

Wi-Fi WPS Test Plan

Wi-Fi Alliance

Version 1.6



Copyright 2007 Wi-Fi Alliance. All Rights Reserved.

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

The Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. This document and any related materials may only be used by Wi-Fi Alliance members for their internal use, such as quality assurance and pre-certification activities, and for their participation in approved Wi-Fi Alliance activities, such as the Wi-Fi Alliance certification program, unless otherwise permitted by the Wi-Fi Alliance through prior written consent. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described above, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from the Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. The Wi-Fi Alliance regards the unauthorized use, duplication or distribution of this document by a member as a material breach of the member's obligations under the organization's rules and regulations, which may result in the suspension or termination of Wi-Fi Alliance membership. Unauthorized use, duplication, or distribution by nonmembers is an infringement of the Wi-Fi Alliance's copyright. Distribution of this document to persons or organizations who are not members of the Wi-Fi Alliance is strictly prohibited.

Change History

Version	Date dd/mm/yy	Remarks
0.1.0	04/12/2006	Initial Release
0.2.0	05/15/2006	Adding test cases collected from UFD, NFC, Legacy Interop and Registrar Tiger teams
0.2.1	05/22/2006	Update upon feedbacks collected in the Task Group Meeting on May 22, 2006
0.2.2	06/18/2006	Update upon feedback from James Yee (Marvell)
0.3.0	07/20/2006	Add in new test cases developed in the Face-to-Face meetings by Tiger Teams
0.4.0	08/18/2006	Update NFC test cases and add narrative to test cases
0.4.1	08/28/2006	Mark test cases not being executed at PF4
0.4.2	08/28/2006	Update the test case 4.1.1 to cover more device capabilities; Update the test case 4.1.7 to add Device Password ID check; Rephrase the unconfigured requirement for AP in the section 4; Change the test case 4.1.2 and 4.1.19 to test AP's function related to UPnP external Registrar through wireless
0.4.3	08/28/2006	Updated 4.2.20 to simplify test to critical components. Deleted redundant check from 4.1.3
0.4.4	8/29/06	Deleted tests agreed redundant at 8/29 TG meeting Change references to EAP based and UPnP external registrars to WLAN and wired external registrars Update some continued references that equated OOB to unconfigured Add wrong PIN (bad checksum and good checksum) to APUT in 4.2.1 Add wrong PIN (bad checksum and good checksum) to STAUT in 5.2.4 Simplified 5.1.1 and 5.1.2 and added the tests for multiple network credentials and identification of dualband AP in PBC active state Bunch of editorial Updated TOC (some errors in auto TOC)
0.4.5	8/30/06	Actually deleted test cases marked for deletion

0.4.6	9/3/06	Minor changes of description in the section 1 and 3 Correct a typo in test 5.1.1
0.4.7	9/5/06	Update the PIN value test case 4.2.1 and 5.2.1 Add test case 4.1.6 to verify that APUT sends its previous wireless configuration settings in the M7 message. Update the general test setup diagram and update the STA and AP reference in all the test cases
0.4.8	9/11/2006	Reviewed test plan with WFA Staff and documented their input. Purpose is to clarify test cases and correct some errors. Deleted test case 4.1.6 as test case was unclear, requirement for APUT was not clear and test was not part of final PlugFest.
0.4.9	10/3/06	Cleaned up version of testplan for test bed qualification {Jeff Mabert}
0.5.0	12/1/06	Added equipment assignments {Giao Pham}
0.5.1	12/14/06 12/20/06 1/4/07	Add in band and channel assignments. Remove Conexant AP. Add Appendix A, list of test bed equipment. Remove Broadcom AP and replace with Conexant AP. Add back the Broadcom AP and Conexant AP.
1.0	1/8/07	Release of initial version for program start.
1.1	1/8/07 1/9/07 1/10/07 1/11/07 1/19/07 1/25/07	Put in equipment information in appendix A. Changed Step 22 in 4.1.1 to clarify SSID. Replace Buffalo AP FW version 1.15 with version 1.17 Change Jumpstart version 2 to 2.0.0.275 Change Buffalo AP SW from 1.17 to version 1.18. Fixed Typos in 5.2.1, 5.3.1, and 5.3.2. Added WFA copyright statement Update Marvell AP SW version
1.2	2/28/07	Changed wording on STAUT to indicate in appropriate situations that a PIN registration process should be started.

1.3	3/28/07 5/18/07	Add in NFC tests Check that test bed vendor contacts and SW are correct.
1.4	7/9/07	Due to VISTA bug, VISTA does not properly support WPA2-personal as it uses TKIP instead of AES (CCMP) so all instances of VISTA as ER have been changed to WPA-personal.
1.5	9/6/07	Update all NFC tests to use DUT's token
1.6	11/8/07	Add product information for NFC equipment. Update Table of Contents

Table of Contents

1	Overview	8
1.1	Definitions.....	8
1.2	Definition of Devices under test (DUT)	9
1.2.1	Access Points (APUT)	9
1.2.2	Station (STAUT).....	9
1.3	Applicability of Tests.....	9
2	Implementation Requirements for Wi-Fi Alliance Certification	10
2.1	Compliance Standard.....	10
3	Test Tool	11
3.1	General Test Setup.....	11
3.2	Default Parameters.....	12
4	AP Tests	13
4.1	Configure APUT.....	13
4.1.1	Check APUT's WPS Protocol frame format and correctness of self-generated SSID and PSK	13
4.1.2	Configure APUT using PIN method through a WLAN external Registrar ..	15
4.1.3	Configure APUT using PIN method through a wired external registrar	16
4.1.4	Configure APUT to use open networking (no security) using PIN method through a wired external registrar and add a STA using internal registrar	17
4.1.5	Check PBC Walk Time is correctly implemented.....	18
4.1.6	Configure APUT using NFC Method with password token through a WLAN external registrar.....	19
4.2	Add Devices.....	21
4.2.1	Manually configure APUT and add device using PIN method, and then add device using PBC method	21
4.2.2	Add device using PIN method, and then add device using PBC method to OOB APUT	22
4.2.3	Add devices using multiple external Registrars and internal Registrar	23
4.2.4	Make APUT generate auto-configuration and manually add a legacy device, which uses only WPA-Personal (not WPA2-Personal)	24
4.2.5	Add device using NFC Method with password token	25
4.2.6	Add device using NFC Method with configuration token.....	26
5	STA Tests.....	28
5.1	Add to AP as an Enrollee.....	28
5.1.1	Add to AP using PIN Config method through WLAN External Registrar...	28
5.1.2	Add to AP using PBC Config method through internal Registrar.....	29
5.1.3	Add to AP using PIN Config method through WLAN external Registrar ...	29
5.1.4	Add to AP using PIN Config method and PASS PHRASE through wired external registrar.....	30
5.1.5	Add to AP using PIN method and open networking setting through WLAN external Registrar	31
5.1.6	AP using PBC method and open network settings through internal Registrar	32
5.1.7	2 minute timeout with multiple push button events for PBC Config method	33

5.1.8	Overlapped PBC Config sessions	34
5.1.9	Add to AP using NFC Method with password token through internal registrar	35
5.1.10	Add to AP using NFC Method with configuration token through internal registrar	36
5.2	Act as Registrar and Configure AP.....	37
5.2.1	Manually configure AP, and then enroll with Registrar using PIN Config method	37
5.2.2	Configure the AP to use PASSPHRASE using PIN.....	39
5.2.3	Configure the AP to use open networking settings using PIN.....	39
5.3	Act as Registrar and add devices	40
5.3.1	Registrar configuring AP using registrar defaults and add device using PIN method	40
5.3.2	Registrar enrolling configured open AP and add device using PIN method	42
5.3.3	Registrar adding device using NFC Method with password token.....	43
5.3.4	Registrar adding device using NFC Method with configuration token	44
6	Appendix A: Vendor Equipment List and Contacts	46
6.1	802.11(A, B, G) Access Points	46
6.2	802.11 (A, B, G) Stations.....	47
6.3	NFC Equipment	48

1 Overview

The goal of the Wi-Fi Alliance (WFA) is to ensure the interoperability among 802.11 products that support the features of WPS from multiple manufacturers, and to promote this technology within the business and consumer markets. To achieve this goal, the WFA has developed the following test plan.

This test plan exercises various combinations of the wireless network usage models and the WPS configuration methods. The wireless network usage models consist of:

- Setting up the network (initial network setup)
- Adding additional clients

The WPS configuration methods include: Pin Input Config (PIN) method, Push Button Config (PBC) method, USB Flash Drive Config (UFD) method and Near Field Communication Contactless Token Config (NFC) method. Each of these four methods utilizes the EAP protocol and/or UPnP protocol as applicable.

The test plan will also verify the conformance of the device's WPS protocol operations according to WPS Protocol Specification.

1.1 Definitions

AP: An infrastructure-mode 802.11 Access Point

Credential: A data structure issued by a Registrar to an Enrollee, allowing the latter to gain access to the network

Device: An independent physical or logical entity capable of communicating with other Devices across a LAN or WLAN

Domain: A set of one or more Devices governed by a common authority for the purpose of gaining access to one or more WLANs

Enrollee: A Device seeking to join a WLAN Domain. Once an Enrollee obtains a valid credential, it becomes a Member

In-band: Data transfer using the WLAN communication channel

Out-Of-Band: Data transfer using a communication channel other than the WLAN

Member: A WLAN Device possessing Domain credentials

NFC Interface: Contactless interface compatible to ISO 18092

NFC Contactless Token: Contactless passive token according to NFC Forum specification

NFC Device: Any device, which implements an NFC interface

(NFC) Touch: The action of touching the NFC Token on the NFC Device. An extra step to activate the NFC Interface may be required depending on the implementation. The user manually approaches the Token to the target mark of the NFC Device until the device notifies successful reading (by beep or similar feedback). If no notification occurs, the touch duration should be at least 10 seconds.

Registration Protocol. A Registration Protocol is a (logically) three party in-band protocol to assign a Credential to the Enrollee. The protocol operates between the Enrollee and the Access Point, via the auspices of the Registrar

Registrar: An entity with the authority to issue and revoke Domain Credentials. A Registrar may be integrated into an AP, or it may be separate from the AP. A Registrar may not have WLAN capability. A given Domain may have multiple Registrars.

External Registrar: A Registrar for an AP's Domain that runs on a device separate from the AP

PushButton Configuration (PBC): A configuration method triggered by pressing a physical or logical button on the Enrollee and on the Registrar

WLAN: A Wi-Fi network

1.2 Definition of Devices under test (DUT)

1.2.1 Access Points (APUT)

The AP is an infrastructure-mode 802.11 Access Point that functions as a WPS AP. A Registrar, which has the authority to issue and revoke Domain Credentials, shall be integrated into the APUT as a built-in Registrar. The APUT also can be an Enrollee, which can register itself to an external Registrar.

1.2.2 Station (STAUT)

The STAUT is an 802.11 STA, which functions as a WSC Enrollee device. If the STAUT has a built-in registrar, the STAUT's registrar function shall be tested.

1.3 Applicability of Tests

- If the submitted device is an AP, the test cases in the section 4, whose required WPS methods matches the WPS methods supported by the AP, shall be performed.
- If an external Registrar is present on the same wireless domain as the APUT, the APUT's internal Registrar and the external Registrar should be able to coexist through the tests.
- If the submitted device is a STA, the test cases in the section 5, whose required WPS methods matches the WPS methods supported by the STA, shall be performed.

2 Implementation Requirements for Wi-Fi Alliance Certification

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

2.1 Compliance Standard

- The device under test shall be Wi-Fi certified.
- The product shall comply with IEEE 802.11a, 802.11g or 802.11b standards.

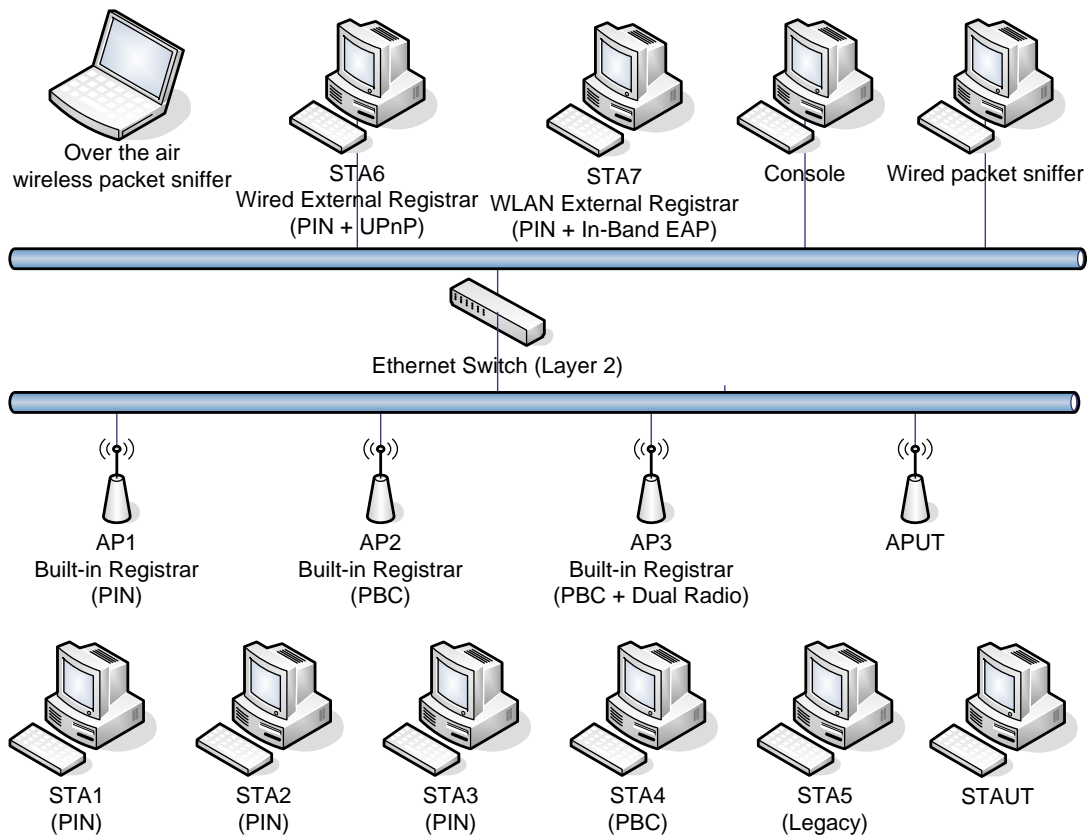
3 Test Tool

Two sniffer are required to execute the tests:

- A wireless sniffer capable of capturing and decoding EAP protocol frame is required for the testing involving exchanging the WPS protocol message through the EAP protocol. An example of such a sniffer is the AiroPeek software.
- A wired sniffer capable of capturing and decoding UPnP protocol message is required for the testing involving exchanging the UPnP protocol message through the UPnP protocol. An example of such a sniffer is the Ethereal sniffer software.

3.1 General Test Setup

The basic test configuration for infrastructure tests is depicted in the following figure:



The following attributes of test bed devices should be noted:

- AP3 is a dual-radio WPS AP that OOB operates simultaneously in both 2.4GHz and 5GHz bands.

- STA2 is an WPS Enrollee capable of optional behavior of including the WPS IE in its Association Request.
- STA7, as a WLAN External Registrar, is capable of issuing multiple credentials to an Enrollee.

3.2 Default Parameters

4 AP Tests

4.1 Configure APUT

All tests within section 4 are required to be run on the APUT for certification.

4.1.1 Check APUT's WPS Protocol frame format and correctness of self-generated SSID and PSK

Channel Assignment: For 802.11a only APs and for dual band APs, use channel 36. For 802.11g only APs, use channel 1.

Test Goal: The test verifies the APUT sets the correct WPS IE content in the Beacon frame, including the WPS version value and WPS state. If APUT is reset to OOB state and its Internal Registrar initiates a new WPS session, the new PSK must be different from the one used in the previous session.

Test Requirement: The APUT must support WPS Protocol

Test bed Devices:

1. A wireless packet sniffer device, which is able to capture the wireless packet including the Beacon packet
2. Buffalo STA, which supports PIN Config method and is acting as an Enrollee. The Probe Request frame sent by the Buffalo STA may optionally contain the WPS IE.
3. Ralink STA, which supports the optional inclusion of the WPS IE in this Association Request.

Broadcom STA, which is a legacy station and does not support any WPS methods.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to OOB configuration
3. Turn on the sniffer device and start to monitor the traffic to/from the APUT
4. If the APUT's OOB configuration is set to Unconfigured, the Beacon packet from the APUT must contain the WPS IE with version 0x10 and WPS State set to Unconfigured (0x01). If the APUT's OOB configuration is set to Configured, the Beacon packet from the APUT must contain the WPS IE with version 0x10 and WPS State set to Configured (0x02). Check on the sniffer.

5. Turn on the Buffalo STA and invoke WPS application to join WLAN. The Buffalo STA sends out Probe Request packet without the WPS IE.
6. The Probe Response from the APUT must include the WPS IE. The Config method attribute in the WPS IE must reflect the correct configuration methods that the Internal Registrar supports. Check on the sniffer to verify that the list of supported method in the IE is a bitwise OR of values from the list below:

0x0001	USBA (Flash Drive)
0x0002	Ethernet
0x0004	Label (PIN)
0x0008	Display (PIN)
0x0010	External NFC Token
0x0020	Integrated NFC Token
0x0040	NFC Interface
0x0080	PushButton
0x0100	Keypad
7. Read the displayed PIN on the Buffalo STA and enter the PIN in the Internal Registrar of the APUT.
8. Repeat Step 4 to 6 with the Ralink STA. On Sniffer verify that the APUT does not initiate 4-way handshake with the Ralink STA.
9. Ping from Console to the Buffalo STA and the Ralink STA must succeed within 90 seconds.
10. The Beacon packet from the APUT must contain the WPS IE with WPS State set to Configured (0x02). Check on the sniffer.
11. The APUT UI must display the SSID. Retrieve the SSID.
12. The APUT UI must display the PSK. Retrieve the PSK.
13. Add the Broadcom STA using manual legacy methods using the SSID and PSK retrieved from the APUT.
14. Ping from the Broadcom STA to the Buffalo STA must succeed within 90 seconds.
15. If OOB state was unconfigured in step 4 then continue through steps 16 to 23. If OOB state was configured in step 4 then test completed.
16. Reset the APUT to the OOB configuration.
17. Ping from the Broadcom STA to the Buffalo STA for 30 seconds. The Ping command must fail.
18. Read the displayed PIN on the Buffalo STA and enter the PIN in the Internal Registrar of the APUT.

19. Ping from Console to the Buffalo STA must succeed within 90 seconds.
20. The Broadcom STA must be in a disconnected state.
21. Retrieve the PSK from the APUT UI. This PSK must be different from the one retrieved in the step 10.
22. Change the Broadcom STA's configuration using manual legacy methods to the PSK and SSID retrieved from the APUT.
23. Ping from the Broadcom STA to the Buffalo STA must succeed within 90 seconds.

Test Pass/Fail Criterion: The APUT must send the correct Beacon and Probe Response frames. The APUT must generate different PSK after being reset for OOB configuration. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

4.1.2 Configure APUT using PIN method through a WLAN external Registrar

Channel Assignment: For 802.11a only APs and for dual band APs, use channel 40. For 802.11g only APs, use channel 6.

Test Goal: This test verifies that the APUT implements the PIN method correctly to act as an Enrollee. The APUT must be configurable by a WLAN External Registrar.

Test Requirement: The APUT must support the PIN Config method. The APUT must be able to act as an Enrollee and register itself with a WLAN external registrar.

Test bed Devices:

1. Intel STA, which is a WLAN external Registrar and supports PIN Config method
- Broadcom STA, which is a legacy station and does not support any WPS methods.
2. A wireless packet sniffer device, which is able to capture the wireless packet including the Beacon packet

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to OOB Configuration.
3. Turn on the Intel STA, which is acting as a WLAN external Registrar

4. The Registrar on the Intel STA will be configured with the new parameters (SSID = “scaptest4.1.2ssid” and WPA(2)-PSK = “scaptest4.1.2psk”) which should be entered when prompted
5. Read the PIN from the APUT and enter the PIN at the Intel STA when prompted by the Registrar.
6. Ping from the Intel STA to Console must succeed within 90 seconds.
7. Manually configure the Broadcom STA with the new parameters (SSID = “scaptest4.1.2ssid” and WPA(2)-PSK = “scaptest4.1.2psk”).
8. Ping from the Broadcom STA to the Intel STA must succeed within 90 seconds.
9. The Beacon packet from the APUT must contain the WPS IE with WPS State set to Configured (0x2). Check on the sniffer.

Test Pass/Fail Criterion: In step 3 and step 10, the WPS state must be set correctly in the IE of Beacon packet. Both Ping commands must be successful. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.3 Configure APUT using PIN method through a wired external registrar

Channel Assignment: For 802.11a only APs and for dual band APs, use channel 44. For 802.11g only APs, use channel 11.

Test Goal: The test verifies that the APUT implements the PIN method to act as an Enrollee with a wired external registrar and supports use of a passphrase.

Test Requirement: The APUT must support the PIN Config method and the APUT must be able to act as an Enrollee and register itself with a wired external registrar.

Test bed Devices:

1. Microsoft STA, which is a wired external registrar and supports PIN Config method

Broadcom STA, which is a legacy station and does not support any WPS methods.

2. A wireless packet sniffer device, which is able to capture the wireless packets including the Beacon packet

Test Procedure:

1. Turn on the APUT.

2. Reset the APUT to OOB Configuration.
3. Turn on the Microsoft STA, which is acting as a wired external registrar
4. The Registrar on the Microsoft STA will be configured with the new wireless configuration settings (SSID = “scaptest4.1.3ssid” and WPA(2)-PSK = “scaptest4.1.3psk”), which should be entered when prompted.
5. Read the PIN from the APUT and enter the PIN at the Microsoft STA when prompted by the Registrar.
6. Manually configure the Broadcom STA with the new parameters (SSID = “scaptest4.1.3ssid” and WPA(2)-PSK passphrase= “scaptest4.1.3psk”).
7. Ping from the Broadcom STA to the Microsoft STA must succeed within 90 seconds.
8. The Beacon packet from the APUT must contain the WPS IE with WPS State set to Configured (0x2). Check on the sniffer.
9. APUT must be capable of displaying the passphrase. The passphrase must be “scaptest4.1.3psk”.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.4 Configure APUT to use open networking (no security) using PIN method through a wired external registrar and add a STA using internal registrar

Channel Assignment: For 802.11g only APs and for dual band APs, use channel 1. For 802.11a only APs, use channel 48.

Test Goal: The test verifies that the APUT can be configured to use open networking setting by a wired external Registrar and that a STA can be added using the internal registrar.

Test Requirement: The APUT must support PIN Config method

Test bed Devices:

1. Microsoft STA, which is acting as a wired external Registrar and supports PIN Config method
2. Broadcom STA, which is a legacy station and does not support any WPS methods.
3. Atheros STA, which is a WPS STA.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to OOB Configuration.
3. Turn on the Microsoft STA, which is acting as a wired external registrar
4. The Registrar on the Microsoft STA will be configured to use open network settings (SSID = “scaptest4.1.5ssid”) which should be entered when prompted
5. Read the PIN from the APUT and enter the PIN at the Microsoft STA when prompted by the Registrar.
6. Ping from the Microsoft STA to Console must succeed within 90 seconds.
7. Enter the PIN for the Atheros STA at the internal Registrar of the APUT.
8. Ping from the Atheros STA to Console must succeed within 90 seconds.
9. Manually associate the Broadcom STA with the APUT using open networking settings (SSID = “scaptest4.1.5ssid”).
10. Ping from the Broadcom STA to the Microsoft STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.5 Check PBC Walk Time is correctly implemented

Channel Assignment: For 802.11g only APs and for dual band APs, use channel 6. For 802.11a only APs, use channel 36.

Test Goal: The test verifies that the APUT implements the 2 minute Walk Time and resets the timer appropriately. If the period between the time when the WPS button on APUT is pushed and the time when the WPS button on STA is pushed is longer than 2 minutes, the APUT must not succeed in this WPS session.

Test Requirement: The APUT must support PBC method

Test bed Devices:

1. A wireless sniffer device
2. Buffalo STA, which supports PBC Config method and is acting as an Enrollee.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to OOB Configuration
3. Turn on the wireless sniffer device, set it to monitor the wireless traffic to/from the APUT
4. Using the wireless sniffer device monitor the APUT Beacon. The SelectedRegistrar flag and Device Password ID attribute in the WPS IE of the Beacon frame must NOT be present.
5. Push the WPS button (which may be a physical button or a soft button on the AP UI) on the APUT
6. Using the wireless sniffer device monitor the APUT Beacon. The SelectedRegistrar flag in the WPS IE of the Beacon frame must be present and have value TRUE. The Device Password ID attribute needs to be set to PushButton (0x0004).
7. Wait 1 minute.
8. Push the WPS button on the APUT
9. Using the wireless sniffer device monitor the APUT Beacon. The SelectedRegistrar flag in the WPS IE of the Beacon frame must be present and have value TRUE. The Device Password ID attribute needs to be set to PushButton (0x0004). The beacon must maintain this state for 2 minutes from the button push in Step 7. After 2 minutes the SelectedRegistrar flag in the WPS IE of the Beacon frame must NOT be present.
10. After the 2 minutes in Step 8 have expired push the WPS button on the Buffalo STA.
11. The Buffalo STA must not indicate success.
12. Wait 1 minute.
13. Push the WPS button on APUT.
14. Ping from the Buffalo STA to Console must succeed within 90 seconds.

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.1.6 Configure APUT using NFC Method with password token through a WLAN external registrar

Test Classification: OPTIONAL Tested if NFC implemented

Test Goal: This test verifies that the APUT implements the NFC Method with password token to act as an Enrollee. The APUT must be configurable by external Registrar using NFC method with password token.

Test Requirement: The APUT must support the NFC Method with password token. The APUT must be able to act as an Enrollee and register itself with a WLAN external registrar. The APUT must provide a writable NFC Token if the NFC Method with password token is implemented by creating a password token on a writable NFC Token.

Test bed Devices:

1. Sony STA, which is a WLAN external Registrar and supports NFC Method with password token.
2. Broadcom STA, which is a legacy station and does not support any WPS methods.
3. A wireless sniffer device

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to OOB Configuration.
3. Turn on the Sony STA, which is acting as a WLAN external Registrar.
4. The Registrar on the Sony STA will be configured with the new parameters (SSID = “scaptest4.1.6ssid” and WPA(2)-PSK = “scaptest4.1.6psk”), which should be entered when prompted.
5. Start a WPS NFC password token registration process on APUT following the vendor directions.
6. Touch the NFC Interface of the Sony STA with the Password Token
7. Manually configure the Broadcom STA with the new parameters (SSID = “scaptest4.1.6ssid” and WPA(2)-PSK = “scaptest4.1.6psk”)
8. Ping from the Broadcom STA to the Sony STA must succeed within 90 seconds.
9. The Beacon packet from the APUT must contain the WPS IE with WPS State set to Configured (0x2). Check on the sniffer.

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2 Add Devices

4.2.1 Manually configure APUT and add device using PIN method, and then add device using PBC method

Channel Assignment: For 802.11g only APs and for dual band APs, use channel 11. For 802.11a only APs, use channel 40.

Test Goal: The test verifies that the APUT implements the PIN and PBC Config method to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using PIN method and then add a STA device using PBC method. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified.

Test Requirement: The APUT must support PIN and PBC Config method

Test bed Devices:

1. Ralink STA, which supports PIN Config method and is acting as an Enrollee
2. Buffalo STA, which supports PBC Config method and is acting as an Enrollee

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to OOB Configuration
3. On the UI of the APUT, configure the APUT with new security settings (SSID = “scaptest4.2.1ssid” and WPA(2)-PSK = “scaptest4.2.1psk”).
4. Turn on the Ralink STA.
5. Enter PIN of 12345671 (invalid checksum PIN) in the internal Registrar on the APUT
6. Internal Registrar must report an invalid PIN
7. Enter PIN of 12345670 (if the Ralink STA’s PIN is 12345670 then use PIN 24681353) in the internal Registrar on the APUT
8. Ping from Console to the Ralink STA must fail
9. Read the PIN displayed on the Ralink STA and enter the PIN in the internal Registrar on the APUT
10. Ping from the Ralink STA to Console must succeed within 90 seconds.
11. Turn on the Buffalo STA.
12. Push the WPS button on the APUT
13. Push the WPS button on the Buffalo STA.

14. Ping from the Buffalo STA to the Ralink STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If the both of Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.2 Add device using PIN method, and then add device using PBC method to OOB APUT

Channel Assignment: For 802.11a only APs and for dual band APs, use channel 48. For 802.11a only APs, use channel 6.

Test Goal: The test verifies that the APUT implements the PIN and PBC Config method to act as an internal Registrar from its OOB state. The APUT must able to add STA device to its WLAN using PIN method and then add STA device using PBC method.

Test Requirement: The APUT must support PIN and PBC Config method

Test bed Devices:

1. Ralink STA, which supports PIN Config method and is acting as an Enrollee
2. Atheros STA, which supports PBC Config method and is acting as an Enrollee.

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to OOB configuration
3. Turn on the Ralink STA.
4. Read the PIN displayed on the Ralink STA and enter the PIN in the internal Registrar on the APUT.
5. Ping from the Ralink STA to Console must succeed within 90 seconds.
6. Turn on the Atheros STA.
7. Push the WPS button on the Atheros STA.
8. Push the WPS button on the APUT
9. Ping from the Atheros STA to the Ralink STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If the both of Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.3 Add devices using multiple external Registrars and internal Registrar

Channel Assignment: For 802.11g only APs and for dual band APs, use channel 11. For 802.11a only APs, use channel 44.

Test Goal: The test verifies that the APUT supports interchangeable use of the internal registrar, a wired external Registrar and a WLAN external Registrar to add enrollees.

Test Requirement: The APUT must support wired and WLAN external Registrars. The APUT must support PIN Config method.

Test bed Devices:

1. Intel STA, which supports PIN Config method and is acting as an WLAN external registrar
2. Buffalo STA, which supports PIN Config method and is acting as an Enrollee
3. Atheros STA, which supports PIN Config method and is acting as an Enrollee
4. Ralink STA, which supports PIN Config method and is acting as an Enrollee
5. Microsoft STA, which supports PIN Config method and is acting as a wired external registrar

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to OOB Configuration
3. Turn on the Microsoft STA, which is acting as a wired external registrar.
4. The Registrar on the Microsoft STA will be configured with the new wireless configuration settings (SSID = “scaptest4.2.3ssid” and WPA(2)-PSK = “scaptest4.2.3psk”), which should be entered when prompted
5. Read the PIN from the APUT and enter the PIN at the Microsoft STA when prompted by the Registrar.
6. The Registrar on the Microsoft STA will display status on completion. The status must be success.
7. Turn on the Intel STA, which is acting as a WLAN external registrar

8. Read the PIN from the APUT and enter the PIN at the WLAN external registrar on the Intel STA when prompted by the Registrar.
9. Ping from the Intel STA to the Microsoft STA must succeed within 180 seconds.
10. Turn on the Buffalo STA, which is acting as an Enrollee
11. Enter the PIN from the Buffalo STA into the wired external Registrar on the Microsoft STA.
12. Ping from the Buffalo STA to the Microsoft STA must succeed within 180 seconds.
13. Turn off the Microsoft STA.
14. Turn on the Atheros STA, which is acting as an Enrollee
15. Enter the PIN from the Atheros STA into the WLAN external registrar on the Intel STA.
16. Ping from the Intel STA to the Atheros STA must succeed within 180 seconds.
17. Turn on the Ralink STA, which is acting as an Enrollee
18. Enter the PIN from the Ralink STA into the internal Registrar on APUT
19. Ping from the Buffalo STA to the Ralink STA must succeed within 180 seconds.

Test Pass/Fail Criterion: If all of PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.4 Make APUT generate auto-configuration and manually add a legacy device, which uses only WPA-Personal (not WPA2-Personal)

Channel Assignment: For 802.11g only APs and for dual band APs, use channel 6. For 802.11a only APs, use channel 40.

Test Goal: The test verifies that the APUT can support WPA/WPA2 mixed mode. A legacy STA which uses only WPA-Personal can be manually added to the APUT’s WLAN.

Test Requirement: The APUT must support PIN Config method.

Test bed Devices:

1. Buffalo STA, which supports PIN Config method and is acting as an Enrollee
2. Broadcom STA, which is a legacy station and uses WPA only

Test Procedure:

1. Turn on the APUT
2. Reset the APUT to OOB Configuration
3. Turn on the Buffalo STA, which is acting as an Enrollee
4. Enter the PIN from the Buffalo STA at internal Registrar on APUT.
5. Ping from the Buffalo STA to Console must succeed within 90 seconds.
6. Retrieve the SSID and PSK from the UI on the APUT.
7. Manually configure the Broadcom STA with the SSID and PSK of the APUT using WPA-Personal.
8. Ping from the Broadcom STA to the Buffalo STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If both of PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.5 Add device using NFC Method with password token

Test Classification: OPTIONAL Tested if NFC Implemented

Test Goal: The test verifies that the APUT implements the NFC Method with password token to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using NFC method with password token.

Test Requirement: The APUT must support NFC Method with password token. The APUT may provide a writable NFC Token which must be used if provided.

Test bed Devices:

1. NXP STA, which supports NFC Method with password token and is acting as an Enrollee. If not provided with the APUT: The writable NFC Token provided with the NXP STA.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to OOB Configuration.

3. Turn on the NXP STA.
4. Create a Password Token for the NXP STA by selecting the password token generation function on the UI of the NXP STA and touching the NFC Interface with the writable NFC Token.
5. Touch the APUT with the created Password Token.
6. Ping from the NXP STA to Console must succeed within 90 seconds.

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

4.2.6 Add device using NFC Method with configuration token

Test Classification: OPTIONAL Tested if NFC Implemented

Test Goal: The test verifies that the APUT implements the NFC Method with configuration token to act as an internal Registrar. The configured APUT must be able to add a STA device to its WLAN using NFC method with configuration token.

Test Requirement: The APUT must support NFC Method with configuration token and provide a writable NFC Token.

Test bed Devices:

1. Sony STA, which supports NFC Method with configuration token and is acting as an Enrollee.

Test Procedure:

1. Turn on the APUT.
2. Reset the APUT to OOB Configuration.
3. Turn on the Sony STA.
4. Create a configuration token by selecting the configuration token generation function on the UI and touching the NFC Interface of the APUT with the writable NFC Token.
5. Touch the Sony STA with the created configuration token.
6. Ping from the Sony STA to the Console must succeed within 90 seconds.

Test Pass/Fail Criterion: If The Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5 STA Tests

5.1 Add to AP as an Enrollee

5.1.1 Add to AP using PIN Config method through WLAN External Registrar

Test Classification: Mandatory

Channel Assignment: For 802.11a only STAUTs and for dual band STAUTs, use channel 36. For 802.11a only APs, use channel 1.

Test Goal: The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP's WLAN through a WLAN external Registrar using PIN method. The WLAN external registrar shall deliver two network credentials, 1 for a network that is present and 1 that is not present. The STAUT must connect using the credentials for the network that is present.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. Marvel AP, which supports PIN Config method.
2. Atheros STA, which is a WLAN external Registrar that has a test mode allowing it to deliver an extra network credential to an enrollee (correct credential is the 2nd credential)

Test Procedure:

1. Turn on the Marvell AP in OOB mode
2. Turn on the Atheros STA.
3. Enter the PIN of the Marvell AP into Registrar on the Atheros STA. Use default configuration
4. Set the Atheros STA into its test mode
5. Turn on STAUT and start a WPS PIN registration process per vendor direction
6. Enter the PIN of STAUT into Registrar on the Atheros STA.
7. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.2 Add to AP using PBC Config method through internal Registrar

Test Classification: Optional Tested if PBC is implemented

Channel Assignment: For 802.11a only STAUTs and for dual band STAUTs, use channel 40. For 802.11a only APs, use channel 6.

Test Goal: The test verifies that the STAUT implements the PBC Config method as an Enrollee. The STAUT must be able to join an AP's WLAN through the AP's internal Registrar using PBC method. This test also checks that a dual-radio STAUT does not incorrectly identify the PBC active state of a dual-radio AP as an overlapping session.

Test Requirement: The STAUT must support PBC Config method.

Test bed Devices:

1. Atheros AP is a dual-radio WPS AP, which supports PBC Config method.

Test Procedure:

1. Turn on the Atheros AP in OOB mode.
2. Turn on the STAUT. If the STAUT scans both bands confirm that it sees the Atheros AP in both bands.
3. Push WPS button on the Atheros AP.
4. Push WPS button on the STAUT or start a WPS PBC registration process per vendor direction.
5. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.3 Add to AP using PIN Config method through WLAN external Registrar

Test Classification: Mandatory

Channel Assignment: For 802.11a only STAUTs and for dual band STAUTs, use channel 40. For 802.11g only APs, use channel 11.

Test Goal: The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP's WLAN using PIN method through a WLAN external registrar.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. Atheros AP, which supports PIN Config method
2. Marvell STA, which supports PIN Config method and is acting as a WLAN external registrar

Test Procedure:

1. Turn on the Atheros AP.
2. Turn on the Marvell STA.
3. The Registrar on the Marvell STA will be configured with the new parameters (SSID = "scstatest5.1.13ssid" and WPA(2)-PSK = "scstatest5.1.3psk") which should be entered when prompted
4. Enter the PIN of the Atheros AP at the Marvell STA when prompted by the Registrar.
5. Wait for the Registrar on the Marvell STA to indicate completion
6. Turn on STAUT and start a WPS PIN registration process per vendor direction
7. On the Marvell STA enter the PIN from the STAUT.
8. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.4 Add to AP using PIN Config method and PASS PHRASE through wired external registrar

Test Classification: Mandatory

Channel Assignment: For 802.11a only STAUTs and for dual band STAUTs, use channel 44. For 802.11a only APs, use channel 1.

Test Goal: The test verifies that the STAUT implements the PIN Config method as an Enrollee. The STAUT must be able to join an AP's WLAN using PIN method through wired external registrar.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. Broadcom AP, which supports PIN Config method
2. Microsoft STA, which supports PIN Config method and is acting as a wired external registrar

Test Procedure:

1. Turn on the Broadcom AP.
2. Turn on the Microsoft STA.
3. The Registrar on the Microsoft STA will be configured with the new parameters (SSID = "scstate5.1.4ssid" and WPA2-Personal PASS PHRASE = "scstate5.1.4psk") which should be entered when prompted
4. Enter the PIN of the Broadcom AP at the Microsoft STA when prompted by the Registrar.
5. Wait for the Registrar on the Microsoft STA to indicate completion
6. Turn on STAUT and start a WPS PIN registration process per vendor direction
7. The STAUT shall generate and show an unique PIN (or it has a PIN on label)
8. Enter the PIN from the STAUT in Registrar on the Microsoft STA.
9. Ping from the Microsoft STA to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise, it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.5 Add to AP using PIN method and open networking setting through WLAN external Registrar

Test Classification: MANDATORY

Channel Assignment: For 802.11a only STAUTs and for dual band STAUTs, use channel 48. For 802.11g only APs, use channel 6.

Test Goal: The test verifies that the STAUT can be configured to use open network settings to join an AP's WLAN using PIN method through WLAN external Registrar.

Test Requirement: The STAUT must support PIN Config method.

Test bed Devices:

1. Marvell AP, which supports PIN Config method
2. Marvell STA, which supports PIN Config method and is acting as an WLAN external registrar

Test Procedure:

1. Turn on the Marvell AP.
2. Turn on the Marvell STA.
3. The Registrar on the Marvell STA will be configured with the open network settings (SSID = "scstatest5.1.15ssid") which should be entered when prompted
4. Enter the PIN of the Marvell AP at the Marvell STA when prompted by the Registrar.
5. Wait for the Registrar on the Marvell STA to indicate completion
6. Turn on STAUT and start a WPS PIN registration process per vendor direction
7. On the Marvell STA enter the PIN from the STAUT.
8. Ping from the Marvell STA to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.6 AP using PBC method and open network settings through internal Registrar

Test Classification: OPTIONAL Tested if PBC implemented

Channel Assignment: For 802.11g only STAUTs and for dual band STAUTs, use channel 1. For 802.11a only APs, use channel 36.

Test Goal: The test verifies that the STAUT can be configured to use open network settings to join an AP's WLAN using PBC method through AP's internal Registrar.

Test Requirement: The STAUT must support PBC Config method.

Test bed Devices:

1. Conexant AP, which supports PBC Config method

Test Procedure:

1. Turn on the Conexant AP.
2. Configure the Conexant AP with the open network settings (SSID = "scstatest5.1.16ssid").
3. Turn on the STAUT
4. Push the WPS button on the Conexant AP.
5. Push the WPS button on STAUT.
6. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.7 2 minute timeout with multiple push button events for PBC Config method

Test Classification: OPTIONAL Tested if PBC implemented

Channel Assignment: For 802.11g only STAUTs and for dual band STAUTs, use channel 6. For 802.11a only APs, use channel 40.

Test Goal: The test verifies that the STAUT exercises the push button 2 minutes timer correctly. As long as the period between when the user pushes the WPS button on the AP and when the user pushes the WPS button on the STAUT is less than 2 minutes, the STAUT must be able to join the AP's WLAN using PBC method through the AP's internal Registrar.

Test Requirement: The STAUT must support PBC method

Test bed Devices:

1. Broadcom AP, which supports PBC Config method

Test Procedure:

1. Turn on the Broadcom AP.
2. Turn on the STAUT
3. Push the WPS button on STAUT
4. Wait 90 seconds
5. Push the WPS button on STAUT again. NOTE: in some station implementations using a "soft" button, the button is not available to push until the 120-second timer has expired. In these cases, the button may be pushed as soon as it is available as long as the 90 seconds has elapsed in step 4.
6. Wait for 1 minute
7. Push the WPS button on the Broadcom AP.
8. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.1.8 Overlapped PBC Config sessions**Test Classification: OPTIONAL Tested if PBC implemented**

Channel Assignment: For 802.11g only STAUTs and for dual band STAUTs, use channel 11. For 802.11a only APs, use channel 48.

Test Goal: The test verifies the STAUT can't join an AP's WLAN using PBC method through the AP's internal Registrar, if another PBC WPS session by another AP exists. Once other PBC WPS session is removed, the STAUT must be able to join the AP's WLAN.

Test Requirement: The STAUT must support PBC method

Test bed Devices:

1. Conexant AP, which supports PBC Config method
2. Atheros AP, which supports PBC Config method

Test Procedure:

1. Turn on the Conexant AP.

2. Turn on the Atheros AP.
3. Turn on the STAUT
4. Push the WPS button on the Atheros AP.
5. Wait for 1 minute and push the WPS button on the Conexant AP.
6. Push the WPS button on STAUT
7. Ping from Console to STAUT must fail.
8. Wait 1 minute
9. Push the WPS button on the STAUT
10. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: The STAUT must indicate that the WPS process fails after pushing the button on STAUT for the first time. The PING command must be successful. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.1.9 Add to AP using NFC Method with password token through internal registrar

Test Classification: OPTIONAL Tested if NFC is implemented

Test Goal: The test verifies the STAUT implements the NFC Method with password token as an Enrollee. The STAUT must be able to join an AP’s WLAN through the AP’s internal Registrar using NFC method with password token. The STAUT must fail the registration protocol if presented a different password token.

Test Requirement: The STAUT must support NFC Method with password token. The STAUT must provide a writable NFC Token if the NFC Method with password token is implemented by creating a password token on a writable NFC Token.

Test bed Devices:

1. NXP AP, which has an internal registrar and supports NFC Method with password token.
2. Sony STA, which supports NFC Method with password token. The writable NFC Token provided with the Sony STA.

Test Procedure:

1. Turn on the Sony STA.

2. Create a Password Token for the Sony STA by selecting the password token generation function on the UI of the Sony STA and touching the NFC Interface with the writable NFC Token.
3. Turn off the Sony STA.
4. Turn on the NXP AP.
5. Turn on STAUT and start a WPS NFC password token registration process per vendor direction.
6. Touch the NFC Interface of the NXP AP with the Sony STA password token.
7. Wait 90 seconds.
8. Ping from Console to STAUT must fail.
9. Restart the NXP AP.
10. Restart the WPS NFC password token registration process on STAUT as per vendor direction.
11. Touch the NFC Interface of the NXP AP with the STAUT password token.
12. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.1.10 Add to AP using NFC Method with configuration token through internal registrar

Test Classification: OPTIONAL Tested if NFC is implemented

Test Goal: The test verifies the STAUT implements the NFC Method with configuration token as an Enrollee. The STAUT must be able to join an AP’s WLAN through the AP’s internal Registrar using NFC method with configuration token. The STAUT must fail the registration protocol if presented a configuration token with an incorrect NDEF record.

Test Requirement: The STAUT must support the NFC Method with configuration token. The STAUT may provide a writable NFC Token which must be used if provided.

Test bed Devices:

1. Sony AP, which has an internal registrar and supports NFC Method with configuration token. If not provided with the STAUT: The writable NFC Token provided with the Sony AP.

Test Procedure:

2. Turn on the Sony AP.
3. Manually configure the Sony AP with new wireless configuration settings (SSID = “scstatest5.1.10ssid-wrong” and WPA(2)-PSK = “scstatest5.1.10psk”) when prompted
4. Create an Configuration Token by executing the configuration token generation function on the Sony AP and touching the NFC Interface with the writable NFC Token.
5. Turn off the Sony AP.
6. Turn on the Sony AP.
7. Manually configure the Sony AP with new wireless configuration settings (SSID = “scstatest5.1.10ssid” and WPA(2)-PSK = “scstatest5.1.10psk”) when prompted
8. Turn on the STAUT.
9. Start the WPS NFC configuration token registration process on STAUT as per vendor directions and touch the NFC Interface with the Configuration Token.
10. Wait 90 seconds.
11. Ping from Console to STAUT must fail.
12. Create an correct Configuration Token by executing the configuration token generation function on the Sony AP and touching the NFC Interface with the writable NFC Token.
13. Start a WPS NFC configuration token registration process per vendor directions and touch the STAUT with the Configuration Token.
14. Ping from Console to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the Ping command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.2 Act as Registrar and Configure AP

This test applies to only those stations that implement a wireless external registrar.

5.2.1 Manually configure AP, and then enroll with Registrar using PIN Config method

Test Classification: OPTIONAL Tested if WLAN External Registrar Implemented

Channel Assignment: For 802.11g only STAUTs and for dual band STAUTs, use channel 6. For 802.11a only APs, use channel 44.

Test Goal: The test verifies that the AP wireless configuration settings established by the user are not silently overwritten by the WPS methods. This test also verifies that the correct PIN must be used and a bad checksum is correctly identified.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as a WLAN external registrar.

Test Classification: **OPTIONAL Tested if WLAN External Registrar Implemented**

Test bed Devices:

1. Atheros AP, which supports PIN Config method and is acting as an Enrollee
2. Broadcom STA, which is a legacy station and does not support any WPS method

Test Procedure:

1. Turn on the Atheros AP.
2. Manually configure the Atheros AP with new wireless configuration settings (SSID = “scstatest5.2.1ssid” and WPA(2)-PSK = “scstatest5.2.1psk”) when prompted
3. Manually configure the Broadcom STA with new wireless configuration settings (SSID = “scstatest5.2.1ssid” and WPA(2)-PSK = “scstatest5.2.1psk”)
4. Ensure ping from the Broadcom STA to Console operates correctly.
5. Turn on STAUT and start a WPS PIN registration process per vendor direction
6. Enter PIN of 12345671 in the Registrar of STAUT
7. Registrar must report an invalid PIN
8. Enter PIN of 123456780 (if the STAUT’s PIN is 12345670, then use PIN 24681353) in the Registrar of STAUT
9. Ping from Console to STAUT must fail
10. Enter the PIN of the Atheros AP in the Registrar of STAUT. If any options are presented by the Registrar the existing configuration setting shall be selected (if there are default selections the existing configuration must be the default).
11. To confirm the existing configuration has been preserved, ping from the Broadcom STA to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.2.2 Configure the AP to use PASSPHRASE using PIN

This test applies to only those stations that implement a wireless external registrar.

Channel Assignment: For 802.11a only STAUTs and for dual band STAUTs, use channel 40. For 802.11a only APs, use channel 1.

Test Goal: The test verifies that the STAUT is able to configure an AP to use PASS PHRASE using PIN Config method.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as a WLAN external registrar.

Test bed Devices:

1. Marvell AP, which supports PIN Config method and is acting as an Enrollee
2. Broadcom STA, which is a legacy station and does not support any WPS method

Test Procedure:

1. Turn on the Marvell AP.
2. Turn on the STAUT
3. Configure the STAUT with new wireless configuration settings (SSID = “scstatest5.2.2ssid” and PASS PHASE = “scstatest5.2.2psk”) when prompted
4. Enter the PIN of the Marvell AP at the Registrar on STAUT when prompted
5. Ping from Console to STAUT must succeed within 90 seconds.
6. Manually configure the Broadcom STA with the wireless configuration settings (SSID = “scstatest5.2.2ssid” and PASS PHRASE = “scstatest5.2.2psk”)
7. Ping from the Broadcom STA to STAUT must succeed within 90 seconds.

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.2.3 Configure the AP to use open networking settings using PIN

This test applies to only those stations that implement a wireless external registrar.

Channel Assignment: For 802.11a only STAUTs and for dual band STAUTs, use channel 44. For 802.11g only APs, use channel 11.

Test Goal: The test verifies that the STAUT is able to configure an AP to use open network settings using PIN Config method.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as a WLAN external registrar.

Test bed Devices:

1. Buffalo AP, which supports PIN Config method and is acting as an Enrollee
2. Broadcom STA, which is a legacy station and does not support any WPS method

Test Procedure:

1. Turn on the Buffalo AP.
2. Turn on the STAUT
3. Configure the STAUT with the open network settings (SSID = "scstatest5.2.3ssid")
4. Enter the PIN at the Registrar on STAUT
5. The Registrar must inform the user that security is not set and require confirmation or require explicit user operation to create this open network.
6. Ping from Console to STAUT must succeed within 90 seconds.
7. Manually associate the Broadcom STA with the Buffalo AP.
8. Ping from the Broadcom STA to STAUT must succeed within 90 seconds

Test Pass/Fail Criterion: If the PING command is successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.3 Act as Registrar and add devices

This test applies to only those stations that implement a wireless external registrar.

5.3.1 Registrar configuring AP using registrar defaults and add device using PIN method

Test Classification: OPTIONAL Tested if Registrar implemented

Channel Assignment: For 802.11g only STAUTs and for dual band STAUTs, use channel 1. For 802.11a only APs, use channel 36.

Test Goal: The test verifies that the STAUT implements WLAN external registrar function. The STAUT must be able to configure an AP with its default settings and add a STA device to the AP's WLAN using PIN method.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as a WLAN external registrar

Test bed Devices:

1. Broadcom AP, which supports PIN Config method.
2. Intel STA, which supports PIN Config method and is acting as an Enrollee.
3. Broadcom STA, which is legacy station and does not support WPS methods.

Test Procedure:

1. Turn on the Broadcom AP.
2. Verify the Broadcom AP is unconfigured. Reset it to OOB Configuration if necessary
3. Turn on the STAUT
4. Enter the PIN of the Broadcom AP at the Registrar on STAUT.
5. Ping from Console to STAUT must succeed within 90 seconds.
6. Turn on the Intel STA.
7. Enter the PIN of the Intel STA at the Registrar on STAUT.
8. Ping from the Intel STA to STAUT must succeed within 90 seconds.
9. In the UI of the Broadcom AP, retrieve the wireless configuration settings (SSID and WPA(2)-PSK)
10. Turn on the Atheros STA.
11. Manually configure the Broadcom STA with retrieved wireless configuration settings from the AP and select to use WPA Personal.
12. Pinging from the Broadcom STA to the Intel STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If all of the PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

5.3.2 Registrar enrolling configured open AP and add device using PIN method

This test applies to only those stations that implement a wireless external registrar.

Channel Assignment: For 802.11g only STAUTs and for dual band STAUTs, use channel 6. For 802.11a only APs, use channel 48.

Test Goal: The test verifies that the STAUT implements the Registrar function. The STAUT must be able to register an AP configured with open network settings and add a STA device to the AP's WLAN using PIN method with the original network settings.

Test Requirement: The STAUT must support PIN Config method and be capable of acting as a WLAN external registrar

Test bed Devices:

1. Buffalo AP, which supports PIN Config method
2. Marvell STA, which supports PIN Config method and is acting as an Enrollee
3. Broadcom STA, which is legacy station and does not support WPS methods

Test Procedure:

1. Turn on the Buffalo AP.
2. Configure the Buffalo AP with the open network settings (SSID = "scstatest5.3.2ssid")
3. Turn on STAUT and start a WPS PIN registration process per vendor direction
4. Enter the PIN of the Buffalo AP at the Registrar on STAUT
5. The Registrar must require explicit user operation to create this open network (if just hitting OK or selecting default path creates the network this test fails).
6. Ping from Console to STAUT must succeed within 90 seconds.
7. Turn on the Marvell STA.
8. Enter the PIN of the Marvell STA at the Registrar on STAUT.
9. Ping from the Marvell STA to STAUT must succeed within 90 seconds.
10. Turn on the Broadcom STA.
11. Manually configure the Broadcom STA with open network settings (SSID = "scstatest5.3.2ssid")
12. Ping from the Broadcom STA to the Marvell STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If all of the PING commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.3.3 Registrar adding device using NFC Method with password token

Test Classification: OPTIONAL Tested if Registrar and NFC implemented

Test Goal: The test verifies that the STAUT implements the Registrar function using NFC Method with password token. The STAUT must be able to add a STA device to the AP’s WLAN using NFC method with password token.

Test Requirement: The STAUT must support NFC Method with password token and be capable of acting as an external Registrar. The STAUT may provide a writable NFC Token which must be used if provided.

Test bed Devices:

1. NXP AP, which supports NFC Method with password token.
2. Sony STA, which supports NFC Method with password token and is acting as an Enrollee. If not provided with the STAUT: The writable NFC Token provided with the Sony STA.

Test Procedure:

1. Turn on the NXP AP.
2. Verify the NXP AP is unconfigured. Reset it to OOB Configuration if necessary
3. Turn on the STAUT
4. Enter the PIN of the NXP AP at the Registrar on STAUT.
5. Ping from Console to STAUT must succeed within 90 seconds.
6. Turn on the Sony STA.
7. Create a Password Token for the Sony STA by selecting the password token generation function on the UI of the Sony STA and touching the NFC Interface with the writable NFC Token.
8. Follow the vendor directions to start a WPS NFC password token registration process on STAUT and touch the NFC Interface with the created Password Token.

9. Ping from Console to the Sony STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as ‘must’ is not fulfilled.

5.3.4 Registrar adding device using NFC Method with configuration token

Test Classification: OPTIONAL Tested if Registrar and NFC implemented

Test Goal: The test verifies that the STAUT implements the Registrar function using NFC Method with configuration token. The STAUT must be able to add a STA device to the AP’s WLAN using NFC method with configuration token.

Test Requirement: The STAUT must support NFC Method with configuration token and be capable of acting as an external Registrar. The STAUT may provide a writable NFC Token which must be used if provided.

Test bed Devices:

1. Sony AP, which supports NFC Method with configuration token.
2. NXP STA, which supports NFC Method with configuration token and is acting as an Enrollee. If not provided with the STAUT: The writable NFC Token provided with the NXP STA.

Test Procedure:

1. Turn on the Sony AP.
2. Verify the Sony AP is unconfigured. Reset it to OOB Configuration if necessary.
3. Turn on the STAUT.
4. Enter the PIN of the NXP AP at the Registrar on STAUT.
5. Ping from Console to STAUT must succeed within 90 seconds.
6. Create a Configuration Token on the STAUT following the vendor directions.
7. Turn on the NXP STA and start the configuration token registration process.
8. Touch the NXP STA with the Configuration Token when prompted.
9. Ping from Console to the NXP STA must succeed within 90 seconds.

Test Pass/Fail Criterion: If both Ping commands are successful, this test is determined as PASS. Otherwise it is determined as FAIL. The test is determined as a FAIL if any condition described as 'must' is not fulfilled.

6 Appendix A: Vendor Equipment List and Contacts

6.1 802.11(A, B, G) Access Points

Product Name/Model	HW Model	SW Version	Contact
Atheros	AR5BAP-00039A	AP5.2.0.112	wfa_external_support@atheros.com
Buffalo	WHR-HP-AMPGV	1.18	MASATO KATO mkato@melcoinc.co.jp Tel: +81-52-619-7752
Broadcom	BCM94704AGR-Rev-E.2.4	OS V 3.131.35.55 Boot Loader 3.91.39.0	Richard Ybarra rybarra@broadcom.com
Marvell	CD-88W-AP85WIFI-AO	v2.1.9.15	Juty Hendarady jutyh@marvell.com 1-408-222-2180
Conexant	Conexant Solos AP RD94515 -WIFI	1.1.2.0	Michael Paljug michael.paljug@conexant.com, Ph: (321) 327-6482.

6.2 802.11 (A, B, G) Stations

Product Name/Model	HW version	SW Version	Contact
Intel (includes wireless ER)	WM3945AGM1 GEN MiniPCI-Express card.	XP OS Proset: 11.1.0.0 Driver: 11.1.0.69	Etsube Gelagay Etsube.gelagay@intel.com
Atheros (includes wireless ER)	AR5002X Universal 802.11a/b/g Wireless Network Adapter (Model # AR5BCB-0065XA)	XP OS Jumpstart: v2.0.0.275 Driver: 5.0.0.1097	See AP section above.
Buffalo	WLI-CB-AMG54V	VISTA Ultimate WSPBC 1.0.5.1 Driver: 5.0.0.107	See AP Section above.
Marvell (includes wireless ER)	CD-88W-USB55WIFI-AO	XP OS FW: 2.0.2.7 Driver: 2.1.1.3 Config Utility: 2.0.1.24 DLL: 2.0.1.18	See AP section above.
Ralink	RT5201U	XP OS Driver: 1.1.3.13 Config: 1.2.5.9 FW: 1.9 EPROM: 1.3	Paul Lin (paul_lin@ralinktech.com.tw) +886-3-5678868 ext 1501
Microsoft wired ER	na	Vista Ultimate RTM	David Roberts droberts@microsoft.com
Broadcom (Legacy, nonWPS, station)	Broadcom 802.11abg CardBus Reference Design – BCM94309CB	4.10.36.0	See AP section above.

6.3 NFC Equipment

Company	HW version	SW Version	Contact
NXP	ADRA-USB	Knoppix OS with NXP image	Philippe teuwen philippe.teuwen@nxp.com
Sony	NFC631KT	fedora-livecd- wps-1.1.2.iso	Daisuke Kawakami Daisuke.Kawakami@jp.sony.com

Note: Both NXP and Sony use the Atheros station card in section 6.2 above with the Madwifi driver.