 6: Roaming test to validate protected success indication and AKA fast reconnect (AKA only)

1. Two testbed APs are configured identically with a WPAv1 SSID.
2. The STAUT's supplicant shall attempt to authenticate to a test bed AS through a first test bed AP.
3. The supplicant shall give some indication that 802.1X authentication has been successful.
4. The STAUT shall then be able to 'ping' the test bed AS.
5. The first testbed AP will be switched off, causing the STAUT to roam to a second test bed AP.
6. The STAUT shall give some indication that the 802.1X (re)authentication has been successful.
7. EAP-AKA fast reauthentication will be used if enabled by the STAUT when the test bed AS is (to be determined).

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
AP Channel	-	6 or 36, dual band use channel 6
Security	Mixed Mode WPA2/WPA-ENTERPRISE RUNNING FAST	WPA-ENTERPRISE RUNNING FAST
Supplicant/Server	-	Hostapd

Table 184 Extended EAP Tests Configuration #ExS21 Configuration (re: WPA2 ExS23)

Procedure for Test 7: Association positive test with authenticated provisioning and GTC inner authentication (FAST only)

1. In order to clear any PACs installed on the server and supplicant: Configure the EAP-FAST PAC lifetime on the server to be one minute.
2. Restart the authentication process to provision a new PAC, and wait in excess of one minute to "time out" the PAC so that the supplicant has no valid PACs which may be used for authentication.
3. Configure a wireless network using WPA version 1. WPA version 1 is required for this test to disable PMK caching.

4. Configure the EAP-FAST server to have a PAC lifetime of one minute, or the shortest time supported by the EAP-FAST server. EAP-FAST should use authenticated provisioning with GTC inner authentication.
5. Within the test bed AS's PAC lifetime, authenticate the STAUT to the network.
6. The supplicant shall give some indication that the 802.1X authentication has been successful, and should give an indication that a new PAC has been provisioned.
7. Ping from the supplicant to the AS. This operation should succeed.
8. Wait for a time period in excess of the testbed AS's PAC lifetime to "time out" the PAC so that it is no longer valid.
9. Attempt to reauthenticate from the supplicant to the AS.
10. Depending on implementation, a new PAC may be generated (this is implementation specific, but all testbed servers generate new PACs).
11. If authentication is successful, then a new ping test should succeed. If the ping test fails, the test fails.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
AP Channel	-	6 or 36, dual band use channel 6
Security	Mixed Mode WPA2/WPA-ENTERPRISE RUNNING FAST	WPA-ENTERPRISE RUNNING FAST
Supplicant/Server	-	Hostapd

Table 185 Extended EAP Tests Configuration #ExS22 Configuration (re: WPA2 ExS24)

Procedure for Test 8: Association positive test with authenticated provisioning and MSCHAPv2 inner authentication (FAST only)

1. Clear any PACs installed on the server and supplicant.
2. Configure the EAP-FAST PAC lifetime on the server to be one minute.
3. Restart the authentication process to provision a new PAC, and wait in excess of one minute to "time out" the PAC so that the supplicant has no valid PACs which may be used for authentication.
4. Configure a wireless network using WPA version 1. WPA version 1 is required for this test to disable PMK caching.
5. Configure the EAP-FAST server to have a PAC lifetime of one minute, or the shortest time supported by the EAP-FAST server. EAP-FAST should use authenticated provisioning with MSCHAPv2 inner authentication.
6. Within the test bed AS's PAC lifetime, authenticate the STAUT to the network.
7. The supplicant shall give some indication that the 802.1X authentication has been successful, and should give an indication that a new PAC has been provisioned.
8. Ping from the supplicant to the AS. This operation should succeed.
9. Wait for a time period in excess of the testbed AS's PAC lifetime to "time out" the PAC so that it is no longer valid.
10. Attempt to reauthenticate from the supplicant to the AS.

11. Depending on implementation, a new PAC may be generated (this is implementation specific, but all testbed servers generate new PACs). If authentication is successful, then a new ping test should succeed. If the ping test fails, the test fails.

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
ESSID	PTB86@^‘	PTB86@^‘
AP Channel	-	6 or 36, dual band use channel 6
Security	Mixed Mode WPA2/WPA-ENTERPRISE RUNNING FAST	WPA-ENTERPRISE RUNNING FAST
Supplicant/Server	-	Hostapd

Table 186 Extended EAP Tests Configuration #ExS23 Configuration (re: WPA2 ExS25)

Procedure for Test 9: Negative test, unknown certificate association failure (FAST only)

1. A server certificate signed by an unknown CA is required for this test, and must be installed on the AS prior to the execution of this test.
2. The STA’s supplicant shall attempt to authenticate with the AS through the AP.
3. The supplicant shall give some indication that 802.1X authentication has not been successful. An attempt to ping a testbed device from the testbed STA will fail.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Qualcomm**
AP Channel	-	6 or 36, dual band use channel 6
Security	WPA2-ENTERPRISE RUNNING AKA ‘	WPA2-ENTERPRISE RUNNING AKA’
Supplicant/Server	-	Hostapd

Table 187 Extended EAP Tests Configuration #ExS24 Configuration (re: WPA2 ExS26)

Procedure for Test 10: Negative test, change username prefix from “6” to “0” (AKA’ only)

1.Change the username prefix from “6” to “0”.

2. The STA’s supplicant shall attempt to authenticate with the AS through the AP.

3. Ping from the STAUT to a PC on the wired Ethernet side of the test bed AP. If ping is successful, then fail the test

5.2.25 Removed

5.2.26 Roaming Test for Single &Dual Band STAs with WPA2-PSK

Purpose and Description

If the station under test does not support both bands, configure all four testbed access points to the one band that the station does support.

This tests the ability of the station to roam between 802.11a, 802.11n and 802.11b or 802.11g access points.

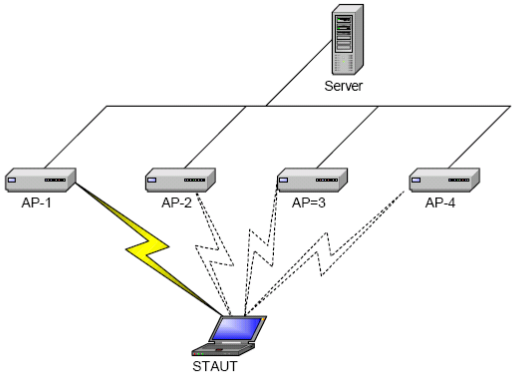


Figure 4: Dual Band Roaming Test for Dual Band STAs with WPA2-PSK Network Diagram

The Station Under Test (STAUT) is forced to roam from AP #1 to AP #2 to AP #3 to AP #4 and back to AP #1.
Pings must not be lost for more than 90 seconds during a roam from one AP to the next.
If the STAUT supports 802.11g, then AP1 and AP2 shall be configured to support 802.11g, else they shall be configured to support 802.11b.

Test Environment
STAUT
AP1: Testbed 802.11g AP
AP2: Testbed 802.11a AP
AP3: Testbed 802.11g AP
AP4: Testbed 802.11a AP
APs 1 – 4 are 11n devices operating in legacy mode

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values	AP2 Values	AP3 Values	AP4 Values
Vendor	-	**Qualcomm**	**Broadcom**	**Marvell**	**MediaTek**
Beacon Interval ms	-	100	100	100	100
Channel	-	6	36 (6 if single band STAUT)	6	36 (6 if single band STAUT)
ESSID	-	012345678901234567890123456789 01	012345678901234567890123456789012345678901	012345678901234567890123456789 01	012345678901234567890123456789 01
Security	-	WPA2-PSK	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key		012345678901234567890123456789 01	012345678901234567890123456789012345678901	012345678901234567890123456789 01	012345678901234567890123456789 01

Note: Basic Rate Set #1 is defined in the 802.11g test plan as: “1, 2, 5.5 and 11 Mbps considered basic rates as defined in 802.11 and 6, 9, 12, 18, 24, 36, 48 and 54 Mbps as supported rates”.

Table 188: Dual Band Roaming Test for Dual Band STAs with WPA2-PSK Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.
Continuous pings at one second intervals are used to validate connectivity with the PC. Pings must not be lost for more than 90 seconds during a roam from one AP to the next.

Steps	STAUT	Testbed 802.1b or g AP1	Testbed 802.11a AP2	Testbed 802.1b or g AP3	Testbed 802.11n AP4	Expected Results
1		Beacon/Probe Response	Disable AP#2	Disable AP#3	Disable AP#4	
2	The STAUT is associated to the AP#1					If STAUT is not associated to AP#1 then fail
3	Start continuous ping to the server					If pings are successful then pass
4		Disable AP#1	Beacon/Probe Response	Disable AP#3	Disable AP#4	
5	Continue ping to the server					If STAUT roams within 90 seconds then Pass
6		Disable AP#1	Disable AP#2	Beacon/Probe Response	Disable AP#4	
7	Continue ping to the server					If STAUT roams within 90 seconds then Pass
8		Disable AP#1	Disable AP#2	Disable AP#3	Beacon/Probe Response	
9	Continue ping to the server					If STAUT roams within 90 seconds then Pass
10		Beacon/Probe Response	Disable AP#2	Disable AP#3	Disable AP#4	
11	Continue ping to the server					If STAUT roams within 90 seconds then Pass

Table 189: Dual Band Roaming Test for Dual Band STAs with WPA2-PSK Procedure and Results

5.2.27 Traffic Differentiation in Single BSS with 802.11n STA

Purpose and Description

Test WMM capability negotiation.
Internal and distributed traffic differentiation between different traffic classes and various PHY rates between a single pair.

This test is performed between a single AP and a single STA to show that a device under test correctly differentiates packets. Two streams with different AC are transmitted from a DUT and the throughputs are compared in the same manner as the above differentiation tests. The background traffic stream provides enough additional traffic to saturate the wireless link.

Test Environment

STAUT
Testbed 802.11n 20 MHz Capable AP1
Wireless Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
ESSID	FGR896lk?	FGR896lk?
Security	WPA2-PSK	WPA2-PSK
Encryption Key	FGR896lk?	FGR896lk?
Supplicant/Server	-	-
AP Control Channel	-	6 or 36, Dual Band use 6
AIFS	Default (see Appendix D)	Default (see Appendix D)
CWmin	Default (see Appendix D)	Default (see Appendix D)
CWmax	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	0
ACM: AC_VI	-	0
ACM: AC_BE	-	0
ACM: AC_BK	-	0
AC Tagging	Default for STAUT	DSCP
Channel Width		0 (20 MHz)

Table 190: Traffic Differentiation in a Single BSS with 802.11n STA Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV20Mbps.scr
RTP2	IPTV16Mbps.scr
RTP3	IPTV16MbpsDelay10sec.scr

Table 191: Traffic Differentiation in a Single BSS with 802.11n STA Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	**Script Name**	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n 20 MHz Capable AP	Expected Results
0		Configure the AP to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
1	-	Beacon	
2	Probe request	Probe Response	SN: If a Probe Request occurs and Probe Request contains any WMM element, FAIL
3	Association Request	Association Response	SN: If Association Request contains WMM information element AND STAUT Associated, PASS
4	Receive RTP1_BE, RTP2_VI Transmit RTP3_BE	Transmit RTP1_BE RTP2_VI Receive RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 85%or more than RTP2 in first phase (1~9s), PASS
5	Transmit RTP1_BE, RTP2_VI RTP3_BE	Receive RTP1_BE RTP2_VI RTP3_BE	SN: In a RTP1_BE QoS Data frame, if QoS Control Field UP=000_2, EOSP=0_2, ACKPOLICY=00_2 and the frame type=10_2, subtype=1000_2, PASS. SN: In a RTP2_VI QoS Data frame, if QoS Control Field UP=101_2 or 100_2, EOSP=0_2, ACKPOLICY=00_2 and the frame type=10_2, subtype=1000_2, PASS. SN: In a RTP3_BE QoS Data frame, if QoS Control Field UP=000_2, EOSP=0_2, ACKPOLICY=00_2 and the frame type=102, subtype=1000_2, PASS. CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 89% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BE, RTP2_VI Receive RTP3_BE	Receive RTP1_BE RTP2_VI Transmit RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 87% or more than RTP2 in first phase (1~9s), PASS
7	Transmit RTP1_BK, RTP2_BE Receive RTP3_BK	Receive RTP1_BK RTP2_BE Transmit: RTP3_BK	SN: In a RTP2_BE QoS Data frame, if QoS Control Field UP=000_2 or 011_2, EOSP=0_2, ACKPOLICY=00_2 and the frame type=10_2, subtype 1000_2, PASS SN: In a RTP1_BK QoS Data frame, if QoS Control Field UP=010_2 or 0012, EOSP=02, ACKPOLICY=00_2 and the frame type=10_2, subtype=1000_2, PASS. CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 81% or more than RTP2 in first phase (1~9s), PASS

8	Transmit RTP1_VI, RTP2_VO Receive RTP3_VI	Receive RTP1_VI RTP2_VO Transmit: RTP3_VI	SN: In a RTP2_VO QoS Data frame, if QoS Control Field UP=110_2 or 111_2, EOSP=0_2, ACKPOLICY=00 and the frame type=10_2, subtype=10002, PASS. CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 87% or more than RTP2 in first phase (1~9s), PASS

Table 192: Traffic Differentiation in a Single BSS with 802.11n STA Procedure and Results

5.2.28 Traffic Differentiation in Single BSS with 2 802.11n STAs

Purpose and Description

Internal and distributed traffic differentiation between different traffic classes at various PHY rates involving an AP and two STAs with downstream/ upstream traffic.

For differentiation tests, the general approach is to run traffic streams using only two different priorities for any one test. Several of the tests use two streams of the lower priority to clearly show the differentiation. The intended load (load – for definition see section 3.5.1 of RFC2285) of the higher priority stream does not exceed the link capacity. The background traffic stream provides enough additional traffic to saturate the wireless link. This is true regardless of whether the priority of the background traffic is higher or lower than the DUT's traffic. Thus the total intended load of the two streams exceeds the link capacity. In this situation, it is simple to compare the backoff algorithms of two devices – the higher priority stream should always get the bandwidth it needs to achieve its intended load, while the lower priority stream gets whatever is left over. The PHY rates of the DUT and the test bed source do not matter.

Test Environment

STAUT
STA2: Testbed 802.11n 20 MHZ Capable
Testbed 802.11n 20 MHZ Capable AP1
Wireless Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	Testbed STA2 Values	Testbed AP1 Values
Vendor	-	**Intel**	**Broadcom**
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	12345678	12345678	12345678
AP Control Channel	-	-	6 or 36, Dual Band use 36
AIFS	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmin	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmax	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	Default for STAUT	DSCP	DSCP
Channel Width		0 (20 MHz)	0 (20 MHz)

Table 193: Traffic Differentiation with 2 802.11n STAs Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV20Mbps.scr
RTP2	IPTV16Mbps.scr
RTP3	IPTV16MbpsDelay10sec.scr

Table 194: Traffic Differentiation with 2 802.11n STAs Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	Script Names	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n 20 MHz Capable STA1	Testbed 802.11n 20 MHz Capable AP	Expected Results
0		Configure the STA to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Configure the AP to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
1	-	-	Beacon	
2	Probe Request	Probe Request	Probe Response	SN: If a Probe Request occurs and STAUT Probe Request contains any WMM element, FAIL
3	Association Request	Association Request	Association Response	SN: If STAUT Association Request contains WMM information element AND STA Associated, PASS
4	Transmit RTP1_BE,	Transmit RTP2_VI RTP3_BE	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
5	Transmit RTP2_VI	Transmit RTP1_BE RTP3_BE	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 88% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BK,	Transmit RTP2_BE RTP3_BK	Receive RTP1_BK RTP2_BE RTP3_BK	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
7	Transmit RTP1_VI,	Transmit RTP2_VO RTP3_VI	Receive RTP1_VI RTP2_VO RTP3_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS

Table 195: Traffic Differentiation with 2 802.11n STAs Procedure and Results

5.2.29 Traffic Differentiation in Single BSS with WMM STA

Purpose and Description

Internal and distributed traffic differentiation between different traffic classes at various PHY rates involving an AP and two STAs with downstream/ upstream traffic.

For differentiation tests, the general approach is to run traffic streams using only two different priorities for any one test. Several of the tests use two streams of the lower priority to clearly show the differentiation. The intended load (Ioad – for definition see Section 3.5.1 of RFC 2285) of the higher priority stream does not exceed the link capacity. The background traffic stream provides enough additional traffic to saturate the wireless link. This is true regardless of whether the priority of the background traffic is higher or lower than the DUT's traffic. Thus the total intended load of the two streams exceeds the link capacity. In this situation, it is simple to compare the backoff algorithms of two devices – the higher priority stream should always get the bandwidth it needs to achieve its intended load, while the lower priority stream gets whatever is left over. The PHY rates of the DUT and the test bed source do not matter.

Test Environment

STAUT
STA2: Testbed 802.11a/b/g WMM Capable
Testbed 802.11n 20 MHz Capable AP1
Wireless Sniffer
STA 2 is an 11n device operating in legacy mode with WMM on

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	Testbed STA2	Testbed AP1 Values
Vendor	-	**Intel**	**Qualcomm**
AP Control Channel	-	-	6 or 36, Dual Band use 6
AIFS	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmin	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmax	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	Default for STAUT	DSCP	DSCP
Channel Width		-	0 (20 MHz)

Table 196: Traffic Differentiation in Single BSS with WMM STA Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV20Mbps.scr
RTP2	IPTV14Mbps.scr
RTP3	IPTV14MbpsDelay10sec.scr

Table 197: Traffic Differentiation in Single BSS with WMM STA Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	Script Names	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g WMM Capable STA1	Testbed 802.11n 20 MHz Capable AP	Expected Results
0			Configure the AP to 20 MHz Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
1	-	-	Beacon	
2	Probe Request	Probe Request	Probe Response	SN: If a Probe Request occurs and STAUT Probe Request contains any WMM element, FAIL
3	Association Request	Association Request	Association Response	SN: If STAUT Association Request contains WMM information element AND STA Associated, PASS
4	Transmit RTP1_BE,	Transmit RTP2_VI RTP3_BE	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
5	Transmit RTP2_VI	Transmit RTP1_BE RTP3_BE	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 88% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BK,	Transmit RTP2_BE RTP3_BK	Receive RTP1_BK RTP2_BE RTP3_BK	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
7	Transmit RTP1_VI,	Transmit RTP2_VO RTP3_VI	Receive RTP1_VI RTP2_VO RTP3_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS

Table 198: Traffic Differentiation in Single BSS with WMM STA Procedure and Results

5.2.30 Traffic Differentiation in Single BSS with Legacy non-WMM STA

Purpose and Description

WMM capability negotiation should indicate 1 STAUT and one legacy non-WMM STA.

The fairness tests address the remaining four of the 20 possible DUT-background traffic pairings.
The test procedure differs from the differentiation tests only in the method by which the link is saturated with traffic. The fairness tests require two sources (one from the DUT and the other from the testbed) of equal AC traffic with the total intended load to exceed the channel capabilities. The two equal-AC traffic come from sources with identical characteristics (e.g., two identical RTP streams), because it is much easier to observe the equal change in frame rate of the streams when the link is saturated.

Test Environment

STAUT
STA2: Testbed 802.11a/b/g non-WMM
Testbed 802.11n AP2 in legacy mode with WMM
Wireless Sniffer
STA 2 is an 11n device operating in legacy mode – WMM off
AP1 is an 11n device operating in legacy mode – WMM on

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	TestbedSTA2	Testbed AP1 Values
Vendor	-	**Intel**	**Broadcom**
ESSID	Bg(*^J78	Bg(*^J78	Bg(*^J78
AP Control Channel	-	-	6 or 36, Dual Band use 36
AIFS	Default (see Appendix D)	-	Default (see Appendix D)
CWmin	Default (see Appendix D)	-	Default (see Appendix D)
CWmax	Default (see Appendix D)	-	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	-	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	Default for STAUT	-	DSCP
Channel Width	-	-	-

Table 199: Traffic Differentiation in Single BSS with Legacy non-WMM STA Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV18Mbps.scr
RTP2	IPTV14Mbps.scr
RTP3	IPTV14MbpsDelay10sec.scr

Table 200: Traffic Differentiation in Single BSS with Legacy non-WMM STA Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	**Script Names**	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g non-WMM STA1	Testbed 802.11n AP in legacy mode with WMM	Expected Results
0				
1	-	-	Beacon	
2	Probe Request	Probe Request	Probe Response	SN: If a Probe Request occurs and STAUT Probe Request contains any WMM element, Fail
3	Association Request	Association Request	Association Response	SN: If STAUT Association Request contains WMM information element AND STA Associated, PASS
4	Transmit RTP1_BE RTP2_VI	Transmit RTP3_BE	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 87% or more than RTP2 in first phase (1~9s), PASS
5	Transmit RTP2_VI	Transmit RTP1_BE RTP3_BE	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 90% or more than RTP2 in first phase (1~9s), PASS
6	Transmit RTP1_BE, Receive RTP2_VI	Transmit RTP3_BE	Receive RTP1_BE RTP3_BE, Transmit RTP2_VI	CH: Receive Data RTP1, RTP2, RTP3 If RTP1 in second phase (11~19s) is 186% or less than RTP3 in second phase (11~19s), PASS (fairness with legacy test). RTP1-P2/RTP3-P2 < 1.86

Table 201: Traffic Differentiation in Single BSS with Legacy non-WMM STA Procedure and Results

5.2.31 Test ACM Bit Conformance

Purpose and Description
Tests if STAUT honors ACM bits.

A STAUT is tested to determine if it behavior conforms to the ACM bit settings. ACM bit tests are only performed on STAUT. The testbed AP is configured to set the ACM bit on a particular AC and further configured to reject any TSpecs it may receive. Reference streams are transmitted on a lower AC for which the ACM bit is not set. A stream is attempted to be transmitted through the STAUT using the AC on which the ACM bit has been set. Since the AP has set the ACM bit (and will reject TSpec requests), the STAUT is not able to use that AC. The STAUT must either discard the frames or choose to use a lower AC on which the ACM bit is not set. Thus the measured throughput should be equal or less than the reference streams.

Test Environment
STAUT
STA2: Testbed 802.11a/b/g WMM Capable

AP1: Testbed 802.11a/b/g WMM Capable AP
STA 2 is an 11n device operating in legacy mode- WMM on
AP1 is an 11n device operating in legacy mode – WMM on

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	Testbed STA2	AP1 Values
Vendor	-	**Marvell**	**Marvell**
AP Control Channel	-	-	6 or 36, Dual Band use 6
AIFS	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmin	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
CWmax	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	1 (Note: testbed AP shall be configured to reject any TSpec requests)
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	Default for STAUT	DSCP	DSCP

Table 202: Test ACM Bit Conformance Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV14Mbps.scr
RTP2	IPTV10Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr

Table 203: Test ACM Bit Conformance Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	Script Name	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g WMM Capable STA1	Testbed 802.11a/b/g WMM Capable AP	Expected Results
1	-	-	Beacon	
2	Probe Request	Probe request	Probe Response	(Probe requests are optional)
3	Association Request	Association Request	Association Response	
4	Transmit RTP2_VI RTP3_BE	Transmit RTP1_BE,	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 115% or less than RTP1 in second phase (11~19s), or if RTP2 in second phase (11~19s) is 115% or less

				than RTP3 in second phase (11~19s), PASS SN: No packets shall be transmitted with QoS level AC_VI.

Table 204: Test ACM Bit Conformance Procedure and Results

5.2.32 Test the AC Parameter Modification

Purpose and Description

Tests if STAUT honors AC Parameters by making a higher number AC have "worse" AC parameters and then make sure it's performance is degraded.

A STAUT is testbed to determine if its behavior conforms to the AC parameter settings (AIFSN, CWmin, TXOP) distributed in the Beacon. AC Parameter tests are only performed on STAUT. In one test, the testbed AP is configured to vary the AC parameters on a particular AC such that a higher number AC has "worse" AC parameters and then make sure that AC's performance is degraded compared to a lower number AC. Thus the measured throughput should be less than the reference streams. In a second test, the TXOP limit for an AC is increased and the throughput is compared to a reference stream. The comparison threshold is directly proportional to the TXOP limit. If the STA is honoring the TXOP limit, its throughput will be less than the threshold.

Test Environment

STAUT
STA2: Testbed 802.11a/b/g WMM Capable
AP: Testbed 802.11a/b/g WMM Capable AP
STA 2 is an 11n device operating in legacy mode – WMM on
AP1 is an 11n device operating in legacy mode – WMM on

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	Testbed STA2	AP1 Values
Vendor	-	**Intel**	**Marvell**
ESSID	WEI823>	WEI823>	WEI823>
AP Control Channel	-	-	6 or 36, Dual Band use 36
AIFS_VO	2	2	2
AIFS_VI	10	10	10
AIFS_BE	2	2	2
AIFS_BK	2	2	2
CWmin (for all 4 ACs)	7 (ECWMIN=3)	7 (ECWMIN=3)	7 (ECWMIN=3)
CWmax (for all 4 ACs)	15 (ECWMAX=4)	15 (ECWMAX=4)	15 (ECWMAX=4)
TXOP Limit: AC_VO	Default	Default	Default
TXOP Limit: AC_VI	Default	Default	Default
TXOP Limit: AC_BE	Default	Default	Default
TXOP Limit: AC_BK	Default	Default	Default
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	Default for STAUT	DSCP	DSCP

Table 205: Test the AC Parameter Modification Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV14Mbps.scr
RTP2	IPTV10Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr

Table 206: Test the AC Parameter Modification Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	Script Name	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14Mbps.scr	IPTV3.5Mbps.scr
RTP2	IPTV10Mbps.scr	IPTV2.8Mbps.scr
RTP3	IPTV10MbpsDelay10sec.scr (with delay)	IPTV2.8MbpsDelay10sec.scr (with delay)
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g WMM Capable STA1	Testbed 802.11a/b/g WMM Capable AP	Expected Results
1	-	-	Beacon	
2	Probe Request	Probe request	Probe Response	(Probe requests are optional)
3	Association Request	Association Request	Association Response	
4	Transmit RTP2_VI RTP3_BE	Transmit RTP1_BE,	Receive RTP1_BE RTP2_VI RTP3_BE	CH: Receive Data RTP1, RTP2, RTP3 If RTP2 in second phase (11~19s) is 115% or less than RTP1 in second phase (11~19s), and

				if RTP2 in second phase (11~19s) is 115% or less than RTP3 in second phase (11~19s), PASS

Table 207: Test the AC Parameter Modification Procedure and Results

5.2.33 TXOP Limit Test

Purpose and Description

The goal of the test is to determine whether a station (STAUT) adheres to the TXOP limit rules broadcast from the AP.

A STAUT is tested to determine if its behavior conforms to the AC parameter settings (AIFSN, CWmin, TXOP) distributed in the Beacon. AC Parameter tests are only performed on STAUT. In one test, the testbed AP is configured to vary the AC parameters on a particular AC such that a higher number AC has "worse" AC parameters and then make sure that AC's performance is degraded compared to a lower number AC. Thus the measured throughput should be less than the reference streams. In a second test, the TXOP limit for an AC is increased and the throughput is compared to a reference stream. The comparison threshold is directly proportional to the TXOP limit. If the STA is honoring the TXOP limit, its throughput will be less than the threshold.

Test Environment

STAUT
STA2: Testbed 802.11a/b/g WMM Capable
AP1: Testbed 802.11a/b/g AP
STA 2 is an 11n device operating in legacy mode – WMM on
AP1 is an 11n device operating in legacy mode – WMM on

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	Testbed STA2	AP1 Values
Vendor	-	**Realtek**	**MediaTek**
AP Control Channel	-	-	6 or 36, Dual Band use 6
AIFS (for all ACs)	2	2	1
CWmin (for all 4 ACs)	7 (ECWMIN=3)	7 (ECWMIN=3)	7 (ECWMIN=3)
CWmax (for all 4 ACs)	15 (ECWMAX=4)	15 (ECWMAX=4)	15 (ECWMAX=4)
TXOPLimit: AC_VO	1 (32μS)	1 (32μS)	1 (32μS)
TXOPLimit: AC_VI	See steps 1, 3, & 5 Below	See steps 1, 3, & 5 Below	0 (one frame)
TXOP Limit: AC_BE	0 (one frame)	0 (one frame)	0 (one frame)
TXOP Limit: AC_BK	1 (32μS)	1 (32μS)	1 (32μS)
ACM: AC_VO	-	-	0
ACM: AC_VI	-	-	0
ACM: AC_BE	-	-	0
ACM: AC_BK	-	-	0
AC Tagging	Default for STAUT	DSCP	DSCP

Table 208: TXOP Test Limit Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV20Mbps.scr
RTP2	IPTV20Mbps.scr

Table 209: TXOP Test Limit Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	Script Name	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV25Mbps.scr	IPTV7Mbps.scr
RTP2	IPTV25Mbps.scr	IPTV7Mbps.scr
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g WMM Capable STA1	Testbed a/b/g Legacy AP	Expected Results
1	-	-	Set TXOP limit: AC_VI = 0 (1 frame)	
2	Transmit RTP1_VI	Transmit RTP2_BE	Receive RTP1_VI, RTP2_BE	CH: Receive Data RTP1, RTP2 If RTP1 is 177% or less than RTP2, PASS
3	-	-	Set TXOP limit: AC_VI = 24 (768 µS)	
4	Transmit RTP1_VI	Transmit RTP2_BE	Receive RTP1_VI, RTP2_BE	CH: Receive Data RTP1, RTP2 If RTP1 is 261% or less than RTP2, PASS
5	-	-	Set TXOP limit: AC_VI = 34 (1088 µS)	
6	Transmit RTP1_VI	Transmit RTP2_BE	Receive RTP1_VI, RTP2_BE	CH: Receive Data RTP1, RTP2 If RTP1 is 377% or less than RTP2, PASS

Table 210: TXOP Test Limit Procedure and Results

5.2.34 STAUT "No Acknowledgement" Test

Purpose and Description

Verify STAUT operates correctly when it receives QoS packets with "No Acknowledgement".

The testbed transmitter is configured to set the ACK policy to "No Acknowledgement" in the QoS control field of a traffic stream. A sniffer is used to verify that Acknowledgement packets are not being sent by the DUT. The throughput with the ACK policy set to "No Acknowledgement" is compared with the ACK Policy set to Acknowledgement. The test passes if the throughput is the same or higher.

Test Environment
STAUT
Testbed 802.11a/b/g WMM Capable AP1
Wireless Legacy Sniffer
AP1 is an 11n device operating in legacy mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
AP Control Channel	-	6 or 36, Dual Band use 36
AIFS	Default (see Appendix D)	Default (see Appendix D)
CWmin	Default (see Appendix D)	Default (see Appendix D)
CWmax	Default (see Appendix D)	Default (see Appendix D)
TXOPLimit	Default (see Appendix D)	Default (see Appendix D)
ACM: AC_VO	-	0
ACM: AC_VI	-	0
ACM: AC_BE	-	0
ACM: AC_BK	-	0
AC Tagging	Default for STAUT	DSCP

Table 211: STAUT "No Acknowledgement" Test Configuration

The following table defines the script that will be used for this test case.

Scripts	Script Names
RTP1	IPTV14MbpsNoAck.scr
RTP2	IPTV10MbpsNoAck.scr

Table 212: STAUT "No Acknowledgement" Test Scripts

Note: The following table defines the scripts used for Non 11n STAUT

Script	Script Name	
	802.11g, 802.11a Equipment	802.11b Equipment
RTP1	IPTV14MbpsNoAck.scr	IPTV3.5MbpsNoAck.scr
RTP2	IPTV10MbpsNoAck.scr	IPTV2.8MbpsNoAck.scr
Details of the script and parameters in Appendix H		

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11a/b/g WMM Capable AP	Expected Results
1	-	Beacon	
2	Probe request	Probe Response	(Probe requests are optional)
3	Association Request	Association Response	
4	Receive RTP1_BE, RTP2_VI	Transmit RTP1_BE RTP2_VI	SN: QoS Data frame Verify ACK policy bits are set to “Acknowledge” in packets from AP. If STAUT generates ACK packets, PASS. CH: Receive Data RTP1 and RTP2 Record values of RTP1 and RTP2 throughput
5		Configure the testbed AP to set the “ACK policy” field to “012” (no acknowledgement) in QoS Control frames for all AC (see § 2.1.6 in [2].	
6	Receive RTP1_BE, RTP2_VI	Transmit RTP1_BE RTP2_VI	SN: QoS Data frame Verify ACK policy bits are set to “No Acknowledge” in packets from AP. If STAUT does not generate ACK packets, PASS. CH: Receive Data RTP1 and RTP2 If RTP1-T06 and RTP2-T06 are 88% or more than RTP1-T04 and RTP2-T04 respectively, PASS

Table 213: STAUT “No Acknowledgement” Test Procedure and Results

5.2.35 Basic Association in 802.11n Environment

Purpose and Description
Test Association Request frame format and the existence of the appropriate information elements. Testing Adherence of STAUT to the operating mode advertisement and protection mechanism used.

Test Environment
802.11n STAUT
AP1: Testbed 802.11n 20/40 MHz Capable AP
STA2: Testbed 802.11n 20 MHz only Capable STA
STA3: Testbed 802.11ag Capable STA
802.11n Sniffer

Test Configuration

The following table defines the parameter values for the devices in the testbed.

Parameter	STAUT Values	STA2 Values	STA3 Values	AP1 Values
Vendor	-	**Intel**	**Marvell**	**MediaTek**
ESSID	%@^98jhB	%@^98jhB	%@^98jhB	%@^98jhB
Security	WPA2-PSK	WPA2-PSK	WPA2-PSK	WPA2-PSK
Encryption Key	%@^98jhB	%@^98jhB	%@^98jhB	%@^98jhB
AP Control Channel	-	-	-	6 or 36, dual band use 6 and 36 (one test run in each channel)
Supported channel width set	-	0 (20 MHz)	-	1 (20/40 MHz)

Table 214: Basic Association in 802.11n Environment Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n 20 MHz Capable STA2	Testbed 802.11ag Legacy STA3	Testbed 802.11n 20/40 MHz Capable AP	Expected Results
1		Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	-	Switch on all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
2	-			Beacon	
3	Association Request			Association Response to STAUT	Look at the HT Capability IE and record the Supported Features [HT Capabilities Info Field] a. Supported Channel Width (20MHz, or 20/40MHz)* b. HT-Greenfield c. SGI 20 d. SGI 40 e. MCS Set (1 SS, 2 SS, or 3 SS) f. MCS 32 g. Tx STBC h. Rx STBC If the supported list does not match the submission then fail. *If 20/40 MHz supported in 2.4 GHz then 20/40 MHz Coexistence support is required
4	Start a continuous Ping to AP (ping <AP IP> -l 10000 –t)				If more that 10% ping failures, then fail.
5		(After 30 seconds) Association Request		Association Response to STA2	If the ping from STAUT to AP is stopped then fail
6			(After 30 seconds) Association Request	Association Response to STA3	
7		(after 30 seconds) Disassociate			
8			(after 30 seconds) Disassociate		

Table 215: Basic Association in 802.11n Environment Procedure and Results

5.2.36 Ability to Receive 1 and 2 Spatial Streams

Purpose & Description

Confirm that 1 SS STAUTs support 1 SS in Rx side and 2 SS STAUTs support 1 and 2SS in Rx side.

Test Environment
802.11n STAUT
One Testbed 802.11n 20/40 MHz Capable AP1
Wireless 802.11n Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
AP Control Channel	-	6 or 36, Dual Band use 6 and36(steps 1-4 should be run in each channel)

Table 216: Ability to Receive 1 and 2 Spatial Streams Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results. If STAUT supports only 1 spatial stream then only use i = 7. If STAUT supports 2 spatial streams, then use i=7 and i=15.

Steps	802.11n STAUT	Testbed 802.11n 20/40 MHz Capable AP	Expected Results
1	-	Beacon/Probe responses	
2	Association Request	Association response	If the STAUT supported MCS set field in the HT Capability IE does not contain 1 in the bitmap indexes 0..7 (1 SS) or 0..15 (2 SS) then fail
For i = 7,and i = 15 execute the following steps			
3		Set the testbed AP fixed Tx rate to MCS[i] (20 MHz only) Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
4		Ping <ISTAUT P> -t –l 10000	If more that 10% ping failures, then fail.
If the STAUT is a 20/40MHz capable STA, then execute steps 5 and 6: For i = 7,and i = 15 execute the following steps			
5		Set the testbed AP fixed TX rate to MCS[i] (40 MHz) Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
6		Ping <STAUT IP> -t –l 10000	If more that 10% ping failures, then fail.

Table 217: Ability to Receive 1 and 2 Spatial Streams Procedure and Results

5.2.37 A-MPDU Aggregation when the STA is the Recipient with and without WPA2-PSK

Purpose & Description

Test Block ACK stream and A-MPDU aggregation traffic in receive side.
Test Block ACK streams from the same AP on the recipient side.
Test A-MPDU aggregation with and without WPA2-PSK security mode

Test Environment

802.11n STAUT
Testbed 802.11n 20 MHz capable AP1
802.11n Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Run all test in batch mode

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom for 1 or 2 SS STAUT** **Marvell for 3 SS STAUT**
ESSID	NONE0WPA2PSK	NONE0WPA2PSK
Security	None & WPA2-PSK	None & WPA2-PSK
Encryption Key	None & NONE0WPA2PSK	None & NONE0WPA2PSK
AP Control Channel	-	6 or 36, Dual Band use 6
Supported channel width set	-	0 (20 MHz)

Table 218: A-MPDU Aggregation when the STA is the Recipient Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20/40 MHz Capable AP	Expected Results
1	-	Enable A-MPDU aggregation Switch off all the optional features. Disable A-MSDU Aggregation.	
2	Association Request	Association Response	If the association response of STAUT is with status different than success then fail
3	Send ADDBA Response	Send ADDBA Request for TID 5	
4		Start UDP Filesndl-HT for TID 5 for 30 seconds	If Downlink throughput is less than 5.2.37T4DT1 then fail SN: Check that there are BAs
5		Change security mode to WPA2-PSK Beacon	
6	Association Request	Association Response to STAUT	If the association response of STAUT is with status different than success then fail
7	Send ADDBA Response to AP	Send ADDBA Request for TID 5	
8		Start UDP Filesndl-HT for TID 5 for 30 seconds	If Downlink throughput is less than 5.2.37T8DT1 then fail SN: Check that there are BAs

Table 219: A-MPDU Aggregation when the STA is the Recipient Procedure and Results

5.2.38 A-MSDU Aggregation when the STA is the Recipient

Purpose and Description
Test the mechanism of the A-MSDU Aggregation when the STAUT is the recipient.

Test Environment
802.11n STAUT
Testbed 802.11n 20 MHz Capable AP1 that supports both 3839 bytes and 7935 bytes Maximum A-MSDU Size in transmission

802.11n Sniffer

Test Configuration and Procedure
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
AP Control Channel	-	6 or 36, Dual Band use 36

Table 220: A-MSDU Aggregation when the STA is the Recipient Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20/40 MHz Capable AP	Expected Results
1		Enable A-MSDU Aggregation Switch off all the optional features. Disable A-MPDU Aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
2	-	Beacon	
3	Association Request	Association Response	
4		Start UDP Filesndl-HT from AP to STAUT for 1.5 minutes	If throughput is less than 5.2.38T4DT1 then fail Note: Use sniffer to check that AP1 packets are > 2346, if not then fail

Table 221: A-MSDU Aggregation when the STA is the Recipient Procedure and Results

5.2.39 Overlapping BSS – 2.4 GHz

Purpose & Description
STAUT will function correctly in an overlapping BSS environment in the 2.4 GHz frequency band.

Test Environment
802.11n STAUT
AP1: One Testbed 802.11n 20 MHz Capable AP
AP2: One Testbed 802.11g O-AP
STA2: One Testbed 802.11g O-STA
STA 2 is an 11n device operating in g legacy mode
AP2 is an 11n device operating in legacy g mode
Test Configuration
The following table defines the parameter values for the devices in the test bed. 5 GHz only devices skip this test case.

Parameter	STAUT Values	AP1 Values	STA2 Values	AP2 Values
Vendor	-	**Marvell for 1SS STAUT Qualcomm for 2SS STAUT MediaTek for 3SS STAUT**	**Broadcom for 1SS STAUT Intel for 2SS STAUT Realtek for 3SS STAUT**	**Broadcom for 1SS STAUT Marvell for 2SS STAUT Qualcomm for 3SS STAUT**
AP Control Channel	-	6	-	6

Supported channel width set	-	0 (20 MHz)	-	-

Table 222: Overlapping BSS – 2.4 GHz Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20 MHz Capable AP1	Testbed 802.11g STA2	Testbed 802.11g AP2	Expected Results
1		Set AP to 20 MHz and channel 6 Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.		Set to channel 6	
2	-	Beacon/Probe responses		Beacon/Probe Responses	
3	Association Request to AP1	Association response to STAUT	Association Request to AP2	Association Response to STA2	
4	Start TCP High Performance Throughput from STAUT to AP1 for 1 minute Uplink 1.1		Start TCP FileSndL from STA2 to AP2 for 1 minute Uplink 2.1		If Uplink 1.1 throughput is less than 5.2.39T4DT2A then fail If Uplink 2.1 throughput is less than 5.2.39T4DT2B then fail

Table 223: Overlapping BSS – 2.4 GHz Procedure and Results

5.2.40 Overlapping BSS – 5 GHz

Purpose & Description

STAUT will function correctly in an overlapping BSS environment in the 5 GHz frequency band.

Test Environment

802.11n STAUT
AP1: One Testbed 802.11n 20 MHz Capable AP
AP2: One Testbed 802.11a
STA2: One Testbed 802.11a
STA 2 is an 11n device operating in a legacy mode
AP2 is an 11n device operating in legacy a mode

Test Configuration

The following table defines the parameter values for the devices in the test bed. 2.4 GHz only devices skip this test case.

Parameter	STAUT Values	AP1 Values	STA2 Values	AP2 Values

Vendor	-	**Marvell for 1SS STAUT** **Qualcomm for 2SS STAUT** **MediaTek for 3SS STAUT**	**Marvell for 1SS or 2SS STAUT** **Realtek for 3SS STAUT**	**MediaTek for 1SS or 2SS STAUT** **Qualcomm for 3SS STAUT**
AP Control Channel	-	36	-	36
Supported channel width set	-	0 (20 MHz)	-	-

Table 224: Overlapping BSS – 5 GHz Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20/40 MHz Capable AP1	Testbed 802.11a STA2	Testbed 802.11a AP2	Expected Results
1		Set AP to 20 MHz and channel 36 Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.		Set to channel 36	
2	-	Beacon/Probe responses		Beacon/Probe Responses	
3	Association Request to AP1	Association response to STAUT	Association Request to AP2	Association Response to STA2	
4	Start TCP High Performance Throughput from STAUT to AP1 for 1 minute Uplink 1.1		Start TCP FileSndL from STA2 to AP2 for 1 minute Uplink 2.1		If Uplink 1.1 throughput is less than 5.2.40T4DT2A then fail If Uplink 2.1 throughput is less than 5.2.40T4DT2B then fail

Table 225: Overlapping BSS – 5 GHz Procedures and Results

5.2.41 HT-Greenfield Operation

Purpose and Description
STAUT is appropriately receiving HT-Greenfield packets.
STAUT appropriately adhere to the Non-Greenfield HT STAs exists indication by the AP.
STAUT will use protection before transmitting GF packets when non-Greenfield HT STAs are associated.

Test Environment
802.11n STAUT
Testbed 802.11n 20 MHz Capable AP1STA2: Testbed 802.11n 20 MHz Capable (HT-GF disabled)
Run in a clean environment (Chamber)
Wireless 802.11n Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	STA2 Values	AP1 Values
Vendor	-	**Realtek**	**MediaTek**
ESSID	G5ee8fi04ld	G5ee8fi04ld	G5ee8fi04ld
AP Control Channel	-	-	6 or 36, Dual Band use 6
Supported channel width set	-	0 (20 MHz)	0 (20 MHz)
Green Field	-	Not supported	1

Table 226: HT-Greenfield Operation Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20 MHz Capable STA2	Testbed 802.11n 20 MHz Capable AP	Expected Results
1		Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Enable HT-GF Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	
2	-		Beacon	
3	Association Request		Association Response to STAUT	
4			Ping <STAUT IP> -l 10000 -t	If more that 10% ping failures, then fail. SN: Verify that the test bed AP is sending with Greenfield preamble. If not, there is a test bed problem. Reconfigure and try again -
5		Association Request	Association Response to STA2	
6	Ping <AP IP> -l 10000 -t			If ping replies do not continue then fail. SN: Verify that 1T1R STAUT sends ICMP Requests with either - Mixed Mode preamble OR - Greenfield preamble with protection - Else FAIL

Table 227: HT-Greenfield Operation Procedure and Results

5.2.42 Short GI Operation

Purpose and Description
STAUT is appropriately receiving Short GI.

Test Environment
802.11n STAUT
Testbed 802.11n 20 MHz Capable AP1 (Support SGI 20 MHz)
Wireless 802.11n Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Marvell**
ESSID	h0rtG7	h0rtG7
AP Control Channel	-	6 or 36, Dual Band use 36
Supported channel width set	-	0 if STAUT supports SGI at 20 MHz, otherwise use 1
SGI	-	1

Table 228: Short GI Operation Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n Capable AP	Expected Results
1		Enable SGI Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
2	-	Beacon/Probe responses	
3	Association Request	Association response	If the STAUT is not setting the SGI in the association request then fail
4		Ping <STAUT IP> -l 10000 –t	If more that 10% ping failures, then fail.

Table 229: Short GI Operation Procedure and Results

5.2.43 Overlapping BSS on the Extension Channel

Purpose and Description
STAUT appropriately sense the extension channel before any 40 MHz transmission.

Test Environment
802.11n 20/40 MHz capable STAUT
AP1: Testbed 802.11n 40 MHz Capable AP
AP2: Testbed 802.11a
STA2: Testbed 802.11a
STA 2 is an 11n device operating in legacy a mode
AP2 is an 11n device operating in legacy a mode

Test Configuration
The following table defines the parameter values for the devices in the test bed. The overlapping BSS has to be on the extension channel.

Parameter	STAUT Values	AP1 Values	STA2 Values	AP2 Values
Vendor	-	MediaTek for 1SS STAUT Marvell for 2SS STAUT MediaTek for 3SS STAUT	Realtek for 1SS STAUT Marvell for 2SS STAUT Realtek for 3SS STAUT	Qualcomm for 1SS STAUT MediaTek for 2SS STAUT Qualcomm for 3SS STAUT
AP Control Channel	-	36	-	40
Supported channel width set	-	1 (20/40 MHz)	-	-

Table 230: Overlapping BSS on the Extension Channel Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 40 MHz Capable AP1	Testbed 802.11a STA2	Testbed 802.11a AP2	Expected Results
1		Set channels 36 and 40 Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.		Set to channel 40	
2	-	Beacon/Probe responses		Beacon/Probe responses	
3	Association Request to AP1	Association response to STAUT	Association Request to the AP2	Association Response to the STA2	
4	Start TCP High Performance Throughput from STAUT to AP1 for 1 minute Uplink 1.1		Start TCP FileSndL from STA2 to AP2 for 1 minute Uplink 2.1		If Uplink 1.1 throughput is less than 5.2.43T4DT2A then fail

					If Uplink 2.1 throughput is less than 5.2.43T4DT2B then fail

Table 231: Overlapping BSS on the Extension Channel Procedure and Results

5.2.44 HT Duplicate Mode (MCS Index = 32)

Purpose and Description
STAUT is ability to receive HT-Duplicate Mode when it is advertised.

Test Environment
802.11n STAUT
Testbed 802.11n 20/40MHZ Capable AP1 (Support MCS 32)

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor	-	**Broadcom**
AP Control Channel	-	1 or 36, dual band use 36
Supported channel width set	-	1 (20/40 MHz)
MCS index 32	-	1

Table 232: HT Duplicate Mode (MCS Index = 32) Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20/40 MHz Capable AP	Expected Results
1	-	Beacon/Probe responses	
2	Association Request	Association response	
		Set the Testbed AP to send data with fixed MCS index 32 Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.	
3		Ping <STAUT IP> -l 10000 –t	If more that 10% ping failures, then fail

Table 233: HT Duplicate Mode (MCS Index = 32) Procedure and Results

5.2.45 RIFS Test

Purpose and Description
STAUT is appropriately receiving RIFS packets in 20 MHz.
STAUT is appropriately receiving RIFS packets in 20/40 MHz.

Test Environment
802.11n STAUT
Testbed 802.11n 20/40 MHz RIFS Capable AP1
802.11n Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.
Run test for 100 pings with length of 30,000 bytes
The test is run multiple times with the testbed RIFS transmitter as outlined in table 258.
2.4 GHz single band devices use row 1, 5 GHz single band devices use row 2, and dual band devices use row 3.

Device Capability	Broadcom AP RIFS Tx
2.4 GHz, 20 MHz	Run test in 20 MHz
5 GHz, 20 MHz, 40 MHz, 20/40 MHz	Run test in 20/40 MHz
2.4 GHz & 5 GHz, 20 MHz, 40 MHz, 20/40 MHz	Run test in 5 GHz, 20/40 MHz

Table 234: RIFS Test Configurations

Parameter	802.11n AP	STAUT Values
Vendor	**Broadcom 11n**	-
ESSID	R1F5%	R1F5%
AP Control Channel	1 or 36	-

Table 235: RIFS Operation Configuration

Test Procedure and Expected Results[5]
The following table defines the test procedures and expected results.

Steps	Testbed 802.11n 20/40 MHz Capable AP	802.11n STAUT	Expected Results
1	Use MCS 4 for single stream devices and MCS 12 for non single stream devices Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the AP to reject any ADDBA request by sending ADDBA response with status DECLINE.		
2	Association Response to STAUT	Association Request	
3	Start a long packet ping to Endpoint 1. Ping xx.xx.xx.xx –l 30000 –v 160 –n 100		The number of lost pings should be less than 30% SN. Check that there are no ACKs during RIFS frame sequence

Table 236: RIFS Operation Procedure and Results

[5]For 1x1 devices use MCS 4

5.2.46 STBC Receive Test

Purpose and Description
Confirm that the STAUT supports STBC on Rx side.
This test is only for STAUTs that support STBC on the Rx side and can be configured to 1x1.

Test Environment
802.11n STAUT
Testbed 802.11n AP1 capable of STBC Transmit
Wireless 802.11n Sniffer
Run in Clean environment (Chamber)

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor		**Qualcomm**
ESSID	5T8CRx%	5T8CRx%
AP Control Channel	-	1 or 36
STBC Rx	-	-
STBC Tx	-	1
Tx Maximum Number Spatial Streams Supported (in Supported MCS Set field)	1	2

Table 237: STBC Receive Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20/40MHz Capable AP	Expected Results
1			
2	-	Beacon	
3	Association Request	Association response to STAUT	If the Rx STBC subfield value in Association Request is 0 then fail
4		Ping STAUT	If more that 10% ping failures, then fail.

Table 238: STBC Receive Test Procedure and Results

5.2.47 A-MPDU Aggregation when the STA is the Transmitter

Purpose and Description
Test the mechanism of the A-MPDU Aggregation when the STAUT is the transmitter.

Test Environment
802.11n STAUT
Testbed 802.11n AP1 that supports 1 Spatial Streams
Testbed 802.11n AP2 that supports 2 Spatial Streams
Testbed 802.11n AP3 that supports 3 Spatial Streams

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values	AP2 Values	AP3 Values
Vendor	-	**MediaTek**	**Qualcomm**	**Marvell**

AP Control Channel	-	6 or 36, Dual Band use 36	6 or 36, Dual Band use 36	6 or 36, Dual Band use 36
Spatial Stream Support	-	1	2	3
Channel width	-	0	0	0
Short GI	-	Disabled	Disabled	Disabled
Green Field	-	Disabled	Disabled	Disabled

Table 239: A-MPDU Aggregation when the STA is the Transmitter Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n AP1	Testbed 802.11n AP2	Testbed 802.11n AP3	Expected Results
1	Association request to AP1	Association response			
2	Send ADDBA request to AP1 on TID0	Send ADDBA response to STAUT			
3	Start UDP Filesndl-HT on TID0 to STA1 x 4 pairs (Uplink 1)				If the Uplink 1 throughput is less than 5.2.47T3DT1 then fail. If the sniffer doesn't indicate Uplink traffic is aggregated – A-MPDU, then fail
If STAUT support more than 1 Spatial stream transmission than continue, else stop test					
4	Association request to AP2		Association response		
5	Send ADDBA request to AP2 on TID0		Send ADDBA response to STAUT		
6	Start UDP Filesndl-HT on TID0 to STA1 x 4 pairs (Uplink 2)				If the Uplink 2 throughput is less than 5.2.47T6DT1then fail. If the sniffer doesn't indicate Uplink traffic is aggregated – A-MPDU, then fail
If STAUT support more than 2 Spatial stream transmission than continue, else stop test					
7	Association request to AP3			Association response	
8	Send Addba request to AP3 on TID0			Send ADDBA response to STAUT	
9	Start UDP Filesndl-HT on TID0 to STA1 x 4 pairs (Uplink 3)				If the Uplink 3 throughput is less than 5.2.47T9DT1 then fail. If the sniffer doesn't indicate Uplink traffic is aggregated – A-MPDU, then fail

Table 240: A-MPDU Aggregation when the STA is the Transmitter Procedure and Results

5.2.48 STA 20/40 MHz Coexistence

Purpose and Description
STAUT is appropriately reporting the existence of a non-HT AP or a 40 MHz-intolerant HT AP.
STAUT is appropriately switching from 40 MHz BW to 20 MHz BW when its AP changes to 20 MHz channel width.

Test Environment
802.11n 20/40 MHz capable STAUT
AP1: Testbed 802.11n 20/40MHz Capable
AP2: Testbed 802.11n 20/40 MHz Capable
AP3: Testbed 802.11g non-HT AP
Wireless 802.11n Sniffer
AP3 is an 11n device operating in legacy g mode

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	802.11n Testbed AP1 Values	802.11n Testbed AP2 Values	802.11g Testbed AP3 Values
Vendor	-	**Qualcomm**	**Broadcom**	**Marvell**
AP Primary Channel	-	5	10	3
Supported Channel Width Set	1 (20/40 MHz)	1 (20/40 MHz)	1 (20/40 MHz)	-

Table 241: 20/40 MHz Coexistence Channel Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	STAUT	Testbed 802.11n 20/40 MHz Capable AP1	Testbed 802.11 20/40 MHz Capable AP2	Testbed 802.11g non-HT AP3	Expected Results
1	Set the STAUT to 20/40 MHz	Set the BSS Channel Width Trigger scan interval to 180 seconds			
2	Association Request ping <AP1_IP> -l 10000 -t	Association Response			If STAUT cannot associate then fail If more that 10% ping failures, then fail. If STAUT is not using 40Mhz rates check your configuration and restart test.
3			Power up AP2 Set the “40 MHz Intolerant” field of the HT Capability Info field to 1	Power up AP3	
4	Wait 200 Seconds				If STAUT didn't send a “20/40 BSS Coexistence” Management frame to AP within the waiting time than fail

					If the “20 MHz BSS Width Request” bit not set to 1 than fail If the “20/40 BSS Intolerant Channel Report” element is not present than fail If the “20/40 BSS Intolerant Channel Report” element does not contain channel 3 in its channel list than fail
5		AP will Set the “STA Channel Width” and “Secondary Channel Offset” fields of HT Operation Element in the Beacon to 0			If more that 10% ping failures, then fail. If STAUT is still using 40 MHz rates than fail.

Table 242: 20/40 Coexistence Operation Procedure and Results

5.2.49 Ability to Receive 3 Spatial Streams

Purpose and Description
Confirm that the STAUT supports 3 SS in Rx side.

Test Environnent
802.11n STAUT
One Testbed 802.11n 20/40 MHz Capable AP1
Wireless 802.11n Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1 Values
Vendor	-	**MediaTek**
ESSID	R811nk5780+_	R811nk5780+_
AP Control Channel	-	6 or 36, Dual Band use 6 and36 (one test run in each channel)

Table 243: Ability to Receive 3 Spatial Streams Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n 20/40 MHz Capable AP	Expected Results
0	-	Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	-
1	-	Beacon/Probe responses	
2	Association Request	Association response	If the STAUT supported MCS set field in the HT Capability IE does not contain 1 in the bitmap indexes 16-23 (3 SS) than fail

For i = 23			
3		Set the testbed AP fixed Tx rate to MCS[i] (20 MHz only)	
4		Ping <STAUT IP> -l 10000 -t	If more that 10% ping failures, then fail.
If the STAUT is a 5 GHz and 20/40MHz capable AP, then execute steps 5 and 6: For i = 23			
5		Set the testbed AP fixed Tx Rate to MCS[i] (40 MHz)	
6		Ping < STAUT IP> -t –l 10000	If more that 10% ping failures, then fail.

Table 244: Ability to Receive 3 Spatial Stream Procedure and Results

5.2.50 STAUT Transmitting to AP using Supported Number of Spatial Streams

Purpose and Description

Confirm that the STAUT transmits using the correct number of spatial streams as advertised by the AP.

Test Environnent

802.11n STAUT
AP1: Testbed 802.11n AP that supports 2 Spatial Streams
AP2: Testbed 802.11n AP that supports 3 Spatial Streams
Wireless 802.11n Sniffer

Test Configuration

The following table defines the parameter values for the devices in the testbed.

Parameter	STAUT Values	AP1 Values	AP2 Values
Vendor	-	**Qualcomm**	**Marvell**
AP Control Channel	-	6 or 36, Dual Band use 36	6 or 36, Dual Band use 6 &36 (one test run per channel)
Supported Channel Width	-	0 (20 MHz)	0 (20 MHz)
Spatial Stream Support		2	3

Table 245: STAUT Transmitting to AP using Supported Number of Spatial Streams Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	802.11n STAUT	Testbed 802.11n AP1	Testbed 802.11n AP2	Expected Results
1	-	Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	Switch off all the optional features. Disable AMPDU and AMSDU aggregation. Configure the STA to reject any ADDBA request by sending ADDBA response with status DECLINE.	
2		Beacon/Probe responses with MCS support rates are 0 to 15		
3	Association Request	Association response		Note Supported MCS set of STAUT
4	ping <AP1_IP> -n 100 –l 1000			If more that 10% ping failures, then fail. Use the sniffer to check that the STAUT transmitted at least 10 ping requests at data rates that are equal to

				or greater than 52 Mbps (MCS = 5) for 1x1 STAUT, then pass Use the sniffer to check that the STAUT transmitted at least 10 ping requests at data rates that are equal to or greater than 104 Mbps (MCS = 13) for 2x2 STAUT, then pass
If the STAUT's maximum supported MCS rate in step 3 equals 15 then end test. Otherwise proceed with steps 5 through 7.				
5			Beacon/Probe responses with MCS support rates are 0 to 23	
6	Association Request		Association response	
7	ping <AP2_IP> -n 100 –l 1000			If more that 10% ping failures, then fail. Use the sniffer to check that the STAUT transmitted at least 10 ping requests at data rates that are equal to or greater than 156 Mbps (MCS = 21) then pass

Table 246: STAUT Transmitting to AP using Supported Number of Spatial Streams Procedure and Results

5.2.51 Disallow TKIP with HT Rates Test

Purpose and Description
Ensure that the STAUT does not use HT rates when using TKIP as the encryption cipher. Skip this test if the STAUT doesn't support mixed mode WPA2/WPA.

Test Environment
802.11n STAUT
AP1: 11n AP
Wireless 802.11n sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	AP1
Vendor		**MediaTek 11n**
ESSID	Bko(621	Bko(621
AP Channel	-	36 0r 11

Table 247: Disallow TKIP with HT Rates Test Configuration

WPA-PSK Only Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Step	Action	Results
1	Set up the test bed AP with HT and WPA-PSK only (TKIP only). Set the STAUT to mixed mode WPA2/WPA	
2	Force the STAUT to do an active scan. Using the 11n sniffer, look at the Beacons and Probe Responses from the test bed AP.	Verify that the Beacons and Probe Responses from the test bed AP contain IE 45 and that TKIP is the only advertised pairwise cipher suite. If not, there is a test bed problem. Correct the configuration and restart test.
3	Try to associate the STAUT to the test bed AP.	
4	Using the 11n sniffer, look at the Association Request from the STAUT.	If there is no Association Request from the STAUT, the STAUT passes the test. Skip the remaining steps. If there is an Association Request from the STAUT and IE 45 is present in the Association Request, the STAUT fails the test. Skip the remaining steps. If there is an Association Request from the STAUT and IE 45 is not present in the Association Request, continue to the next step.
5	Run a test script that emulates a long file transfer from the STAUT to a PC on the wired Ethernet side of the test bed AP for at least 10 seconds.	
6	Using the 11n sniffer, collect 10 seconds of data packets.	If any of the data packets from the STAUT are sent at HT rates, the STAUT fails the test. Skip the remaining steps. If all of the data packets from the STAUT are sent at non-HT rates, the the STAUT passes the test.
7		

Table 248: Disallow TKIP with HT Rates Test Procedure and Results

5.2.52 STA Negative tests to ensure WEP is not used with HT associations in 11n devices

Purpose and Description
The 11n test bed AP must allow association using WEP with HT. Note that this is a special capability, and is for testing purposes only.
Mandatory test if WEP is implemented on the 11n STAUT.

Test Environment
802.11n STAUT
11n test bed AP
Wireless 802.11n sniffer
AP has the ability to set WEP + HT

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT values	AP values
Vendor	-	**Marvell**
AP channel	-	36 or 11
Security	-	WEP
Encryption Key	-	0x9876543210

Table 249STA Negative WEP Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Step	Action	Results
1	Set up the test bed AP with HT and WEP.	
2	Force the STAUT to do an active scan. Using the 11n sniffer, look at the Beacons and Probe Responses from the test bed AP.	Verify that the Beacons and Probe Responses from the test bed AP contain IE 45 and that WEP is the only advertised security. If not, there is a test bed problem. Correct the configuration and restart test.
3	Try to associate the STAUT to the test bed AP.	
4	Using the 11n sniffer, look at the Association Request from the STAUT.	If there is no Association Request from the STAUT, the STAUT passes the test. Skip the remaining steps. If there is an Association Request from the STAUT and IE 45 is present in the Association Request, the STAUT fails the test. Skip the remaining steps. If there is an Association Request from the STAUT and IE 45 is not present in the Association Request, continue to the next step.
5	Run 1000 byte pings from a PC on the wired Ethernet side of the test bed AP to the associated STAUT for at least 10 seconds.	
6	Using the 11n sniffer, collect 10 seconds of pings.	If any of the data packets from the STAUT are sent at HT rates, the STAUT FAILS the test. Skip the remaining steps. If all of the data packets from the STAUT are sent at non-HT rates, the STAUT passes the test.
7		

Table 250STA Negative WEP Test Procedure and Results

5.2.53 Support for WPA2/AES if WPA/TKIP is supported

Purpose and Description
The purpose of this test is to ensure that STAs that support WPA/TKIP also support WPA2/AES concurrently. When presented with an AP in mixed WPA2/WPA security mode, the STAUT must always select WPA2 usage over WPA. Skip if WPA/TKIP is not implemented.

Test Environment
802.11 STAUT
AP capable of selecting 3 separate authentication methods (WPA, WPA/WPA2 mixed mode and WPA2 only).

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	MediaTek
SSID	-	PcachePc
Beacon Interval (ms)	-	100
Channel	-	6 or 36, Dual Band use 6
Security Type 1	Mixed Mode WPA2/WPA-PSK=Pcache	WPA-PSK=PcachePc
Security Type 2	Mixed Mode WPA2/WPA-PSK=Pcache	Mixed Mode WPA2/WPA-PSK=PcachePc
Security Type 3	Mixed Mode WPA2/WPA-PSK=Pcache	WPA2-PSK=PcachePc

Table 251b: Support for AES if TKIP is supported Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	AP1	Expected Results
0		Configure the AP for non-11n mode and pure WPA-PSK using key "12345678"	
1	Association Request	Association Response	
2	Initiate a directed ping from the STAUT to a PC connected to the Ethernet port of AP1 to ensure that STAUT can both receive and send application-level traffic.		The STAUT can connect to AP1 using WPA (TKIP) then send and receive ping traffic on the associated network **If pings do not succeed, the test fails**
3	Do not change anything on the STAUT.	Configure the AP for WPA/WPA2 mixed mode using key "12345678"	
4	(Re)Association Request	(Re)Association Response	
4.1	Optional – Disconnect the STAUT from the AP and then reconnect to the AP.		
5	Initiate a directed ping from the STAUT to a PC connected to the Ethernet port of AP1 to ensure that STAUT can both receive and send application-level traffic.		The STAUT can connect to AP1 using WPA/WPA2 mixed mode then send and receive ping traffic on the associated network. Verify with sniffer that he STAUT connects using AES. If the STAUT connects using TKIP, wait for 65 seconds to see if the STAUT changes from TKIP to AES. **If pings do not succeed, or the STAUT does not change to AES, the test fails**
6	Do not change anything on the STAUT.	Configure the AP for WPA2 using key "12345678"	
7	(Re)Association Request	(Re)Association Response	
8	Initiate a directed ping from the STAUT to a PC connected to the Ethernet port of AP1 to ensure that STAUT can both receive and send application-level traffic.		The STAUT can connect to AP1 using WPA2 then send and receive ping traffic on the associated network. **If pings do not succeed, the test fails**

5.2.54 removed

5.2.55 OOB-STAUT association (Testbed AP: PMF enabled, supports SHA-1 only)

Purpose and Description
Verify that the STAUT can associate to a PMF enabled AP which advertises only SHA-1 in the RSN IE.

Note: If STAUT doesn't support PMF in OOB, execute **procedure a** else execute **procedure b**.

Test Environment

STAUT
PMF Testbed AP
PMF Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameters	STAUT Values	AP1 Values
Vendor	-	Qualcomm Atheros PMF AP
SSID	-	Association
Channel	-	11 or 40, Dual Band use 11
Security	WPA2-PSK	WPA2-PSK
Encryption Key	Association	Association
Supplicant	default	-
PMF configuration	OOB	Enabled, but not required

OOB-STAUT Association (Testbed AP: PMF enabled, supports SHA-1 only)

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Note: If STAUT doesn't support "PMF" in OOB, execute **procedure a** else execute **procedure b**.

Test Procedure a: STAUT doesn't support PMF in OOB

Steps	STAUT	AP1	Expected Results
1		Configure the test bed AP to have PMF enabled, but not required.	Using the wireless sniffer, check the RSN IE of the beacons from the test bed AP and verify the following information: a) AKM (Authentication key management) is set to SHA-1. b) MFPC (Management frame protection capable) bit is set to 1. c) MFPR (Management frame protection required) bit is set to 0. Continue the test if the above (a, b, c) steps are pass, else stop the test and check the test bed configuration.
2	Associate the STAUT to the test bed AP.		Using the wireless sniffer, check the RSN IE of the association request from STAUT and verify the following information: a) AKM set to SHA-1 b) MFPC bit is set to 0. c) MFPR bit is set to 0. Using the wireless sniffer, also verify: d) The 4-way handshake negotiation was completed. Continue the test if the above (a, b, c, d) steps are pass, else the test failed.
3		Start a ping from a console connected to the test bed AP to the STAUT.	If the STAUT responds to the ping requests within 90 seconds, the test passes.

Test Procedure b: STAUT supports PMF in OOB

Steps	STAUT	AP1	Expected Results
1		Configure the test bed AP to have PMF enabled, but not required.	Using the wireless sniffer, check the RSN IE of the beacons from the test bed AP and verify the following information: a) AKM (Authentication key management) is set to SHA-1. b) MFPC (Management frame protection capable) bit is set to 1. c) MFPR (Management frame protection required) bit is set to 0.

			Continue the test if the above (a, b, c) steps are pass, else stop the test and check the test bed configuration.
2	Associate the STAUT to the test bed AP.		Using the wireless sniffer, check the RSN IE of the association request from STAUT and verify the following information: a) AKM set to SHA-1 b) MFPC bit is set to 1. Using the wireless sniffer, also verify: c) The PMF key negotiation was completed. Continue the test if the above (a, b, c) steps are pass, else the test failed.
3		Start a ping from a console connected to the test bed AP to the STAUT.	If the STAUT responds to the ping requests within 90 seconds, the test passes.

5.2.56 removed

5.2.57 removed

5.2.58 removed

5.2.59 removed

5.2.60 removed

5.3 IBSS STAUT Test Cases

If stations under test (STAUT) support IBSS, these tests are required. IBSS interoperability testing is divided into a campaign that covers all of the requirements in section 2. Each test has a separate test bed configuration that utilizes different options so that all meaningful combinations are verified.

For all dual-band devices (5 GHz and 2.4 GHz), all IBSS tests are run for both bands; i.e., the tests are run twice, once in the 5 GHz band and once in the 2.4 GHz band.

For the STAUT acting as the IBSS creator, if the supplicant does not allow the channel to be set, then the STAUT is allowed to select the channel for the IBSS. For sniffer monitoring, the test bed stations' supplicant may tell what channel is being used; if not, then the tester will need to scan for the channel. For the cases where the test bed station is the creator, the STAUT will join on the appropriate channel.

Use Ethernet network to handle the management data for all IBSS tests.

All tests are run for 90 seconds.

5.3.1 IBSS Test

Purpose and Description
Verify that the STAUT can create an IBSS and pass data.

Test Environment
STAUT Testbed 802.11n 20/40 MHz capable STA2 – operating in 802.11 a/b/g mode
Wireless Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	TestbedSTA2 Values
Vendor	-	**Marvell**
ESSID	WI-FI_IBSS	WI-FI_IBSS
Channel	6 or 48	-

Table 251: IBSS Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11 STAUT	STA1	Expected Results
1	Create IBSS Network Start Sniffer		-
2	-	Start IBSS Mode	STAUT responds with Basic rate enumerated in beacon message is per default channel is correct
3	Start TCP throughput FILESNDL to testbed STA 1.1, run for 90 seconds	Start TCP throughput FILESNDL to STAUT 2.1, run for 90 seconds	If 1.1 throughput is less than 5.3.1SI1DT2 then fail If 2.1 throughput is less than 5.3.1SI1DT1 then fail

Table 252: IBSS Scanning Test Procedure and Results

5.3.2 IBSS WEP On & Off Test

Purpose and Description
This tests that beacons are distributed fairly among participating IBSS, validates that the STAUT can join an established, WEP *enabled* IBSS and communicate with stations having RTS off or on. Group traffic operation is also tested.
If WEP is not supported, run this test using no security.

Test Environment
STAUT (operating in Legacy mode)
STA2: Testbed 802.11n 20/40 MHz capable STA – operating in Legacy mode
STA3: Testbed 802.11n 20/40 MHz capable STA – operating in Legacy mode
Wireless Sniffer

Test Configuration
The following table defines the parameter values for the devices in the test bed. The test is performed twice (WEP On and Off).

Parameter	STAUT Values	Testbed STA2 Values	Testbed STA3 Values
Vendor	-	**Broadcom**	**Marvell**
Security	Open & WEP 0xdeadbeef12	Open & WEP 0xdeadbeef12	Open & WEP 0xdeadbeef12
ESSID	IBSS WEP on	IBSS WEP on	IBSS WEP on
Channel	-	-	6 or 44

Table 253: IBSS WEP On & Off Test Configuration

Test Procedure and Expected Results
The following table defines the test procedures and expected results.

Steps	802.11n STAUT	STA1	STA2	Expected Results
1	-	.	Create IBSS Network Start Sniffer	-
2	Start IBSS Mode	Start IBSS Mode	-	If the STAUT does not join IBSS network then fail (verify basic rate enumeration in the beacon message is the default). If beacons not distributed evenly between participating STAs, then fail. (33% +/- 20%) (13% to 53%)
3	Start TCP throughput FILESNDL to testbed STA1 1.1 for 90 seconds	Start TCP throughput FILESNDL to STAUT 2.1 for 90 seconds	-	If 1.1 completes without errors then pass If 2.1 completes without errors then pass
4	-	-	Start group traffic real-audio test as broadcaster – REALAUD.scr	If STAUT does not receive group traffic fail
5	Start group traffic real-audio test as broadcaster	-	-	If STA1 does not receive group traffic fail If STA2 does not receive group traffic fail

Table 254: IBSS WEP On & Off Test Procedure and Results

5.3.3 IBSS Rejoin Test

Purpose and Description

Tests the ability of the STAUT to leave an IBSS and later rejoin it.

The STAUT is initially a member of an IBSS. It is then isolated from the IBSS, without restarting it. This isolation may be achieved either by physically moving the stations or by isolating in a suitable RF cage. Once isolated, the STAUT is then brought back within range of the original IBSS.

The TE cannot perform this test if the STAUT is physically removed from the test area. If removed, the test must be done manually.

Test Environment

802.11n 20/40 MHz capable STAUT (operating in Legacy mode)
STA2: Testbed 802.11n 20/40 MHz capable STA – operating Legacy mode
STA3: Testbed 802.11n 20/40 MHz capable STA – operating in Legacy mode
Wireless Sniffer

Test Configuration

The following table defines the parameter values for the devices in the test bed.

Parameter	STAUT Values	Testbed STA2 Values	Testbed STA3 Values
Vendor	-	**Marvell**	**Broadcom**
ESSID	Rejoin	Rejoin	Rejoin
Channel	-	-	6 or 36

Table 255: IBSS Rejoin Test Configuration

Test Procedure and Expected Results

The following table defines the test procedures and expected results.

Steps	STAUT	STA1	STA2	Expected Results
1	-		Create IBSS Network Start Sniffer All STAs are co-located and within range of each other	-
2	Start IBSS Mode	Start IBSS Mode	-	If the STAUT does not join IBSS network then fail (sniff beacon messages and record contents of a beacon for this IBSS network).
3	Move STAUT out of range of the IBSS network	-	-	Verify that beacons from STAUT are no longer received (the original IBSS survives without STAUT).
4	Move STAUT back within range of the IBSS network	-	-	Verify that all 3 STAs have rejoined into one IBSS by sniffing beacon messages (each STA must use the BSS parameter of the original IBSS, including basic rate set).
5	Ping STA1 Ping STA2	-	-	If no ping response from STA1, then fail. If no ping response from STA2, then fail.

Table 256: IBSS Rejoin Test Procedure and Results

6 Appendix A: Test Bed Products

All vendor equipment is available exclusively from:

Amber Buscemi
Melvin Simmonds

Tessco Technologies
11126 McCormick Road
Hunt Valley, Maryland 21031

buscemia@tessco.com
simmonsm@tessco.com

Note that the distributor does NOT supply technical support and cannot answer technical questions regarding this equipment. A contact person for each device is listed herein. They may be able to direct technical questions to the correct resource.

The current list of all testbed equipment for all Wi-Fi Alliance testbeds can be accessed at the following ftp site:

wlabs.wi-fi.org
UN: testbeds
PW: {this changes on a frequent basis, please visit **http://www.wi-fi.org/testing_information.php**

Laptops for testbed stations should have Gigabit Ethernet port

Switches should have gigabit Ethernet ports

802.11n Stations

	Product	Version	Contact
Realtek	RTL8812BU	WTS – 10.9.1222.2016 Driver – 1030.14.920.2016 Windows 10 64-bit	wfa_help@realtek.com
Broadcom	BCM94360MC	6.30.190.17 Wi-Fi Test Suite version: 1.137	wfa-support-list@broadcom.com
Intel	6300 633AN.HMWG 633AN.HMWWB	13.5.0.6 Windows 7	wfa.external.support@intel.com
Marvell	RD-88W-8897-WIFI-S0	WTS - 11N(07:26:04 Mar 7 2016), 11N Testbed 1.04 Driver - PCIE8897-15.68.6.p5-M2615485.p3-GPL-(FP68)	wifilab-support@marvell.com

Table 257: 802.11n Stations

802.11n Access Points

	Product	Version	Contact
Qualcomm	CA-65-Y9345-LCT	IPQ8064.ILQ.3.2.r3-000000014-P-1	wfa_external_support@mailman.atheros.com
Broadcom	BCM94718NR	5.22.69.2	wfa-support-list@broadcom.com
Marvell	CD-88W-AP95-A0	5.0.6.2C	wifilab-support@marvell.com
MediaTek	RT3800PDAP2	2.4.3.5	wfa-support@mediatek.com
Qualcomm Atheros	AR5KAP-096PMF	hostapd v0.8.x-qca-3	wfa_external_support@mailman.atheros.com

Table 258: 802.11n Access Points

Servers

Company	Product	Version	Contact
Qualcomm	Hostapd	2.4	Jouni Malinen jouni.malinen@atheros.com
Microsoft	Windows Server 2012	R2 Essentials	wfasupport@microsoft.com

OSC	Radiator	4.14.4	Mike McCauley mikem@open.com.au

Table 259 Servers

Supplicants

	Product	Version	Contact
Atheros	WPA_Supplicant	0.6.6	Jouni Malinen jouni.malinen@atheros.com
Microsoft	Windows XP Professional, Service Pack 2, KB893357-V2-X86 patch		wfasupport@microsoft.com

Table 260 Supplicants

	Product	Version	Contact
Ixia	Chariot	6.4 or higher	support@ixiacom.com
WFA	WFA-EMT	1.0.1	support@wi-fi.org
Wireshark Ubuntu Sniffer	AR5BHB-00112A or AR5BXB-00114A	Refer to the PMF sniffer package in the Wi-Fi Test Suite release	support@wi-fi.org

Table 261 Test Tools

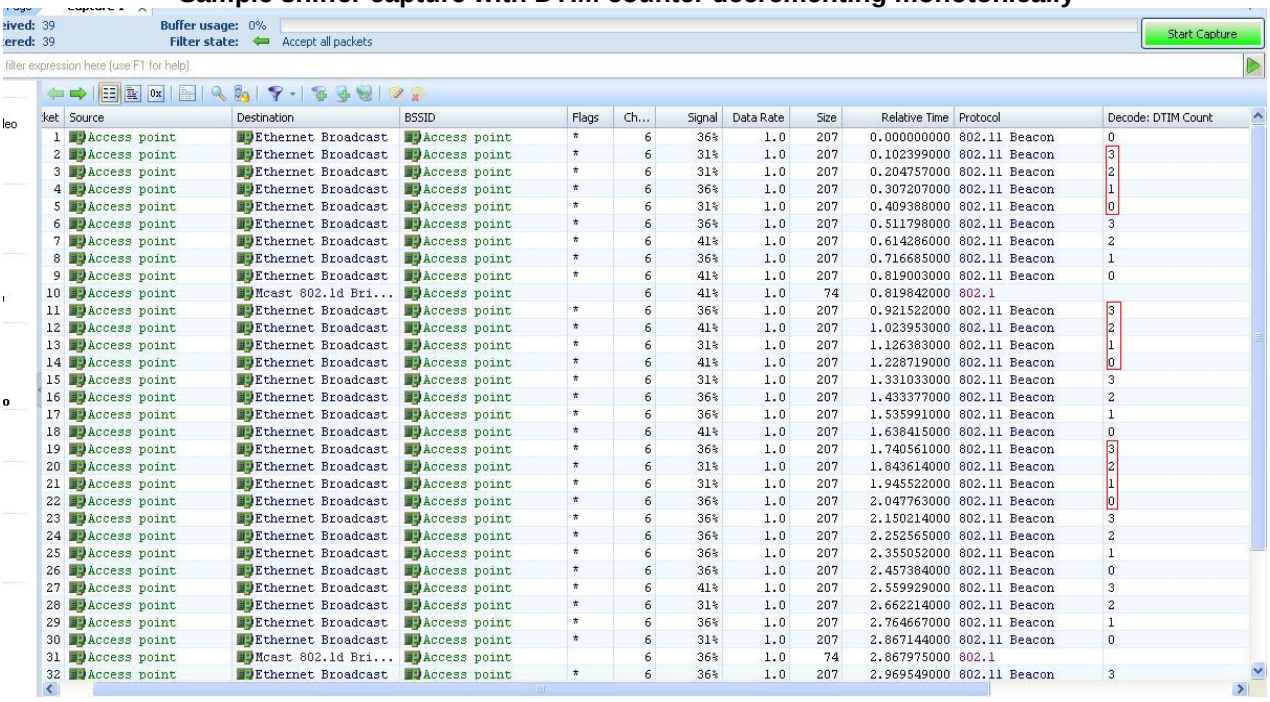
7 Appendix B: Testing Notes

Testbed layout. Place all APs on a shelf that can be about 12 inches above the bench where the STAs are positioned. Ensure a line of sight between all APs and STAs. The distance between APs and STAs should not exceed 12 feet and not be less than 1 foot. If testing in an RF chamber ensure that there is about 25% or greater reflectivity.

MPDU aggregation tests 4.2.29 and 5.2.37 can be performed without using an Ethernet 1Gbps switch by connecting directly to the AP from the Console.

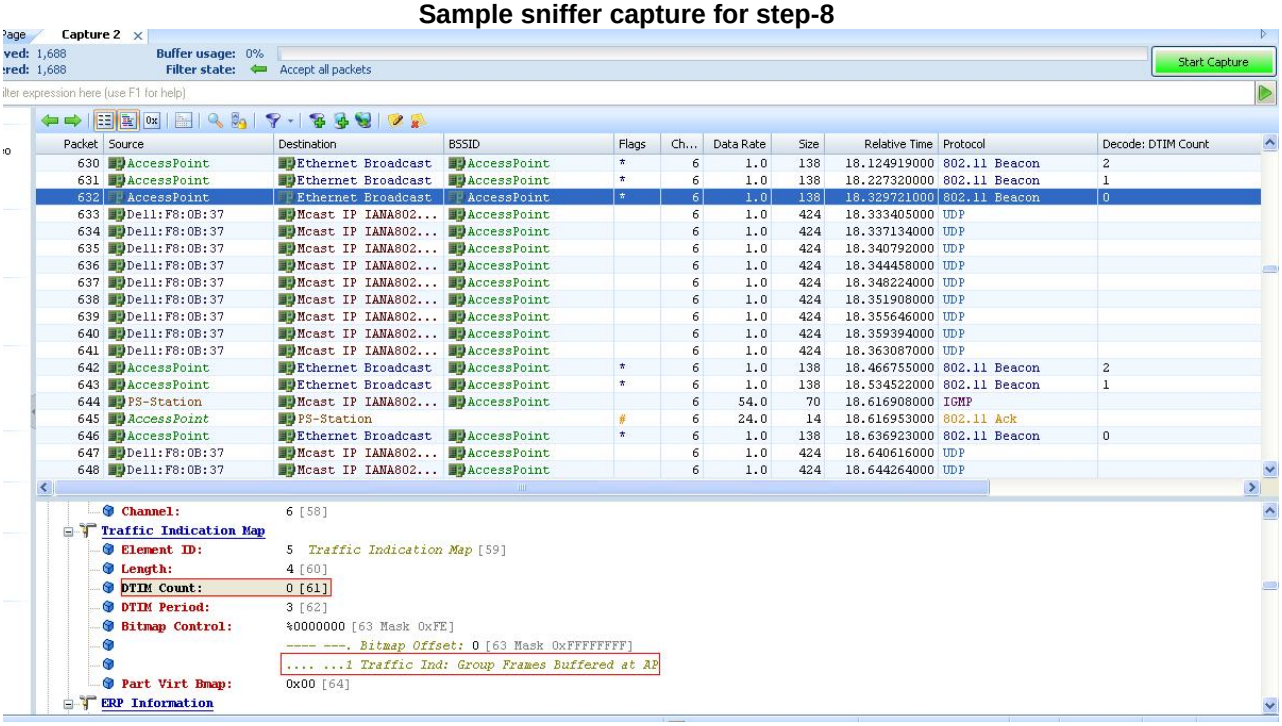
4.2.10
Omni peek sniffer is used for illustration. For testing, any 11n wireless sniffer may be used.

Sample sniffer capture with DTIM counter decrementing monotonically



ket	Source	Destination	BSSID	Flags	Ch...	Signal	Data Rate	Size	Relative Time	Protocol	Decode: DTIM Count
1	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	0.000000000	802.11 Beacon	0
2	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	0.102399000	802.11 Beacon	3
3	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	0.204757000	802.11 Beacon	2
4	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	0.307207000	802.11 Beacon	1
5	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	0.409388000	802.11 Beacon	0
6	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	0.511798000	802.11 Beacon	3
7	Access point	Ethernet Broadcast	Access point	*	6	41%	1.0	207	0.614286000	802.11 Beacon	2
8	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	0.716685000	802.11 Beacon	1
9	Access point	Ethernet Broadcast	Access point	*	6	41%	1.0	207	0.819003000	802.11 Beacon	0
10	Access point	Mcast 802.1d Bri...	Access point		6	41%	1.0	74	0.819842000	802.1	
11	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	0.921522000	802.11 Beacon	3
12	Access point	Ethernet Broadcast	Access point	*	6	41%	1.0	207	1.023953000	802.11 Beacon	2
13	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	1.126383000	802.11 Beacon	1
14	Access point	Ethernet Broadcast	Access point	*	6	41%	1.0	207	1.228719000	802.11 Beacon	0
15	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	1.331033000	802.11 Beacon	3
16	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	1.433377000	802.11 Beacon	2
17	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	1.535991000	802.11 Beacon	1
18	Access point	Ethernet Broadcast	Access point	*	6	41%	1.0	207	1.638415000	802.11 Beacon	0
19	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	1.740561000	802.11 Beacon	3
20	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	1.843614000	802.11 Beacon	2
21	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	1.945522000	802.11 Beacon	1
22	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	2.047763000	802.11 Beacon	0
23	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	2.150214000	802.11 Beacon	3
24	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	2.252565000	802.11 Beacon	2
25	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	2.355052000	802.11 Beacon	1
26	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	2.457384000	802.11 Beacon	0
27	Access point	Ethernet Broadcast	Access point	*	6	41%	1.0	207	2.559929000	802.11 Beacon	3
28	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	2.662214000	802.11 Beacon	2
29	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	2.764667000	802.11 Beacon	1
30	Access point	Ethernet Broadcast	Access point	*	6	31%	1.0	207	2.867144000	802.11 Beacon	0
31	Access point	Mcast 802.1d Bri...	Access point		6	36%	1.0	74	2.867975000	802.1	
32	Access point	Ethernet Broadcast	Access point	*	6	36%	1.0	207	2.969549000	802.11 Beacon	3

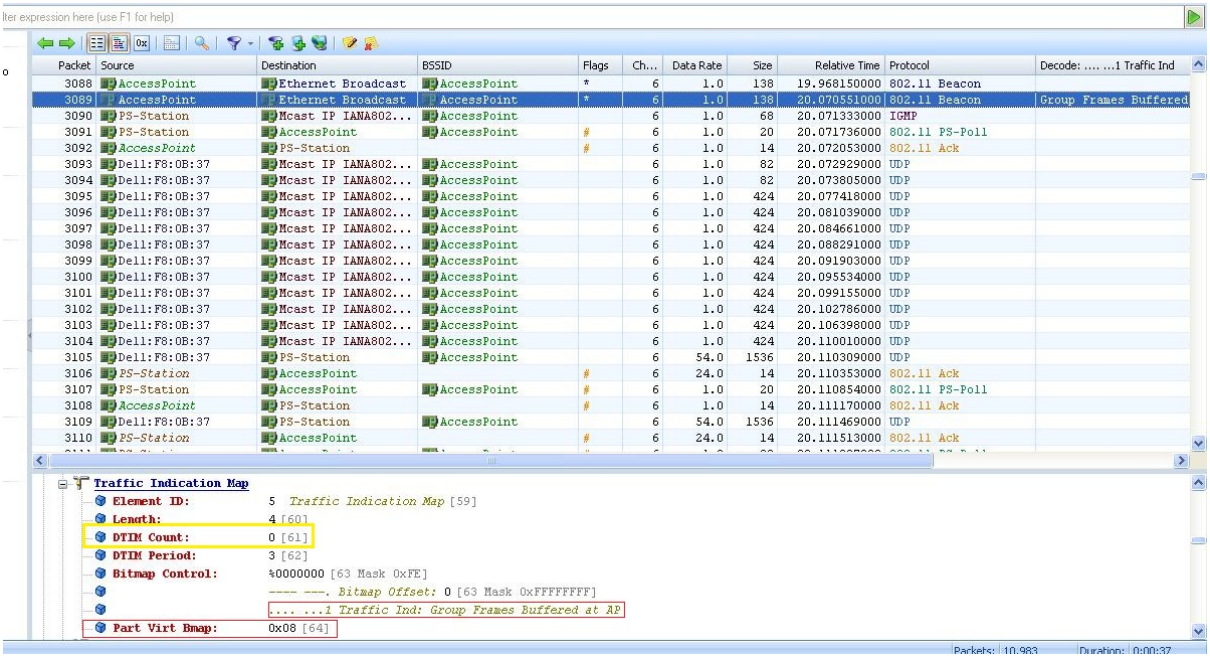
Sample sniffer capture for step-8



AP delivers group traffic data when DTIM=0 and TIB=1

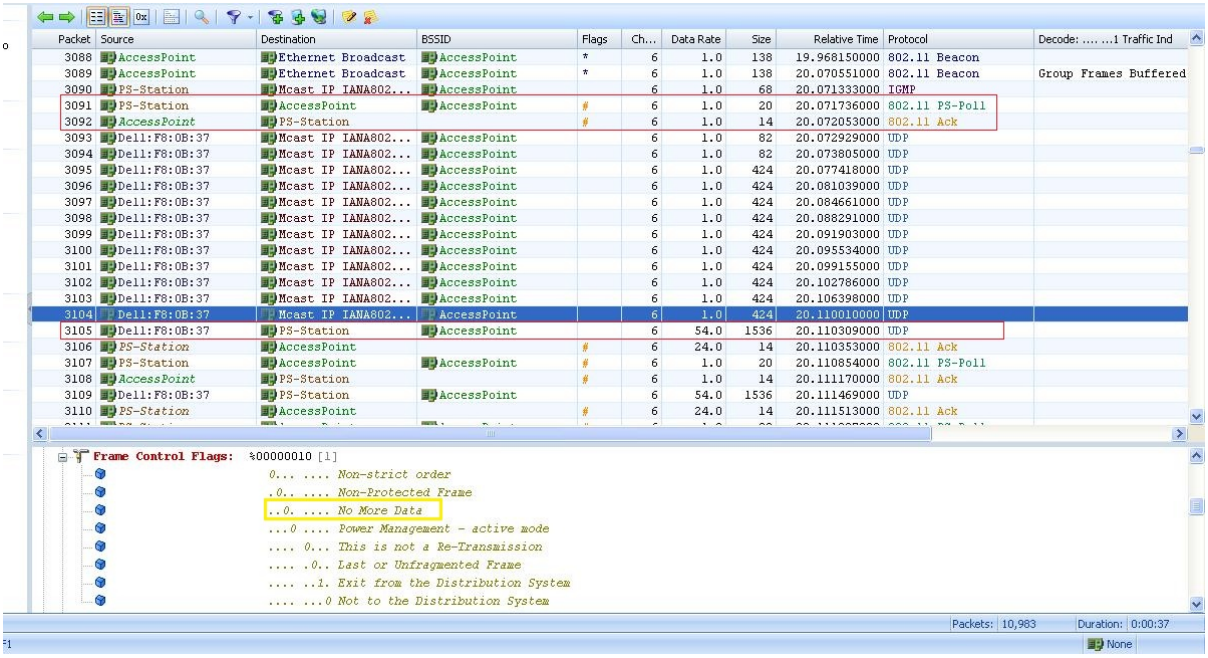
Sample sniffer capture for step-8

1.



AP has both group traffic and directed traffic to deliver for clients

2.



Packet	Source	Destination	BSSID	Flags	Ch...	Data Rate	Size	Relative Time	Protocol	Decode: ....1 Traffic Ind
3088	AccessPoint	Ethernet Broadcast	AccessPoint	*	6	1.0	138	19.968150000	802.11 Beacon	
3089	AccessPoint	Ethernet Broadcast	AccessPoint	*	6	1.0	138	20.070551000	802.11 Beacon	Group Frames Buffered
3090	PS-Station	Mcast IP IANA802...	AccessPoint		6	1.0	68	20.071333000	IGMP	
3091	PS-Station	AccessPoint	AccessPoint	#	6	1.0	20	20.071736000	802.11 PS-Poll	
3092	AccessPoint	PS-Station		#	6	1.0	14	20.072053000	802.11 Ack	
3093	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	82	20.072929000	UDP	
3094	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	82	20.073805000	UDP	
3095	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.077418000	UDP	
3096	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.081039000	UDP	
3097	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.084661000	UDP	
3098	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.088291000	UDP	
3099	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.091903000	UDP	
3100	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.095534000	UDP	
3101	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.099155000	UDP	
3102	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.102786000	UDP	
3103	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.106398000	UDP	
3104	Dell:F8:0B:37	Mcast IP IANA802...	AccessPoint		6	1.0	424	20.110010000	UDP	
3105	Dell:F8:0B:37	PS-Station	AccessPoint		6	54.0	1536	20.110309000	UDP	
3106	PS-Station	AccessPoint		#	6	24.0	14	20.110353000	802.11 Ack	
3107	PS-Station	AccessPoint	AccessPoint	#	6	1.0	20	20.110854000	802.11 PS-Poll	
3108	AccessPoint	PS-Station		#	6	1.0	14	20.111170000	802.11 Ack	
3109	Dell:F8:0B:37	PS-Station	AccessPoint		6	54.0	1536	20.111469000	UDP	
3110	PS-Station	AccessPoint		#	6	24.0	14	20.111513000	802.11 Ack	

Even though PS-poll is sent by PS-client for directed traffic, AP delivers directed data only after entire group traffic is delivered (i.e. after more data bit in last group addressed data is set to “0”). Note that in the test, the directed traffic is sent to the station that is not in PS mode. This is just an example.

8 Appendix C: Channel Frequencies

Please refer to Annex E of the IEEE 802.11 standard.

9 Appendix D: Default WMM AC Parameters

AC	CW_{min}	CW_{max}	AIFSN	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
AC_BK	15 {4}	1023 {10}	7	0	0
AC_BE	15 {4}	1023 {10}	3	0	0
AC_VI	7 {3}	15 {4}	2	188 (6.016ms)	94 (3.008ms)
AC_VO	3 {2}	7 {3}	2	102 (3.264ms)	47 (1.504ms)

Table 262Default WMM Parameters for the STA

AC	CW_{min}	CW_{max}	AIFSN	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
AC_BK	15 {4}	1023 {10}	7	0	0
AC_BE	15 {4}	63 {6}	3	0	0
AC_VI	7 {3}	15 {4}	1	188 (6.016ms)	94 (3.008ms)
AC_VO	3 {2}	7 {3}	1	102 (3.264ms)	47 (1.504ms)

Table 263 Default WMM Parameters for the AP

Numbers in {} are x in {2^x-1}

10 Appendix E: Threshold Values

The values shown in each of these tables are the thresholds that are required to pass each throughput test. When a device is running in Legacy Mode use the 1SS (1 Spatial Stream) column. If the device is required to be run for 2 SS then use this column. Finally when a device is required to run in 3 SS then use this column.

APUT

	Chariot and Wi-Fi Test Suite (Mbps)		
AP Thresholds	1 x 1	2 x 2	3 x 3
4.2.3A1DT1	3.66	N/A	N/A
4.2.3A1DT2	3.70	N/A	N/A
4.2.3A1DT3	0.64	N/A	N/A
4.2.4A2DT1	13.98	N/A	N/A
4.2.4A2DT2	6.85	N/A	N/A
4.2.4A2DT3	0.85	N/A	N/A
4.2.7A5DT1WPA2	6.44	N/A	N/A
4.2.7A5DT1WPA	6.31	N/A	N/A
4.2.7A5DT2WPA2	4.00	N/A	N/A
4.2.7A5DT2WPA	5.00	N/A	N/A
4.2.7A5DT3WPA2	0.35	N/A	N/A
4.2.7A5DT3WPA	0.30	N/A	N/A
4.2.8A6DT1WPA2	6.80	N/A	N/A
4.2.8A6DT1WPA	4.50	N/A	N/A
4.2.8A6DT2WPA2	4.30	N/A	N/A
4.2.8A6DT2WPA	2.80	N/A	N/A
4.2.8A6DT3WPA2	0.40	N/A	N/A
4.2.8A6DT3WPA	0.30	N/A	N/A
4.2.19DBA1DT1	9.95	N/A	N/A
4.2.19DBA1DT2	6.90	N/A	N/A
4.2.29T4DT2	25.98	51.96	73.20
4.2.29T8DT2	22.79	45.58	66.21
4.2.30T4DT2	14.41	25.53	41.22

4.2.31T4DT1A	4.00	4.00	4.00
4.2.31T4DT1B	2.50	2.50	2.50
4.2.32T4DT1A	4.00	4.00	4.00
4.2.32T4DT1B	3.00	3.00	3.00
4.2.35T4DT1A	2.50	2.50	2.50
4.2.35T4DT1B	2.50	2.50	2.50
4.2.37T6DT2	12.49	12.49	12.49
4.2.37T7DT2	9.2	9.2	9.2
4.2.40T3DT1	21.40		
4.2.40T6DT1		66.60	
4.2.40T10DT1			92.50

Mobile AP Thresholds	Chariot and Wi-Fi Test Suite (Mbps)
4.2.3A1DT1	2.373
4.2.3A1DT2	2.300
4.2.3A1DT3	0.166
4.2.4A2DT1	1.812
4.2.4A2DT2	1.092
4.2.4A2DT3	0.120
4.2.7A5DT1WPA2	0.440
4.2.7A5DT1WPA	0.682
4.2.7A5DT2WPA2	2.614
4.2.7A5DT2WPA	0.518
4.2.7A5DT3WPA2	0.001
4.2.7A5DT3WPA	0.299
4.2.8A6DT1WPA2	0.707
4.2.8A6DT1WPA	0.480
4.2.8A6DT2WPA2	2.444

4.2.8A6DT2WPA	0.457
4.2.8A6DT3WPA2	0.178
4.2.8A6DT3WPA	0.170
4.2.19DBA1DT1	9.950
4.2.19DBA1DT2	6.900
4.2.29T4DT2	5.347
4.2.29T8DT2	5.923
4.2.30T4DT2	0.560
4.2.31T4DT1A	0.711
4.2.31T4DT1B	0.370
4.2.32T4DT1A	1.522
4.2.32T4DT1B	2.885
4.2.35T4DT1A	2.500
4.2.35T4DT1B	2.394
4.2.37T6DT2	12.490
4.2.37T7DT2	9.200
4.2.40T3DT1	9.269
4.2.40T6DT1	21.938
4.2.40T10DT1	92.500

STAUT

	Chariot and Wi-Fi Test Suite (Mbps)		
STA Thresholds	1 x 1	**2 x 2**	**3 x 3**
5.2.3S1DT1	3.48	N/A	N/A
5.2.3S1DT2	3.28	N/A	N/A
5.2.3S1DT3	0.30	N/A	N/A
5.2.4S2DT1	2.00	N/A	N/A

5.2.4S2DT2	3.10	N/A	N/A
5.2.4S2DT3	0.70	N/A	N/A
5.2.5MS8GDT1	0.90	N/A	N/A
5.2.5MS8BDT1	0.87	N/A	N/A
5.2.5MS8GDT2	0.50	N/A	N/A
5.2.5MS8BDT2	0.85	N/A	N/A
5.2.5MS8GDT3	0.33	N/A	N/A
5.2.5MS8BDT3	0.35	N/A	N/A
5.2.6MS9GDT1	0.67	N/A	N/A
5.2.6MS9BDT1	0.64	N/A	N/A
5.2.6MS9GDT2	0.89	N/A	N/A
5.2.6MS9BDT2	0.89	N/A	N/A
5.2.6MS9GDT3	0.20	N/A	N/A
5.2.6MS9BDT3	0.25	N/A	N/A
5.2.7MS10GDT1	1.20	N/A	N/A
5.2.7MS10BDT1	1.72	N/A	N/A
5.2.7MS10GDT2	0.20	N/A	N/A
5.2.7MS10BDT2	1.80	N/A	N/A
5.2.7MS10GDT3	0.27	N/A	N/A
5.2.7MS10BDT3	0.32	N/A	N/A
5.2.8MS11GDT1	0.90	N/A	N/A
5.2.8MS11BDT1	1.50	N/A	N/A
5.2.8MS11GDT2	2.07	N/A	N/A
5.2.8MS11BDT2	1.42	N/A	N/A
5.2.9T3DT1	12.10	N/A	N/A
5.2.9T4DT2	9.57	N/A	N/A
5.2.9T5DT3	1.10	N/A	N/A
5.2.10T3DT1	2.50	N/A	N/A
5.2.10T4DT2	3.80	N/A	N/A
5.2.10T5DT3	0.45	N/A	N/A
5.2.12T3DT1	1.90	N/A	N/A
5.2.12T4DT2	3.25	N/A	N/A
5.2.12T5DT3	0.36	N/A	N/A

5.2.13T3DT1	2.17	N/A	N/A
5.2.13T4DT2	3.82	N/A	N/A
5.2.13T5DT3	0.42	N/A	N/A
5.2.37T4DT1	25.98	51.96	73.20
5.2.37T8DT1	22.79	45.58	66.21
5.2.38T4DT1	14.41	28.82	41.22
5.2.39T4DT2A	4.00	4.00	4.00
5.2.39T4DT2B	2.50	2.50	2.50
5.2.40T4DT2A	4.00	4.00	4.00
5.2.40T4DT2B	3.00	3.00	3.00
5.2.43T4DT2A	2.50	2.50	2.50
5.2.43T4DT2B	2.50	2.50	2.50
5.2.47T3DT1	30.20		
5.2.47T6DT1		65.70	
5.2.47T9DT1			81.20
5.3.1SI1DT1	1.18		
5.3.1SI1DT2	0.85		

Handset Thresholds	Chariot and Wi-Fi Test Suite (Mbps)
5.2.3S1DT1	0.096
5.2.3S1DT2	0.097
5.2.3S1DT3	0.150
5.2.4S2DT1	1.328
5.2.4S2DT2	1.000
5.2.4S2DT3	0.201
5.2.5MS8GDT1	0.900
5.2.5MS8BDT1	0.870

5.2.5MS8GDT2	0.059
5.2.5MS8BDT2	0.719
5.2.5MS8GDT3	0.061
5.2.5MS8BDT3	0.350
5.2.6MS9GDT1	0.670
5.2.6MS9BDT1	0.640
5.2.6MS9GDT2	0.510
5.2.6MS9BDT2	0.484
5.2.6MS9GDT3	0.129
5.2.6MS9BDT3	0.250
5.2.7MS10GDT1	0.554
5.2.7MS10BDT1	1.720
5.2.7MS10GDT2	0.099
5.2.7MS10BDT2	1.286
5.2.7MS10GDT3	0.101
5.2.7MS10BDT3	0.320
5.2.8MS11GDT1	0.108
5.2.8MS11BDT1	0.362
5.2.8MS11GDT2	0.102
5.2.8MS11BDT2	0.657
5.2.9T3DT1	4.454
5.2.9T4DT2	4.227
5.2.9T5DT3	0.232
5.2.10T3DT1	2.500
5.2.10T4DT2	3.800
5.2.10T5DT3	0.038
5.2.12T3DT1	1.900
5.2.12T4DT2	2.909
5.2.12T5DT3	0.183
5.2.13T3DT1	1.674
5.2.13T4DT2	3.025

5.2.13T5DT3	0.180
5.2.37T4DT1	18.501
5.2.37T8DT1	17.974
5.2.38T4DT1	13.503
5.2.39T4DT2A	3.189
5.2.39T4DT2B	2.345
5.2.40T4DT2A	0.094
5.2.40T4DT2B	3.000
5.2.43T4DT2A	2.500
5.2.43T4DT2B	2.500
5.2.47T3DT1	21.845
5.2.47T6DT1	58.685
5.2.47T9DT1	81.200
5.3.1SI1DT1	1.180
5.3.1SI1DT2	0.850

TV Thresholds	Chariot and Wi-Fi Test Suite (Mbps)
5.2.3S1DT1	2.641
5.2.3S1DT2	0.911
5.2.3S1DT3	0.399
5.2.4S2DT1	1.373
5.2.4S2DT2	2.674
5.2.4S2DT3	0.145
5.2.5MS8GDT1	0.900
5.2.5MS8BDT1	0.870
5.2.5MS8GDT2	0.500

5.2.5MS8BDT2	0.850
5.2.5MS8GDT3	0.150
5.2.5MS8BDT3	0.104
5.2.6MS9GDT1	0.384
5.2.6MS9BDT1	0.640
5.2.6MS9GDT2	0.789
5.2.6MS9BDT2	0.650
5.2.6MS9GDT3	0.139
5.2.6MS9BDT3	0.063
5.2.7MS10GDT1	1.200
5.2.7MS10BDT1	1.720
5.2.7MS10GDT2	0.200
5.2.7MS10BDT2	1.597
5.2.7MS10GDT3	0.102
5.2.7MS10BDT3	0.107
5.2.8MS11GDT1	0.900
5.2.8MS11BDT1	1.074
5.2.8MS11GDT2	2.070
5.2.8MS11BDT2	1.110
5.2.9T3DT1	10.847
5.2.9T4DT2	7.364
5.2.9T5DT3	0.698
5.2.10T3DT1	2.500
5.2.10T4DT2	3.800
5.2.10T5DT3	0.012
5.2.12T3DT1	1.900
5.2.12T4DT2	3.178
5.2.12T5DT3	0.188
5.2.13T3DT1	1.462
5.2.13T4DT2	3.123
5.2.13T5DT3	0.196

5.2.37T4DT1	14.460
5.2.37T8DT1	15.453
5.2.38T4DT1	9.997
5.2.39T4DT2A	0.891
5.2.39T4DT2B	1.828
5.2.40T4DT2A	1.587
5.2.40T4DT2B	3.000
5.2.43T4DT2A	1.997
5.2.43T4DT2B	2.500
5.2.47T3DT1	7.415
5.2.47T6DT1	47.422
5.2.47T9DT1	81.200
5.3.1SI1DT1	1.180
5.3.1SI1DT2	0.850

Printer Thresholds	Chariot and Wi-Fi Test Suite (Mbps)
5.2.3S1DT1	2.222
5.2.3S1DT2	2.500
5.2.3S1DT3	0.300
5.2.4S2DT1	1.764
5.2.4S2DT2	2.640
5.2.4S2DT3	0.430
5.2.5MS8GDT1	0.604
5.2.5MS8BDT1	0.870
5.2.5MS8GDT2	0.500
5.2.5MS8BDT2	0.810
5.2.5MS8GDT3	0.330

5.2.5MS8BDT3	0.350
5.2.6MS9GDT1	0.555
5.2.6MS9BDT1	0.640
5.2.6MS9GDT2	0.447
5.2.6MS9BDT2	0.890
5.2.6MS9GDT3	0.200
5.2.6MS9BDT3	0.250
5.2.7MS10GDT1	0.615
5.2.7MS10BDT1	1.720
5.2.7MS10GDT2	0.006
5.2.7MS10BDT2	1.544
5.2.7MS10GDT3	0.257
5.2.7MS10BDT3	0.320
5.2.8MS11GDT1	0.700
5.2.8MS11BDT1	1.500
5.2.8MS11GDT2	1.244
5.2.8MS11BDT2	1.420
5.2.9T3DT1	3.130
5.2.9T4DT2	2.566
5.2.9T5DT3	0.767
5.2.10T3DT1	1.040
5.2.10T4DT2	2.280
5.2.10T5DT3	0.450
5.2.12T3DT1	1.803
5.2.12T4DT2	2.094
5.2.12T5DT3	0.360
5.2.13T3DT1	1.424
5.2.13T4DT2	2.767
5.2.13T5DT3	0.041
5.2.37T4DT1	3.086

5.2.37T8DT1	3.050
5.2.38T4DT1	2.050
5.2.39T4DT2A	0.903
5.2.39T4DT2B	2.500
5.2.40T4DT2A	4.000
5.2.40T4DT2B	3.000
5.2.43T4DT2A	2.500
5.2.43T4DT2B	2.500
5.2.47T3DT1	3.668
5.2.47T6DT1	65.700
5.2.47T9DT1	81.200
5.3.1SI1DT1	1.180
5.3.1SI1DT2	0.850

Set Top Box Thresholds	Chariot and Wi-Fi Test Suite (Mbps)
5.2.3S1DT1	3.480
5.2.3S1DT2	3.280
5.2.3S1DT3	0.300
5.2.4S2DT1	1.891
5.2.4S2DT2	3.068
5.2.4S2DT3	0.605
5.2.5MS8GDT1	0.900
5.2.5MS8BDT1	0.870
5.2.5MS8GDT2	0.496
5.2.5MS8BDT2	0.745
5.2.5MS8GDT3	0.330
5.2.5MS8BDT3	0.350

5.2.6MS9GDT1	0.670
5.2.6MS9BDT1	0.640
5.2.6MS9GDT2	0.567
5.2.6MS9BDT2	0.890
5.2.6MS9GDT3	0.200
5.2.6MS9BDT3	0.250
5.2.7MS10GDT1	1.200
5.2.7MS10BDT1	1.720
5.2.7MS10GDT2	0.200
5.2.7MS10BDT2	1.425
5.2.7MS10GDT3	0.270
5.2.7MS10BDT3	0.320
5.2.8MS11GDT1	0.900
5.2.8MS11BDT1	1.074
5.2.8MS11GDT2	2.070
5.2.8MS11BDT2	1.324
5.2.9T3DT1	5.843
5.2.9T4DT2	6.784
5.2.9T5DT3	0.295
5.2.10T3DT1	2.500
5.2.10T4DT2	3.800
5.2.10T5DT3	0.090
5.2.12T3DT1	1.900
5.2.12T4DT2	3.250
5.2.12T5DT3	0.360
5.2.13T3DT1	1.856
5.2.13T4DT2	3.284
5.2.13T5DT3	0.420
5.2.37T4DT1	25.980
5.2.37T8DT1	22.790

5.2.38T4DT1	14.41
5.2.39T4DT2A	4.000
5.2.39T4DT2B	2.500
5.2.40T4DT2A	4.000
5.2.40T4DT2B	3.000
5.2.43T4DT2A	2.500
5.2.43T4DT2B	2.500
5.2.47T3DT1	20.146
5.2.47T6DT1	10.101
5.2.47T9DT1	81.200
5.3.1SI1DT1	1.180
5.3.1SI1DT2	0.850

	Chariot and Wi-Fi Test Suite (Mbps)		
Audio Thresholds	1 x 1	2 x 2	3 x 3
5.2.3S1DT1	1.00	N/A	N/A
5.2.3S1DT2	1.00	N/A	N/A
5.2.3S1DT3	0.30	N/A	N/A
5.2.4S2DT1	1.00	N/A	N/A
5.2.4S2DT2	1.00	N/A	N/A
5.2.4S2DT3	0.30	N/A	N/A
5.2.5MS8GDT1	0.90	N/A	N/A
5.2.5MS8BDT1	0.87	N/A	N/A
5.2.5MS8GDT2	0.50	N/A	N/A
5.2.5MS8BDT2	0.85	N/A	N/A
5.2.5MS8GDT3	0.33	N/A	N/A
5.2.5MS8BDT3	0.267	N/A	N/A
5.2.6MS9GDT1	0.67	N/A	N/A
5.2.6MS9BDT1	0.64	N/A	N/A

5.2.6MS9GDT2	0.89	N/A	N/A
5.2.6MS9BDT2	0.89	N/A	N/A
5.2.6MS9GDT3	0.20	N/A	N/A
5.2.6MS9BDT3	0.25	N/A	N/A
5.2.7MS10GDT1	1.157	N/A	N/A
5.2.7MS10BDT1	0.72	N/A	N/A
5.2.7MS10GDT2	0.20	N/A	N/A
5.2.7MS10BDT2	1.80	N/A	N/A
5.2.7MS10GDT3	0.27	N/A	N/A
5.2.7MS10BDT3	0.32	N/A	N/A
5.2.8MS11GDT1	0.70	N/A	N/A
5.2.8MS11BDT1	0.88	N/A	N/A
5.2.8MS11GDT2	0.65	N/A	N/A
5.2.8MS11BDT2	1.22	N/A	N/A
5.2.9T3DT1	4.00	N/A	N/A
5.2.9T4DT2	4.00	N/A	N/A
5.2.9T5DT3	0.60	N/A	N/A
5.2.10T3DT1	4.00	N/A	N/A
5.2.10T4DT2	4.00	N/A	N/A
5.2.10T5DT3	0.45	N/A	N/A
5.2.12T3DT1	2.00	N/A	N/A
5.2.12T4DT2	2.00	N/A	N/A
5.2.12T5DT3	0.30	N/A	N/A
5.2.13T3DT1	2.00	N/A	N/A
5.2.13T4DT2	2.00	N/A	N/A
5.2.13T5DT3	0.30	N/A	N/A
5.2.37T4DT1	12.99	25.98	36.60
5.2.37T8DT1	11.40	22.79	33.10
5.2.38T4DT1	7.21	14.41	20.61
5.2.39T4DT2A	4.00	4.00	4.00
5.2.39T4DT2B	2.50	2.50	2.50

5.2.40T4DT2A	4.00	4.00	4.00
5.2.40T4DT2B	3.00	3.00	3.00
5.2.43T4DT2A	2.50	2.50	2.50
5.2.43T4DT2B	2.50	2.50	2.50
5.2.47T3DT1	15.10		
5.2.47T6DT1		32.85	
5.2.47T9DT1			40.60
5.3.1SI1DT1	1.18		
5.3.1SI1DT2	0.85		

	Chariot and Wi-Fi Test Suite (Mbps)		
Network Camera Thresholds	1 x 1	**2 x 2**	**3 x 3**
5.2.3S1DT1	1.00	N/A	N/A
5.2.3S1DT2	1.00	N/A	N/A
5.2.3S1DT3	0.10	N/A	N/A
5.2.4S2DT1	0.60	N/A	N/A
5.2.4S2DT2	1.00	N/A	N/A
5.2.4S2DT3	0.15	N/A	N/A
5.2.5MS8GDT1	0.30	N/A	N/A
5.2.5MS8BDT1	0.30	N/A	N/A
5.2.5MS8GDT2	0.20	N/A	N/A
5.2.5MS8BDT2	0.30	N/A	N/A
5.2.5MS8GDT3	0.10	N/A	N/A
5.2.5MS8BDT3	0.10	N/A	N/A
5.2.6MS9GDT1	0.12	N/A	N/A
5.2.6MS9BDT1	0.20	N/A	N/A
5.2.6MS9GDT2	0.20	N/A	N/A
5.2.6MS9BDT2	0.20	N/A	N/A
5.2.6MS9GDT3	0.10	N/A	N/A
5.2.6MS9BDT3	0.10	N/A	N/A

5.2.7MS10GDT1	0.05	N/A	N/A
5.2.7MS10BDT1	0.50	N/A	N/A
5.2.7MS10GDT2	0.10	N/A	N/A
5.2.7MS10BDT2	0.20	N/A	N/A
5.2.7MS10GDT3	0.10	N/A	N/A
5.2.7MS10BDT3	0.10	N/A	N/A
5.2.8MS11GDT1	0.30	N/A	N/A
5.2.8MS11BDT1	0.30	N/A	N/A
5.2.8MS11GDT2	0.30	N/A	N/A
5.2.8MS11BDT2	0.30	N/A	N/A
5.2.9T3DT1	1.00	N/A	N/A
5.2.9T4DT2	1.00	N/A	N/A
5.2.9T5DT3	0.15	N/A	N/A
5.2.10T3DT1	1.00	N/A	N/A
5.2.10T4DT2	1.00	N/A	N/A
5.2.10T5DT3	0.30	N/A	N/A
5.2.12T3DT1	1.00	N/A	N/A
5.2.12T4DT2	1.00	N/A	N/A
5.2.12T5DT3	0.10	N/A	N/A
5.2.13T3DT1	1.00	N/A	N/A
5.2.13T4DT2	1.00	N/A	N/A
5.2.13T5DT3	0.10	N/A	N/A
5.2.37T4DT1	3.00	27.84	73.20
5.2.37T8DT1	3.00	27.60	66.21
5.2.38T4DT1	3.00	20.73	41.22
5.2.39T4DT2A	1.20	4	4
5.2.39T4DT2B	0.75	2.50	2.50
5.2.40T4DT2A	4.00	4.00	4.00
5.2.40T4DT2B	3.00	3.00	3.00

5.2.43T4DT2A	2.50	2.50	2.50
5.2.43T4DT2B	2.50	2.50	2.50
5.2.47T3DT1	6.82		
5.2.47T6DT1		40.51	
5.2.47T9DT1			81.20
5.3.1SI1DT1	1.18		
5.3.1SI1DT2	0.85		

	Chariot and Wi-Fi Test Suite (Mbps)		
Client Card Thresholds	1 x 1	**2 x 2**	**3 x 3**
5.2.3S1DT1	0.04	N/A	N/A
5.2.3S1DT2	0.04	N/A	N/A
5.2.3S1DT3	0.01	N/A	N/A
5.2.4S2DT1	0.04	N/A	N/A
5.2.4S2DT2	0.04	N/A	N/A
5.2.4S2DT3	0.01	N/A	N/A
5.2.5MS8GDT1	0.04	N/A	N/A
5.2.5MS8BDT1	0.04	N/A	N/A
5.2.5MS8GDT2	0.04	N/A	N/A
5.2.5MS8BDT2	0.04	N/A	N/A
5.2.5MS8GDT3	0.01	N/A	N/A
5.2.5MS8BDT3	0.01	N/A	N/A
5.2.6MS9GDT1	0.04	N/A	N/A
5.2.6MS9BDT1	0.04	N/A	N/A
5.2.6MS9GDT2	0.04	N/A	N/A
5.2.6MS9BDT2	0.04	N/A	N/A
5.2.6MS9GDT3	0.01	N/A	N/A
5.2.6MS9BDT3	0.01	N/A	N/A
5.2.7MS10GDT1	0.04	N/A	N/A
5.2.7MS10BDT1	0.04	N/A	N/A
5.2.7MS10GDT2	0.04	N/A	N/A
5.2.7MS10BDT2	0.04	N/A	N/A

5.2.7MS10GDT3	0.01	N/A	N/A
5.2.7MS10BDT3	0.01	N/A	N/A
5.2.8MS11GDT1	0.04	N/A	N/A
5.2.8MS11BDT1	0.04	N/A	N/A
5.2.8MS11GDT2	0.04	N/A	N/A
5.2.8MS11BDT2	0.04	N/A	N/A
5.2.9T3DT1	0.04	N/A	N/A
5.2.9T4DT2	0.04	N/A	N/A
5.2.9T5DT3	0.01	N/A	N/A
5.2.10T3DT1	0.04	N/A	N/A
5.2.10T4DT2	0.04	N/A	N/A
5.2.10T5DT3	0.01	N/A	N/A
5.2.12T3DT1	0.04	N/A	N/A
5.2.12T4DT2	0.04	N/A	N/A
5.2.12T5DT3	0.01	N/A	N/A
5.2.13T3DT1	0.04	N/A	N/A
5.2.13T4DT2	0.04	N/A	N/A
5.2.13T5DT3	0.01	N/A	N/A
5.2.37T4DT1	0.04	N/A	N/A
5.2.37T8DT1	0.04	N/A	N/A
5.2.38T4DT1	0.04	N/A	N/A
5.2.39T4DT2A	0.04	N/A	N/A
5.2.39T4DT2B	0.04	N/A	N/A
5.2.40T4DT2A	0.04	N/A	N/A
5.2.40T4DT2B	0.04	N/A	N/A
5.2.43T4DT2A	0.04	N/A	N/A
5.2.43T4DT2B	0.04	N/A	N/A
5.2.47T3DT1	0.04		
5.2.47T6DT1		N/A	

5.2.47T9DT1			N/A
5.3.1SI1DT1	0.04		
5.3.1SI1DT2	0.04		

11 Appendix F: WPA2 Interoperability Test Case

See section 4.1 and 5.1 for the tables of test cases. WPA2 test cases are listed under WPA2 APUT Test Cases (section 4.1) and WPA2 STAUT Test Cases (section 5.1).

12 Appendix G: WMM Interoperability Test Case

See section 4.1 and 5.1 for the tables of test cases. WMM test cases are listed under WMM APUT Test Cases (section 4.1) and WMM STAUT Test Cases (section 5.1).

13 Appendix H: Traffic description

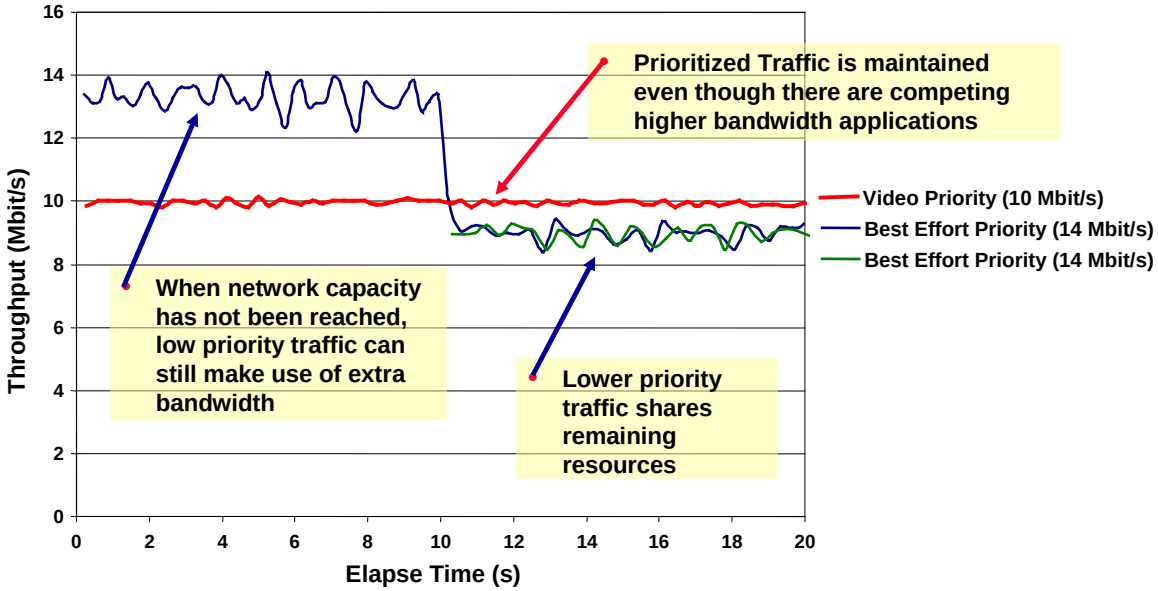
- IPTV10Mbps.scr RTP 10Mbps IPTV script
- IPTV14Mbps.scr RTP 14Mbps IPTV script
- IPTV20Mbps.scr RTP 20Mbps IPTV script
- IPTV10MbpsDelay10sec.scr RTP 10Mbps IPTV with 10 second delay script

14 Appendix I: Example WMM Run

The following is an example of differentiated services throughput of three streams. Pair 1 and 2 start simultaneously. Since there is enough network capacity, the video priority (AC_VI) stream achieves its constant 10Mbit/s bandwidth. The Pair 1, Best Effort Priority, stream is almost able to achieve it's desired 14 Mbit/s throughput. After 10 seconds, Pair 3 also tries to transmit 14Mbit/s, however there is insufficient network capacity and the two best effort streams are forced to share the remaining bandwidth after the Video Priority stream fully transmits its 10Mbbit/s payload.

Example Streams

Pair 1 (Blue)	RTP1_BE	IPTV14Mbps.scr
Pair 2 (Red)	RTP2_VI	IPTV10Mbps.scr
Pair 3 (Green)	RTP3_BE	IPTV14MbpsDelay10sec.scr (with delay)



Differentiated Throughput Example

15 Appendix J: Acknowledgments

I, Daniel R. Borges technical editor for TGn technical test plan, would like to acknowledge the following individuals for their efforts and contributions to the Wi-Fi 802.11n system interoperability test plan.

Name	Company	Email
Joe Andonieh	Intel Corporation	joe.andonieh@intel.com
Moussa Bavafa	Broadcom Corporation	moussa@broadcom.com
Andy Davidson	Atheros Communications	adavidson@atheros.com
Tracy Kane	Qualcomm	tkane@qualcomm.com
Michael Paljug	N/A	michael.paljug@conexant.com
Alexander Tolpin	Intel Corporation	alexander.tolpin@intel.com
Peter Loc	Ralink	peterloc@gmail.com
Shani Ben-Haim	Intel Corporation	shani.ben-haim@intel.com

Table 264: 802.11n Test Plan Acknowledgements

- End -