Wi-Fi CERTIFIED Agile Multiband™
Test Plan

Version 1.1

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

Latest version available at: https://www.wi-fi.org/members/certification-programs

WI-FI ALLIANCE PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

Table of contents

List of tables

List of figures

1   Overview

1.1   Scope and purpose

A primary goal of Wi-Fi Alliance is to ensure interoperability among Wi-Fi CERTIFIED Agile Multiband™ products from multiple manufacturers, and to promote this technology within both the business and consumer markets. To this end, the following interoperability and performance test suite was developed. Working in conjunction with authorized test labs, these tests will be executed on vendor products to grant products Wi-Fi CERTIFIED Agile Multiband certification upon successful test completion.

The scope of this test plan is governed by the Wi-Fi Alliance Marketing Requirements Document (MRD) for Multiband Operations [1], specifically section 6.3.

1.2   Definition of devices under test

The device under test (DUT) may be an Access Point (APUT) or Station (STAUT). The general characteristics of the DUT are entered in the Wi-Fi Alliance website registration system and are summarized in Table 1.

Prior to submission to the authorized test labs, the implementer shall complete the following capabilities declaration tables for use in performing Wi-Fi CERTIFIED certification testing.

Table 1.   General DUT capabilities declaration

Item	Test case	Vendor response
DUT type		**STA/AP**
Primary product category		**Value**
Secondary product category		**Value**
Device serial number		**Value**
Device firmware version		**Value**
Please provide user instructions to configure the following parameters: 　　SSID 　　Wireless Operational Mode, a/g/n/ac 　　Channel 　　Local IP Address and Netmask 　　Security: WPA2-Personal or WPA2-Enterprise 　　WPA2-Personal pass phrase		**Values**

Item	Test case	Vendor response
Does the DUT support WPA2-Enterprise?		**Yes/No**
Does the APUT support 4-frame GAS exchange?	4.2.4.2	
Is the APUT cellular data aware?	4.2.4.3, 4.2.5.2. 4.2.5.5	**Yes/No**
Does the APUT automatically populate the BSS Transition Candidate List?	4.2.5	**Yes/No**
Does the APUT support FT with WPA2-Enterprise (802.1X)?	4.2.6	**Yes/No**
Does the APUT support FT with WPA2-Personal?	4.2.6	**Yes/No**
Which Beacon Report Measurement Modes are supported by the STAUT? Note: Beacon Table mode is a mandatory Beacon Report Measurement mode for the STAUT to support	5.2.3	**Passive, Active**
Is the STAUT cellular data capable?	5.2.4.2, 5.2.9	**Yes/No**
Does the STAUT support ANQP?	5.2.4	**Yes/No**
Does the STAUT support BTM Query?	5.2.5.1	**Yes/No**
Does the STAUT support FT with WPA2-Enterprise (802.1X)?	5.2.6	**Yes/No**
Does the STAUT support FT with WPA2-Personal?	5.2.6	**Yes/No**
If the STAUT does not autonomously send a WNM Notification frame when the non-preferred channel's setting is changed, then provide instructions on how to trigger the STAUT to send a WNM Notification frame.	5.2.8	**Instructions**

1.3   References

The documents listed in this section are included in requirements made in the body of this test plan. Knowledge of their contents is required for the understanding and implementation of this test plan. If a listing includes a date or a version identifier, only that specific version of the document is required. If the listing includes neither a date nor a version identifier, the latest version of the document is required.

[1] Multiband Operations Marketing Requirements Document, version 1.4, https://www.wi-fi.org/members/certification-programs

[2]   Wi-Fi Agile Multiband Technical Specification, version 1.0, https://www.wi-fi.org/members/certification-programs

[3] IEEE Std 802.11™-2016 - IEEE Standard for Local and Metropolitan Area Networks -Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[4] P802.11-REVmd/D1.5 - IEEE Draft Standard for Information Technology -- Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks -- Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

1.4   Definitions, acronyms and abbreviations

1.4.1   Definitions

The following definitions are applicable to this document.

Table 2.   Definitions

Term	Definition
Candidate AP	A Wi-Fi Agile Multiband AP to which the STA is currently not associated
MBO ANQP-element	ANQP-element defined for the Wi-Fi Agile Multiband program
MBO-OCE IE	Information element defined for the Wi-Fi Agile Multiband program
Wi-Fi Agile Multiband AP	An AP that is capable of and has Wi-Fi Agile Multiband features and functions enabled
Wi-Fi Agile Multiband STA	A station that is capable of and has Wi-Fi Agile Multiband features and functions enabled
Wi-Fi Agile Multiband multimode STA	A station that is both Wi-Fi and cellular data capable and is in addition capable of and has Wi-Fi Agile Multiband features and functions enabled
Serving AP	The AP to which an STA is associated
Wi-Fi Agile Multiband Cellular-data aware AP	An AP that has Wi-Fi Agile Multiband features and functions enabled, and has awareness of a cellular data network which enables the AP to indicate to a STA a preference for the STA to switch to that cellular data network

1.4.2   Acronyms and abbreviations

This section defines the acronyms and abbreviations used throughout this document. Some acronyms and abbreviations are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance. Refer to the Wi-Fi Alliance Acronyms Terms Definitions document for a complete list of approved acronyms and abbreviations.

Table 3.   Acronyms and abbreviations

Acronym/Term	Definition
AAA	Authentication, authorization, and accounting

AKM	Authentication and key management
AP	Access Point
BSSID	Basic Service Set Identifier
BTM	BSS Transition Management
ESS	Extended service set
FT	Fast BSS Transition
FTAA	Fast BSS transition authentication algorithm
FTE	Fast BSS transition element
GHz	Giga Hertz
ID	Identifier
IE	Information Element
LSB	Least Significant Bit
MAC	Medium Access Control
Mbps	Megabits per second
MDE	Mobility Domain element
MDID	Mobility domain identifier
MIC	Message integrity code
OFDM	Orthogonal Frequency Division Multiplexing
OUI	Organizationally Unique Identifier
PMKID	Pairwise master key identifier
PSK	Preshared key
RA	Receiver Address
RM	Radio measurement
RSNE	Robust Security Network element
SN	Sniffer

SSID	Service Set Identifier
STA	Station
TA	Transmitter Address
TIE	Timeout Interval element
TSF	Timing synchronization function
TUs	Time Units
WLAN	Wireless Local Area Network
WMM™	Wi-Fi CERTIFIED Wi-Fi Multimedia™
WNM	Wireless network management

2   Test tools, methodology and approach

This section defines the tools, methodology, and approach for testing and certifying Wi-Fi Agile Multiband devices.

2.1   Sniffer

A sniffer test tool is required for test cases throughout this test plan. The capabilities for the sniffer are listed below.

1. Capable of capturing data over wireless and wired interfaces.

2. Capable of capturing and decoding IEEE 802.11a/b/g/n/ac frames.

3. Capable of capturing, decoding and displaying MBO-OCE information element.

4. Capable of capturing, decoding and displaying Beacon requests and Beacon reports, BSS Transition Management Request frames, WNM Notification frames and GAS ANQP frames.

2.2   Wi-Fi Test Suite software

The Wi-Fi Alliance's Wi-Fi Test Suite provides configuration, test control, traffic generation, and results analysis services. The entire test plan may be executed in a fully automated manner using Wi-Fi Alliance-distributed command scripts and the Unified CAPI console. Additional information is available through the member website https://www.wi-fi.org/members/certification-testing/wi-fi-test-suite.

2.3   Basic system test configuration

Figure 1 depicts the basic system test configuration for testing and certifying Wi-Fi Agile Multiband devices.

The test bed layout shall meet the following requirements:

1. All APs shall be placed on a shelf approximately 12 inches above the bench where the STAs are positioned.

2. A line of sight shall exist between all APs and STAs. The distance between APs and STAs should not exceed 12 feet and should not be less than 1 foot.

3. If testing in an RF chamber, ensure that there is 25% or greater reflectivity.
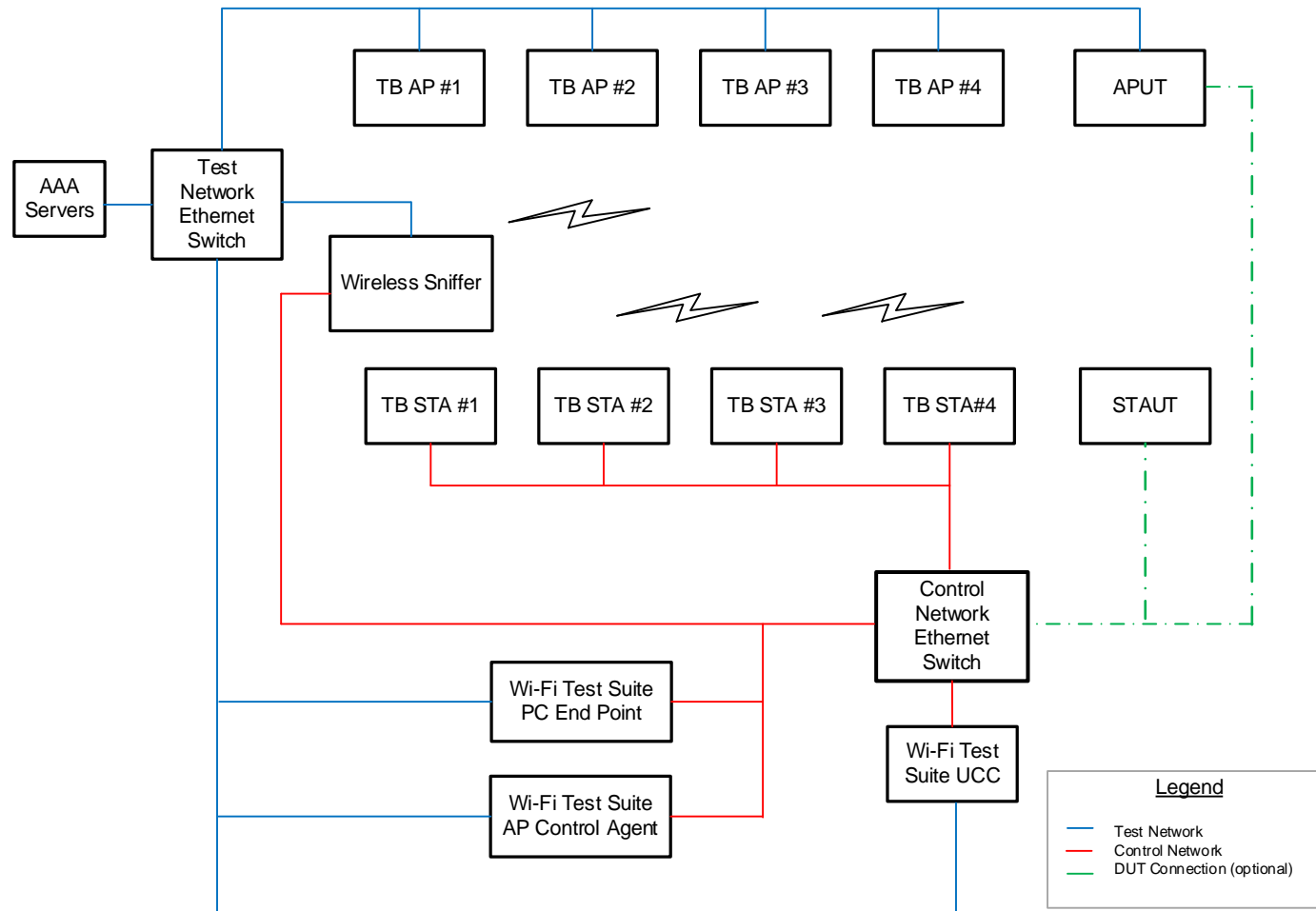
Figure 1. System test configuration

2.4 Test bed capability requirements

2.4.1 Test bed AP requirements

The test bed AP shall support all three Beacon request Measurement Modes, and generate an appropriate Beacon report (see section 5.2.3).

The test bed AP shall support a configuration option to include or not include the Last Beacon Report Indication Request subelement in the Beacon request (see section 5.2.3).

The test bed AP shall support a configuration option to enable capabilities in order to transmit Beacon frames greater than 255 octets in length.

Table 4 defines the Wi-Fi Agile Multiband default parameters for a test bed AP. If required, the following parameter values are modified for specific test cases.

Table 4.   Test bed AP default parameter values

Parameter	Description	Default value
SSID	Service Set Identifier	Wi-Fi
Security	802.11 Security method	WPA2-Personal
Encryption Key	Key used for encryption	MBORocks
Channel width	Width of the channel used for testing	20 MHz
AP Primary channel	Primary channel used for the test	36 (if 5GHz capable else 6)
Disassociation Imminent bit in the BTM Request		Disabled (0)
BSS termination bit in the BTM Request		Disabled (0)
Association disallowed		Disabled (0)
PMF (Protected Management Frame)		MFPC (bit 7) set to 1 MFPR (bit 6) set to 0
Validity Interval in the BTM Request		Minimum of 15 TBTTs

2.4.2   Test bed STA requirements

The test bed STA requirements are:

1. The test bed STA shall trigger an Association Request frame even if the AP is disallowing association requests.

2. The test bed STA shall send a BTM query that includes a non-existent AP.

3. The test bed STA shall support all three Beacon request Measurement Modes and respond with an appropriate Beacon report (see section 4.2.3).

Table 5 defines the Wi-Fi Agile Multiband default parameters for a test bed STA. If required, the following parameter values are modified for specific test cases.

Table 5.   Test bed STA default parameter values

Parameter	Description	Default value
SSID	Service Set Identifier	Wi-Fi
Security	802.11 Security method	WPA2-Personal
Encryption Key	Key used for encryption	MBORocks
Channel width	Width of the channel used for testing	20 MHz
AP Primary channel	Primary channel used for the test	36 (if 5GHz capable else 6)
PMF (Protected Management Frame)		MFPC (bit 7) set to 1 MFPR (bit 6) set to 0

3 Requirements for Wi-Fi Alliance certification

The following items describe the necessary features that are required for a DUT to pass Wi-Fi CERTIFIED Agile Multiband certification.

3.1 General requirements

3.1.1 Prerequisite certification requirements

Products submitted for Wi-Fi CERTIFIED Agile Multiband certification shall have the following pre-requisite certifications:

- Wi-Fi CERTIFIED™ a OR Wi-Fi CERTIFIED™ b OR Wi-Fi CERTIFIED™ g

AND

- Wi-Fi CERTIFIED WPA2™ with Protected Management Frames

3.1.2 General DUT testing requirements

The APUT shall provide a mechanism to perform the following general test requirements.

- Configure parameters sent in a Beacon request.
- Trigger the AP to send a Beacon request.
- Trigger the AP to steer a specified STA away from its BSS with and without the Disassociation Imminent bit set.

3.2 Applicability of tests

The applicable tests for certification are the tests of mandatory features and tests of optional features that a vendor chooses to declare or that are indicated by the DUT as described in the underlying technical specifications. Table 6 and Table 7 list the applicable tests for the APUT and STAUT respectively.

"Applicability" indicates whether a feature and its associated tests are either mandatory or optional to implement. Mandatory (M) tests are required for certification.

Optional (O) tests are performed if the vendor declares the feature, or the DUT indicates the feature as described in the underlying technical specifications via transmitted frames or transmitted messages or user interfaces. If the optional feature is declared and if that test fails, the DUT shall fail the Wi-Fi CERTIFIED Agile Multiband certification. Conditional (C) tests are mandatory if certain specified conditions pertain to the DUT (again, as declared by the vendor during the submission or indicated by the DUT), and are optional otherwise.

If the feature requires information, in particular if the vendor implements or supports an optional feature, the fourth column contains a "Y" and the vendor shall provide information in the DUT Information spreadsheet. (A copy of the spreadsheet is accessible through the online Wi-Fi Alliance Certification System.)

If a vendor declares an optional feature, that feature shall be indicated by the DUT as described in the underlying technical specifications. Declaration of an optional feature by a vendor comprises inclusion of the feature in the appropriate Wi-Fi Alliance registration and DUT Information spreadsheet at the time of submission. An optional feature that was not declared, but is indicated within an associated capabilities field(s), IE's, or any transmitted frames comprises inclusion of the feature.

Each vendor shall fill out the DUT Information spreadsheet completely. Test labs will verify that the list of optional features declared by the vendor matches the list indicated by the DUT; each optional feature for which any test exists in this test plan and that appears in one list shall also appear in the other. The information determines which tests and which test parameters apply to the certification.

A "Y" in the last column indicates the certain subset of optional capabilities that will be indicated on the interoperability certificate if they are declared by the vendor.

3.2.1 APUT tests

Table 6 summarizes the APUT tests for the Wi-Fi Agile Multiband program.

Table 6.   APUT test applicability

Test case description	Test Plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Should Feature be listed in the Capabilities Form? (Y/N)	If implemented, displayed in certificate as " Wi-Fi CERTIFIED Agile Multiband Capability" (Y/N)?
APUT configuration requirements validation test	4.1.1	M		
APUT out-of-the-box test	4.2.1	M		
APUT MBO capability indication test	4.2.2	M		
APUT Beacon request test	4.2.3	M		
APUT ANQP 2-way support test, Neighbor Report with ANQP test	4.2.4			
GAS ANQP response and Neighbor Report element with Zero GAS Comeback Delay test	4.2.4.1	M		
GAS ANQP response and Neighbor Report element with Non-Zero GAS Comeback Delay test	4.2.4.2	O		
GAS ANQP response with Cellular Data Connection Preference test	4.2.4.3	C		
APUT BSS Transition Management tests	4.2.5			

Test case description	Test Plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Should Feature be listed in the Capabilities Form? (Y/N)	If implemented, displayed in certificate as " Wi-Fi CERTIFIED Agile Multiband Capability" (Y/N)?
BSS Transition Management Query and Request between an associated STA and an AP test	4.2.5.1	M		
BSS Transition Management Query and Request between a multimode STA and a cellular data aware AP test	4.2.5.2	C		
Unsolicited BSS Transition Management Request frame with and without Disassociation Imminent bit test	4.2.5.3	M		
Unsolicited BSS Transition Management Request frame with BSS Termination bit test	4.2.5.4	M		
Unsolicited BSS Transition Management Request frame to Multimode STA test	4.2.5.5	C		
APUT Fast BSS Transition test	4.2.6	O		
APUT Association Disallowed Capability test	4.2.7	M		
APUT usage of non-preferred channels information from STA test	4.2.8	M		

3.2.2   STAUT tests

Table 7 summarizes the STAUT tests for the Wi-Fi Agile Multiband program.

Table 7.   STAUT test applicability

Test case description	Test Plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Should Feature be listed in the Capabilities Form? (Y/N)	If implemented, displayed in certificate as "Wi-Fi CERTIFIED Agile Multiband Capability" (Y/N)?
STAUT out-of-the-box test	5.2.1	M		
STAUT MBO Capability Indication test	5.2.2	M		
STAUT Beacon report test	5.2.3	M		
STAUT GAS ANQP test	5.2.4			
Interworking element indication in Probe requests and GAS ANQP Request test	5.2.4.1	O		
GAS ANQP Request for Cellular Data Connection Preference test	5.2.4.2	O		
STAUT BTM tests	5.2.5			

Test case description	Test Plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Should Feature be listed in the Capabilities Form? (Y/N)	If implemented, displayed in certificate as "Wi-Fi CERTIFIED Agile Multiband Capability" (Y/N)?
BSS Transition Query Request test	5.2.5.1	O		
STA Response to AP BSS Transition Management Request frame with Disassociation Imminent bit set to one test	5.2.5.2	M		
STA Response to AP BSS Transition Management Request Frame with BSS Termination Included bit set to one test	5.2.5.3	M		
STAUT Fast BSS Transition test	5.2.6	O		
STAUT Association Disallowed Capability test	5.2.7	M		
STAUT Channel and Band Indication and Preference test	5.2.8	M		
STAUT Multimode Indication test	5.2.9	CM		

3.3 Configuration requirements

3.3.1 APUT configuration requirements

Table 8 lists the default APUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Note: If APUT vendor is using its own AP device for test case 4.2.5 and 4.2.8, then these additional AP devices shall be identical to the APUT.

Table 8.   APUT default mode configuration

Item	Mode Name	Default
1	SSID	Wi-Fi
2	Security	WPA2-Personal
3	Encryption Key	MBORocks
4	Channel width	20 MHz
5	AP Primary channel	36 (if 5 GHz capable else 6)
6	Disassociation Imminent bit in the BTM Request	Disabled (0)
7	BSS termination bit in the BTM Request	Disabled (0)
8	PMF (Protected Management Frame)	MFPC (bit 7) set to 1 MFPR (bit 6) set to 0

3.3.2   STAUT configuration requirements

Table 9 lists the default STAUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 9.   STAUT default mode configuration

Item	Mode Name	Default
1	Spatial streams	1
2	Bandwidth	20 MHz
3	SSID	Wi-Fi
4	Security	WPA2-Personal
5	Encryption Key	MBORocks
6	PMF (Protected Management Frame)	MFPC (bit 7) set to 1 MFPR (bit 6) set to 0

3.4   Testing rules

3.4.1   General testing rules

Multiple test procedures in this document verify successful association. Association is verified by transmitting a ping (ICMP Echo request) from the AP to the STA and waiting for the AP to receive a positive response (ICMP Echo Response) from the STA.

3.4.2   APUT testing rules

1. If the APUT fails any tests, no further testing will be performed until the vendor addresses the problems and has updated the device.

2. The default APUT parameters listed in Table 8 shall be configured on devices at the start of each test case. If any of the parameters cannot be configured through the user interface, then the APUT test fails.

3.4.3   STAUT testing rules

1. If the STAUT fails any tests, no further testing shall be performed until the vendor addresses the problems and has updated the device.

2. The default STAUT parameters listed in Table 9 shall be configured on devices at the start of each test case. If any of the parameters cannot be configured through the user interface, then the STAUT test fails.

4 APUT test cases

4.1 Configurability tests

4.1.1 APUT configuration requirements validation test

Objective

This test validates that the APUT is configurable with the parameters required for the test cases in section 4. Note that this test case is not automated by a Wi-Fi Test Suite script. The technician shall manually configure the required parameters through the user interface.

Applicability: Mandatory

References

N/A

Test environment

- APUT

Test configuration

Table 8 defines the specific parameter values required for this test case.

Test procedure and expected results

Table 10 provides the specific test procedure and expected results for this test case.

Table 10. APUT configuration requirements validation test procedure and expected results

Step	APUT	Expected result
1	Configure the SSID.	If able to configure the SSID, then CONTINUE, else FAIL.
2	Configure the Security.	If able to configure the Security, then CONTINUE, else FAIL.
3	Configure the Encryption Key.	If able to configure the Encryption Key, then CONTINUE, else FAIL.
4	Configure the Channel width.	If able to configure the Channel width, then CONTINUE, else FAIL.
5	Configure the AP Primary channel.	If able to configure the AP Primary channel, then PASS, else FAIL.

4.2   APUT tests

4.2.1   APUT out-of-the-box test

Objective

This test verifies the APUT's out-of-the-box configuration as defined in Table 8 to simulate using the device for the first time after initial power on. It also verifies that the APUT sets the BTM, Interworking Capability and RM Capability bits and advertises the RM Enabled Capabilities, Interworking, Advertisement Protocol with ANQP and MBO-OCE information element in its out-of-the-box configuration.

Applicability: Mandatory

References

Section 4.1 [2]

Section 9.4.2.45, 9.4.5 [3]

Test environment

- APUT
- Test bed STA
- Wireless sniffer

Test configuration

Table 5, Table 8, and Table 11 define the specific parameter values required for this test case.

Table 11.   APUT out-of-box test configuration

PARAMETER	APUT VALUE	Test bed STA value
Test bed vendor	N/A	Marvell STA

Test procedure and expected results

Table 12 provides the specific test procedure and expected results for this test case.

Table 12.   APUT out-of-the -box test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT to the operating band, channel, and channel width specified in Table 8.	Configure the STA to the default mode specified in Table 5.	
2	The APUT transmits Beacon frames		SN: Verify that the Beacon frame from the APUT contains the following: • Bit 19 (BSS Transition Management Capability) and bit 31 (Interworking Capability) of the Extended Capabilities field set to 1 • An RM Enabled Capabilities element is present • Bit 1 in the RM Enabled Capabilities field of the RM Enabled Capabilities element is set to 1 • The Interworking element is present (element ID 0x6B) and the length is equal to 1, 3, 7 or 9 • A Country element is present (element ID 7) and the third octet of the Country String field is set to 0x04 • The Advertisement Protocol element is present (element ID 0x6C) and the length is greater than or equal to 2 • ANQP is advertised in the Advertisement Protocol element, and there is at least one Advertisement Protocol Tuple with Advertisement Protocol ID equal to zero (ANQP). • An MBO-OCE IE is present with the following format: ▪ Element ID is set to 0xDD ▪ Length value is set to ≥ 7 ▪ OUI is set to 0x506F9A ▪ OUI Type is set to 0x16 ▪ Attribute ID is set to 0x01 (MBO AP Capability Indication) If all the conditions listed above are true, then CONTINUE, else FAIL.
3		The STA transmits a Probe Request frame to the APUT.	
4	The APUT transmits a Probe Response frame to the STA.		SN: Verify that the Probe Response frame from the APUT contains the following: • Bit 19 (BSS Transition Management) and bit 31 (Interworking Capability) of the Extended Capabilities field set to 1 • An RM Enabled Capabilities element is present • Bit 1 from the RM Enabled Capabilities field of the RM Enabled Capabilities element is set to 1 • The Interworking element is present (element ID 0x6B) and the length is equal to 1, 3, 7 or 9 • A Country element is present (element ID 7) and the third octet of the Country String field is set to 0x04 • Advertisement Protocol element is present (element ID 0x6C) and the length is greater than or equal to 2

Step	APUT	Test bed STA	Expected result
			• An MBO-OCE IE is present with the following format: ▪ Element ID is set to 0xDD ▪ Length value is set to ≥ 7 ▪ OUI is set to 0x506F9A ▪ OUI Type is set to 0x16 ▪ Attribute ID is set to 0x01 (MBO AP Capability Indication) If all the conditions listed above are true, then CONTINUE, else FAIL
5		The STA transmits an Association Request frame to the APUT.	
6	The APUT transmits an Association Response frame to the STA.		SN: Verify that the Association Response frame from the APUT contains the following: • Bit 19 of the Extended Capabilities field (BSS Transition Management) set to 1 • An RM Enabled Capabilities element is present • Bit 1 from the RM Enabled Capabilities field of the RM Enabled Capabilities element is set to 1 • An MBO-OCE IE is present with the following format: ▪ Element ID is set to 0xDD ▪ Length value is set to ≥ 7 ▪ OUI is set to 0x506F9A ▪ OUI Type is set to 0x16 ▪ Attribute ID is set to 0x01 (MBO AP Capability Indication) If all the conditions listed above are true, then PASS, else FAIL

4.2.2 APUT MBO capability indication test

Objective

This test verifies that the AP transmits a correctly formatted MBO-OCE IE carrying an MBO AP Capability Indication attribute in the Beacon, Probe Response and Association Response frames.

Applicability: Mandatory

References

Section 4.2.1 [2]

Sections 9.3.3.2, 9.3.3.3, 9.3.3.6, 9.3.3.11 [3]

Test environment

- APUT
- Test bed STA
- Wireless sniffer

Test configuration

Table 5, Table 8 and Table 13 define the specific parameter values required for this test case.

Table 13. APUT MBO capability indication test configuration

Parameter	APUT value	Test bed STA value
Test bed vendor	N/A	Broadcom STA

Test procedure and expected results

Table 14 provides the specific test procedure and expected results for this test case.

Table 14.   APUT MBO capability indication test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 8.	Configure the STA as described in Table 5.	
2	The APUT starts transmitting Beacon frames.		SN: Verify that the APUT transmits a Beacon frame with an MBO-OCE IE carrying an MBO AP Capability Indication attribute, with the following format: - Element ID is set to value 0xDD - Length value is set to ≥ 7 - OUI is set to 0x506F9A - OUI Type is set to 0x16 - Attribute ID is set to 0x01 (MBO AP Capability Indication) - Attribute Length is set to 1 - MBO AP Capability Indication field value is set to 0x00 if the APUT is not cellular data aware, or is set to 0x40 if the APUT is cellular data aware - A Country element is present (element ID is 7) where the third octet of the Country String field is set to the value 0x04 When all the above conditions are true then CONTINUE, else FAIL.
3		Trigger the STA to send a Probe Request frame to the APUT with an MBO-OCE IE, in the Primary Channel of the APUT.	
4	The APUT responds with a Probe Response frame.		SN: Verify that the APUT transmits a Probe Response frame with an MBO-OCE IE carrying an MBO AP Capability Indication attribute, with the following format: - Element ID is set to value 0xDD - Length value is set to ≥ 7 - OUI is set to 0x506F9A - OUI Type is set to 0x16 - Attribute ID is set to 0x01 (MBO AP Capability Indication) - Attribute Length is set to 1 - MBO AP Capability Indication field value is set to 0x00 if the APUT is not cellular data aware, or 0x40 if the APUT is cellular data aware. - A Country element is present (element ID is 7) where the third octet of the Country String field is set to the value 0x04 When all the above conditions are true then CONTINUE, else FAIL.

Step	APUT	Test bed STA	Expected result
5		Trigger the STA to associate to the APUT, by sending an Association Request frame to the APUT with an MBO-OCE IE, in the Primary Channel of the APUT.	
6	The APUT responds with an Association Response frame.		SN: Verify that the APUT transmits an Association Response frame with an MBO-OCE IE carrying an MBO AP Capability Indication attribute, with the following format: - Element ID is set to value 0xDD - Length value is set to ≥ 7 - OUI is set to 0x506F9A - OUI Type is set to 0x16 - Attribute ID is set to 0x01 (MBO AP Capability Indication) - Attribute Length is set to 1 - MBO AP Capability Indication field value is set to 0x00 if the APUT is not cellular data aware, or 0x40 if the APUT is cellular data aware. When all the above conditions are true then PASS, else FAIL.

4.2.3   APUT Beacon request test

Objective

This test verifies that the APUT transmits correctly formatted Beacon requests with various parameter settings and is able to receive corresponding Beacon reports from a STA.

The test procedure is repeated for various parameter settings for the Beacon request. If the APUT supports both 2.4 GHz and 5 GHz bands, run each set of six tests once for the 2.4 GHz band and once for the 5 GHz band. If the APUT is single-band, run the set only for the band that the APUT supports. The APUT shall run and pass all six test cases to verify that it supports all three Measurement Modes.

Applicability: Mandatory

References

Section 3.4 [2]

Section 11.11.9.1 [3]

Section 9.4.2.20.7 [4]

Test environment

- APUT
- Test bed Wi-Fi CERTIFIED dual-band n/ac AP, with the ability to support multiple BSSIDs
- Test bed STA
- Wireless sniffer

Test configuration

Table 15 defines the specific parameter values required for this test case. Test bed AP shall use a unique BSSID for each BSS/SSID.

Table 15.   APUT Beacon request test configuration

Parameter	APUT value	Test bed AP value	Test bed STA value
Test bed vendor	N/A	Mediatek AP (2.4 GHz) Qualcomm AP (5 GHz)	Intel STA (2.4 GHz) Broadcom STA (5 GHz)
AP Primary Channel	6 when running test for 2.4 GHz band 36 when running test for 5 GHz band	48 (on 5 GHz) and 1 (on 2.4 GHz) NOTE: Same setting of one channel on each band when running test for 2.4 GHz or 5 GHz band.	
Channel Width	20 MHz	20 MHz	20 MHz

Parameter	APUT value	Test bed AP value	Test bed STA value
SSID1	WiFi1	WiFi1	
SSID2		WiFi2	
SSID3		WiFi3	
Regulatory Domain	Global if device supports (or any that the device supports)	Same as APUT's Regulatory Domain	
FT	FT Enabled if supported (Over-The-Air FT Protocol)	FT Enabled if supported (Over-The-Air FT Protocol)	
Other			Roaming disabled

Table 16.   APUT Beacon request field values

Field	Case 1 value	Case 2 value	Case 3 value	Case 4 value	Case 5 value	Case 6 value
Destination MAC address	Address of STA	Address of STA	Address of STA	Address of STA	Address of STA	Address of STA
Operating class	Global Regulatory Domain: 81 when running test for 2.4 GHz band; 115 when running test for 5 GHz band	Global Regulatory Domain: 81 when running test for 2.4 GHz band; 115 when running test for 5 GHz band	Global Regulatory Domain: 81 when running test for 2.4 GHz band; 115 when running test for 5 GHz band	Global Regulatory Domain: 81 when running test for 2.4 GHz band; 115 when running test for 5 GHz band	Global Regulatory Domain: 81 when running test for 2.4 GHz band; 115 when running test for 5 GHz band	Global Regulatory Domain: 81 when running test for 2.4 GHz band; 115 when running test for 5 GHz band
Channel number	0	255	0	Single Channel set to the channel of AP	Single Channel set to the channel of AP	255
Randomization interval	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000
Number of repetitions	0					
Measurement duration	20 ms	50 ms	20 ms	112 ms	20 ms	50 ms
Measurement mode	Active (1)	Active (1)	Table (2)	Passive (0)	Active (1)	Active (1)
BSSID	Wildcard	Wildcard	Wildcard	Wildcard	BSSID corresponding to WiFi1 SSID of AP	Wildcard

Field	Case 1 value	Case 2 value	Case 3 value	Case 4 value	Case 5 value	Case 6 value
SSID	WiFi1	WiFi1	WiFi1	SSID sub-element absent (implies wildcard SSID)	SSID sub-element absent (implies wildcard SSID)	WiFi1
Reporting Condition	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA
Reporting Detail	1	1	0	1	1	1
Duration Mandatory	0	0	0	0	0	0
AP Channel Report	NA	Channel 1 and 6 when running test for 2.4 GHz band, Channel 36 and 48 when running test for 5 GHz band	NA	NA	NA	Channel 1 and 6 when running test for 2.4 GHz band, Channel 36 and 48 when running test for 5 GHz band
Request	0 (SSID), 54 (Mobility Domain) if Fast Transition is supported by the APUT, 221 (Vendor Specific)	0 (SSID), 54 (Mobility Domain) if Fast Transition is supported by the APUT, 221 (Vendor Specific)	NA	0 (SSID), 54 (Mobility Domain) if Fast Transition is supported by the APUT, 221 (Vendor Specific)	0 (SSID), 54 (Mobility Domain) if Fast Transition is supported by the APUT, 221 (Vendor Specific)	0 (SSID), 54 (Mobility Domain) if Fast Transition is supported by the APUT, 221 (Vendor Specific)
Repetition	0	0	0	0	0	0
Last Beacon Report Indication Request subelement	Present, Data field value=1	Default	Default	Default	Default	Default

Test procedure and expected results

Table 17 provides the specific test procedure and expected results for this test case.

Table 17. APUT Beacon request test procedure and expected results

Step	APUT	Test bed AP	Test bed STA	Expected result
1	Configure the APUT as defined in Table 8 and Table 15.		Configure the STA as defined in Table 5 and Table 15.	
2	The APUT starts transmitting Beacon frames.			
3			Allow the test bed STA to associate to the APUT using the WiFi1 BSSID.	
4		Configure the test bed AP as defined in Table 4 and Table 15. The test bed AP starts transmitting Beacon frames.		
Case 1				
5	Trigger the APUT to generate a Beacon request using the values specified in Case 1 in Table 16.			SN: If the APUT transmits a correctly protected and correctly formatted Beacon request with the values as specified in Case 1 in Table 16, then CONTINUE else FAIL. SN: If the Beacon Request includes a correctly formatted Last Beacon Report Indication Request subelement with the Data field value set to 1, then CONTINUE else FAIL.
6			Wait 5 seconds. The STA responds with a Beacon report.	
Case 2				
7	Trigger the APUT to generate a Beacon request frame using the values specified in Case 2 in Table 16.			SN: If the APUT transmits a correctly protected and correctly formatted Beacon request with the values as specified in Case 2 in Table 16, then CONTINUE else FAIL.

Step	APUT	Test bed AP	Test bed STA	Expected result
8			Wait 5 seconds. The STA responds with a Beacon report.	
Case 3				
9	Trigger the APUT to generate a Beacon request using the values specified in Case 3 in Table 16.			SN: If the APUT transmits a correctly protected and correctly formatted Beacon request with values as specified in Case 3 in Table 16, then CONTINUE else FAIL.
10			Wait 5 seconds. The STA responds with a Beacon report.	
Case 4				
11	Trigger the APUT to generate a Beacon request using the values specified in Case 4 in Table 16.			SN: If the APUT transmits a correctly protected and correctly formatted Beacon request with values as specified in Case 4 in Table 16, then CONTINUE else FAIL.
12			Wait 5 seconds. The STA responds with a Beacon report.	
Case 5				
13	Trigger the APUT to generate a Beacon request using the values specified in Case 5 in Table 16.			SN: If the APUT transmits a correctly protected and correctly formatted Beacon request with values as specified in Case 5 in Table 16, then CONTINUE else FAIL.
14			Wait 5 seconds. The STA responds with a Beacon report	
Case 6				
15	Trigger the APUT to generate a Beacon request using the values specified in Case 6 in Table 16.			SN: If the APUT transmits a correctly protected and correctly formatted Beacon request with values as specified in Case 6 in Table 16, then PASS else FAIL.

4.2.4 APUT ANQP 2-way support test, Neighbor Report with ANQP test

4.2.4.1 GAS ANQP response and Neighbor Report element with Zero GAS Comeback Delay test

Objective

This test verifies that the APUT transmits correctly formatted GAS Response frames and ANQP responses. It also verifies that the APUT responds to the test bed STA's requests using GAS and ANQP responses with a Neighbor report with no delay.

Applicability: Mandatory

References

Sections 11.25.3.2, 9.4.5.19 [3]

Test environment

- APUT
- Test bed STA
- Wireless sniffer

Test configuration

Table 18 defines the specific parameter values required for this test case.

Table 18. GAS ANQP response and Neighbor Report element with Zero GAS Comeback Delay test configuration

Parameter	APUT value	Test bed STA value
Test bed vendor	N/A	Marvel STA
AP Primary Channel	36 (if 5 GHz capable; else 1)	36 (if 5 GHz capable; else 1)
GAS Comeback Delay	0	
Association	N/A	Not associated

Test procedure and expected results

Table 19 provides the specific test procedure and expected results for this test case.

Table 19.   GAS ANQP response and Neighbor Report element with Zero GAS Comeback Delay test procedure and expected results

Description	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 18.	Configure the STA as described in Table 18.	
2	The APUT starts to transmit Beacon frames.		
3		The STA does not associate with the APUT.	
4		Trigger the STA to transmit an ANQP query for Neighbor report to the APUT.	
5	The APUT transmits an ANQP response.		SN: Verify that the GAS Initial Response frame is properly formatted including: • Address 1 field is set to the MAC address of the STA and Address 3 field is set to the wildcard BSSID value • Dialog Token (DT) matches DT in the GAS Initial Request frame • Advertisement protocol element for ANQP is present • Query Response contains one of more Neighbor Reports elements (Info ID 272) • Query Response Length is correct • Verify the response contains the Neighbor report, where the Element ID (52) and Length are included in each Neighbor Report element. If the GAS Response frame satisfies all the requirements above, then PASS, else FAIL.

4.2.4.2   GAS ANQP response and Neighbor Report element with Non-Zero GAS Comeback Delay test

Objective

This test verifies that the APUT transmits correctly formatted GAS Response frames and ANQP responses in a GAS Comeback Response.

Applicability: Optional. This test shall be executed only if the APUT declared support for 4-frame GAS exchange in Table 1.

References

Sections 11.25.3.2, 9.4.2.37, 9.4.5.19, 11.25.3.1 [3]

Test environment

- APUT
- Test bed STA
- Wireless sniffer

Test configuration

Table 20 defines the specific parameter values required for this test case.

Table 20.   GAS ANQP response and Neighbor Report element with Non-Zero GAS Comeback Delay test configuration

Parameter	APUT value	Test bed STA value
Test bed vendor	N/A	Qualcomm STA
AP Primary Channel	36 (if 5 GHz capable; else 1)	36 (if 5 GHz capable; else 1)
GAS Comeback Delay	5 seconds (as closely as possible, in TUs)	
Association		Not associated

Test procedure and expected results

Table 21 provides the specific test procedure and expected results for this test case.

Table 21.   GAS ANQP response and Neighbor Report element with Non-Zero GAS Comeback Delay test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 20.	Configure the STA as described in Table 20.	
2	The APUT starts to transmit Beacon frames.		

Step	APUT	Test bed STA	Expected result
3		The STA does not associate with the APUT.	
4		Trigger the STA to transmit an ANQP query for Neighbor report to the APUT.	
5	The APUT transmits an ANQP response.		SN: Verify that the GAS Initial Response frame is properly formatted including: • Address 1 field is set to the MAC address of the STA and Address 3 field is set to the wildcard BSSID value • Dialog Token (DT) matches DT in GAS Initial Request frame • Advertisement protocol element for ANQP is present • Query Response Length is correct • GAS Comeback Delay is set per Table 20 If the GAS Response frame satisfies all the requirements above, then CONTINUE, else FAIL.
6		The STA waits for the Comeback Delay time, transmits a GAS Comeback Request; and continues transmitting GAS Comeback Request frames until a GAS Comeback Response frame is received.	
7	The APUT transmits an ANQP response with a Neighbor report to the STA.		SN: Verify that the GAS Comeback Response frame is properly formatted including: • Address 1 field is set to the MAC address of the STA and Address 3 field is set to the wildcard BSSID value • Dialog Token (DT) matches DT in GAS Initial Request frame • Comeback Delay value set to 0 • Advertisement protocol element for ANQP is present • Query response contains one or more Neighbor Reports elements (Info ID 272) • Query response length is correct • The response contains a Neighbor report

Step	APUT	Test bed STA	Expected result
			If the GAS Response frame satisfies all the requirements above, then PASS, else FAIL

4.2.4.3   GAS ANQP response with Cellular Data Connection Preference test

Objective

This test verifies that the APUT transmits a correctly formatted Cellular Data Connection Preference subtype in the GAS Response frame and ANQP response.

Applicability: Conditionally mandatory. This test case is required if the APUT is a cellular data aware AP.

References

Section 3.3, 4.3.2 [2]

Section 11.25.3.2 [3]

Test environment

- APUT
- Test bed Wi-Fi Agile Multiband multimode STA
- Wireless sniffer

Test configuration

Table 22 defines the specific parameter values for the devices in this test case.

Table 22.   GAS ANQP response with Cellular Data Connection Preference test configuration

Parameter	APUT value	Test bed STA value
Test bed vendor	N/A	Intel STA
AP Primary Channel	36 (if 5 GHz capable; else 1)	36 (if 5 GHz capable; else 1)
Channel Width	20 MHz	20 MHz
Association	N/A	Not associated

Test procedure and expected results

Table 23 provides the specific test procedure and expected results for this test case.

Table 23. GAS ANQP response with Cellular Data Connection Preference test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 22.	Configure STA as described in Table 22.	
2	The APUT starts to transmit Beacon frames.		SN: Verify that the APUT transmits a Beacon frame with an MBO-OCE IE carrying an MBO AP Capability Indication attribute, with the following format: • Element ID is set to 0xDD • Length is set to ≥ 7 • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x01 (MBO AP Capability Indication) • Attribute Length is set to 1 • MBO AP Capability Indication field value is 0x40 (cellular data aware) When all the above conditions are true then CONTINUE, else FAIL.
3		The STA does not associate with the APUT.	
4		Trigger the STA to transmit an ANQP query with MBO Query List ANQP element including a Cellular Data Connection Preference subtype ANQP element.	
5	The APUT transmits an ANQP response.		SN: Verify that the GAS Initial Response frame is properly formatted including: • Dialog Token (DT) matches DT in GAS Initial Request frame • Advertisement protocol element for ANQP is present • Query Response Length is correct • Query Response contains MBO ANQP-element • InfoID is set to 56797 • OUI is set to 0x506F9A

Step	APUT	Test bed STA	Expected result
			• OUI Type is set to 0x12 • Subtype 2 (Cellular Data Connection Preference) • Payload contains a value of {0,1, or 255} If the GAS Response frame satisfies all the requirements above and the GAS Comeback Delay value is 0, then PASS, If the GAS Response frame satisfies all the requirements above and the GAS Comeback Delay value is non-zero, then CONTINUE, otherwise FAIL
6		The STA waits for the Comeback Delay time, transmits a GAS Comeback Request; and continues transmitting GAS Comeback Request frames until a GAS Comeback Response frame is received.	
7	The APUT transmits an ANQP response.		SN: Verify that the GAS Comeback Response frame is properly formatted, including: • DT matches DT in GAS Initial Request frame • Comeback Delay value set to 0 • Advertisement protocol element for ANQP is present • Query response length is correct • Query Response contains MBO ANQP-element • InfoID is set to 56797 • OUI is set to 0x506F9A • OUI Type is set to 0x12 • Subtype 1 (Cellular Data Connection Preference) • Payload contains a value of {0,1 255} If the GAS Response frame satisfies all the requirements above then PASS, else FAIL.

4.2.5 APUT BSS Transition Management tests

4.2.5.1 BSS Transition Management Query and Request between an associated STA and an AP test

Objective

This test verifies that the APUT correctly responds to the BTM Query from an associated STA.

Part A tests that the APUT correctly provides the BSS Transition Candidate Preference list to the STA.

Part B tests that the APUT overwrites the candidate preference values received from the STA.

Applicability: Mandatory

References

Section 3.5.1.2 [2]

Sections 9.6.14.8, 9.6.14.9, 9.4.2.37 [3]

Test environment

- APUT
- AP1: Either test bed or optionally supplied by APUT vendor (unused in test, it is only present to enable inclusion in the BSS Transition Candidate List Entries)
- AP2: Either test bed or optionally supplied by APUT vendor (unused in test, it is only present to enable inclusion in the BSS Transition Candidate List Entries)
- Test bed STA
- Wireless sniffer

Test configuration

Table 24 defines the specific parameter values required for this test case.

Table 24. BSS Transition Management Query and Request between an associated STA and an AP test configuration

Parameter	APUT value	AP1 and AP2 value	Test bed STA value
Test bed vendor	N/A	Mediatek AP1 Intel AP2	Qualcomm STA
BSS Transition Management Capability	Enabled	Enabled	Enabled
Disassociation Imminent bit in the BTM Request	Not set	Not set	N/A

Parameter	APUT value	AP1 and AP2 value	Test bed STA value
BSS termination bit in the BTM Request	Not set	Not set	N/A
Action upon BTM Request	-	-	STA is configured not to transition away upon receiving a BTM request
Operating Class	0x73 (Global operating class) if STA is 5 GHz capable, 0x51 (Global operating class) if STA is not 5 GHz capable	0x73 (Global operating class) if STA is 5 GHz capable, 0x51 (Global operating class) if STA is not 5 GHz capable	0x73 (Global operating class) if STA is 5 GHz capable, 0x51 (Global operating class) if STA is not 5 GHz capable
Channel Number	36 (if 5 GHz supported, else 1)	40 (if 5 GHz supported, else 6)	36 (if 5 GHz supported) else 1
BSS Transition Candidate Preference	If configurable, value for own BSS is 255, for AP1 is 254, for AP2 is 253	-	Value for AP1 is 154, for AP2 is 155

Test procedure and expected results

Table 25 provides the specific test procedure and expected results for this test case.

Table 25. BSS Transition Management Query and Request between an associated STA and an AP test procedure and expected results

Step	APUT	AP1/AP2	Test bed STA	Expected result
1	Configure the APUT as described in Table 8 and Table 24.		Configure the STA as described in Table 5 and Table 24 and disable roaming on the STA.	
2	The APUT starts to transmit Beacon frames.			SN: If the APUT transmits a Beacon frame with an Extended Capabilities element with bit 19 set to 1 (BSS Transition enabled), then CONTINUE, else FAIL.
3			The STA sends an Association Request frame to the APUT.	
4		Configure AP1 and AP2 as described in Table 4 and Table 24. AP1 and AP2 start to transmit Beacon frames.		
5	The APUT responds with an Association Response frame.			SN: If the APUT transmits an Association Response frame with an Extended Capabilities element with bit 19 set to

Step	APUT	AP1/AP2	Test bed STA	Expected result
				1 (BSS Transition enabled), then CONTINUE, else FAIL.
6	If the APUT does not populate the BSS Transition Candidate List automatically, then configure the BSS Transition Candidate List Entries to contain at least AP1 and AP2, per Table 24 settings.			
Part A: BTM Query requesting for BSS candidate APs				
7			Trigger the STA to transmit a BTM Query Action frame to the APUT with no BSS Transition Candidate List Entries included.	
8	The APUT responds by sending a BTM Request Action frame to the STA.			SN: Verify that the APUT transmits a correctly protected BTM Request Action frame with the following format: • Category is set to 0x0A (WNM) • Action field is set to 0x07 (BSS Transition Management Request) • Dialog Token is set to the same value as received in step 6 • Request Mode indicates: ▪ Preferred Candidate List Included bit is set to 1 ▪ Disassociation Imminent bit is set to 0 ▪ BSS Termination Included bit is set to 0 ▪ ESS Disassociation Imminent bit is set to 0 ▪ Abridged bit is not tested • The Validity Interval is set to a nonzero value • The BSS Transition Candidate List Entries contains at least three Neighbor Report elements with the list of neighbors including the APUT's own BSS, AP1 and AP2, and with Operating class and Channel Number field values in the BSS Transition Candidate Preference sub elements set as per Table 24

Step	APUT	AP1/AP2	Test bed STA	Expected result
				• If the Preference values were configured, verify they match the values in Table 24 • If the Preference values were not configured, verify they are in some combination of 255, 254 and 253, without skipping any value higher than any used value If all the conditions above are true then CONTINUE, else FAIL.
9			STA sends a BTM Response Action Frame.	Note: No results should be checked in/after this response.
Part B BTM Query indicating STA's transition Preference				
10			Configure the BSS transition Candidate List Entries containing two Neighbor Report elements, including AP1 and AP2. Configure the Neighbor Report elements with the Operating Class and Channel Number specified in Table 24.	
11			Trigger the STA to transmit a BTM Query Action frame to the APUT with the configured BSS candidate list and transition reason set to 19 (Preferred BSS transition candidate list included).	
12	APUT responds by sending a BTM Request Action frame to the STA.			SN: Verify that the APUT transmits a correctly protected BTM Request Action frame with the following format: • Category is set to 0x0A (WNM) • Action field is set to 0x07 (BSS Transition Management Request) • Dialog Token is set to the same value as received in step 8 • Request Mode indicates: ▪ Preferred Candidate List Included bit is set to 1

Step	APUT	AP1/AP2	Test bed STA	Expected result
				▪ Disassociation Imminent bit is set to 0 ▪ BSS Termination Included bit is set to 0 ▪ ESS Disassociation Imminent bit is set to 0 ▪ Abridged bit is not tested • Validity Interval is set to a nonzero value • BSS Transition Candidate List Entries contain at least three Neighbor reports, with the list of neighbors including the APUT's own BSS, AP1 and AP2 with Operating class and Channel Number values in the BSS Transition Candidate Preference sub elements set as per Table 24 • If the Preference values were configured, verify they match the values in Table 24. • If the Preference values were not configured, verify they are some combination of 255, 254 and 253, without skipping any value higher than any used value When all the above conditions are true then PASS, else FAIL.
13			STA sends a BTM Response Action frame.	
Note: No additional verification is required beyond this point.				

4.2.5.2 BSS Transition Management Query and Request between a multimode STA and a cellular data aware AP test

Objective

This test verifies that a cellular data aware APUT correctly responds to the BTM Query from an associated multimode STA by including the Cellular Data Connection Preference attribute in the BSS Transition Management Request frame.

Applicability: Conditionally mandatory. This test case is required if the APUT is capable of indicating cellular data network preference.

References

Section 3.5.1.2 [2]

Sections 9.6.14.8, 9.6.14.9 [3]

Test environment

- APUT
- Test bed Multimode STA
- Wireless sniffer

Test configuration

Table 26 defines the specific parameter values required for this test case.

Table 26. BSS Transition Management Query and Request between a multimode STA and a cellular data aware AP test configuration

Parameter	APUT value	Test bed STA value
Test bed vendor	N/A	Intel STA
BSS Transition Management Capability	Enabled	Enabled
Cellular Data Connection Preference attribute	Enabled, any valid Cellular Data Preference value	
Cellular Data Capabilities attribute		Cellular data connection available

Test procedure and expected results

Table 27 provides the specific test procedure and expected results for this test case.

Table 27. BSS Transition Management Query and Request between a multimode STA and a cellular data aware AP test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 8 and Table 26.	Configure the STA as described in Table 5 and Table 26.	
2	The APUT starts to transmit Beacon frames.		SN: Verify that the following conditions are true: • APUT transmits a Beacon frame with an Extended Capabilities element with bit 19 set to 1 (BSS Transition is enabled). • MBO AP Capability Indication field set to 0x40 If all the conditions above are true then CONTINUE, else FAIL
3		The STA sends an Association Request frame to the APUT containing an MBO-OCE IE with a Cellular Data Capabilities attribute.	
4	The APUT responds with an Association Response frame.		SN: If the APUT transmits an Association Response frame with an Extended Capabilities element with bit 19 set to 1 (BSS Transition is enabled), then CONTINUE, else FAIL.
5		Trigger the STA to send a BTM Query Action frame to the APUT.	

6	The APUT responds by sending a BTM Request Action frame to STA.		SN: Verify that the APUT transmits a correctly protected BTM Request Action frame with the following format:
			• Category is set to 0x0A (WNM)
			• Action field is set to 0x07 (BSS Transition Management Request)
			• Dialog Token is set to the same value as received in step 5
			• The Request Mode indicates:
			  ▪ Preferred Candidate List Included bit is set to 1
			  ▪ Disassociation Imminent bit is set to 0
			  ▪ BSS Termination Included bit is set to 0
			  ▪ ESS Disassociation Imminent bit is set to 0

Step	APUT	Test bed STA	Expected result
			▪ Abridged bit is not tested • BSS Transition Candidate List Entries contains one of more Neighbor reports including the APUT's own BSS • MBO-OCE IE containing Cellular Data Connection Preference attribute, with any valid preference value • Preference value for the cellular data connection and the APUT's own BSS shall not be both set to zero (either or both can be non-zero) When all the above conditions are true then PASS, else FAIL.
7		STA sends a BTM Response.	
Note: No additional verification is required beyond this point.			

4.2.5.3 Unsolicited BSS Transition Management Request frame with and without Disassociation Imminent bit test

Objective

This test verifies the following:

- An unsolicited APUT's request to the STA for BSS transition with and without the Disassociation Imminent bit set.
- One or more Neighbor Report elements in the BSS Transition Candidate List corresponds to the APUT's BSS and AP1's BSS
- Successful test bed STA non-FT re-association between AP1 and the APUT.

Applicability: Mandatory

References

Section 3.5.2 [2]

Sections 9.6.14.8, 9.6.14.9, 9.6.14.10, 9.4.2.37 [3]

Test environment

- APUT
- AP1: AP supplied by APUT vendor, or the BSS corresponding to AP1 may be configured on the 2.4 GHz band of a dual-band capable APUT
- Test bed STA
- Wireless sniffer

Test configuration

Table 28 defines the specific parameter values required for this test case.

Table 28. Unsolicited BSS Transition Management Request frame with and without Disassociation Imminent bit test configuration

Parameter	APUT value	AP1 value	Test bed STA value
Test bed vendor	N/A	Intel AP	Broadcom STA
BSS Transition Management Capability	Enabled	Enabled	Enabled
BSS Transition Candidate List Entries	Configure the BSS Transition Candidate List Entries on the APUT, if necessary, to contain at least two Neighbor Report elements, including the APUT and AP1		
Disassociation Imminent bit in the BTM Request Action Frame	Not set	N/A	
BSS termination bit in the BTM Request Action Frame	Not set	N/A	

Parameter	APUT value	AP1 value	Test bed STA value
			STA is configured not to transition away upon receiving a BTM Request Action Frame
			STA is configured to not send a Disassociation Frame to APUT upon receiving a BTM Request with Disassociation Imminent bit set to1.
Channel Number	36 if 5 GHz is supported, else 1	6 if 2.4 GHz is supported, else 40	

Test procedure and expected results

Table 29 provides the specific test procedure and expected results for this test case.

Table 29. Unsolicited BSS Transition Management Request frame with and without Disassociation Imminent bit test procedure and expected results

Step	APUT	AP1	Test bed STA	Expected result
1		Configure AP1 per Table 8 and Table 28. AP1 starts transmitting Beacon frames.	Configure the STA as described in Table 5 and Table 28 and disable roaming on the STA.	
2			The test bed STA associates to AP1.	
3	Configure the APUT as described in Table 8 and Table 28. The APUT starts to transmit Beacon frames.			SN: If the APUT transmits a Beacon frame with an Extended Capabilities element with bit 19 set to 1 (BSS Transition is enabled), then CONTINUE, else FAIL.
4			Wait 5 seconds, then the test bed STA sends an Authentication frame, and subsequently a Reassociation Request frame. In both frames, the DA is set to the BSSID of the APUT.	
5	The APUT sends a Reassociation Response frame.			SN: If the APUT transmits an Reassociation Response frame with an Extended Capabilities element with bit 19 set to 1 (BSS Transition is enabled) and with Status Code indicating success (0), then CONTINUE, else FAIL.

Step	APUT	AP1	Test bed STA	Expected result
6	Trigger APUT to transmit a BTM Request Action frame to the STA.			SN: Verify that the APUT transmits a correctly protected BTM Request Action frame with the following format: • Category is set to 0x0A (WNM) • Action field is set to 0x07 (BSS Transition Management Request) • Request Mode indicates: ▪ Preferred Candidate List Included bit is set to 1 ▪ Disassociation Imminent bit is set to 0 ▪ BSS Termination Included bit is set to 0 ▪ ESS Disassociation Imminent bit is set to 0 ▪ Abridged bit is not tested • Validity Interval is set to nonzero value • BSS Transition Candidate List Entries contains one or more Neighbor reports, including AP1 • MBO-OCE IE has the transition Reason Code set as follows: ▪ Element ID is set to 0xDD ▪ Length value is ≥ 7 ▪ OUI is set to 0x506F9A ▪ OUI Type is set to 0x16 ▪ Attribute ID is set to 0x06 ▪ Attribute Length is set to 1 ▪ Attribute value is ≥ 0 and ≤ 9 ▪ Disassociation Imminent bit in the BTM Request is not set to 1 ▪ BSS termination bit in the BTM Request is not set to 1 When all the above conditions are true, then CONTINUE, else FAIL.
7			STA sends the BSS Transition Response with reject status code.	
8	Configure and trigger the APUT to transmit a BTM Request Action frame to the STA with			SN: Verify that the APUT transmits a correctly protected BTM Request Action frame in the following format: • Category is set to 0x0A (WNM)

Step	APUT	AP1	Test bed STA	Expected result
	Disassociation Imminent bit set to 1.			- Action field is set to 0x07 (BSS Transition Management Request) - Request Mode indicates: - Preferred Candidate List Included bit is set to 1 - Disassociation Imminent bit is set to 1 - BSS Termination Included bit is set to 0 - ESS Disassociation Imminent bit is set to 0 - Abridged bit is not tested - Validity Interval is set to nonzero value - Disassociation timer is set to a nonzero value. Record the Disassociation timer value. - BSS Transition Candidate List Entries contains one or more Neighbor reports including AP1. The largest non-zero Preference field value in the Neighbor reports is 255, and non-zero Preference field values in other Neighbor reports either have the same value or decrement consecutively from 255. - APUT's preference value (if present) is set to 0 - The MBO-OCE IE contains at least the transition Reason Code attribute and the Association Retry Delay attribute. The MBO-OCE IE is set as follows - Element ID is set to 0xDD - Length value is set to a value ≥ 11 - OUI is set to 0x506F9A - OUI Type is set to 0x16 - Transition Reason Code attribute is set as follows: - Attribute ID is set to 0x06 - Attribute Length is set to 1 - Attribute value is ≥ 0 and ≤ 9 - Association Retry Delay attribute is set as follows: - Attribute ID is set to 0x08 (Association Retry Delay) - Attribute length is set to 2 - Attribute value is set to a non-zero value When all the above conditions are true then CONTINUE, else FAIL.

Step	APUT	AP1	Test bed STA	Expected result
9			The STA sends a BTM Response Action frame.	
Wait for (2 seconds + Disassociation timer value from step 8).				
10				If the APUT sends a correctly protected Disassociation frame to the STA within 2 seconds after the Disassociation timer expires, then PASS, else FAIL.

4.2.5.4 Unsolicited BSS Transition Management Request frame with BSS Termination bit test

Objective

This test verifies the APUT's request to the STA for BSS transition to show that the APUT correctly sends an unsolicited request for BSS transition to an associated STA.

Applicability: Mandatory

References

Section 3.5.2 [2]

Section 9.6.14.9 [3]

Test environment

- APUT
- Test bed STA
- Wireless sniffer

Test configuration

Table 30 defines the specific parameter values required for this test case.

Table 30. Unsolicited BSS Transition Management Request frame with BSS Termination bit test configuration

Parameter	APUT value	Test bed STA value
Test bed vendor	N/A	Marvell STA
BSS Transition Management Capability	Enabled	Enabled
BSS Termination TSF	Set to a non-zero value	

Test procedure and expected results

Table 31 provides the specific test procedure and expected results for this test case.

Table 31. Unsolicited BSS Transition Management Request frame with BSS Termination bit test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 8 and Table 30.	Configure the STA as described in Table 5 and Table 30.	

Step	APUT	Test bed STA	Expected result
2		The STA associates with the APUT.	
3	Trigger the APUT to transmit a BTM Request Action frame to the STA with BSS Termination bit set to 1, the BSS Termination TSF field set to 5 seconds, and the Duration field set to 2 minutes.		SN: Verify that the APUT transmits a correctly protected BTM Request Action frame in the following format: • Category is set to 0x0A (WNM) • Action field is set to the 0x07 (BSS Transition Management Request) • Request Mode indicates: ▪ BSS Termination Included bit is set to 1 ▪ Other bits are not tested • BSS Termination Duration subelement is present and its fields are set to: ▪ Length field is set to 0x0A ▪ BSS Termination TSF is set to a non-zero value ▪ Duration field is set to 2 minutes • BSS Transition Candidate List Entries contains zero or more Neighbor reports; and ▪ if the APUT's own BSS is present, its preference value is set to 0 ▪ If the BSS Transition Candidate List Entries contains one or more entries (is present), the Preferred Candidate List Included bit in the Request Mode field is set to 1 ▪ If the BSS Transition Candidate List Entries is not present (no entries), the Preferred Candidate List Included bit in the Request Mode field is set to 0 • MBO-OCE IE does not include the Association Retry Delay attribute When all the above conditions are true then CONTINUE, else FAIL.
4		The STA responds by sending a BTM Response frame.	
Wait for the BSS Termination TSF period.			
5			If the APUT sends a Disassociation frame to the STA and stops sending Beacon frames, then PASS, else FAIL.

4.2.5.5 Unsolicited BSS Transition Management Request frame to Multimode STA test

Objective

This test verifies that a cellular data aware APUT request to a multimode STA to show that the APUT correctly sends an unsolicited request for BSS transition by including the Cellular Data Connection Preference attribute to an associated multimode STA.

Applicability: Conditionally mandatory. This test case is required if the APUT is capable of indicating cellular data network preference.

References

Section 3.5.2 [2]

Section 9.6.14.9 [3]

Test environment

- APUT
- Test bed Multimode STA
- Wireless sniffer

Test configuration

Table 32 defines the specific parameter values required for this test case.

Table 32.   Unsolicited BSS Transition Management Request frame to Multimode STA test configuration

Parameter	APUT value	Test bed STA value
Test bed vendor	N/A	Broadcom STA
BSS Transition Management Capability	Enabled	Enabled
Cellular Data Connection Preference attribute	Enabled, any valid Cellular Data Preference value	
Cellular Data Capabilities attribute		Cellular data connection available

Test procedure and expected results

Table 33 provides the specific test procedure and expected results for this test case.

Table 33. Unsolicited BSS Transition Management Request frame to Multimode STA test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 8 and Table 32.	Configure the STA as described in Table 5 and Table 32	
2		The STA associates with the APUT.	
3	Trigger the APUT to transmit a BTM Request Action frame to the STA.		SN: Verify that the APUT transmits a correctly protected BTM Request Action frame with the following format: • Category is set to 0x0A (WNM) • Action field is set to 0x07 (BSS Transition Management Request) • Request Mode indicates that other bits are not tested • Validity Interval is set to nonzero value • BSS Transition Candidate List Entries contains zero or more Neighbor reports • Includes an MBO-OCE IE containing the Cellular Data Connection Preference attribute with any valid preference value • Preference value for the cellular data connection and the APUT's own BSS (if the latter is included) shall not be both set to zero (either or both can be non-zero) When all the above conditions are true, then PASS, else FAIL.
4		The STA sends a BTM Response Action frame.	
Note: No additional verification is required beyond this point.			

4.2.6   APUT Fast BSS Transition test

Objective

This test verifies that the APUT performs Fast BSS Transition using the Over-the-Air FT protocol when a STA moves between the APUT and another AP in the same mobility domain.

If the APUT supports both Fast BSS Transition with PSK and Fast BSS Transition with 802.1X, then the test is run twice (once for each mode), and the APUT shall pass both tests. If the APUT only supports one of the two modes, only that mode is tested.

NOTE: The APUT shall advertise support for the Fast BSS Transition AKM(s) in this test. If the APUT also supports other authentication algorithms (e.g. FILS SK), it may also advertise those AKMs.

Applicability: Optional. This test shall be executed only if the APUT declared support for FT with WPA2-Personal and/or WPA2-Enterprise (802.1X) in Table 1.

References

Section 3.7 [2]

Section 13 [3]

Test environment

- APUT
- AP1: Provided by APUT vendor and is part of same mobility domain as APUT
- AAA Server (required for FT with 802.1X test): May be provided by the APUT vendor, or as part of WFA test bed
- Test bed STA: FT capable and capable of disabling autonomous roaming while leaving directed roaming operational
- Network Ping Endpoint: A test bed laptop that is on the same IP subnet as the APUT and AP1 and reachable from both APs
- Wireless sniffer

Test configuration

Table 34 defines the specific parameter values required for this test case.

Table 34.   APUT Fast BSS Transition test configuration

Parameter	APUT value	AP1 value	Test bed STA value
Test bed vendor	N/A	Provided by APUT vendor	Broadcom STA (WPA2-Personal) Intel STA (WPA2-Enterprise)
AP Primary Channel	36 (if 5 GHz capable; else 6)	48 (if 5 GHz capable; else 1)	36 (if 5 GHz capable; else 6)

Parameter	APUT value	AP1 value	Test bed STA value
Channel Width	20 MHz	20 MHz	20 MHz
SSID1	WiFi1	WiFi1	
Security	For FT with PSK test: WPA2, For FT with 802.1X test: EAP-TTLS/MSCHAPv2	For FT with PSK test: WPA2 For FT with 802.1X test: EAP-TTLS/MSCHAPv2	For FT with PSK test: WPA2 For FT with 802.1X test: EAP-TTLS/MSCHAPv2
Security Encryption key/credentials	For FT with PSK test: MBORocks, For FT with 802.1X test: username="ttls-user", password="password" (AAA server is common between APUT and AP1)	For FT with PSK test: MBORocks, For FT with 802.1X test: username="ttls-user", password="password" (AAA server is common between APUT and AP1)	For FT with PSK test: MBORocks, For FT with 802.1X test: username="ttls-user", password="password"
FT	FT Enabled (Over-The-Air FT Protocol), For FT with PSK test: configured to advertise support for FT with PSK, For FT with 802.1X test: configured to advertise support for FT with 802.1X, Note: APUT may also enable and advertise support for other authentication methods	FT Enabled (Over-The-Air FT Protocol), For FT with PSK test: configured to advertise support for FT with PSK, For FT with 802.1X test: configured to advertise support for FT with 802.1X, Note: APUT may also enable and advertise support for other authentication methods	FT Enabled (Over-The-Air FT Protocol), For FT with PSK test: configured to use FT with PSK, For FT with 802.1X test: configured to use FT with 802.1X
RSNA	Supported	Supported	Supported
BTM Config	Configure to send BTM with AP1 at preference 255 and its own BSS at preference 0	Configure to send BTM with APUT at preference 255 and its own BSS at preference 0	
Other			Roaming disabled

Test procedure and expected results

Table 35 provides the specific test procedure and expected results for this test case.

Table 35.   APUT Fast BSS Transition test procedure and expected results

Step	APUT	AP1	Test bed STA	Expected result
1	Configure the APUT and AP1 as defined in Table 35, according to the test mode being used (PSK or 802.1X). Configure the APUT and AP1 to the same mobility domain.		Configure the STA as defined in Table 35.	
2	Turn on APUT. APUT starts to transmit Beacon frames.			SN: Verify that APUT transmits a correctly formatted Beacon with the Mobility Domain element (MDE) with:

Step	APUT	AP1	Test bed STA	Expected result
				• MDID is present and valid • Fast BSS Transition over DS bit set to 0 • RSNE with AKM Suite List field includes at least the following AKM, depending on the test mode: ▪ for FT with PSK test: 00-0F-AC:4 ▪ for FT with 802.1X test: 00-0F-AC:3 SN: Record the actual AKM Suite Count and AKM Suite List from the RSNE When all the above conditions are true, then CONTINUE else FAIL
3			Allow the STA to associate to the APUT to the WiFi1 SSID using FT in the corresponding test mode (PSK or 802.1X). The STA sends an Association Request to the APUT.	
4	The APUT responds by sending an Association Response frame.			SN: Verify that the APUT transmits a correctly formatted Association Response frame to STA, containing: • Fast Transition IE (FTE) containing the R1KH-ID and R0KH-ID and having ▪ MIC element count set to 0 ▪ ANonce set to 0 ▪ SNonce set to 0 ▪ MIC set to 0 • MDE as advertised in the Beacon When all the above conditions are true, then CONTINUE else FAIL
5	Wait 2 seconds for FT 4-way handshake to occur.			SN: Verify the following are true: • A successful FT 4-way handshake is performed • EAPOL message 3 of the handshake, the APUT includes the following: ▪ RSNE with PMKR1Name in the PMKID field of the RSNE ▪ FTE and MDE are present ▪ TIE with PTK key lifetime

Step	APUT	AP1	Test bed STA	Expected result
				- TIE with reassociation deadline timeout and that reassociation deadline ≤ PTK key lifetime - PMKR1Name in message 3 from the APUT matches the PMKR1Name in message 2 from the STA When all the above conditions are true, then CONTINUE else FAIL
6			The STA starts a continuous ping to the Network Ping Endpoint. Wait 10 seconds. Ensure that ping packets are sent via the APUT and that the ping is successful.	
7		Turn on AP1. AP1 starts to transmit Beacon frames. Wait 10 seconds.		
8	Trigger APUT to send a BTM Request to the STA asking it to move to AP1's BSSID.			SN: Verify that the APUT sends a correctly protected and correctly formatted BTM Request Action frame to the STA with the following format: - Category is set to 0x0A (WNM) - Action field is set to 0x07 (BSS Transition Management Request) - Request Mode indicates: - Preferred Candidate List Included bit is set to 1 - Disassociation Imminent bit is set to 0 - BSS Termination Included bit is set to 0 - ESS Disassociation Imminent bit is set to 0 - Abridged bit is not tested - Validity Interval is set to nonzero value - BSS Transition Candidate List Entries contains two Neighbor reports, including the APUT's own BSS at priority 0 and AP1 at priority 255 - MBO-OCE IE has the transition Reason Code set as follows: - Element ID is set to 0xDD - Length value is set to ≥ 7 - OUI is set to 0x506F9A - OUI Type is set to 0x16

Step	APUT	AP1	Test bed STA	Expected result
				▪ Attribute ID is set to 0x06
				▪ Attribute Length is set to 1
				▪ Attribute value is set to a value ≥ 0 and ≤ 9
				▪ Disassociation Imminent bit in the BTM Request is not set to 1
				▪ BSS termination bit in the BTM Request is not set to 1
				When all the above conditions are true, then CONTINUE else FAIL
9			The STA roams to AP1 by performing FT Reassociation. Wait 10 seconds and ensure that ping packets are sent via AP1 and that the ping is successful.	SN: Verify that the APUT transmits a correctly formatted Reassociation Response frame to the test bed STA, containing • FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID • MDE • RSNE with PMKR1Name, RSN version set to 1, and AKM Suite Count field and AKM Suite List field exactly matching those recorded in Step 2 When all the above conditions are satisfied, then CONTINUE else FAIL.
10		Trigger AP1 to send a BTM Request to the STA asking it to move to the APUT's BSSID.		
11			The STA sends an Authentication Request to the APUT with a FT Authentication Algorithm.	
12	The APUT responds with an Authentication Response frame.			SN: Verify that the APUT transmits a correctly formatted Authentication Response frame to the STA, containing • FTE with ANonce, SNonce, R1KH-ID and R0KH-ID • MDE • RSNE with PMKR0Name When all the above conditions are true, then CONTINUE else FAIL
13			The STA sends a Reassociation Request to the APUT containing	

Step	APUT	AP1	Test bed STA	Expected result
			FTE, MDE and RSNE, where RSNE indicates support for the tested FT mode by setting AKM Suite Count field to 1 and AKM Suite List field to the following: • for FT with PSK test: 00-0F-AC:4 • for FT with 802.1X test: 00-0F-AC:3 Ensure that the time between the Authentication Request and Reassociation Request does not exceed the Reassociation Deadline Time.	
14	The APUT responds to the Reassociation Request by sending a Reassociation Response frame.			SN: Verify that the APUT transmits a correctly formatted Reassociation Response frame to the STA, containing • FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID • MDE • RSNE with PMKR1Name, RSN version set to 1, and AKM Suite Count field and AKM Suite List field exactly matching those recorded in Step 2 When all the above conditions are true, then CONTINUE else FAIL
15			Wait 10 seconds	SN: Verify the following are true: • A 4-way handshake is not performed between the STA and APUT. • Correctly protected ping packets are sent via the APUT and that the ping is successful When all the above conditions are true, then PASS else FAIL

4.2.7   APUT Association Disallowed Capability test

Objective

This test verifies that the AP transmits a correctly formatted MBO-OCE IE carrying an Association Disallowed attribute in the Beacon and Probe Response frames.

Applicability: Mandatory

References

Sections 3.6, 4.2.4 [2]

Sections 9.3.3.2, 9.3.3.6, 9.3.3.8, 9.3.3.10 [3]

Test environment

- APUT
- Test bed STA
- Wireless sniffer

Test configuration

Table 36 defines the specific parameter values required for this test case.

Table 36.   APUT Association Disallowed Capability test configuration

Parameter	APUT value	Test bed STA value
Test bed Vendor	N/A	Marvell STA

Test procedure and expected results

Table 37 provides the specific test procedure and expected results for this test case.

Table 37.   APUT Association Disallowed Capability test procedure and expected results

Step	APUT	Test bed STA	Expected result
1	Configure the APUT as described in Table 8 and Table 36.		
2	Configure the APUT to disallow associations.		

Step	APUT	Test bed STA	Expected result
3	The APUT starts to transmit Beacon frames.		SN: Verify that the APUT transmits a Beacon frame with an MBO-OCE IE carrying an Association Disallowed attribute, with the following format: • Element ID is set to 0xDD • Length value is set to a value ≥ 10 (as the Capability Indication attribute shall also be present) • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x04 (Association Disallowed) • Attribute Length is set to 1 • Reason Code is set to any value between 0x01 and 0x05 When all the above conditions are true, then CONTINUE, else FAIL.
4		Configure the STA as described in Table 5 and trigger the STA to send a Probe Request frame to the APUT.	
5	The APUT responds with a Probe Response frame.		SN: Verify that the APUT transmits a Probe Response frame with an MBO-OCE IE carrying an Association Disallowed attribute, with the following format: • Element ID is set to 0xDD • Length value is set to a value ≥ 10 (as the Capability Indication attribute shall also be present) • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x04 (Association Disallowed) • Attribute Length is set to 1 • Reason Code is set to any value between 0x01 and 0x05 When all the above conditions are true, then CONTINUE, else FAIL.
6		Trigger the STA to associate to the APUT. NOTE: The STA shall meet the requirement in item 1 from section 2.4.2.	Verify that the test bed STA sends an Association Request to the APUT. If it does not, check the test setup and resume the test from Step 1.
7	The APUT responds with an Association Response frame.		SN: Verify that the APUT transmits an Association Response frame with an MBO-OCE IE carrying an Association Disallowed attribute, with the following format: • Element ID is set to 0xDD

Step	APUT	Test bed STA	Expected result
			• Length value is set to a value ≥ 10 (as the Capability Indication attribute shall also be present) • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x04 (Association Disallowed) • Attribute Length is set to 1 • Reason Code is set to any value between 1 and 5 SN: Verify the Status Code field in the Association Response frame is set to the value of 17 or 30. When all the above conditions are true, then PASS, else FAIL

4.2.8   APUT usage of non-preferred channels information from STA test

Objective

This test verifies that the APUT does not steer a STA to a non-operable channel, and also verifies that the APUT discards any previously cached non-preferred channels information for a STA when the STA sends an update.

Applicability: Mandatory

References

Section 3.2 [2]

Section 11.24.7.3 [3]

Test environment

- APUT
- AP1: a Wi-Fi CERTIFIED n/ac AP. AP1 can have any of the following configurations:
    - Two-channels, one operating on 2.4 GHz and the other on 5 GHz. In this case, AP2 is not required.
    - Two channels, both operating on 2.4 GHz or on 5 GHz. In this case, AP2 is not required.
    - A single channel AP operating on either 2.4 GHz or 5 GHz. If this configuration is used, AP2 is required.
- AP2: a Wi-Fi CERTIFIED n/ac AP. AP2 operates on a single channel either on 2.4 GHz or 5 GHz. AP2 if used, is configured on the same channel as AP1CH2.
- Test bed STA: a Wi-Fi CERTIFIED dual-band n/ac and Wi-Fi Agile Multiband multimode STA, capable of disabling autonomous roaming while leaving directed roaming operational
- Wireless sniffer

Test configuration

0 defines the specific parameter values required for this test case.

APUT usage of non-preferred channels information from STA test configuration

Parameter	APUT value	AP1/AP2 value	Test bed STA value
Test bed vendor	N/A	Mediatek AP1 (and if needed Intel AP2)	Intel STA
AP Primary Channel	36 (if APUT is 5 GHz capable), else 6	AP1CH1 = 1 and AP1CH2 = 44 (if dual band is supported by APUT), AP1CH1 = 1 and AP1CH2 = 11 (if only 2.4 GHz is supported by APUT),	36 (if APUT is 5 GHz capable; else 6)

Parameter	APUT value	AP1/AP2 value	Test bed STA value
		AP1CH1 = 40 and AP1CH2 = 44 (if only 5 GHz is supported by APUT)	
Channel Width	20 MHz		20 MHz
SSID	WiFi1	WiFi1 on both bands	
Non-preferred channels			AP1CH2 at preference 0
BTM Candidate options (if needed to be configured)	AP1CH1 and AP1CH2		
Other			Configured to reject any unsolicited BSS Transition Management Requests, Roaming disabled
Cellular Data Aware	If APUT is cellular data aware, enable the feature (set the field in MBO AP Capability Indication to 1)		If APUT is cellular data aware, enable the feature on test bed STA, and set to "available" (value=1).

Table 38.   APUT Beacon request parameters

Field	Beacon request 1 value	Beacon request 2 value
Destination MAC address	Address of STA	Address of STA
Operating class	Global Regulatory Domain: 81 (if AP1CH1 is in 2.4 GHz band) else 115	Global Regulatory Domain: 81 (if AP1CH2 is in 2.4 GHz band) else 115
Channel number	AP1CH1	AP1CH2
Randomization interval	Any value between 0 and 1000	Any value between 0 and 1000
Repetition	0	0
Measurement duration	50 ms	50 ms
Measurement mode	Active (1)	Active (1)
BSSID	Wildcard	Wildcard
SSID	WiFi1	WiFi1
Reporting Condition	Default (0) – Report to be issued after each measurement	Default (0) – Report to be issued after each measurement

Field	Beacon request 1 value	Beacon request 2 value
Reporting Detail	1	1
Measurement Duration Mandatory	0	0
Request Information	0 (SSID)	0 (SSID)

Test procedure and expected results

Table 39 provides the specific test procedure and expected results for this test case.

Table 39. APUT usage of non-preferred channels information from STA test procedure and expected results

	Step	APUT	Test bed STA	Expected result
1	Configure the APUT as defined in Table 8 and 0.		Configure the STA as defined in Table 5 (default configuration) and 0. Additionally, configure the STA to send Non-Preferred Channel attribute with the specified configuration in Association Requests.	
2			Allow the STA to associate to APUT. The STA specifies that it is capable of operating on both 2.4 and 5 GHz bands. The STA also specifies channel AP1CH2 as a non-operable channel in the Association Request. After the test bed STA has associated to the APUT, configure and start AP1 as defined in Table 8 and 0. After AP1 is fully operational, configure (via Wi-Fi Test Suite or other means, as needed) the APUT to recognize AP1CH1 and AP1CH2 as both being valid (non-zero preference) candidates. NOTE: No external configuration of these BSSs or their preference is allowed after this point in the test.	
3	Trigger the APUT to send a Beacon Request frame to the STA with the values specified in Table 38, column "Beacon request 1 Values".			SN: If the APUT transmits a correctly protected and correctly formatted Beacon Request with the values specified in "Beacon request 1 Values" column in Table 38, then CONTINUE else FAIL
4			The STA responds with info on AP1 for channel AP1CH1.	
5	Trigger the APUT to send a Beacon Request frame to the STA with the values specified in Table 38, column "Beacon request 2 Values".			SN: If the APUT transmits a correctly protected and correctly formatted Beacon request with values as specified in "Beacon request 2 Values" column in Table 38, then CONTINUE else FAIL

	Step	APUT	Test bed STA	Expected result
6			The STA responds with info on AP1 for channel AP1CH2.	

7	Trigger the APUT to steer the STA away from its BSS (without Disassociation Imminent bit set).
	
	NOTE: Do NOT manually adjust the Neighbor info for the BSS Transition Management Request, nor provide any neighbor preference information via the Wi-fi Test Suite. The APUT shall independently compute the BSS Transition Management Request parameters as described in section 3.1.2.
				SN: Verify that the APUT transmits a correctly protected and correctly formatted BSS Transition Management Request frame containing:
				• Category set to 10
				• Action set to 7
				• Dialog Token set to a non-zero value
				• Request mode containing
				  ▪ Preferred Candidate List Included bit set to 1
				  ▪ Abridged bit set to 0 or 1
				  ▪ Disassociation Imminent bit set to 0
				  ▪ BSS Termination bit set to 0
				  ▪ ESS Disassociation Imminent bit set to 0
				• Validity Interval field set to a non-zero value
				• BSS Transition Candidate List Entries may contain a Neighbor report with its own BSS information.
				• BSS Transition Candidate List Entries also contains a Neighbor Report element that has
				  ▪ Element ID set to 52
				  ▪ Length set to 16 or higher
				  ▪ BSSID field set to the BSSID of AP1 on channel AP1CH1
				  ▪ BSSID Information field present but not verified
				  ▪ Operating Class set to 81 (if AP1 CH1 is on 2.4 GHz) or to 115 (if AP1CH1 is on 5GHz)
				  ▪ Channel Number set to AP1CH1
				  ▪ BSS Transition Candidate Preference subelement present with:Subelement ID set to 3, Length set to 1, Preference set to a non-zero value
				• The BSS Transition Candidate List Entries either does not have a Neighbor Report element for AP1's BSSID on channel AP1CH2, or it contains a Neighbor report for the same with the following values:
				  ▪ Element ID set to 52
				  ▪ Length set to 16 or higher
				  ▪ BSSID field set to BSSID of AP1 on channel AP1CH2

Step		APUT	Test bed STA	Expected result
				• BSSID Information field present but not verified
				• Operating Class set to 81 (if AP1CH2 is on 2.4 GHz) or to 115 (if AP1CH2 is on 5 GHz)
				• Channel Number set to AP1CH2
				• BSS Transition Candidate Preference subelement present with Subelement ID set to 3, Length set to 1, and Preference set to 0
				When all the above conditions are true, then CONTINUE else FAIL.
8			The STA responds with a BSS Transition Management Response, rejecting the BSS Transition Management Request.	
9			Trigger the STA to update its non-preferred channels by sending a WNM Notification frame specifying: • Channel AP1CH1 as non-operable (preference level 0) • Channel AP1CH2 as an operable channel by not including channel AP1CH2 in the non-preferred channels list • A non-preferred channel element for the band not used by AP1CH1(Ch 40 for dual band APUT or 2G-only APUT, Ch 1 for 5G-only APUT) • If the APUT is cellular data aware, include a cellular data capabilities subelement with the Cellular Data Connectivity field set to the value of 2 (Cellular data connection not available).	
10		Trigger the APUT to steer the STA away from its BSS (with Disassociation Imminent bit set). NOTE: Do NOT manually adjust the Neighbor info for the BSS Transition Management Request, nor provide any neighbor preference information via the Wi-fi Test Suite. The APUT shall		SN: Verify that APUT transmits a correctly protected and correctly formatted BSS Transition Management Request frame containing: • Category set to 10 • Action set to 7 • Dialog Token set to a non-zero value • Request mode containing

Step	APUT	Test bed STA	Expected result
independently compute the BSS Transition Management Request parameters.			- Preferred Candidate List Included bit set to 1 - Abridged bit set to 0 or 1 - Disassociation Imminent bit set to 1 - BSS Termination bit set to 0 - ESS Disassociation Imminent bit set to 0 - Validity Interval field set to a non-zero value - BSS Transition Candidate List Entries contains a Neighbor Report element that has - Element ID set to 52 - Length set to 16 or higher - BSSID field set to the BSSID of AP1 on channel AP1CH2 - BSSID Information field present but not verified - Operating Class set to 81 (if AP1CH2 is on 2.4 GHz) or to 115 (if AP1CH2 is on 5 GHz) - Channel Number set to AP1CH2 - BSS Transition Candidate Preference subelement present with Subelement ID set to 3, Length set to 1, and Preference set to a non-zero value - The BSS Transition Candidate List Entries either does not have a Neighbor Report element for AP1's BSSID on channel AP1CH1, or it contains a Neighbor report for the same with the following values: - Element ID set to 52 - Length set to 16 or higher - BSSID field set to BSSID of AP1 on channel AP1CH1 - BSSID Information field present but not verified - Operating Class set to 81 (if AP1CH1 is on 2.4 GHz) or to 115 (if AP1CH1 is on 5 GHz) - Channel Number set to AP1CH1 - BSS Transition Candidate Preference subelement present with Subelement ID set to 3, Length set to 1, Preference set to 0 When all the above conditions are true, then PASS else FAIL.

5 STAUT test cases

5.1 Configurability tests

There are no general configuration requirement tests for the STAUT.

5.2 STAUT tests

5.2.1 STAUT out-of-the-box test

Objective

This test sets the STAUT to its out-of-the-box configuration to simulate using the device for the first time after initial power on. It also verifies that a Wi-Fi Agile Multiband STA sets the BSS Transition and RM Capabilities fields correctly in its out-of-the-box state.

Applicability: Mandatory

References

Section 9.4.2.45 [3]

Test environment

- STAUT:
- Test bed Wi-Fi Agile Multiband AP
- Wireless sniffer

Test configuration

Table 9 and Table 40 give the specific parameter values required for this test case.

Table 40. STAUT out-of-the-box test configuration

Parameter	STAUT value	Test bed AP value
Test bed vendor	N/A	Intel AP

Test procedure and expected results

Table 41 provides the specific test procedure and expected results for this test case.

Table 41.   STAUT out-of-box test procedure and expected results

Step	STAUT	Test bed AP	Expected Result
1		Configure the AP to start sending Beacon frames.	
2	Trigger the STAUT to associate to the AP. Wait 5 seconds.		SN: Verify the conditions below are true: • If the STAUT transmits a Probe Request, then the STAUT transmits a Probe Request frame with an Extended Capabilities element; with bit 19 of the Extended Capabilities field (BTM Capability) set to 1 • The Association Request frame contains an Extended Capabilities element with bit 19 of the Extended Capabilities field set to 1 • The Association Request frame contains an RM Enabled Capabilities field with bit 6 (Beacon report Table Mode) set to 1 • If the STAUT declared support for FT, then verify the Association Request frame contains an RM Enabled Capabilities field with bits 4 (Beacon report Passive Mode) and 5 (Beacon report Active mode) set to 1 If all the conditions above are true, then PASS, else FAIL.

5.2.2   STAUT MBO Capability Indication test

Objective

This test verifies that a Wi-Fi Agile Multiband STA transmits a correctly formatted MBO-OCE IE carrying a Cellular Data Capabilities attribute in the Probe Request and Association Request frames.

Applicability: Mandatory

References

Sections 3.3, 4.2.3 [2]

Sections 9.3.3.6, 9.3.3.8, 9.3.3.10 [3]

Test environment

- STAUT
- Test bed Wi-Fi Agile Multiband AP
- Wireless sniffer

Test configuration

Table 9 and Table 42 give the specific parameter values required for this test case.

Table 42.   STAUT MBO Capability Indication test configuration

Parameter	STAUT value	Test bed AP value
Test bed vendor	N/A	Ruckus AP

Test procedure and expected results

Table 43 provides the specific test procedure and expected results for this test case.

Table 43.   STAUT MBO Capability Indication test procedure and expected results

Step	STAUT	Test bed AP	Expected result
1	Configure the STAUT as described in Table 9.	Configure the AP as described in Table 4.	
2	The STAUT optionally sends a Probe Request frame to the AP. Wait for 5 seconds.		SN: If the STAUT transmits a Probe Request, verify that the STAUT transmits a Probe Request frame with an MBO-OCE IE carrying a Cellular Data Capabilities attribute with the following format:

Step	STAUT	Test bed AP	Expected result
			• Element ID is set to 0xDD • Length value is set to ≥ 7 • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x03 (Cellular Data Capabilities) • Attribute Length is set to 1 • Cellular Data Connectivity field value is set to 0x01, 0x02 or 0x03 When all the above conditions are true, then CONTINUE, else FAIL.
3	Trigger the STAUT to associate to the AP.		SN: Verify that the STAUT transmits an Association Request frame with an MBO-OCE IE carrying a Cellular Data Capabilities attribute, with the following format: • Element ID is set to 0xDD • Length value is set to ≥ 7 • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x03 (Cellular Data Capabilities) • Attribute Length is set to 1 • Cellular Data Connectivity field value is set to 0x01, 0x02 or 0x03 When all the above conditions are true, then PASS, else FAIL.

5.2.3 STAUT Beacon report test

Objective

This test verifies that the STAUT correctly responds to Beacon Requests with various parameter settings and produces correctly formatted Beacon Reports containing appropriate values.

If the STAUT supports both 2.4 GHz and 5 GHz bands, run the test twice, once for the 2.4 GHz band and once for the 5 GHz band. If the STAUT is single band, run the test only for the band that the STAUT supports.

If the STAUT does not support FT, only Case 3 in Table 45 is required. The other cases are optional and tested if implemented. Steps 4 - 7 and steps 10 - 15 are skipped, based on the STAUT's capabilities as signaled in the RM Enabled Capabilities element.

Applicability: Mandatory

References

Section 3.4 [2]

Section 11.11.9.1 [3]

Section 9.4.2.20.7, 9.4.2.21.7 [4]

Test environment

- AP1: Test bed Wi-Fi CERTIFIED dual-band n/ac AP, supporting FT, configured with 3 SSIDs and capable of sending Beacon Request frames (or 3 different APs)
- AP2: Test bed Wi-Fi CERTIFIED dual-band n/ac AP, supporting FT, configured with 3 SSIDs
- STAUT
- Wireless sniffer

Test configuration

Table 44 defines the specific parameter values required for this test case. APs shall use a unique BSSID for each BSS/SSID.

Table 44. STAUT Beacon report test configuration

Parameter	Test bed AP1 value	Test bed AP2 value	STAUT value
Test bed vendor	Qualcomm AP (2.4 GHz) Qualcomm AP (5 GHz)	Mediatek AP (2.4 GHz) Mediatek AP (5 GHz)	N/A
AP Primary Channel	36 (if STAUT is 5 GHz capable; else 6)	48 (on 5 GHz) and 1 (on 2.4 GHz) NOTE: Use this setting independent of the bands supported by the STAUT	36 (if 5 GHz capable; else 6)

Parameter	Test bed AP1 value	Test bed AP2 value	STAUT value
Channel Width	20 MHz	20 MHz	20 MHz
SSID1	WiFi1	WiFi1	
SSID2	WiFi2	WiFi2	
SSID3	WiFi3	WiFi3	
Regulatory Domain	Global (if supported), else Regulatory Domain supported by the country	Global (if supported), else Regulatory Domain supported by the country	
FT	FT Enabled (Over-The-Air FT Protocol)	FT Enabled (Over-The-Air FT Protocol)	
Other			Roaming disabled

Table 45. AP1 Beacon request field values

Field	Case 1 value	Case 2 value	Case 3 value	Case 4 value	Case 5 value	Case 6 value
Destination MAC address	Address of STAUT	Address of STAUT	Address of STAUT	Address of STAUT	Address of STAUT	Address of STAUT
Operating class	Global Regulatory Domain, 81 when running the test for 2.4 GHz band, 115 when running the test for 5 GHz band	Global Regulatory Domain, 81 when running the test for 2.4 GHz band 115 when running the test for 5 GHz band	Global Regulatory Domain, 81 when running the test for 2.4 GHz band, 115 when running the test for 5 GHz band	Global Regulatory Domain, 81 when running the test for 2.4 GHz band, 115 when running the test for 5 GHz band	Global Regulatory Domain, 81 when running the test for 2.4 GHz band, 115 when running the test for 5 GHz band	Global Regulatory Domain, 81 when running the test for 2.4 GHz band, 115 when running the test for 5 GHz band
Channel number	0	255	0	Single Channel set to the channel of AP2	Single Channel set to the channel of AP2	255
Randomization interval	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000	Any value between 0 and 1000
Measurement duration	20 ms	50 ms	20 ms	112 ms	20 ms	50 ms
Measurement mode	Active (1)	Active (1)	Table (2)	Passive (0)	Active (1)	Active (1)
BSSID	Wildcard	Wildcard	Wildcard	Wildcard	BSSID corresponding to WiFi1 SSID of AP2	Wildcard

Field	Case 1 value	Case 2 value	Case 3 value	Case 4 value	Case 5 value	Case 6 value
SSID	WiFi1	SSID sub-element absent (implies wildcard SSID)	WiFi1	SSID sub-element absent (implies wildcard SSID)	SSID sub-element absent (implies wildcard SSID)	WiFi1
Reporting Condition	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA	Default (0) "Report to be issued after each measurement" if APUT supports Reporting Condition, else NA
Reporting Detail	1	1	0	2	1	1
Measurement Duration Mandatory	0	0	0	0	0	0
AP Channel Report	NA	Channels 1and 6 when running the test for 2.4 GHz band, Channels 36 and 48 when running the test for 5 GHz band	NA	NA	NA	Channels 1and 6 when running the test for 2.4 GHz band, Channels 36 and 48 when running the test for 5 GHz band
Request	0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)	0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)	NA	N/A	0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)	0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)
Repetition	0	0	0	0	0	0
Last Beacon Report Indication Request subelement	Not present	Present	Present	Present	Present	Present

Table 46. STAUT Beacon report field values

Field	Case 1 value	Case 2 value	Case 3 value	Case 4 value	Case 5 value	Case 6 value
Operating class	Global Regulatory Domain, 81 for 2.4 GHz band, 115 for 5 GHz band	Global Regulatory Domain, 81 for 2.4 GHz band, 115 for 5 GHz band	Global Regulatory Domain, 81 for 2.4 GHz band, 115 for 5 GHz band	Global Regulatory Domain, 81 for 2.4 GHz band, 115 for 5 GHz band	Global Regulatory Domain, 81 for 2.4 GHz band, 115 for 5 GHz band	Global Regulatory Domain, 81 for 2.4 GHz band, 115 for 5 GHz band

Field	Case 1 value	Case 2 value	Case 3 value	Case 4 value	Case 5 value	Case 6 value
Channel number field	Channel(s) corresponding to AP2 and AP1.	When test is run for 2.4 GHz, channels 1 and 6 required. Other channels 2-8 may be included. When test is run for 5 GHz, channels 36 and 48, only.	Channel(s) corresponding to AP2 and AP1.	Channel corresponding to AP2 (as specified in the request)	Channel corresponding to AP2 (as specified in the request)	When test is run for 2.4 GHz, channels 1 and 6 required. Other channels 2-8 may be included. When test is run for 5 GHz, channels 36 and 48, only.
Actual Measurement Start Time	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified
Measurement Duration	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified
Report Contents	Entries corresponding to WiFi1 BSSID transmitted from AP2 and AP1. May also contain other entries.	6 entries corresponding to all BSSIDs of AP1 and AP2	Entries corresponding to WiFi1 BSSID transmitted from AP2 and AP1.	One entry corresponding to each BSSID transmitted from AP2 in the specified channel.	One entry corresponding to WiFi1 BSSID transmitted from AP2	One entry corresponding to WiFi1 BSSID transmitted from AP2. May also contain other entries.
Reported Frame Information	All fixed fields match Beacon from AP2 for WiFi1 SSID. The following IE's are present: 0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)	All fixed fields match all Beacons from AP1 and AP2. The following IE's are present: 0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)	No information	All fixed fields and IEs from AP2 beacon are present	All fixed fields match Beacon from AP2. The following IE's are present: 0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)	All fixed fields match all Beacons from AP1 and AP2. The following IE's are present: 0 (SSID), 54 (Mobility Domain) if STAUT supports Fast Transition, 221 (Vendor Specific)
RCPI	Value not verified	Value not verified	Value not verified	Value not verified	Value not verified	Value not verified
RSNI	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified	Value present but not verified
BSSID	BSSID corresponding to WiFi1 Beacon from AP2 on the requested channels. May also contain other entries	BSSIDs corresponding to all BSSIDs transmitted by AP1 and AP2 on the requested channels. May also	BSSID(s) corresponding to WiFi1 Beacons from AP1 and AP2 on the requested channels. May also	BSSIDs corresponding to all SSIDs transmitted by AP2 in the specified channel. May also contain other entries	BSSID corresponding to WiFi1 Beacon from AP2. May also contain other entries from	BSSIDs corresponding to WiFi1 Beacon from AP2 and AP1 on the requested channels. May also contain other

Field	Case 1 value	Case 2 value	Case 3 value	Case 4 value	Case 5 value	Case 6 value
	from overlapping channels with WiFi1 SSID.	contain other entries from overlapping channels.	contain other entries from overlapping channels with WiFi1 SSID.	from overlapping channels.	overlapping channels with WiFi1 SSID.	entries from overlapping channels with WiFi1 SSID.
Antenna ID	Value not verified	Value not verified	Value not verified	Value not verified	Value not verified	Value not verified
Parent TSF	Value not verified	Value not verified	Value not verified	Value not verified	Value not verified	Value not verified

Test procedure and expected results

Table 47 provides the specific test procedure and expected results for this test case.

Table 47. STAUT Beacon report test procedure and expected results

Step	STAUT	Test bed AP1 and AP2	Expected result
1	Configure the STAUT as described in Table 9 and Table 44.	Configure AP1 and AP2 as described in Table 4 and Table 44.	
2		AP1 and AP2 start to transmit Beacon frames.	
3	Trigger the STAUT to associate with WiFi1 SSID at AP1's BSSID.		SN: • Confirm the RM Enabled Capabilities element in the Association Request frame indicates the stated STAUT support for Beacon Measurement Capabilities enabled, per Table 1. • Execute the following cases, only for those Measurement Modes supported by the STAUT.
Case 1			
4		Using the Case 1 values specified in Table 45, trigger AP1 to generate a Beacon Request frame that does not contain a Last Beacon indication request subelement	
5	Wait for 5 seconds for the STAUT to respond to the Beacon Request frame.		SN: • Verify that the STAUT transmits one or more correctly protected and formatted Beacon reports with the Case 1 values in Table 46. • Verify that the Dialog Token from the Measurement Report frame matches the Dialog Token of the Measurement Request

Step	STAUT	Test bed AP1 and AP2	Expected result
			frame. If multiple Measurement Report frames are received, the Dialog Token in each Measurement Report frame should match the Dialog Token in the Measurement Request frame. • Verify that the Beacon report does NOT include the Last Beacon Report Indication subelement. When all the above conditions are satisfied, then CONTINUE else FAIL.
Case 2			
6		Trigger AP1 to generate a Beacon Request frame using the Case 2 values specified in Table 45.	
7	Wait for 5 seconds for the STAUT to respond to the Beacon Request frame. Note: This step should be done only if the previous step is executed.		SN: Verify that the STAUT transmits one or more correctly protected and correctly formatted Beacon reports with the Case 2 values in Table 46. Verify that the Dialog Token from the Measurement Report frame matches the Dialog Token of the Measurement Request frame. If multiple Measurement Report frames are received, the Dialog Token in each Measurement Report frame should match the Dialog Token in the Measurement Request frame. When all the above conditions are satisfied, then CONTINUE else FAIL.
Case 3			
8a	Trigger the STAUT to scan for all BSSs/channels in all supported bands (2.4 GHz and/or 5 GHz, as supported). Wait for the STAUT to complete scanning.		
8b		Trigger AP1 to generate a Beacon Request frame using the Case 3 values specified in Table 45.	
9	Wait for 5 seconds for the STAUT to respond to the Beacon Request frame.		SN: Verify that the STAUT transmits one or more correctly protected and correctly formatted Beacon reports with the Case 3 values as specified in Table 46. Verify that the Dialog Token from the Measurement Report frame matches the Dialog Token of the Measurement Request frame. If multiple Measurement Report frames are received, the Dialog Token in

Step	STAUT	Test bed AP1 and AP2	Expected result
			each Measurement Report frame should match the Dialog Token in the Measurement Request frame. When all the above conditions are satisfied, then CONTINUE else FAIL.
Case 4:			
10		Using the Case 4 values specified in Table 45, trigger AP1 to generate a Beacon Request frame. AP2 Beacon frame fixed fields and IEs must be longer than 255 octets. .	
11	Wait for 5 seconds for the STAUT to respond to the Beacon Request frame.		SN: • Wait 5 seconds. • Using the Case 4 values specified in Table 46, verify that the STAUT transmits one or more correctly protected and formatted Beacon reports. • Verify that the Dialog Token from the Measurement Report frame matches the Dialog Token of the Measurement Request frame. If multiple Measurement Report frames are received, the Dialog Token in each Measurement Report frame should match the Dialog Token in the Measurement Request frame. • Verify that the Measurement Report frame(s) include the "Last Beacon Report Indication" subelement and that is set to zero, except for the last frame, when it is set to 1. • Verify that the RSN IE is included in the report and it is not truncated. • Verify that the Measurement Reports include the "Reported Frame Body Fragment ID" subelement and the format of the fields of the subelement are set correctly. When all the above conditions are satisfied, then CONTINUE else FAIL.
Case 5:			
12		Using the Case 5 values specified in Table 45, trigger AP1 to generate a Beacon Request frame.	

Step	STAUT	Test bed AP1 and AP2	Expected result
13	Wait 5 seconds for the STAUT to respond to the Beacon Request frame.		SN: • Verify that the STAUT transmits one or more correctly protected and correctly formatted Beacon reports with the Case 5 values as specified in Table 46. • Verify that the Dialog Token from the Measurement Report frame matches the Dialog Token of the Measurement Request frame. If multiple Measurement Report frames are received, the Dialog Token in each Measurement Report frame should match the Dialog Token in the Measurement Request frame. When all the above conditions are satisfied, then CONTINUE else FAIL.
Case 6:			
14		Trigger AP1 to generate a Beacon Request frame using the Case 6 values specified in Table 45.	
15	Wait for 5 seconds for the STAUT to respond to the Beacon Request frame. Note: This step should be done only if the previous step was executed.		SN: • Verify that the STAUT transmits one or more correctly protected and correctly formatted Beacon reports with the Case 6 values as specified in Table 46. • Verify that the Dialog Token from the Measurement Report frame matches the Dialog Token of the Measurement Request frame. If multiple Measurement Report frames are received, the Dialog Token in each Measurement Report frame should match the Dialog Token in the Measurement Request frame. When all the above conditions are satisfied, then PASS else FAIL.

5.2.4 STAUT GAS ANQP test

5.2.4.1 Interworking element indication in Probe requests and GAS ANQP Request test

Objective

This test verifies that the STAUT transmits correctly formatted Probe Requests including the Interworking element. It also verifies that the STAUT transmits correctly formatted GAS frames and ANQP queries.

Note: a Wi-Fi Agile Multiband STAUT that declares support for ANQP is expected to also support the Neighbor Report ANQP element.

Applicability: Optional. This test shall be executed only if the STAUT declared support for ANQP in Table 1.

References

Section 9.4.2.27, 11.25.3.2 [3]

Test environment

- STAUT
- Test bed AP
- Wireless sniffer

Test configuration

Table 48 defines the specific parameter values required for this test case. The STAUT is not associated with any AP.

Table 48. Interworking element indication in Probe requests and GAS ANQP Request test configuration

Parameter	STAUT value	Test bed AP value
Test bed vendor	N/A	Intel AP
AP Primary Channel	N/A	36 (if 5 GHz capable; else 6)
Channel Width	N/A	any
SSID	N/A	Wi-Fi
Interworking	Enabled, if not already enabled	Enabled

Test procedure and expected results

Table 49 provides the specific test procedure and expected results for this test case.

Table 49. Interworking element indication in Probe requests and GAS ANQP Request test procedure and expected results

Step	STAUT	Test bed AP	Expected result
1	Configure the STAUT as described in Table 48.		
2		The AP starts to transmit Beacon frames.	
3	The STAUT optionally sends a Probe Request frame to the AP.	The AP sends a Probe Response frame to the STAUT if a Probe Request frame was received.	SN: Verify the following if a Probe Request frame is detected. - Interworking element is present (0x6B) and the length is equal to 1, 3, 7 or 9 - Extended Capabilities element is present with bit 31(Interworking) set to 1 When all the above requirements are true, then CONTINUE, else FAIL. If no Probe Request frame is detected for 30 seconds, then CONTINUE.
4	Trigger the STAUT to transmit a GAS ANQP Query for a Neighbor report.		SN: Verify a GAS Initial Request frame is transmitted and properly formatted including: - Address 1 field is set to the MAC address of AP and Address 3 field is set to the wildcard BSSID value - Advertisement Protocol element is present for ANQP - ANQP Request Length field is ≥ 6 - Query Request field contains a Query List ANQP element where: - Info ID field is set to 0x0100 (two-octet 256, Query List InfoID) - Length field is ≥ 2 - ANQP Query ID field contains the value 0x0110 (two-octet 272, Neighbor Report element Info ID) If the GAS Initial Request frame satisfies all requirements above then PASS, else FAIL

5.2.4.2 GAS ANQP Request for Cellular Data Connection Preference test

Objective

This test verifies that the STAUT transmits correctly formatted ANQP queries for a Cellular Data Connection Preference element.

Applicability: Optional. This test shall be executed only if the STAUT declared support for ANQP in Table 1 and is cellular data capable.

References

Section 11.25.3.2 [3]

Test environment

- STAUT
- Test bed AP
- Wireless sniffer

Test configuration

Table 50 defines the specific parameter values required for this test case. The STAUT is not associated with any AP.

Table 50. GAS ANQP Request for Cellular Data Connection Preference test configuration

Parameter	STAUT value	Test bed AP value
Test bed vendor	N/A	Mediatek AP
AP Primary Channel	N/A	36 (if 5 GHz capable; else 6)
Channel Width	N/A	any
SSID	N/A	Wi-Fi

Test procedure and expected results

Table 51 provides the specific test procedure and expected results for this test case.

Table 51. GAS ANQP Request for Cellular Data Connection Preference test procedure and expected results

Step	STAUT	Test bed AP	Expected result
1	Configure the STAUT as described in Table 50 and Table 9.	Configure the AP as described in Table 50 and Table 4.	

Step	STAUT	Test bed AP	Expected result
2		The AP starts to transmit Beacon frames.	

3	Trigger the STAUT to transmit a GAS ANQP Query for Cellular Data Connection Preference.		SN: Verify a GAS Initial Request frame is transmitted and properly formatted including:
			
			• Address 1 field is set to the MAC address of AP and Address 3 field is set to the wildcard BSSID value
			• Advertisement Protocol element is present for ANQP
			• ANQP Request Length field is ≥ 10
			• Query Request field contains an MBO Query List ANQP element where:
			  ▪ Info ID field is set to 56797 (InfoID for Vendor Specific)
			  ▪ Length field ≥ 6
			  ▪ OUI field is set to 0x506F9A (WFA OUI)
			  ▪ OUI Type field is set to 0x12 (MBO ANQP-element ID)
			  ▪ Subtype field is set to 1 (MBO Query List)
			  ▪ Payload contains the single octet with value 0x02 (Subtype for Cellular Data Connection Preference)
			
			If the GAS Initial Request frame satisfies all requirements above then PASS, else FAIL.

5.2.5 STAUT BTM tests

5.2.5.1 BSS Transition Query Request test

Objective

This test verifies that the STAUT correctly sends a BTM Response to an AP's BTM Request frame.

Applicability: Optional. This test shall be executed only if the STAUT declared support for BTM Query in Table 1.

References

Section 3.5.1.2 [2]

Sections 9.6.14.8, 9.6.14.9, 9.4.2.37 [3]

Test environment

- STAUT
- AP1: Test bed AP
- AP2: Test bed AP
- Wireless sniffer

Test configuration

Table 52 defines the specific parameter values required for this test case.

Table 52. BSS Transition Query Request test configuration

Parameter	STAUT value	Test bed AP1 value	Test bed AP2 value
Test bed vendor	N/A	Ruckus AP	Ruckus AP
BSS Transition Management Capability	Enabled	Enabled	Enabled
BSS Transition Candidate List Entries		If Preference values are configurable, then set: AP1 to Preference 254, and AP2 to Preference 255. If Preference values are autoconfigured, then they should to be a combination of 255 and 254.	Contains one BSSID (its own) with Preference set to 255.
Other	Roaming disabled		

Test procedure and expected results

Table 53 provides the specific test procedure and expected results for this test case.

Table 53.   BSS Transition Query Request test procedure and expected results

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
1	**Configure the STAUT as described in Table 9 and Table 52.**	**Configure the AP1 as described in Table 4 and Table 52.**	**Configure AP2 as described in Table 4 and Table 52.**	
2		AP1 starts to transmit Beacon frames.		
3	The STAUT sends an Association Request frame to AP1.			SN: If the STAUT transmits an Association Request with an Extended Capabilities element with bit 19 set (BSS Transition is enabled), then CONTINUE, else FAIL
4		AP1 accepts the Association Request by responding with an Association Response frame.		
5			AP2 transmits Beacon frames.	
6	Trigger the STAUT to transmit a BTM Query Action frame to AP1.			SN: Verify that the STAUT transmits a correctly protected BTM Query Action frame with the following format: • The Category is set to 0x0A (WNM) • The Action field is set to 0x06. (BSS Transition Management Query) • The Dialog Token is set to a non-zero value • The BSS Transition Query Reason is set to a valid Reason Code When all the above conditions are true, then CONTINUE, else FAIL.
7		AP1 responds with a BSS Transition Request frame with the settings listed below. • Dialog Token is set to the value received in the BTM Query • Preferred Candidate List Included bit is set to 1		

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
		• Candidate List contains two entries as specified in Table 52 (AP1 and AP2) • Reason Code attribute has Transition Reason Code set to 0 (unspecified) • Disassociation Imminent bit is set to 0 • BSS Termination Included bit is set to 0 • ESS Disassociation Imminent bit is set to 0		
8	Wait 5 seconds to allow the STAUT to optionally send a BSS Transition Management Response.			SN: If the STAUT transmits a BTM Response frame, verify it is correctly protected with the following format: • Category is set to 0x0A (WNM) • WNM Action is set to 8 (BTM Response) • Dialog Token identical to Dialog Token from BSS Transition Request • BTM Status Code has a valid value When all the above conditions are true, then PASS, else FAIL. If the STAUT does not send a BTM Response for 5 seconds, then PASS.

5.2.5.2 STA Response to AP BSS Transition Management Request frame with Disassociation Imminent bit set to one test

Objective

This test verifies that the STAUT correctly responds to an unsolicited BSS Transition management request by roaming using reassociation. This test requires BSS Transition Candidate List Entries containing two or more Neighbor Report elements (including its own BSS) to be configured in the AP.

Applicability: Mandatory

References

Section 3.5.2 [2]

Sections 9.6.14.8, 9.6.14.9, 9.6.14.10, 9.4.2.37 [3]

Test environment

- Testing to be performed in a RF isolated chamber
- STAUT
- AP1, AP2: Test bed dual band AP (not cellular data aware)
- Wireless sniffer
- PC Endpoint reachable from both APs

Test configuration

Table 54 defines the specific parameter values required for this test case.

Table 54. STA Response to AP BSS Transition Management Request frame with Disassociation Imminent bit set to one test configuration

Parameter	STAUT value	Test bed AP1 value	Test bed AP2 value
Test bed vendor	N/A	Qualcomm AP	Qualcomm AP
SSIDs		Wi-Fi	Wi-Fi
BSS Transition Management Capability	Enabled	Enabled	
Transition candidate lists		Configure in AP1 the BSS transition Candidate List Entries containing AP2 (with non-zero preference) in the Neighbor Report elements	Configure in AP2 the BSS transition Candidate List Entries containing AP1 (with non-zero preference) in the Neighbor Report elements
Beacon Interval		100 ms	100 ms
AP primary channel		1 (when STAUT is 2.4 GHz capable only), 36 (when STAUT is 5 GHz capable only),	11 (when STAUT is 2.4 GHz capable only), 44 (when STAUT is 5 GHz capable only),

Parameter	STAUT value	Test bed AP1 value	Test bed AP2 value
		36 (when STAUT is both 2.4 GHz and 5 GHz capable	6 (when STAUT is both 2.4 GHz and 5 GHz capable
Other	Client initiated roaming disabled		

Test procedure and expected results

Table 55 provides the specific test procedure and expected results for this test case. Figure 2 illustrates the timing for this test case.

Figure 2. STA Response to AP BSS Transition Management Request frame timing

Table 55. STA Response to AP BSS Transition Management Request frame with Disassociation Imminent bit set to one test procedure and expected results
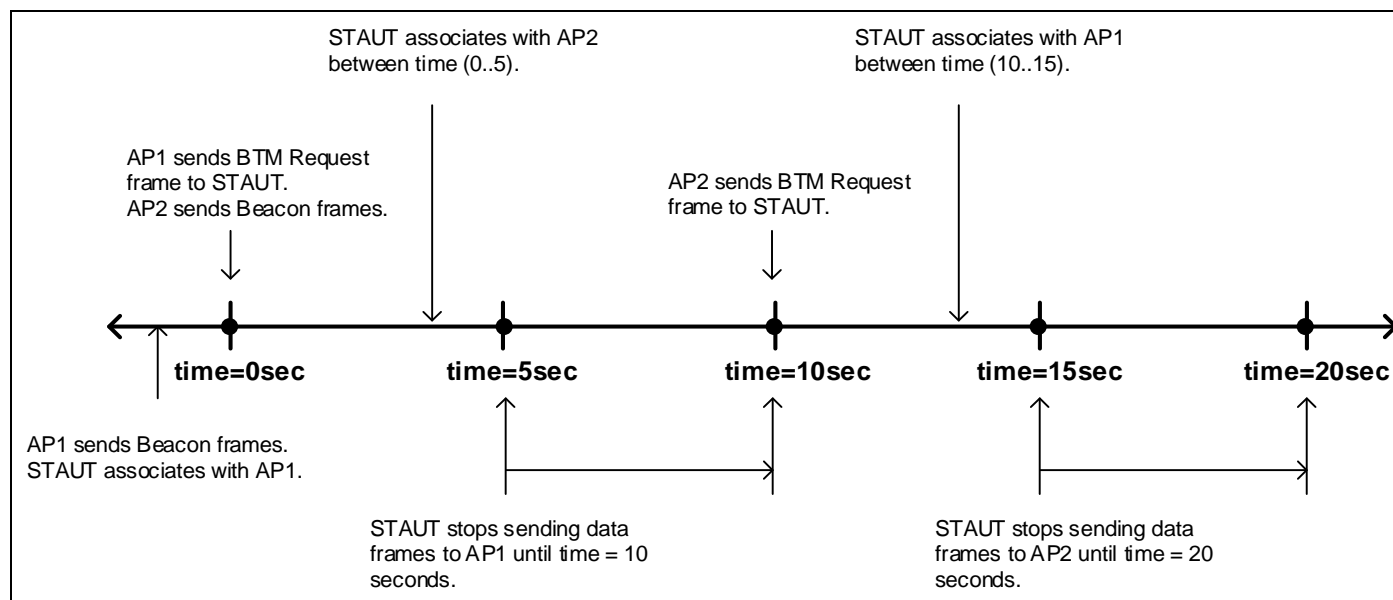
Step	STAUT	Test bed AP1	Test bed AP2	Expected result
1	Configure the STAUT as described in Table 9 and Table 54.	Configure AP1 as described in Table 4 and Table 54.		
2		AP1 starts to send Beacon frames.		
3	Trigger the STAUT to associate with AP1.			SN: If the STAUT transmits an Association Request with an Extended Capabilities element with bit 19 (BSS Transition is enabled) set to one, then CONTINUE, else FAIL.
4		AP1 accepts the association.		
5			Configure AP2 as described in Table 4 and Table 54.	
6	The STAUT start to ping traffic from the PC endpoint, every 200 ms for 40 seconds.			
7		Trigger AP1 to transmit a BTM Request frame to the STAUT with the following settings. • Disassociation Imminent field set to 1 • Disassociation Timer field set to 50 • Re-Association Delay field value indicating 10 seconds (set time = 0 seconds)	AP2 starts to send Beacon frames Note: Ideally, the first Beacon of AP2 should be sent out at the same time as the BTM Request from AP1.	
8				SN: If a BTM Response is generated by the STAUT, verify that it is correctly protected and includes: • Status Code indicating accept 0x0 • If Target BSSID field is present, it is set to the BSSID of AP2 When all the above conditions are true, then CONTINUE else FAIL.

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
9	Note: The STAUT should associate with AP2 within time = (0…5) seconds.			Wait 5 seconds (until time=5 seconds). SN: Verify that the STAUT transmits an Authentication frame, and subsequently a Reassociation Request. In both frames, the DA should be set to the BSSID of AP2 within 5 seconds of the BTM Request frame generation Note: An Association Request frame is not an alternative to a Reassociation Request frame. SN: Within time=0…5 seconds, while subsequent steps are ongoing, verify that no (re)association requests. SN: Within time = 5…10 seconds, verify that no data frames are sent from the STAUT to AP1's BSSID. When all the above conditions are true, then CONTINUE else FAIL.
10		Wait until 5 seconds have expired since the BTM Request frame generation.		
11			Wait until time time=10 seconds. Trigger AP2 to transmit a BTM Request frame to the STAUT with the following settings. • Disassociation Imminent field set to 1 • Disassociation Timer field set to 50 (5 seconds) • Re-Association Delay field value set to 10 seconds	
12				SN: If a BTM Response is generated by the STAUT that it is correctly protected and includes a Status Code indicating accept 0x0, then CONTINUE else FAIL.
13			Wait until 5 seconds have expired since the (2nd) BTM Request frame generation.	
14				SN: Wait until 5 seconds have expired since the BTM Request frame generation.

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
				SN: Verify that the STAUT sends an Authentication frame, and subsequently a Reassociation Request. In both frames, the DA should be set to the BSSID of AP1 within 5 seconds of the 2nd BTM Request frame generation (within time=10…15s).
				SN: While subsequent steps are ongoing, verify that no association request or data frames are sent from the STAUT to AP2's BSSID for the following 5 seconds (within time=15…20s). Note: An Association Request frame is not an alternative to a Reassociation Request frame.
				When all the above conditions are true, then CONTINUE else FAIL.
15		Wait until time=16 seconds. Trigger AP1 to transmit a Disassociation frame to the STAUT with any valid Reason Code.		SN: Verify that a (Re)Association Request frame is not sent to AP2 during time=15-20 seconds. When all the above conditions are true, then PASS else FAIL.

5.2.5.3   STA Response to AP BSS Transition Management Request Frame with BSS Termination Included bit set to one test

Objective

This test verifies that the STAUT correctly reacts to an unsolicited BSS Transition Management Request with the BSS Termination Included bit set to one. This test requires BSS Transition Candidate List Entries containing one or more Neighbor Report elements to be configured in the AP (in addition to the AP's own BSS).

Applicability: Mandatory

References

Section 3.5.2 [2]

Sections 9.6.14.8, 9.6.14.9, 9.6.14.10, 9.4.2.37 [3]

Test environment

- Testing to be performed in a RF isolated chamber
- STAUT
- AP1, AP2: Test bed dual band AP (not cellular data aware)
- Wireless Sniffer
- PC Endpoint reachable from both APs

Test configuration

Table 56 defines the specific parameter values required for this test case.

Table 56. STA Response to AP BSS Transition Management Request Frame with BSS Termination Included bit set to one test configuration

Parameter	STAUT value	Test bed AP1 value	Test bed AP2 value
Test bed vendor	N/A	Mediatek AP	Intel AP
SSIDs		Wi-Fi	Wi-Fi
BSS Transition Management Capability	Enabled	Enabled	
Transition candidate lists		Configure in AP1 the BSS transition Candidate List Entries containing AP2 (with non-zero preference) in the Neighbor Report elements	
Beacon Interval		100 ms	100 ms
AP primary channel		1 (when STAUT is 2.4 GHz capable only),	11 (when STAUT is 2.4 GHz capable only),

Parameter	STAUT value	Test bed AP1 value	Test bed AP2 value
		36 (when STAUT is 5 GHz capable only),	44 (when STAUT is 5 GHz capable only),
		36 (when STAUT is both 2.4 GHz and 5 GHz capable	6 (when STAUT is both 2.4 GHz and 5 GHz capable
Other	Roaming disabled		

Test procedure and expected results

Table 57 provides the specific test procedure and expected results for this test case.

Table 57. STA Response to AP BSS Transition Management Request Frame with BSS Termination Included bit set to one test procedure and expected results

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
1	Configure the STAUT as described in Table 9 and Table 56.	Configure AP1 as described in Table 4 and Table 56.		
2		AP1 starts to send Beacon frames.		
3	Trigger the STAUT to associate with AP1.			SN: If the STAUT transmits an Association Request with an Extended Capabilities element with bit 19 (BSS Transition is enabled) set to 1, then CONTINUE, else FAIL.
4		AP1 accepts the association.		
5			Configure AP2 as described in Table 4 and Table 56	
7		Trigger AP1 to transmit a BTM Request frame to STAUT with the BSS Termination Included bit set to 1 and the BSS Termination TSF field in the BSS Termination Duration subelement set to 5 seconds.		
8				SN: If a BTM Response is generated by the STAUT, verify that it is correctly protected and is formatted with: • Status Code indicating accept 0x0 • If Target BSSID field is present, it is set to the BSSID of AP2

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
				When all the above conditions are true, then CONTINUE else FAIL.
9				Wait until the time indicated in the BSS Termination TSF expires.
				SN:
				If the STAUT sends a (Re)Association Request to AP2 before the BSS Termination TSF timer value expires, then PASS else FAIL.

5.2.6   STAUT Fast BSS Transition test

Objective

This test verifies that the STAUT performs Fast BSS Transition using Over-the-Air FT protocol when the STA moves between two APs in the same mobility domain. To verify correct STAUT operation when the AP supports both FT and non-FT authentication, the test bed APs advertise both corresponding AKMs.

If the STAUT supports both Fast BSS Transition with PSK and Fast BSS Transition with 802.1X, then the test is run twice (once for each mode), and the STAUT shall pass both tests. If the STAUT supports only one of the two modes, only that mode is tested.

NOTE: If the STAUT also supports other authentication algorithms (such as FILS SK) then it shall be configured to use the corresponding Fast BSS Transition mode for this test case.

Applicability: Optional. This test shall be executed only if the STAUT declared support for FT with WPA2-Personal and/or WPA2-Enterprise (802.1X) in Table 1.

References

Section 3.7 [2]

Section 12 [3]

Test environment

- STAUT
- AP1: Test bed Wi-Fi CERTIFIED dual-band n/ac AP, capable of FT
- AP2: Test bed Wi-Fi CERTIFIED dual-band n/ac AP, capable of FT, and is part of the same mobility domain as AP1
- AAA Server (required for FT with 802.1X test): Test bed AAA server
- Network Ping Endpoint: A test bed laptop that is on the same IP subnet as STAUT, AP1and AP2 and reachable from both APs
- Wireless sniffer

Test configuration

Table 58 defines the specific parameter values required for this test case.

Table 58.   STAUT Fast BSS Transition test configuration

Parameter	Test bed AP1 value	Test bed AP2 value	STAUT value
Test bed vendor	Ruckus AP (WPA2-Personal) Qualcomm AP (WPA2-Enterprise)	Ruckus AP (WPA2-Personal) Qualcomm AP (WPA2-Enterprise)	N/A
AP Primary Channel	36 (if 5 GHz capable; else 6)	48 (if 5 GHz capable; else 1)	36 (if 5 GHz capable; else 6)

Parameter	Test bed AP1 value	Test bed AP2 value	STAUT value
Channel Width	20 MHz	20 MHz	20 MHz
SSID1	WiFi1	WiFi1	
Security	For FT with PSK test: WPA2, For FT with 802.1X test: EAP-TTLS/MSCHAPv2 Note: If STAUT does not support EAP-TTLS, execute the test using EAP-TLS	For FT with PSK test: WPA2, For FT with 802.1X test: EAP-TTLS/MSCHAPv2 Note: If STAUT does not support EAP-TTLS, execute the test using EAP-TLS	For FT with PSK test: WPA2, For FT with 802.1X test: EAP-TTLS/MSCHAPv2 Note: If STAUT does not support EAP-TTLS, execute the test using EAP-TLS
Security Encryption key/credentials	For FT with PSK test: MBORocks, For FT with 802.1X test: username="ttls-user", password="password"	For FT with PSK test: MBORocks, For FT with 802.1X test: username="ttls-user", password="password"	For FT with PSK test: MBORocks, For FT with 802.1X test: username="ttls-user", password="password"
Mobility Domain ID (MDID)	0x0101	0x0101	N/A
FT	FT Enabled (Over-The-Air FT Protocol), For FT with PSK case: Configured to advertise support for both of the following AKM Suites: 00-0F-AC:4 (FT authentication over PSK) and 00-0F-AC:2 (PSK), For FT with 802.1X test: Configured to advertise support for both of the following AKM Suites: 00-0F-AC:3 (FT authentication negotiated over IEEE Std 802.1X) and 00-0F-AC:1 (Authentication negotiated over IEEE Std 802.1X)	FT Enabled (Over-The-Air FT Protocol), For FT with PSK case: Configured to advertise support for both of the following AKM Suites: 00-0F-AC:4 (FT authentication over PSK) and 00-0F-AC:2 (PSK), For FT with 802.1X test: Configured to advertise support for both of the following AKM Suites: 00-0F AC:3 (FT authentication negotiated over IEEE Std 802.1X) and 00-0F-AC:1 (Authentication negotiated over IEEE Std 802.1X)	FT Enabled (Over-The-Air FT Protocol), For FT with PSK test: Configured to use FT with PSK, For FT with 802.1X test: Configured to use FT with 802.1X
RSNA	Supported	Supported	Supported
BTM Configuration	Neighbor list configured to only include AP2's BSSID at preference value 255 and its own BSSID at preference value 0		
Other	Roaming disabled		

Test procedure and expected results

Table 59 provides the specific test procedure and expected results for this test case.

Table 59. STAUT Fast BSS Transition test procedure and expected results

Step	Test bed AP1	Test bed AP2	STAUT	Expected result
1	Configure AP1 and AP2 as defined in Table 58, according to the test mode being used (PSK or 802.1X). Configure the AP1 and AP2 to the same mobility domain.		Configure the STAUT as defined in Table 58.	
2	Turn on AP1. AP1 starts to transmit Beacon frames.			SN: Verify that the following conditions are true: • AP1 Beacon frames contain RSNE with AKM Suite Count set to 2 or more • AKM Suite List field includes at least the 2 AKMs specified in Table 58 for the corresponding test mode. If the above conditions are not true, fix the test bed configuration and start test again.
3			Trigger the STAUT to associate to AP1 to the WiFi1 SSID	SN: Verify that the STAUT sends a correctly formatted Association Request frame, containing • RM Capabilities IE indicating support for active mode Beacon report and passive mode Beacon report • MDE with the MDID used in the test • RSNE where AKM Suite Count field is set to 1 • AKM Suite List field is set to the following: ▪ - for FT with PSK test: 00-0F-AC:04 ▪ - for FT with 802.1X test: 00-0F-AC:03 When all the above conditions are true, then CONTINUE else FAIL.
4	AP1 responds with an Association Response containing FTE and MDE.			
5	Wait 2 seconds for a FT 4-way handshake to occur.			SN: Verify that the following conditions are true: • A successful FT 4-way handshake is performed • In the EAPOL message 2 of the handshake, the STAUT includes the following: ▪ RSNE where PKMID field is set to PMKR1Name ▪ AKM Suite Count field is set to 1 ▪ AKM Suite List field is set to 00-0F-AC:04 for FT with PSK test, or 00-0F-AC:3 for FT with 802.1X test: ▪ FTE and MDE are present and are the same as those present in AP1's Association Response frame

Step	Test bed AP1	Test bed AP2	STAUT	Expected result
				When all the above conditions are true, then CONTINUE else FAIL.
6			Start a continuous ping from the STAUT to the Network Ping Endpoint. Wait 10 seconds. Ensure that ping packets are sent via AP1 and that the ping is successful.	
7		Turn on AP2. AP2 starts to transmit Beacon frames. Wait 10 seconds.		SN: Verify that the following conditions are true: • AP2 Beacon frames contain RSNE with AKM Suite Count set to 2 or more • AKM Suite List field includes at least the 2 AKMs specified in Table 58 for the corresponding test mode. If the above conditions are not true, fix the test bed configuration and start test again.
8	Trigger AP1 to transmit a BTM Request frame to the STAUT with the following settings. • Disassociation Imminent field set to 1 • Disassociation Timer field set to 50 • Re-Association Delay field value set to 10 seconds			
9			The STAUT sends an Authentication Request frame to AP2.	SN: Verify that the STAUT transmits a correctly formatted Authentication Request frame to AP2, containing • - FTAA as the Authentication Algorithm • - FTE with SNonce and R0KH-ID • - MDE • RSNE where PMKID field is set to PMKR0Name, AKM Suite Count field is set to 1, and AKM Suite List field is set to the following: ▪ for FT with PSK test: 00-0F-AC:04 ▪ for FT with 802.1X test: 00-0F-AC:03 When all the above conditions are true, then CONTINUE else FAIL.

Step	Test bed AP1	Test bed AP2	STAUT	Expected result
10		AP2 responds with an Authentication Response frame.		

11			STAUT sends a Reassociation Request frame to AP2.	SN: Verify that the STAUT sends a correctly formatted Reassociation Request frame, containing
				• FTE, MDE and RSNE where AKM Suite Count field is set to 1
				• AKM Suite List field is set to the following:
				  ▪ FT with PSK test: 00-0F-AC:04
				  ▪ FT with 802.1X test: 00-0F-AC:03
				SN: Verify that the time between the Authentication Request and Reassociation Request from the STAUT does not exceed the Reassociation Deadline Time.
				When all the above conditions are true, then CONTINUE else FAIL.

12		AP2 transmits a Reassociation Response frame to the STAUT, containing FTE, MDE and RSNE.		
13			Wait 10 seconds.	SN: Verify the following conditions: • A 4-way handshake is not performed between the STAUT and AP2 • Correctly protected ping packets are sent via AP2 • The ping is successful When all the above conditions are true, then PASS else FAIL.

5.2.7   STAUT Association Disallowed Capability test

Objective

This test verifies that the STAUT does not attempt to associate with an AP after receiving an MBO-OCE IE carrying an Association Disallowed attribute in the Beacon, Probe Response and Association Response frames from that AP.

Applicability: Mandatory

References

Sections 3.6, 4.2.4 [2]

Sections 9.3.3.2, 9.3.3.6, 9.3.3.8 [3]

Test environment

- STAUT
- AP1: Test bed AP
- AP2: Test bed AP
- Wireless sniffer

Test configuration

Table 60 defines the specific parameter values required for this test case.

Table 60.   STAUT Association Disallowed Capability test configuration

Parameter	STAUT value	Test bed AP1 value	Test bed AP2 value
Test bed vendor	N/A	Ruckus AP	Ruckus AP

Test procedure and expected results

Table 61 provides the specific test procedure and expected results for this test case.

Table 61.   STAUT Association Disallowed Capability test procedure and expected results

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
1		Configure AP1 as described in Table 4 and Table 60.	Configure AP2 as described in Table 4 and Table 60.	

Step	STAUT	Test bed AP1	Test bed AP2	Expected result
2		Configure AP1 to disallow associations.	Configure AP2 to allow associations.	
3		AP1 starts to transmit Beacon frames.	AP2 starts to transmit Beacon frames.	
4	Configure the STAUT as described in Table 9 and in Table 60.			
5	Trigger the STAUT to scan in the APs' Primary Channel and associate to SSID "Wi-Fi".			SN: Verify the following conditions are true: • STAUT does not send an Association Request frame to AP1 • STAUT sends an Association Request frame to AP2 When all conditions are true, then CONTINUE, else FAIL.
6			AP2 accepts the association.	
7		Trigger AP1 to allow associations.	Trigger AP2 to disallow associations.	
8	Trigger the STAUT to disassociate from AP2.			
9	Trigger the STAUT to scan and associate to associate to SSID "Wi-Fi".			SN: Verify the following conditions are true: • STAUT does not send an Association Request frame to AP2 • STAUT sends an Association Request frame to AP1 When all conditions are true, then PASS, else FAIL.

5.2.8   STAUT Channel and Band Indication and Preference test

Objective

This test verifies that the STAUT transmits a correctly formatted Supported Operating Classes element and non-preferred Channels attributes in an Association Request and transmits correctly formatted WNM Notification frames to update its non-preferred channels.

Applicability: Mandatory

References

Section 3.2 [2]

Section 11.24.7.4 [3]

Test environment

- Test bed dual-band 2.4 GHz and 5 GHz capable AP
- STAUT
- Wireless sniffer

Test configuration

This test uses the configuration specified in Table 9.

Table 62.   STAUT Channel and Band Indication and Preference test configuration

Parameter	STAUT value	Test bed AP value
Test bed vendor	N/A	Intel AP

Test procedure and expected results

Table 63 provides the specific test procedure and expected results for this test case.

Table 63. STAUT Channel and Band Indication and Preference test procedure and expected results

Step	STAUT	Test bed AP	Expected result
1	Configure the STAUT as described in Table 9. Additionally, configure the STAUT to have non-preferred channels below: • Channel 48 at Preference 0 and Channel 44 at Preference 1 if the STA is 5 GHz capable • Channel 1 at Preference 0 and channel 11 at Preference 1 if the STA is not 5 GHz capable	Configure the AP as described in Table 4.	
2		The AP starts to transmit Beacon frames.	

3	Allow the STAUT to associate to the AP to the WiFi1 SSID.		SN: Verify that the STAUT transmits a correctly formatted Association Request frame containing the following:
			Supported Operating Classes element containing:
			1. Element ID set to 59
			2. Length correctly set to the length of the element
			3. Operating Classes field terminated by 0x82 (OneHundredAndThirty delimiter), 0x00 (Zero delimiter) or end of element, and containing at least of the following bytes (as applicable):
			   a. 0x51 (if STA is 2.4 GHz capable)
			   b. 0x73 (is STA is 5 GHz capable)
			MBO-OCE IE containing:
			1. Element ID set to 0xDD
			2. Length set to 19 or higher
			3. OUI set to 0x506F9A
			4. OUI Type set to 0x16
			5. A Non-preferred Channel Report attribute containing
			   a. Attribute ID set to 0x02
			   b. Length set to 4
			   c. Operating Class set to one of the below
			   d. 0x73 (Global operating class) if STA is 5 GHz capable
			   e. 0x51 (Global operating class) if STA is not 5 GHz capable
			   f. Channel List set to either 0x30 or 0x01
			   g. Preference set to 0x00
			   h. Reason Code set to 0x00
			6. Another Non-preferred Channel Report attribute containing
			   a. Attribute ID set to 0x02

Step	STAUT	Test bed AP	Expected result
			b. Length set to 4
			c. Operating Class set to one of the below
			0x73 (Global operating class) if STA is 5 GHz capable
			0x51 (Global operating class) if STA is not 5 GHz capable
			d. Channel List set to either 0x2C or 0x0B
			e. Preference set to 0x01
			f. Reason Code set to 0x00
			When all the above conditions are true, then CONTINUE else FAIL.
4	Delete the non-preferred channel configuration from the STAUT. Configure the STAUT to have non-preferred channels as • Channel 40 at Preference 1 and channel 44 at Preference 1 if the STA is 5 GHz capable • Channel 3 at Preference 1 and channel 11 at Preference 1 if the STA is not 5 GHz capable		
5	If the STAUT does not autonomously transmit a WNM Notification frame, trigger the STAUT to send a WNM Notification frame.		SN: Verify that the STAUT transmits a correctly protected and correctly formatted WNM Notification frame containing either one or two non-preferred Channel Report subelements, each containing • Subelement ID set to 0xDD • Length set to 9 (if one sub-element) or 8 (if two-subelements) • OUI set to 0x506F9A • OUI Type set to 0x02 • If one Non-preferred Channel Report subelement, with values as specified in Table 64 or, if two Non-preferred Channel Report subelements, with values as specified in Table 65 When all the above conditions are true, then CONTINUE else FAIL.
6	Configure the STAUT to have no non-preferred channels.		
7	If the STAUT does not autonomously transmit a WNM Notification frame, trigger the STAUT to send a WNM Notification frame.		SN: Verify that the STAUT transmits a correctly protected and correctly formatted WNM Notification frame containing one Non-preferred Channel Report subelement containing • Element ID set to 0xDD • Length set to 4

Step	STAUT	Test bed AP	Expected result
			• OUI set to 0x506F9A • OUI Type set to 0x02 When all the above conditions are true, then PASS else FAIL.

Table 64.   Field values when STAUT sends only one Non-preferred Channel Report subelement for step 5 in Table 63

Field	Value
Operating Class	0x73 (Global operating class) if STA is 5 GHz capable 0x51 (Global operating class) if STA is not 5 GHz capable
Channel List	Two bytes either containing 0x28 and 0x2C, or containing 0x03 and 0x0B
Preference	0x01
Reason Code	0x00
Reason Detail	Not verified

Table 65.   Field values when STAUT sends two Non-preferred Channel Report subelement for step 5 in Table 63

Field	Value
Operating Class	0x73 (Global operating class) if STA is 5 GHz capable 0x51 (Global operating class) if STA is not 5 GHz capable
Channel List	One subelement with channel list set to 0x28 or 0x03 Other subelement with channel list set to 0x2C or 0x0B
Preference	0x01
Reason Code	0x00
Reason Detail	Not verified

5.2.9　STAUT Multimode Indication test

Objective

This test verifies that a Wi-Fi Agile Multiband multimode STA transmits a correctly formatted MBO-OCE IE carrying a Cellular Data Capabilities attribute in Probe, Association Request and WNM-Notification Request frames.

Applicability: Conditionally mandatory. This test case is required if the STAUT is a Wi-Fi Agile Multiband multimode STA.

References

Sections 3.3, 4.2.3 [2]

Sections 9.3.3.6, 9.3.3.8, 9.3.3.10 [3]

Test environment

- STAUT: A Wi-Fi Agile Multiband multimode STA
- Test bed Wi-Fi Agile Multiband AP
- Wireless sniffer

Test configuration

Table 66 defines the specific parameter values required for this test case.

Table 66.　STAUT Multimode Indication test configuration

Parameter	STAUT Value	Test bed AP Value
Test bed vendor	N/A	Mediatek AP

Test procedure and expected results

Table 67 provides the specific test procedure and expected results for this test case.

Table 67.　STAUT Multimode Indication test procedure and expected results

Step	STAUT	Test bed AP	Expected result
1	Configure the STAUT as described in Table 9 and Table 66.	Configure the AP as described in Table 4 and Table 66.	
2	Trigger the STAUT to enable a cellular data connection.		

Step	STAUT	Test bed AP	Expected result
3	Trigger the STAUT to scan and associate to the AP.		SN: If the STAUT sends a Probe Request frame, verify that the STAUT transmits a Probe Request frame with an MBO-OCE IE carrying a Cellular Data Capabilities attribute, with the following format: • Element ID is set to 0xDD • Length is set to ≥ 7 • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x03 • Attribute Length is set to 1 • Cellular Data Connectivity field is set to 0x01 When all the above conditions are satisfied then CONTINUE, else FAIL. SN: Verify that the STAUT transmits an Association Request frame with an MBO-OCE IE carrying a Cellular Data Capabilities attribute, with the following format: • Element ID is set to 0xDD • Length is set to ≥ 7 • OUI is set to 0x506F9A • OUI Type is set to 0x16 • Attribute ID is set to 0x03 • Attribute Length is set to 1 • Cellular Data Connectivity field is set to 0x01 If all the conditions above are true then CONTINUE, else FAIL.
4	Trigger the STAUT to disable the cellular data connection.		
5	The STAUT transmits a WNM-Notification Request frame to notify the AP of its change of cellular data connectivity status.		SN: Verify that the STAUT transmits a correctly protected WNM-Notification Request frame with an MBO-OCE IE carrying a Cellular Data Capabilities subelement, with the following format: • Subelement ID is set to 0xDD • Length value is set to 5 • OUI is set to 0x506F9A • OUI Type is set to 0x03 • Cellular Data Connectivity field is set to 0x02 If all the conditions above are true then CONTINUE, else FAIL.
6	Trigger the STAUT to enable a cellular data connection.		SN: If a WNM-Notification Request frame is sent by the STAUT, verify that the STAUT transmits a correctly protected WNM-Notification Request frame with an

Step	STAUT	Test bed AP	Expected result
	Note: The STAUT may send a WNM-Notification Request frame at this time.		MBO-OCE IE carrying a Cellular Data Capabilities Subelement, with the following format: • Subelement ID is set to 0xDD • Length is set to 5 • OUI is set to 0x506F9A • OUI Type is set to 0x03 • Cellular Data Connectivity field is set to 0x01 If all the conditions above are true, then PASS else FAIL.

Appendix A Test bed products

A.1 Approved test bed vendors

All test bed equipment is available exclusively from:

> Tessco Technologies
>
> 11126 McCormick Road
>
> Hunt Valley, Maryland 21031

Amber Buscemi buscemia@tessco.com

Melvin Simmons 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 that may be able to direct technical questions to the correct resource.

The current list of all approved test bed equipment for all Wi-Fi Alliance test beds may be accessed at the following ftp site: https://www.wi-fi.org/members/certification-testing/test-bed-information.

Visit https://www.wi-fi.org/members/certifications-testing/testing-information to obtain a username and password for the FTP site listed above.

A.2 Approved test bed equipment

This section provides the approved test bed equipment for all DUT listed in this test plan.

Table 68. Approved test bed Access Points

Vendor	Product	Software version(s)	Contact
Intel	GRX550	05.03.00.56_MBO_20170712T1210	arnon.meydav@intel.com gur.sannikov@intel.com
Mediatek	MT7615	4.4.1.0-mbo1.15	haipin.liang@mediatek.com kyle.lee@mediatek.com yiwei.chung@mediatek.com ci.wang@mediatek.com
Qualcomm	IPQ8065	IPQ8064.ILQ.5.0.r2-000000013-P-1	wfa.external.support@qti.qualcomm.com
Ruckus	R710	9.13	Bowen.Zhang@brocade.com

Table 69. Approved test bed Stations

Vendor	Product	Software version(s)	Contact
Broadcom	BCM94361	MBOTB_REL_1_6.1/1.2.15-r-842587:01-807748bf	wfa-support-list@broadcom.com
Intel	8265	31.518275.0	wfa.external.support@intel.com
Marvell	EC8997P	PCIE8997-7.31.17.p1-C3X16C247-MBO-0731-GPL-(FP68)	wifilab-support@marvell.com
Qualcomm	STA	drv=/wpas=v2.7-devel-7.0/hapd=v2.7-devel-7.0/sigma=android-7.0-msm8996-WFA-MBO-1.1	wfa.external.support@qti.qualcomm.com

Table 70. Approved servers

Vendor	Product	Software version(s)	Contact
N/A	HostAPD	N/A	support@wi-fi.org

Table 71. Approved test tools

Vendor	Product	Software version(s)	Contact
Qualcomm	Sniffer/ CA-65-Y9345-LCT (OpenWrt Chaos Calmer, r48067)	Linux OpenWrt 3.14.77	wfa.external.support@qti.qualcomm.com

Appendix B   Document revision history

Table 72.   Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2017-08-25	Initial public release.
1.1	2019-10-02	Beacon Report Enhancement ECN release. Tests to validate Beacon Reporting were added. The ASUS sniffer hardware was replaced with the Qualcomm AP sniffer. The Qualcomm AP, MediaTek AP, Broadcom STA, and Intel STA, firmware versions have been updated.