Application Report
SWRA503–March 2016

Certification Testing Guidelines for Wi-Fi Alliance® System Interoperability Test Plans

ABSTRACT

The purpose of this document is to ensure readiness of TI's customers for the certification process of the Wi-Fi Alliance® (WFA).

Contents

List of Figures

1 Background

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

This document concerns the following certifications:

- WMM-PS (WMM-Powersave_testplan_v2-1-6.pdf)
- TGn (TGnInteropTP_2.8.pdf)
- WPS (Wi-Fi_Protected_Setup_Test_Plan_v2.0.15.pdf)
- Wi-Fi® Direct (wfa_wifi_direct_interoperability_test_plan_version_1.3.pdf)

1.1 Definition of the Device Under Test

A precise selection of the definition for device under test (DUT) impacts the WFA test plans. A slow or weak host processor can impact on the performance of the device. In such cases, an application specific device (ASD) document is required.

1.1.1 Define Your Access Points Under Test

For example, the access points under test (APUT) is a mobile Wi-Fi AP that supports both 2.4-GHz and 5-GHz bands with 20-MHz channel width on 2.4 GHz and 40 MHz on 5 GHz. The APUT only supports personal authentication.

1.1.2 Define Your Station Under Test

For example, the station under test (SUT) is a Wi-Fi station that supports 2.4-GHz and 5-GHz bands with 40-MHz channel width in 5 GHz.

The SUT can be categorized according to the following types of devices:

- Cellular
- Audio
- Terminal audio
- Network camera
- PDA
- DLNA multimedia adapter
- VOIP phone
- Wi-Fi phone
- Converged cellphone
- DVD player
- Tablet PC

1.2 Basic System Test Configuration

Figure 1 shows the basic test configuration for infrastructure tests and a physical connection diagram (there are two logical networks to separate chariot traffic from configuration traffic).

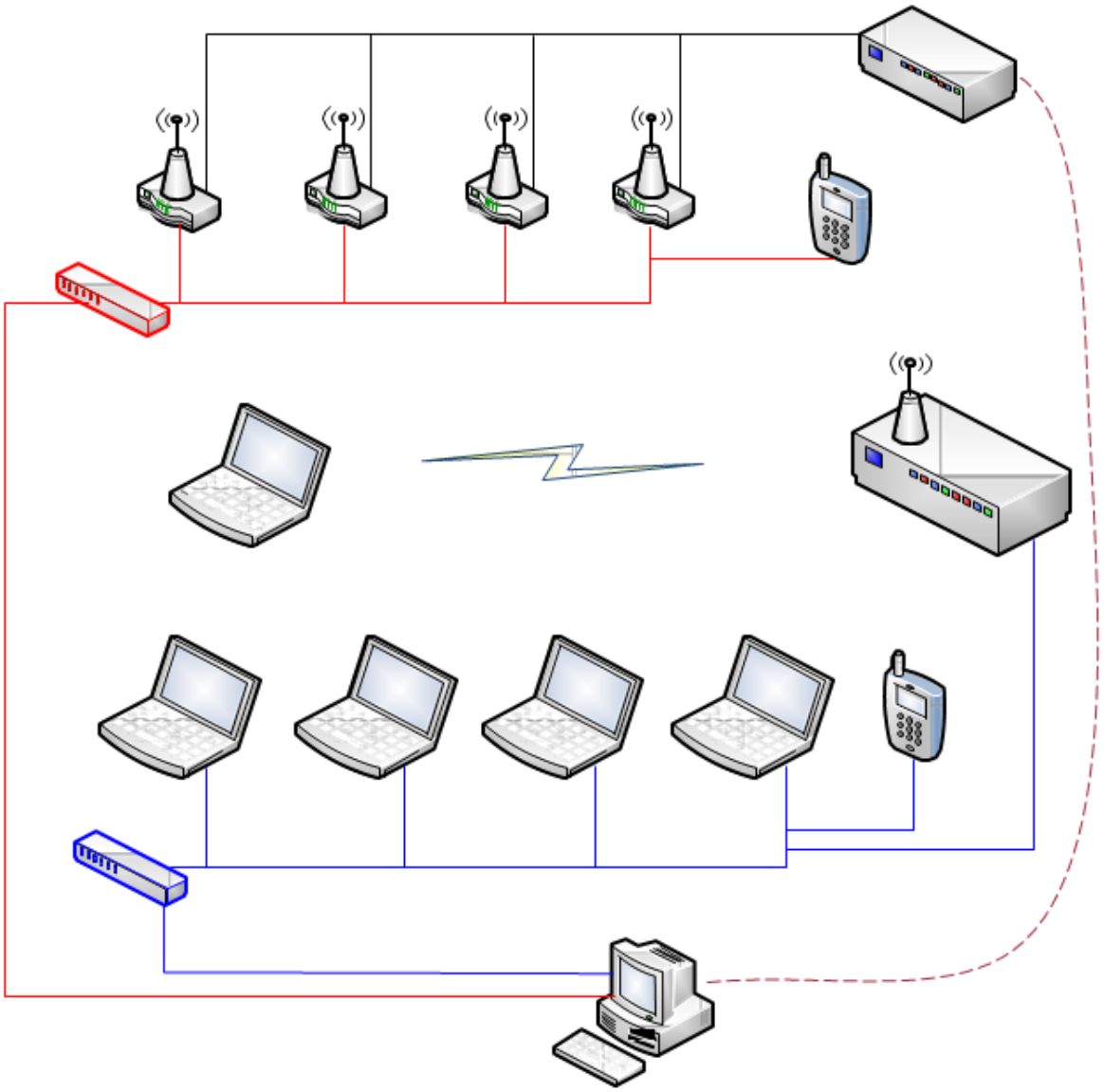
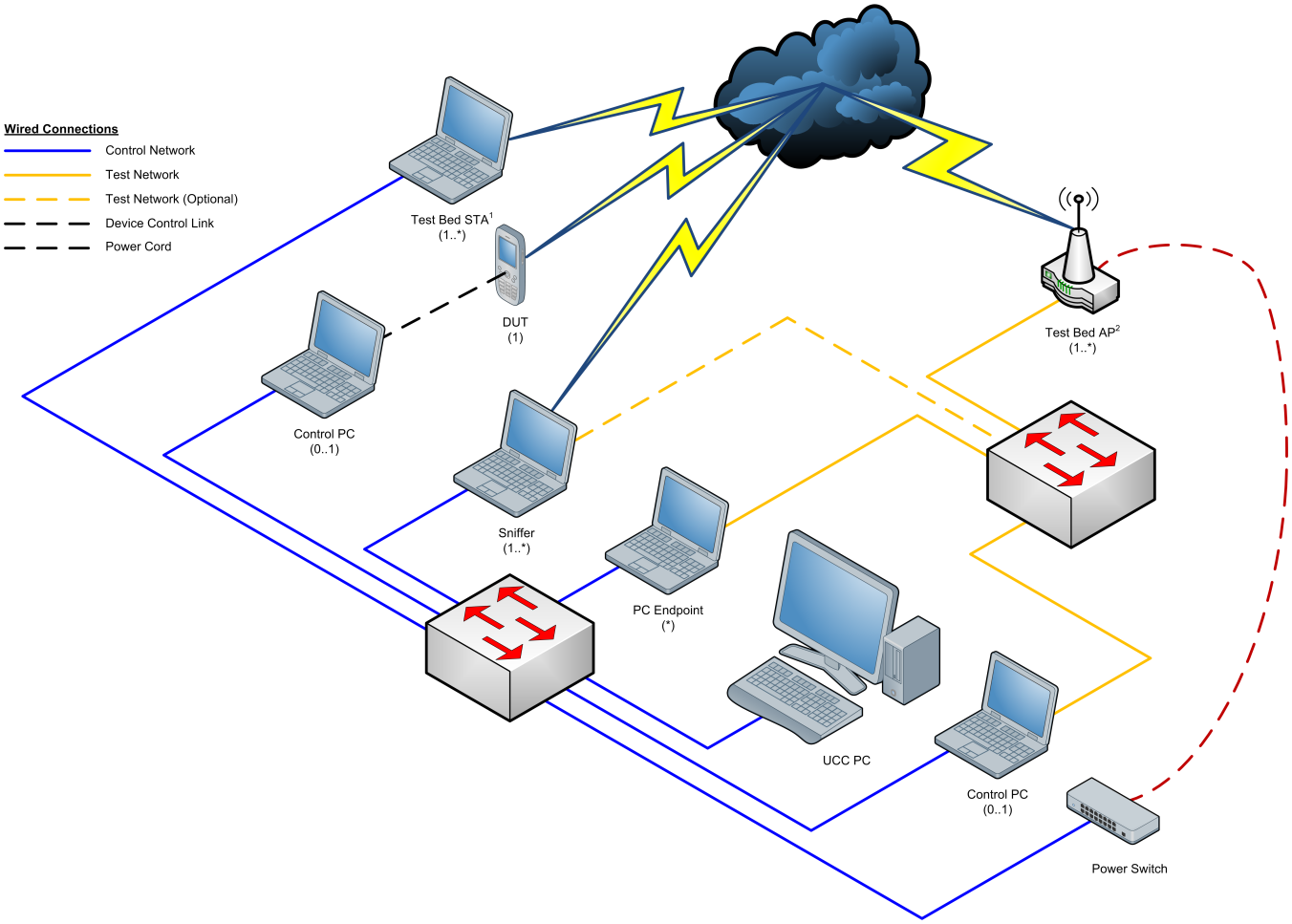


Figure 1. Chariot Basic System Test Configuration

The stations and the IxChariot™ server operate as IxChariot endpoints, with the tests configured and controlled from the IxChariot console. The IxChariot console and three RADIUS™ servers can run on the same machine. The DEVICESCAPE™ runs on a Linux® OS machine. WLAN stations (STAs) run on Windows XP® with SP2. In Figure 1, the RADIUS servers are DEVICESCAPE, HostAPd, Radiator, and Microsoft®. When a DUT is tested in a station mode, only the SUT is typically present. When the DUT is tested in the AP mode, only the APUT is typically present. Use the Wi-Fi Test Suite (WTS) approach as an alternative test bed arrangement to automate the certification tests. Figure 2 shows the standard configuration of the unified CAPI console (UCC).



A A Test Bed STA may also be a converged, nonconverged voice or other device with or without a control PC.

B If used, the control PC uses the Test Network as a Control Network for Test Bed APs before and after testing

C Multiplicity Notation

- (*) 0 or more
- (0.1) 0 or 1
- (1) 1
- (1 *) 1 or more

For example: The UCC PC connects directly to the DUT or through a control PC; each control PC connects to 1 and only 1 device.

Figure 2. Sigma System Test Configuration

2 How to Prepare the DUT for WFA Certification

The following sections describe the testing methodology and guidelines for preparing the product.

2.1 Recommendations from TI

- Read this document before to externally certifying.
- Perform precertification testing on the DUT of the customer.

2.2 WFA Certification Process

To perform WFA certification, do as follows:

1. Register as a WFA member at https://www.wi-fi.org/about/become-member.
2. Select an authorized lab for testing and certifying your product from http://www.wi-fi.org/authorized_labs.php.
3. Choose the testing programs (STA, AP, or p2p) for your device according to its capabilities and purpose (for example, a p2p device must run Wi-Fi TGn for STA, WPS for STA, Wi-Fi Direct, and can skip AP testing programs and STA-WMM-PS certification).
4. Ensure you mark the capabilities of the DUT because this impacts the optional tests that must be executed like siso, mimo, 20 MHz, 20/40 MHz, enterprise security, and 5 GHz. (If your DUT supports 20/40 MHz in 2.4 GHz, test 5.2.48 must be executed.)

2.3 Preparation Process for Certifying the DUT

2.3.1 Prerequisites for Certification

- The DUT must be fully functional.
- The performance of the DUT must be similar to what TI publishes in the test results.
- The DUT must pass precertification tests (if there are modifications to the software or hardware due to TI configuration [host processor, major code changes, and so forth], this step is mandatory).
- The correct device category most be chosen (this impacts on the TP threshold).
- The DUT file system must be ready to read and write (the file system must save modifications after reboot so the customer or lab engineer can download files to it with ftp, tftp, sdcard or any other procedure).

2.3.2 Applications Required for Certification

- WTS—Download the WTS files from www.ti.com.

  NOTE: The WTS must be adapted to the platform environment of the customer.

- IxChariot Endpoint—Download from www.ixiacom.com (not required)

  NOTE: You can substitute iperf for IxChariot. iperf can be downloaded for free.

- IW—Download IW from an open source community and compile it to the environment of the customer
- Busybox—Download Busybox from an open source community and compile it to the environment of the customer.

2.3.3 DUTs at the WFA Lab

If you must ship two DUTs to the WFA lab, ensure that those are tested devices.

Include operation instructions when sending the devices to the lab.

TI recommends supporting the WFA lab during the certification process (during the initial phase).

3 The Testing Tools, Methodology, and Approach

This section defines tools, methodology, and approach for testing during WFA certification.

3.1 IxChariot Software

IxChariot software from IXIA can be used. The IxChariot includes a large set of standard, editable scripts that can be used to define a particular traffic flow between two endpoints. The IxChariot console (a separate machine from the units under test) manages the definition, test configuration, test execution, and results reporting of the scripts.

Unless otherwise specified, use default parameters. Typically, tests run for 1.5 minutes.

3.1.1 IxChariot Scripts

Change the scripts used during the testing as follows:

- Change the buffer size to 1456 bytes.
- Change the data rate (throughput) according to the ASD document (if it exists).
- Change the packet size in the InquiryL.scr script to 1000B to align with the definition of WTS.

3.1.2 Environment Preparation on DUT

To prepare the environment, do as follows:

1. Upload the IxChariot file and extract (perform once and skip if already done).
   cd /home/root/chariot
   tftp -g -r endpoint.tar 20.1.1.10
   tar –xvf endpoint.tar
2. Start IxChariot Endpoint (after every reboot).
   cd /home/root/chariot
   ./endpoint &

3.2 WTS Software

As an alternative to IxChariot, the WTS automation suite can be used. This tool suite provides configuration, test control, traffic generation, and results analysis services. The test plan can be automated through the WFA-distributed WTS command scripts and the WTS-unified CAPI console. Additional information is available on the test tools pages at http://www.ti.com/tool/WILINK8-WIFI-NLCP and http://www.ti.com/tool/WILINK8-WIFI-MCP8 (WILINK8-WIFI-SIGMA is the section).

3.2.1 Environment Preparation on DUT

The files follow:

For p2p certification: WTS9dut_nlcp_p2p.tar

For TGn and WMM-PS certifications: WTS9dut_nlcp_tgn_and_wmmps.tar

To prepare the environment, do as follows:

1. Create a directory on the DUT to hold the package files (perform once and skip if already done).
   For example:
   mkdir/home/root
   cd/home/root
2. Upload the WTS file to the directory (use ftp/tftp/sdcard).
   For example: tftp -g -r WTS9dut_nlcp_xxxx.tar 20.1.1.10
3. Extract ti_WTS_files.tar.
   tar -xvf WTS9dut_nlcp_xxxx.tar

   NOTE: This operation create a test_engine folder with the WTS files.

4. Start the WTS on the DUT (perform after every reboot).
   cd /home/root
   ifconfig eth0 <ethernet ip address> up
   cd /home/root/test_engine
   killall wfa_ca
   killall wfa_dut
   ./wfa_dut eth0 8000 &
   export WFA_ENV_AGENT_IPADDR=<ethernet ip address>
   export WFA_ENV_AGENT_ PORT=8000
   ./wfa_ca eth0 9000 &

4 TGn SUT Certification

4.1 Basics

Test Plan: TGnInteropTP_2.8.pdf

ASD document number: None

Testing tool: WTS and chariot are available.

4.1.1 SUT Role Start

To start the SUT role, do as follows:

1. Start the driver on the DUT (perform after every reboot).
   cd /home/root
   sh ./sta_start.sh
2. Configure current date (perform after every reboot).
   Date <MMDDHHMMYYYY> (example: date 110712252011 for 07Nov2011 12:25)

4.2 Special Instructions

- Test 5.2.15 Pre-authentication
  Add background scan in the network configuration profile:
  wpa_cli -iwlan0 set_network 0 bgscan '"learn:5:-65:5"'
- Test 5.2.24 (test 2)
  The maximal configurable clock for STAUT is 010101012038 (1-Jan 2038)
- Test 5.2.41 Greenfield
- Force MediaTek AP to work with GF. WTS does not configure it properly.

5 TGn APUT Certification

5.1 Basics

Test Plan: TGnInteropTP_2.8.pdf

ASD document number: None

Testing tool: WTS and chariot are available.

5.1.1 APUT Role Start

Start the driver on the DUT (perform after every reboot).

cd /home/root

sh ./ap_start.sh

5.2 6.2 WTS Preparations

5.2.1 Setup Topology

Figure 3 shows the topology of the setup.

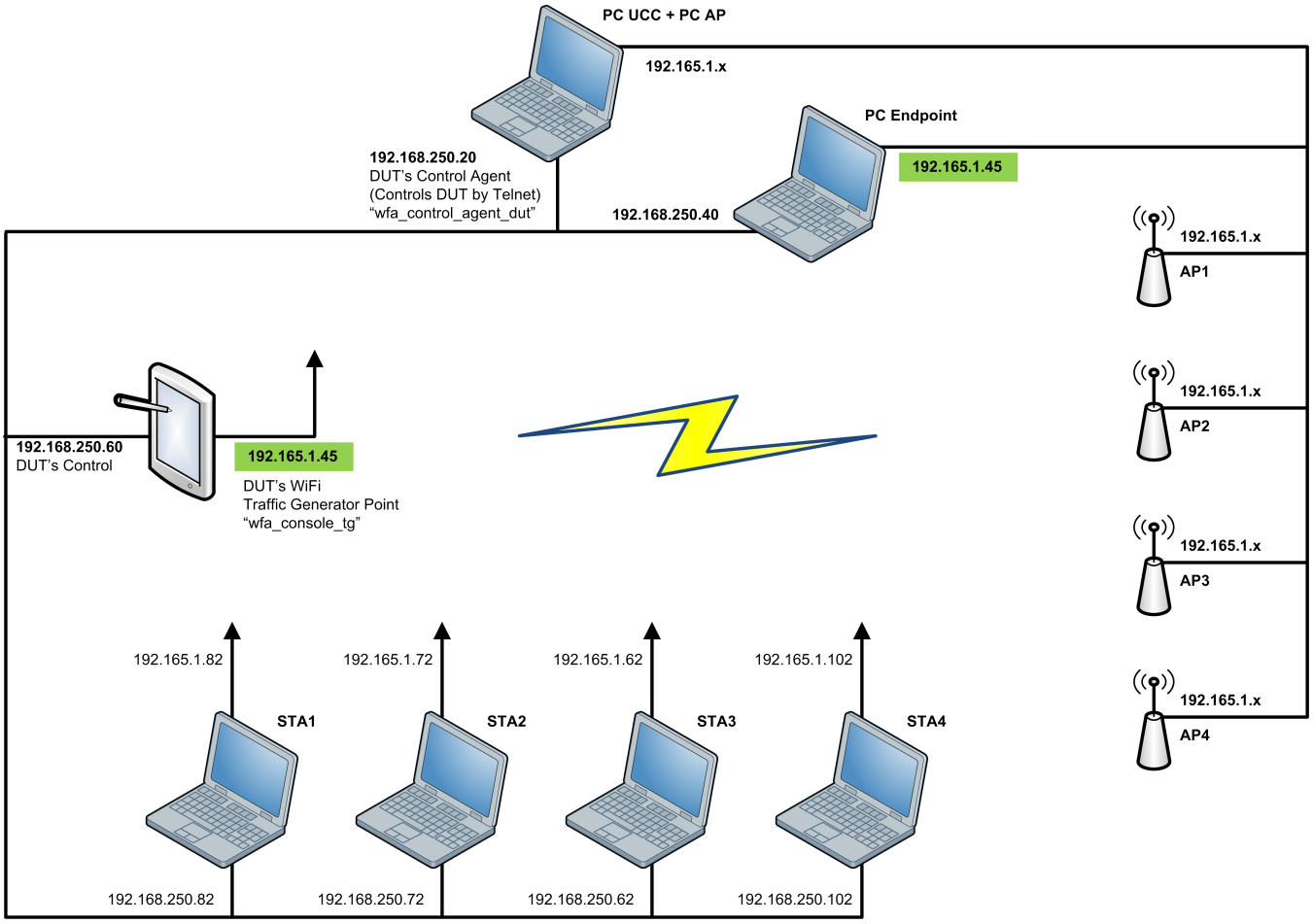


Figure 3. Setup Topology

The APUT is running as traffic generator.

Update init_802.11n.txt accordingly:

########## PC Endpoint (WFA traffic generator console) #####

info!Connecting to PC Endpoint!

Control IP Address for Console

wfa_console_ctrl!ipaddr= **APUT's ETH IP**,port=9000!

Traffic generator IP Address for Console

wfa_console_tg!**APUT's WLAN IP**!

5.2.2 AP Configuration Agent Changes

- TIWilinkAPInfo.tcl
  1. Place this file in CA PC under include\AP.
  2. Update the Control IP address (eth0) and Power Switch port of the DUT.
  3. If the device has login and password (through telnet), update it:
     (a) Set TIWiLinkAPLogin root (through telnet the password is root).
     (b) Set the TIWiLinkAPPassword password.
- TIWilinkAPCLI.tcl
  1. Place this file in CA PC under src\DevSpec\AP.
  2. Change the path in TIWiLinkAPCommands array to the location of the DUT WTS files on your device:

```
array set TIWiLinkAPCommands { \
CFGKEY "cd /home/root/test_engine/; sh ./ap_cfgkey.sh "\
DELKEY "cd /home/root/test_engine/; sh ./ap_delkey.sh "\
ADDTOKEY "cd /home/root/test_engine/; sh ./ap_addtokey.sh "\
DELFROMKEY "cd /home/root/test_engine/; sh ./ap_delfromkey.sh "\
RECONFIG "cd /home/root/test_engine/; sh ./ap_reconfig.sh "\
MISC ""
}
```

Update the following control agent files under Wi-FiTestSuite_APConfigurationAgent-Windows_v9.0.0\AP_ControlAgent\include \DUTInfo.tcl your DUT mode (A/B/G).

1. Add the following line to the APs list under Wi-FiTestSuite_APConfigurationAgent-Windows_v9.0.0\AP_ControlAgent\src\CLI.tcl:source [file join $path "src\\DevSpec\\AP\\" TIWiLinkAPCLI.tcl]
2. Add the following line to the APs list under Wi-FiTestSuite_APConfigurationAgent-Windows_v9.0.0\AP_ControlAgent\src\Common.tcl: source [file join $path "include\\AP\\" TIWilinkAPInfo.tcl]
3. Add the following line under Wi-FiTestSuite_APConfigurationAgent-Windows_v9.0.0\AP_ControlAgent\src\TelnetLib.tcl: TIWiLinkAP 0\
4. Add 11b configuration for Atheros AP: UnderWi-FiTestSuite_APConfigurationAgent-Windows_v9.0.0\AP_ControlAgent\src\ DevSpec\AP\AtherosAPCLI.
5. Search for *# check the 11n wireless*.
6. Replace the *if* with the following:

```
if { [regexp -nocase "NA" $Value match]} {
set channelInfo "11NAHT"
} elseif {[regexp -nocase "NG" $Value match]} {
set channelInfo "11NGHT"
} elseif {[regexp -nocase "11B" $Value match]} {
set channelInfo "11B"
} elseif {[regexp -nocase "11b" $Value match]} {
set channelInfo "11B"
} elseif {[regexp -nocase "11G" $Value match]} {
set channelInfo "11G"
} elseif {[regexp -nocase "11a" $Value match]} {
set channelInfo "11A"
}
```

5.3 Special Instructions

The access point is configured through hostapd text configuration file hostapd.conf. Use editor *vi* to change the values of the parameters: vi /home/root/hostapd.conf.

Security configuration options:

Open – no security:

#wep_default_key=0

wpa=0

WEP40:

wep_default_key=0

wep_key0=9876543210

WPA2-PSK:

wpa=2

wpa_passphrase=12345678

wpa_key_mgmt=WPA-PSK

rsn_pairwise=CCMP

Mixed WPA+WPA2:

wpa=3

wpa_passphrase=12345678

wpa_key_mgmt=WPA-PSK

wpa_pairwise=TKIP

rsn_pairwise=CCMP

WTS does not always configure STAs properly. Verify that the STAs are configured as required in the test.

If the STAs are not configured properly, configure them manually as follows:

1. Open the STA log file: C:\WFASTA.log.
2. Search for the command.
3. Open the following command line: cd to C:\WFA\CLIs\<STA Name>
4. Run the command.

   Sometimes the network must be disabled and enabled for changes to take effect.

   - For Atheros STA
     (a) Set RTS threshold and Frag parameters are set through the regedit (Start→ Run→ Window→ type regedit).
     (b) Navigate to the Atheros network interface cards (NICs) in the registry editor: My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{nics}
     (c) Choose the folder that contains the parameters.
     (d) Double-click RTS or Frag parameter to change them.
     (e) Set the default value for RTS threshold at 2347.
     (f) Set the default value for fragmentation at 2346.
     (g) Disable the network.
     (h) Enable the network.
   - For Intel STA– To enable or disable the WMM through the registry editor, do as follows:
     (a) Navigate to the list of the parameters.

(b) Double-click the TGeEnableBits parameter.

(c) Set the parameter to 1 to enable or set it to 0 to disable.

NOTE: If the parameter is missing, do as follows:

(i) Right-click the screen.

(ii) Click DWORD.

(iii) Modify the name to TGeEnableBits

- Test 4.2.7

  This test is not supported (test 4.2.8 tests the same scenario with PSK).
- Test 4.2.10: Multicast traffic, when using WTS.
  1. Add the multicast route to the APUT as follows:

     route add –net 224.0.0.0 netmask 240.0.0.0 dev wlan1

     route add default wlan1
  2. Verify that WTS configures Power Save on Broadcom STA.

     (a) Right-click Network Drive.

     (b) Click Properties.

     (c) Click Configure.

     (d) Click Advanced Tab.

     (e) Click Power Save Mode.

     (f) Change Fast to Enable.
  3. Disable Power Save on Broadcom STA.
- Test 4.2.28

  Requires reset before execution.
- Tests 4.2.9, 4.2.31, and 4.2.32

  Because of limitations of using APUT as a traffic generator for the stream of APUT and external devices stream. Traffic must be generated by chariot or Iperf in these tests. For test 4.2.9, send a ping manually.

6 Wi-Fi Direct Certification

6.1 Basic Information

Test Plan: WFA Wi-Fi Direct Interoperability Test Plan Version 1.3.pdf

ASD document number: None

Testing tool: WTS

6.1.1 DEVUT (P2P) Role Start

- The Dynamic IP address is required for Wi-Fi direct connections.
  1. Configure the DHCP server with range of IP addresses in the udhcpd.conf file.
  2. Align the WTS script of the DUT that starts the DHCP server for the GO role with the DHCP server on your platform.

NOTE: The files to edit follow:

test_engine/p2p_dhcp_server.sh

test_engine/p2p_dhcp_client.sh

test_engine/udhcpd_p2p.conf

  3. After establishing a P2P connection, verify that the DEVUT receive an IP from DHCP server.
- Start the driver on the DUT (perform after every reboot):

cd /home/root sh

./sta_start.sh

7 WMM-PS SUT Certification

7.1 Basics

Test Plan: WMM_Power_Save_Testplan_V_2-1-6.pdf

ASD document number: None

Testing tool: WTS

7.1.1 SUT Role Start

Start the driver on the DUT (perform after every reboot):

cd /home/root sh

./sta_start.sh

7.2 Special Instructions

WTS removes power save configuration after connection.

1. Modify the following connection scripts:
   - STA-Config-WMMPS-STAUT-VoVi.txt
   - STA-Config-WMMPS-STAUT.txt
   - STA-Config-WMMPS-WPA2-STAUT.txt
   - STA-Config-WMMPS-STAUT_Cap_Asso.txt
   - STA-Config-WMMPS.txt
   - STA2-Config-WMMPS.txt
   - STA-Config-WMMPS-WPA2.txt
   - STA2-Config-WMMPS-WPA2.txt
   - STA-Config-WMMPS-VoVi.txt
   - STA-Config-WMMPS-Legacy.txt

   NOTE: These files mark the command that turns off Power Save and add a command that turns it on:

   wfa_control_agent_dut!sta_set_pwrsave,interface,$1,mode,on!DEFAULT

2. Turn on APs manually.
3. For the Cisco AP, delete SSID profiles before running a test.
4. Change the band of tests L.1, M.K, and M.W to match the test plan for the MasterTestInfo.xml.

For detailed instructions, see Sigma WMM-PS beta release v1_0_8.

8 WPSv2 SUT Certification

8.1 Basics

Test Plan: Wi-Fi Protected Setup Test Plan_v2-0-15.pdf

ASD document number: None

Testing tool: Manual

8.2 Device Preparation

8.2.1 SUT Role Start

- Start the driver on the DUT (perform after every reboot).
  cd /home/root
  sh ./sta_start.sh
- Set a static IP address on the wireless interface.
  ifconfig wlan0 X.X.X.X netmask X.X.X.X

8.3 Special Instructions

- If your DUT has a UI, Wi-Fi requires that WPS testing occurs through UI.
- The wpa_supplicant configuration utility wpa_cli includes several commands used for WPS tests:
  – wpa_cli -iwlan0 wps_pin any – to start WPS PIN method
  – wpa_cli -iwlan0 wps_pbc – to start WPS Push Button Configuration

9 WPSv2 APUT Certification

9.1 Basics

Test Plan: Wi-Fi Protected Setup Test Plan_v2-0-15.pdf

ASD document number: None

Testing tool: Manual

If your device is MAPUT, run tests mandatory for Mobile-APUT.

If your device is APUT, run tests that are mandatory for APUT. See Section 9.4.

9.2 Device Preparation

9.2.1 APUT Role Start

1. Start the driver on the DUT (perform after every reboot).
   cd /home/root
   sh ./ap_start.sh
2. Set a static IP address on the wireless interface.
   ifconfig wlan1 X.X.X.X netmask X.X.X.X

9.3 Special Instructions

- If your DUT has a UI, Wi-Fi requires that WPS testing occur though UI.
- The APUT is configured through hostapd configuration file hostapd.conf. Use editor *vi* to change value of parameters:

  vi /home/root/hostapd.conf
- Security configuration options:

  Open – no security:

  wpa=0

  WEP40:

  wep_default_key=0

  wep_key0=9876543210

  WPA2-PSK:

  wpa=2

  wpa_passphrase=12345678

  wpa_key_mgmt=WPA-PSK

  rsn_pairwise=CCMP

  Mixed WPA+WPA2:

  wpa=3

  wpa_passphrase=12345678

  wpa_key_mgmt=WPA-PSK

  wpa_pairwise=TKIP

  rsn_pairwise=CCMP
- Restart the APUT to get the new parameters:

  sh ap_stop.sh

  sh ap_start.sh
- The hostapd configuration utility hostapd_cli includes several commands that can be used for WPS tests:

  hostapd_cli -iwlan1 wps_pbc

  hostapd_cli -iwlan1 wps_pin any
- Test 4.1.13

  hostapd_cli -iwlan1 -p /home/root/wlan1 wps_pin <enrolee's UUID> <PIN> 300 <enrolee's MAC Address>
- Tests 4.2.1, 4.2.2, 4.2.4– PIN's integrity:

  Incorrect PIN

  – hostapd_cli -iwlan1 –p/home/root/wlan1 wps_check_pin <abnormal PIN>

  Correct PIN

  – hostapd_cli -iwlan1 -p /home/root/wlan1 wps_pin any <correct PIN>

9.4 APUT Additional Tests (not for MAPUT)

9.4.1 Device Prerequisites

Must perform these tests if your device is a bridge.

Must have additional hostapd.conf parameters.

Must connect the Ethernet cable to the data switch.

9.4.2 Additional hostapd.conf Parameters

To add additional hostapd.conf parameters, do as follows:

1. Comment all WPS parameters in the hostapd.conf file.
2. Add the following parameters for out-of-box mode: (see example for a TI AP)
   - wps_state=1
   - uuid=12345678-9abc-def0-1234-56789abcdef0
   - device_name=Sitara
   - manufacturer=TexasInstruments
   - model_name=TI_Connectivity_module
   - model_number=wl18xx
   - serial_number=12345
   - device_type=6-0050F204-1
   - config_methods=virtual_display virtual_push_button keypad
   - ap_pin=12345670
   - upnp_iface= [Device's bridge interface]
   - friendly_name=TI Access Point
   - manufacturer_url=http://www.ti.com/
   - model_description=TI wireless Access Point
   - model_url=http://www.ti.com/model/
   - wps_rf_bands=ag

9.4.3 Special Commands

- To generate a random APUT pin:
  - hostapd_cli wps_ap_pin random
- To get current APUT configuration:
  - hostapd_cli get_config
- To configure APUT with new parameters:
  - hostapd_cli wps_config <new SSID> <auth> <encr> <new key>
    Examples:
  - hostapd_cli wps_config testing WPA2PSK CCMP 12345678
  - hostapd_cli wps_config "no security" OPEN NONE ""
  - <auth> must be one of the following: OPEN WPAPSK WPA2PSK
  - <encr>must be one of the following: NONE WEP TKIP CCMP

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265