WL1271 System Test Guidelines User's Guide

Literature Number: SPRUGT7
January 2010

Contents

List of Figures

List of Tables

Revision History

Version	Date	Description
1.0	November 2009	Release

Reference Documents

The documents listed below provide complementary specifications and information for the device:

- None

About This Document

This document describes the recommended system test guidelines for the OMAP3 and the 1271 chipset. It requires basic knowledge of Bluetooth™ (BT) and Wireless Local Area Network (WLAN) specifications, and provides a low-cost setup.

The document contains the following chapters:

- **Chapter 1, Test Strategy,** page 7, describes the WiLink system that is tested.
- **Chapter 2, Test Setup,** page 9, describes the recommended test setup and testing tools for performing the tests.
- **Chapter 3, Test Plan,** page 13, describes the various tests that are performed for the testing strategy.
- **Appendix A, Using Iperf,** page 37, describes how to the use the Iperf application to generate traffic for testing.
- **Appendix B, QoS Support in Windows,** page 41, describes how to add a key to the Windows registry to provide QoS support.

Note: Throughout this document, characters in **blue** represent output form the CLI and the kernel. Characters in **red** indicate what the user types. Characters in **black** show the CLI menu.

Test Strategy

Topic

1.1 Tested System

The system tested is the WiLink 6 WLAN and BT firmware running on WL1271 hardware (HW). These components are controlled by a driver running on an OMAP™ platform. The system is operated by an application running on a PC called **wlan_cu**.

The interface between the OMAP board and the WL1271 is a four-bit SDIO.

Test Setup

Topic Page

2.1 Recommended Test Setup

The following figure shows the recommended test setup.

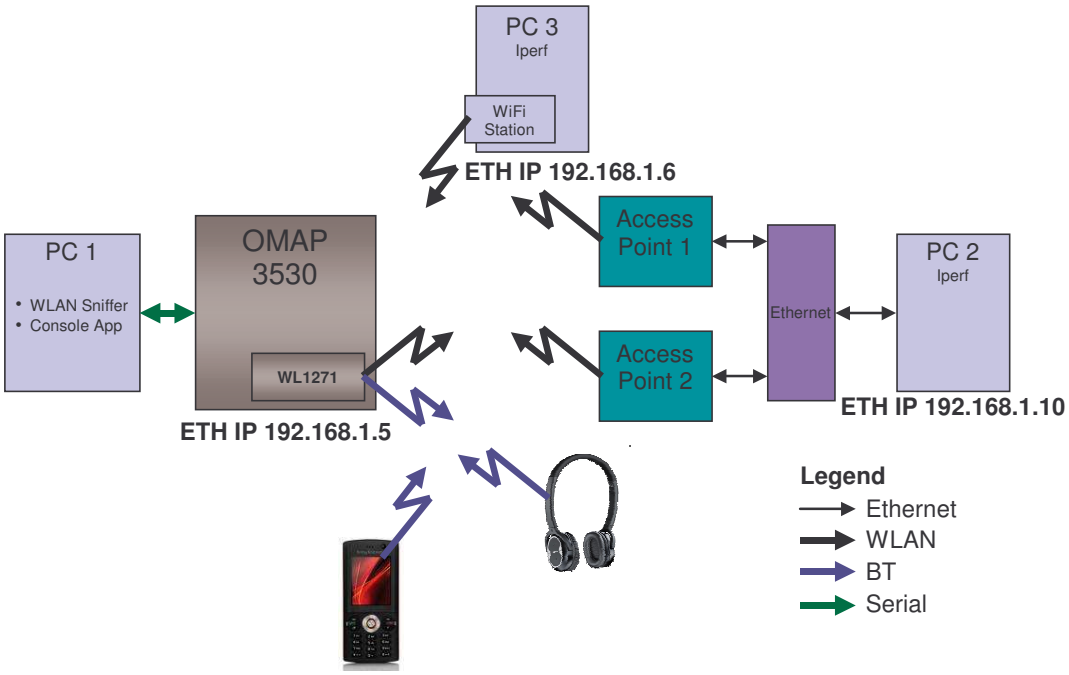

Figure 1: Recommended Test Setup

2.2 Testing Tools

The following tools are required for testing:

- Console application.
- WLAN Sniffer: The sniffer is an IEEE 802.11 protocol analyzer, capable of receiving and decoding WLAN traffic over the air.
- Iperf: A traffic generator. The Iperf tool generates data at a given rate. It runs as an embedded components on the host. Iperf supports transport Layer 4 TCP and UDP protocols.
- Two access points (APs).
- One WiFi station (STA).
- BT Advanced Audio Distribution Profile (A2DP) sink (BT headsets support A2DP).
- Handset with BT that supports FTP.

2.3 Test Categories

The table below summarizes the test categories that are fully or partially described in this document.

Table 1: Test Categories

Test Category	Covered in This Document	Not Covered in This Document
Functionality	X	
Security	X	
Performance	X	
Basic Features	X	
Reliability	X	
Stability	X	
Radio Frequency (RF) Performance		X
Interoperability		X
Certification Tests		X

This page was intentionally left blank.

Test Plan

Topic **Page**

3.1 Security

The Security test validates the use of security connections, including WEP, WPA-PSK and WPA2-PSK, as well as the behavior of the system under test (SUT) when attempting to connect with incorrect security settings.

3.1.1 WEP

- Configure the AP and SUT to WEP with Open System authentication using a 64-bit key index 1. You may run the following commands on the wlan_cu:
  - / Privacy Authentication 0
  - / Privacy encRyption 1
  - / Privacy Wep add 0123456789 1 1
  - / Connection Connect YourSSID

```
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassph
rase, cerTificate, Supplicant/, Wep/
a 0

Setting privacy authentication to 0
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassph
rase, cerTificate, Supplicant/, Wep/
r
0 - None, 1 - WEP, 2 - TKIP, 3 - AES

.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassph
rase, cerTificate, Supplicant/, Wep/
r 1

Setting privacy encryption to 1

.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassph
rase, cerTificate, Supplicant/, Wep/
w

.../Wep> Add, Remove, Get default key id
a

Add WEP: Add <Key Value (0..64 chars)>
<Tx Key Index)>
<Default Key (yes - 1 /no - 0)>
[key type (hex | text) [hex] (0..5 chars)]

.../Wep> Add, Remove, Get default key id
a 88f2c58643 1 1 hex
```

```
.../Connection> Bssid_list, Connect, Disassociate, Status, Full_bssid_list, wPs/
c peterpan


14
Trying to associate with SSID 'peterpan'
OK
************ NEW CONNECTION ************
-- SSID  = peterpan
-- BSSID = 0-f-b5-e6-ed-fc
****************************************
Associated with 00:0f:b5:e6:ed:fc
CTRL-EVENT-CONNECTED - Connection to 00:0f:b5:e6:ed:fc completed (reauth) [id=14
id_str=]
```

- Configure the IP address on the SUT using the following command from the Linux shell:

```
#
# ifconfig tiwlan0 192.168.1.5 netmask 255.255.255 up
#
```

- Send a ping from the PC behind the AP to the SUT.

Expected result:

The SUT successfully connects the AP, and the SUT replies to the ping.

3.1.1.1 WPA PSK

- Configure the AP and SUT to WPA authentication with TKIP encryption. You may run the following commands on the wlan_cu:
  - / Privacy Authentication 4
  - / Privacy encRyption 2
  - / Privacy Psk 12345678
  - / Connection Connect SSID

```
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassphrase, cerTificate, Supplicant/, Wep/
a 4
Setting privacy authentication to 4
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassphrase, cerTificate, Supplicant/, Wep/
r
0 - None, 1 - WEP, 2 - TKIP, 3 - AES
Encryption = 0
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassphrase, cerTificate, Supplicant/, Wep/
r 2
Setting privacy encryption to 2
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassphrase, cerTificate, Supplicant/, Wep/
p osopanda


Setting PSKPassphrase to osopanda
```

```
\> Driver/, Connection/, Management/, Show/, Privacy/, scAn/, roaminG/, qOs/, poWer/,
eVents/, Bt coexsistence/, Report/, dEbug/, biT/, aboUt, Quit
c c peterpan

.../Connection> Bssid_list, Connect, Disassociate, Status, Full_bssid_list, wPs/
Trying to associate with SSID 'peterpan'
OK
Associated with 00:0f:b5:e6:ed:fc
************ NEW CONNECTION ************
-- SSID  = peterpan
-- BSSID = 0-f-b5-e6-ed-fc
****************************************
WPA: Key negotiation completed with 00:0f:b5:e6:ed:fc [PTK=TKIP GTK=TKIP]
CTRL-EVENT-CONNECTED - Connection to 00:0f:b5:e6:ed:fc completed (reauth) [id=23
id_str=]
```

- Send a ping from the PC behind the AP to the SUT.

Expected result:

The SUT successfully connects the AP, and the SUT replies to the ping.

3.1.1.2 WPA2 PSK

- Configure the AP and SUT to WPA2 authentication with AES encryption. You may run the following commands on the wlan_cu:
  - / Privacy Authentication 7
  - / Privacy encRyption 3
  - / Privacy Psk 12345678
  - / Connection Connect SSID

```
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassph
rase, cerTificate, Supplicant/, Wep/
a 7
Setting privacy authentication to 7
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassphrase, cerTificate, Supplicant/, Wep/
r 3
Setting privacy encryption to 3
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassphrase, cerTificate, Supplicant/, Wep/
p aabbccddee
Setting PSKPassphrase to aabbccddee
.../Privacy> Authentication, Eap, encRyption, Keytype, Mixedmode, aNywpamode,
Credentials, pskPassphrase, cerTificate, Supplicant/, Wep/
/ c c peterpan
\> Driver/, Connection/, Management/, Show/, Privacy/, scAn/, roaminG/, qOs/, poWer/,
eVents/, Bt coexsistence/, Report/, dEbug/, biT/, aboUt, Quit
.../Connection> Bssid_list, Connect, Disassociate, Status, Full_bssid_list, wPs/
0
Trying to associate with SSID 'peterpan'
OK
```

```
Associated with 00:0f:b5:e6:ed:fc
************ NEW CONNECTION ************
-- SSID  = peterpan
-- BSSID = 0-f-b5-e6-ed-fc
**************************************
WPA: Key negotiation completed with 00:0f:b5:e6:ed:fc [PTK=CCMP GTK=CCMP]
CTRL-EVENT-CONNECTED - Connection to 00:0f:b5:e6:ed:fc completed (auth) [id=0 id_str=]
```

- Send a ping from the PC behind the AP to the SUT.

Expected result:

The SUT successfully connects the AP, and the SUT replies to the ping.

3.1.1.3 Negative Security Test

- Configure the AP and SUT to WPA2 authentication with AES encryption.
- Configure the SUT to use a different key than that defined on the AP.
- You may run the following commands on the wlan_cu:
  - / Privacy Authentication 7
  - / Privacy encRyption 3
  - / Privacy Psk 1234567**9**
  - / Connection Connect SSID
- Send a ping from the PC behind the AP to the SUT.

Expected results:

The SUT tries to connect to the AP, but connection cannot be established. The SUT does not reply to the pings.

3.2 Functionality

The Functionality test category validates the system-level functionality of the features and overall system performance. To verify performance compliance with specifications and/or predefined system requirements, each feature is tested in several different scenarios.

Each feature is tested according to a specified, detailed test method. The test description includes the tests described below.

3.2.1 Scanning

The Scanning test validates the ability of the SUT to discover and track APs and STAs within its range in various modes.

3.2.1.1 Application Scan

The Application Scan is executed by the application level upon the driver. This scan inserts the APs in the SUT range into the Basic Service Set ID (BSSID) list. This test performs the following operations:

- Enables more than one AP to run in your environment.
- Runs an application scan on the SUT. You may use the following commands from the wlan_cu:
  - / scAn Start

```
\> Driver/, Connection/, Management/, Show/, Privacy/, scAn/, roaminG/, qOs/, poWer/,
eVents/, Bt coexsistance/, Report/, dEbug/, biT/, aboUt, Quit
a
.../scAn> Start, sTop, Wextstart, configApp/, configpEriodic/, configPolicy/
s
Application scan started
```

- On the WLAN sniffer, observes that the SUT sends probe requests when running the application scan.
- Reads the BSSID list. You may use the following commands from the wlan_cu:
  - / Connection Bssid_list

```
.../Connection> Bssid_list, Connect, Disassociate, Status, Full_bssid_list, wPs/
b

BssId List: Num=1
         MAC         Privacy Rssi  Mode    Channel    SSID
 00.0f.b5.e6.ed.fc     0    -62  Infra      3        peterpan
```

- Turns off one of the APs and runs the scan command again.

  Reads the BSSID list.

Expected result:

The SUT removes the APs from the BSSID list.

3.2.1.2 Background Scan

The Background Scan runs in order to discover and track APs with the same SSID and insert them into the AP Neighbor list that the SUT uses for roaming. This test performs the following operations:

- Enables more than one AP to run in your environment.
- Configures the same Service Set Identifier (SSID) for all APs with WPA2 security and the same Pre-shared Key (PSK) by running a Scan command . You should see two APs with the same SSID in your BSSID list.

```
.../Connection> Bssid_list, Connect, Disassociate, Status, Full_bssid_list, wPs/
b

BssId List: Num=2
         MAC         Privacy Rssi  Mode    Channel    SSID
 00.0f.b5.e6.ed.fc     1    -65  Infra      6        peterpan
*00.23.69.37.c3.9f     1    -65  Infra     11        peterpan
```

- Connects the SUT to one of the APs.

- Your SUT is configured by default to run a background scan. You may review it using the following command:
  - / scAn configPolicy Display

```
.../configPolicy> Global, Band/, Display, cLear, Store, bsslisT
d

Scan Policy:
Normal scan interval: 10000, deteriorating scan interval: 5000
Max track attempt failures: 3
BSS list size: 4, number of BSSes to start discovery: 1
Number of configured bands: 1

Band: 2.4 GHz
RSSI Threshold: -80 dBm
Number of channels for each discovery interval: 3

Tracking Method:
Scan type: Active Normal Scan
Max channel dwell time: 30000, Min channel dwell time: 15000
ET condition: ET disabled  , ET number of frames: 0
Probe request number: 3, probe request rate: Auto    , TX level: 205

Discovery Method:
Scan type: Active Normal Scan
Max channel dwell time: 30000, Min channel dwell time: 15000
ET condition: ET disabled  , ET number of frames: 0
Probe request number: 3, probe request rate: Auto    , TX level: 205

Immediate Scan Method:
Scan type: Active Normal Scan
Max channel dwell time: 30000, Min channel dwell time: 15000
ET condition: ET disabled  , ET number of frames: 0
Probe request number: 3, probe request rate: Auto    , TX level: 205

Channel list:   1   2   3   4   5   6   7   8   9  10  11  12  13  14
.../configPolicy> Global, Band/, Display, cLear, Store, bsslisT
```

- On the WLAN sniffer, observe that the SUT sends probe requests according to the Scan Policy – Channel, Rate and the number of probe requests.
- The SUT should find the second AP and display it in a neighbor list called BSS List for future roaming purposes:
  - / scAn configPolicy Display

```
.../configPolicy> Global, Band/, Display, cLear, Store, bsslisT
t

BSS List:
BSSID              Band     Channel  RSSI  Neighbor?
-----------------------------------------------------
00.0f.b5.e6.ed.fc  2.4 GHz  6        -65   No
```

Expected result:

The second AP appears in the table.

Note: You should use the same setup for the next test.

3.2.2 Roaming

The Roaming test validates the ability of the SUT to roam to other APs for common roaming triggers, described below, and to continue handling the traffic:

- BSS Loss
- Low Receive Signal Strength Indication (RSSI)

3.2.2.1 Roaming Trigger – BSS Loss

- Use the same setup from the previous section.
- Verify that you see the second AP on the Neighbor APs list.
- Enable roaming on the SUT using the following command:
  - / roaminG Enable

```
\> Driver/, Connection/, Management/, Show/, Privacy/, scAn/, roaminG/, qOs/, poWer/,
eVents/, Bt coexsistence/, Report/, dEbug/, biT/, aboUt, Quit
/ g e
.../roaminG> Enable, Disable, Low pass filter, Quality threshold, Get , Thresholds/
Roaming is enabled
```

- Run a continuous ping from the PC behind the APs to the SUT.
- Unplug the AP you are connected to from the power supply.

Expected result:

The SUT roams to other APs and ping resumes.

3.2.2.2 Roaming Trigger – Low RSSI

- Connect the AP to the power supply again.
- Use the same setup from the previous section.
- Verify that you see the second AP on the Neighbor APs list.
- Run a continuous ping from the PC behind the APs to the SUT.
- Decrease the signal received from the AP using one of the following methods:
  - Walk far from the AP to which you are connected and approach the other AP.
  - Remove the antenna from the AP to which you are currently connected.
  - Use an attenuator to decrease the AP signal.

Expected result:

The SUT roams to the second AP and ping resumes.

3.2.3 Low-Power Mode

This test verifies the ability of the system to use automatic power-save mode. In this power mode, the SUT should remain in Power Save mode for low data rates and should exit from Power Save mode when a high data rate is running.

- Configure the SUT to use Automatic Power Save mode.
  - / poWer set_Power_mode 0

```
.../poWer> set_Power_mode, set_powersave_powerLevel, set_deFault_powerlevel,
set_doZe_mode_in_auto, traffic_Thresholds, eNable, Disable
P 0


Power mode: 0
0 - AUTO, 1 - ACTIVE, 2 - SHORT_DOZE, 3 - LONG_DOZE
```

- Connect the SUT to the AP.
- Observe the sniffer and verify that the SUT sends null data with the power-save bit on right after the connection is established.
- Send a ping from the SUT to the PC behind the AP.
- Observe on the sniffer that the SUT receives a PS Poll packet before each packet from the AP.
- Start high data rate TCP traffic using Iperf from your SUT to the PC behind the AP. You may refer to *Appendix A*, *Using Iperf*, on page 37 for more information.
- Observe on the sniffer that there are no PS-Poll packets.
- Stop the Iperf command using Ctrl+C.
- Send a ping from the PC behind the AP to the SUT. Observe on the sniffer that a PS Poll is sent by the SUT before any packet from the AP.

Expected result:

The SUT enters and exits from Power Save mode according to the traffic type.

3.2.4 QoS

The QoS test category verifies that the SUT is capable of transmitting and receiving data with the correct tagging. In order to run QoS traffic from the PC behind the AP, you should add a key to the registry. You may refer to *Appendix B*, *QoS Support in Windows*, on page 41 for more details.

3.2.4.1 Transmit Voice

- Connect the SUT to the AP that supports QoS.
- Run Iperf UDP in a Voice queue from the SUT to the PC behind the AP and observe the sniffer. You may refer to *Appendix A*, *Using Iperf*, on page 37 for more details.

Expected result:

Packets from the SUT are tagged as Voice packets.

3.2.4.2 Receive Voice

- Connect the SUT to the AP that supports QoS.
- Run Iperf from the PC behind the AP to the SUT in Voice queue and observe the sniffer. You may refer to *Appendix A*, *Using Iperf*, on page 37 for more details.

Expected result:

Packets sent to the SUT are tagged as Voice packets and the SUT acknowledges them successfully.

3.2.5 Ad Hoc (IBSS)

The *ad hoc* test validates the ability of the SUT to create or join a peer-to-peer connection with other stations.

3.2.5.1 Create IBSS Network

- Configure the SUT from the wlan_cu to create an Independent Basic Service Set (IBSS) network using the following command lines:
  - / Management Mode 0
  - / Management Channel 6
  - / Connection Connect MyIBSS

```
/ m m 0
.../Management> connect moDe, Channel, Rate, Mode, Frag, rTs, prEamble, sLot, rAdio
on/off, Info, siGnal, snr ratiO, tX_power_table, tx_power_dBm_div10, tx_poWer_level,
802_11d_h/, beacoN/, adVanced/
Current mode = AD-Hoc
0 - AD-Hoc, 1 - Infr., 2 - Auto
c 6
\> Driver/, Connection/, Management/, Show/, Privacy/, scAn/, roaminG/, qOs/, poWer/,
eVents/, Bt coexsistance/, Report/, dEbug/, biT/, aboUt, Quit
C c MyIBSS
.../Connection> Bssid_list, Connect, Disassociate, Status, Full_bssid_list, wPs/
Trying to associate with SSID 'MyIBSS'
OK
%%%%    SELF SELECT SUCCESS, bssid: 02.00.00.72.09.04 %%%%
/ c s
============================
Status    : running
MAC       : 08.00.28.12.34.56
SSID      : MyIBSS
BSSID     : 02.00.00.72.09.04
Channel   : 6
============================
```

Expected result:

The SUT sends beacons on the correct channel with the correct SSID. The WiFi station connects successfully to the SUT and replies to a ping.

3.2.5.2 Join IBSS Network

- Configure the WiFi station to create an IBSS network.
- Execute an Application Scan command from the wlan_cu to discover the IBSS network you created.
- Connect the SUT to the IBSS network you created using an SSID that you select. You may use the following commands from the wlan_cu:
  - / Management Mode 0
  - / Connection Connect MyChosenSSID
- Configure a static IP address on both stations.
- Run a Ping command from the SUT to the WiFi station.

Expected result:

The SUT successfully joins the IBSS network and replies to a ping.

3.2.6 Recovery

This test validates the recovery feature in the WiLink system. The recovery process is performed by the driver when an issue arises with the system, such as when the last command was not completed within the expected time frame.

The process resets the system HW and boots the system to the same setup as before the recovery.

- Connect the SUT to the AP.
- Run a ping from the PC behind the AP to the SUT.
- Execute a software (SW) recovery trigger that simulates the real recovery operation using the following line on the wlan_cu:
  - / dEbug Print 2002
  - .../dEbug> Print, Fw debug

```
p 2002
CuCmd_PrintDriverDebug: FUN_ID: 2002
***** recovery trigger: MBOX_FAILURE *****, ts=6048520
.....drvMain_Recovery, ts=6048525
SDIO clock Configuration is now set to 24Mhz
CHIP VERSION... set 1273 chip top registers
Working on a 1273 PG 2.0 board.
Starting to process NVS...
NVS found, EEPROM Image addr=0xc34a0000, EEPROM Len=0x0x14c
Chip ID is 0x4030111.
FEM Type 1
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Finished downloading firmware.
Firmware running.
-----------------------------------------------------------------
Driver Version  : WiLink_Driver_6.1.0.0.84
```

```
Firmware Version: Rev 6.1.0.0.204
Station ID      : 08-00-28-12-34-56
---------------------------------------------------------------------

Interrogate TX/RX parameters
.....drvMain_RecoveryNotify: End Of Recovery, ts=6049019
```

Expected result:

The SUT executes the recovery, returns to a normal operation and replies to a ping after the recovery.

3.2.7 Flight Mode

The Flight mode test verifies the proper behavior of the SUT while enabling and disabling the WLAN with different traffic types and connection modes.

- Connect the SUT to the AP.
- Send a continuous ping command from the PC behind the AP to the SUT.
- Put the station in Flight mode. You may use the following commands from the wlan_cu:
  - / Driver Stop

```
.../Driver> Start, sTop, stAtus
t
.../Driver> Start, sTop, stAtus
a
Driver is stopped!
```

- Exit the SUT from Flight mode. You may use the following commands from the wlan_cu:
  - / Driver Start

```
.../Driver> Start, sTop, stAtus
s

SDIO clock Configuration is now set to 24Mhz
CHIP VERSION... set 1273 chip top registers
Working on a 1273 PG 2.0 board.
Starting to process NVS...
No Nvs, Setting default MAC address
pHwInit->uEEPROMCurLen: 1c
Chip ID is 0x4030111.
FEM Type 1
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Starting to download firmware...
Finished downloading firmware.
Firmware running.

---------------------------------------------------------------------
Driver Version  : WiLink_Driver_6.1.0.0.84
Firmware Version: Rev 6.1.0.0.204
```

```
Station ID      : 08-00-28-12-34-56
-------------------------------------------------------------------


Interrogate TX/RX parameters
```

Expected result:

The SUT does not reply to a ping when in Flight mode, but resumes ping replies after exiting from this state.

3.2.8 Hidden SSID

This test validates the ability of the station to connect to an AP that does not advertise the SSID in the beacons.

- Configure the AP to Hidden SSID mode with the SSID value **MyHiddenSSID**. In this state, the AP does not advertise the SSID in the beacons.
- Execute a Scan command from the wlan_cu. You may use the following command:
  - / scAn Start
- You should get the following output in the BSSID List:

```
.../Connection> Bssid_list, Connect, Disassociate, Status, Full_bssid_list, wPs/
b


BssId List: Num=1
         MAC         Privacy Rssi  Mode    Channel    SSID
 00.15.2b.78.f1.90     1    -61  Infra      1        ****
```

- Connect the SUT to the AP. You may use the following lines in the wlan_cu:
  - / Connection Connect MyHiddenSSID
- Run a ping from the PC behind the AP to the SUT.

Expected result:

The SUT successfully connects to the AP and replies to a ping.

3.3 Performance

This test category validates the performance of the system in different scenarios. It verifies that behavior complies with predefined system requirements.

3.3.1 Throughput

1. Configure the AP to 802.11b mode, such that it supports only the following rates: 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps.
2. Connect the SUT to the AP. You may use the following line on the wlan_cu:
   - / Connection Connect MySSID
3. Run an Iperf command for an Rx TCP test and then a Tx TCP test.
4. Record the results in a table, such as that shown in Table 2 below.
5. Configure the AP to 11g mode, and repeat Steps **2**-**4** above. Record the results in a table, such as that shown in Table 2 below.

6 Configure the AP to 11n mode, and repeat Steps **2**-**4** above. Record your results in a table, such as that shown in Table 2 below.

Table 2: Throughput Test Results

AP Configuration	Transmit (Station to AP)	Receive (AP to Station)	Expected Results
802.11b			> 5 Mbps
802.11g			> 15 Mbps
802.11n			> 20 Mbps

Note: You may get low throughput results when the environment is busy with many WLAN transmissions. Texas Instruments recommends that you select the least-occupied channel.

3.3.2 Range Test

The Range test verifies system performance for a variable range from the AP.

- Connect the SUT to the AP.
- Run a continuous ping from the PC behind the AP to the SUT.
- Move far away from the AP location in such a way that the receive signal at the SUT decreases until the SUT disconnects.

  You may get a similar effect by decreasing the output power of the AP using a differential RF attenuator connected to the antenna port of the AP or the SUT.
- You may use the RSSI by typing the following on the wlan_cu, as follows:
  - / Management signal

```
.../Management> connect moDe, Channel, Rate, Mode, Frag, rTs, prEamble, sLot, rAdio
on/off, Info, siGnal, snr ratiO, tX_power_table, tx_power_dBm_div10, tx_poWer_level,
802_11d_h/, beacoN/, adVanced/
g
Current dataRSSI=0  beaconRssi=-81
```

- Return the SUT to the appropriate AP range.

Expected result:

A ping is replied to for a valid receive signal of -85dBm and below.

The SUT reconnects again after returning the AP range, and replies to a ping.

3.3.3 Packet Error Rate

The Transmit Packet Error Rate (PER) test verifies that the SUT transmits in high quality with a low PER when using a WLAN sniffer.

- Configure the AP to the least-occupied channel. You may use the WLAN sniffer for this purpose.
- Connect the SUT to the AP.
- Run Iperf UDP of 1 Mbps for one minute from the SUT to the PC behind the AP. Record the sniffer trace for the entire session.
- Run Iperf UDP of 1Mbps for one minute from the PC behind the AP to the SUT. Record the sniffer trace for the entire session.

Expected result:

The number of data packets with a Retry flag is less than 5% of the total packets.

3.4 BT Testing

BT testing tests the basic operation of the BT stack and the functionality of the BT Device Under Test (DUT). The WLAN should be turned off during BT tests.

3.4.1 A2DP Profile

For this test, BT should be able to connect an A2DP-supported headset and an audio file should be played with high quality.

Configure the BT DUT to an A2DP source by running the following commands on the Linux shell:

- After loading the device, type the following from the Linux prompt:

```
/ # export LD_LIBRARY_PATH=/WiLink_Demo_Target/lib:$LD_LIBRARY_PATH
/ # /WiLink_Demo_Target/sbin/hciattach /dev/ttyS1 texas 3000000
Found a Texas Instruments' chip!
Firmware file : /lib/firmware/TIInit_7.2.31.bts
Loaded BTS script version 1
texas: changing baud rate to 3000000, flow control to 1
Device setup complete
/ # /WiLink_Demo_Target/sbin/hciconfig
hci0:   Type: UART
        BD Address: 00:00:00:00:00:00 ACL MTU: 0:0 SCO MTU: 0:0
        DOWN
        RX bytes:0 acl:0 sco:0 events:0 errors:0
        TX bytes:0 acl:0 sco:0 commands:0 errors:0
/ # /WiLink_Demo_Target/sbin/hciconfig hci0 up
/ # /WiLink_Demo_Target/sbin/hciconfig hci0 piscan
/ # /WiLink_Demo_Target/sbin/hciconfig
hci0:   Type: UART
        BD Address: 00:21:BA:FA:BF:86 ACL MTU: 1021:4 SCO MTU: 180:4
        UP RUNNING PSCAN ISCAN
        RX bytes:359 acl:0 sco:0 events:11 errors:0
        TX bytes:50 acl:0 sco:0 commands:11 errors:0
/ # /WiLink_Demo_Target/bin/hcitool scan
Scanning ...
        00:13:E7:48:3C:95       MCS-IL-X0052323 AVRCP Test APP
        00:03:C9:87:29:83       n/a
        00:12:62:02:22:5A       Yuval cell
        00:1C:A4:57:25:E8       K610i
        00:12:D2:96:99:EA       Nokia 6230i
        00:22:A5:B9:67:65       TI Android Bluetooth
        00:12:1C:BB:05:46       Parrot MK6000v1.01c
        00:16:41:B4:A8:C7       Shlomi_PC
        00:1A:6B:77:1D:F4       CBC0664
        00:12:62:26:0A:D6       Nokia 6230
```

```
        00:14:A4:DF:B0:3E       MCS086596
        00:10:C6:C2:D3:7F       CN
        00:17:E3:10:B9:6B       Assaf's cell.
        00:1F:5D:5D:3C:EA       Asher Golomb phone
        00:1D:28:6D:AD:0A       K610i ohad
/ # rm /WiLink_Demo_Target/var/run/messagebus.pid
/ # /WiLink_Demo_Target/bin/dbus-daemon -system
/ # /WiLink_Demo_Target/sbin/bluetoothd -n &
/etc # bluetoothd[1523]: Bluetooth daemon 4.40
bluetoothd[1523]: Starting SDP server
bluetoothd[1523]: Can't create GN bridge
bluetoothd[1523]: HCI dev 0 registered
bluetoothd[1523]: HCI dev 0 up
bluetoothd[1523]: Starting security manager 0
bluetoothd[1523]: Adapter /org/bluez/1523/hci0 has been enabled
bluetoothd[1523]: Failed to access HAL
```

- Create or edit the file **asound.conf** on the target file system under the directory /**etc**/ with the following content in it:

```
/ # cat /etc/asound.conf
pcm.!bluetooth {
                type bluetooth
                device 00:12:1C:BB:05:46 / This should be your BT A2DP sinc BD Address
}
pcm.!default {
                type plug
                slave.pcm "bluetooth"
}
/ # /WiLink_Demo_Target/sbin/agent --path /org/bluez/agent 0000 & / 0000 is the pass key
of your BT Sink device
/# /WiLink_Demo_Target/bin/dbus-send --system --print-reply --dest=org.bluez /
\org.bluez.Manager.DefaultAdapter
method return sender=:1.0 -> dest=:1.2 reply_serial=2
   object path "/org/bluez/1523/hci0"
/# /WiLink_Demo_Target/sbin/sdptest -i hci0 00:12:1C:BB:05:46
bluetoothd[1523]: link_key_request (sba=00:21:BA:FA:BF:86, dba=00:12:1C:BB:05:46)
00 06 00 06 12 34 56 78  11 22 33 44 11 11 22 22
55 55 55 55 55 55 66 66  55 55 66 67
/# /home/root/alsa_install/bin/aplay -Dplug:bluetooth
/home/root/alsa_install/bin/seaman.wav / Plays the File seaman.wav under the path
/home/root/alsa_install/bin
```

Expected result:

The file plays successfully and music sounds clear.

3.4.2 Object Push Profile

Using an Object Push Profile (OPP), BT should be able to send or receive a file saved on the OMAP to a remote device (for example, a mobile phone).

- Configure the BT DUT to connect to an OPP-supported BT device by running the following commands on the Linux shell:

```
/ # export LD_LIBRARY_PATH=/WiLink_Demo_Target/lib:$LD_LIBRARY_PATH

/ # /WiLink_Demo_Target/sbin/hciattach /dev/ttyS1 texas 3000000
Found a Texas Instruments' chip!
Firmware file : /lib/firmware/TIInit_7.2.31.bts
Loaded BTS script version 1
texas: changing baud rate to 3000000, flow control to 1
Device setup complete
/ # /WiLink_Demo_Target/sbin/hciconfig
hci0:   Type: UART
        BD Address: 00:00:00:00:00:00 ACL MTU: 0:0 SCO MTU: 0:0
        DOWN
        RX bytes:0 acl:0 sco:0 events:0 errors:0
        TX bytes:0 acl:0 sco:0 commands:0 errors:0
/ # /WiLink_Demo_Target/sbin/hciconfig hci0 up
/ # /WiLink_Demo_Target/sbin/hciconfig hci0 piscan
/ # /WiLink_Demo_Target/sbin/hciconfig
hci0:   Type: UART
        BD Address: 00:21:BA:FA:BF:86 ACL MTU: 1021:4 SCO MTU: 180:4
        UP RUNNING PSCAN ISCAN
        RX bytes:359 acl:0 sco:0 events:11 errors:0
        TX bytes:50 acl:0 sco:0 commands:11 errors:0
/ # /WiLink_Demo_Target/bin/hcitool scan
Scanning ...
        00:13:E7:48:3C:95       MCS-IL-X0052323 AVRCP Test APP
        00:03:C9:87:29:83       n/a
        00:12:62:02:22:5A       Yuval cell
        00:1C:A4:57:25:E8       K610i
        00:12:D2:96:99:EA       Nokia 6230i
        00:22:A5:B9:67:65       TI Android Bluetooth
        00:12:1C:BB:05:46       Parrot MK6000v1.01c
        00:16:41:B4:A8:C7       Shlomi_PC
        00:1A:6B:77:1D:F4       CBC0664
        00:12:62:26:0A:D6       Nokia 6230
        00:14:A4:DF:B0:3E       MCS086596
        00:10:C6:C2:D3:7F       CN
        00:17:E3:10:B9:6B       Assaf's cell.
        00:1F:5D:5D:3C:EA       Asher Golomb phone
        00:1D:28:6D:AD:0A       K610i ohad
/ # rm /WiLink_Demo_Target/var/run/messagebus.pid
/ # /WiLink_Demo_Target/bin/dbus-daemon -system
/ # /WiLink_Demo_Target/sbin/bluetoothd -n &
```

```
/etc # bluetoothd[1523]: Bluetooth daemon 4.40
bluetoothd[1523]: Starting SDP server
bluetoothd[1523]: Can't create GN bridge
bluetoothd[1523]: HCI dev 0 registered
bluetoothd[1523]: HCI dev 0 up
bluetoothd[1523]: Starting security manager 0
bluetoothd[1523]: Adapter /org/bluez/1523/hci0 has been enabled
bluetoothd[1523]: Failed to access HAL
/ # /WiLink_Demo_Target/bin/sdptool browse local / Prints the DUT supported profiles
/ # /WiLink_Demo_Target/bin/sdptool browse 00:24:03:3D:2F:C0 / enter the BD Address of the
device you are working with
Service Name: OBEX Object Push
Service RecHandle: 0x10001
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 9                                          / copy the channel # fot the next
command
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
```

- Copy the channel from the OPP to the next command:

```
/WiLink_Demo_Target/bin/sdptool add --channel=CH OPUSH
/ # /WiLink_Demo_Target/bin/sdptool add --channel=9 OPUSH
```

- Using the following command, send a file from the BT DUT to the BT device:

```
/WiLink_Demo_Target/bin/ussp-push {BTADDR@[BTCHAN]} LocalFile RemoteFile
/ # /WiLink_Demo_Target/bin/ussp-push 00:24:03:3D:2F:C0@9 SourceFile.jpg DestFile.jpg
```

Expected result:

The file is received successfully and can be opened.

3.4.3 BT Inquiry and Inquiry Scan

This test validates the ability of the BT device to scan all remote devices and to be discoverable by other devices.

3.4.3.1 BT Inquiry

Enable an Inquiry scan on the BT devices available in your environment. For some devices, this option is called *Find Me* or *Make Your Device Discoverable*.

- Start the Bluetooth from the Linux shell using the following commands:

```
/ # export LD_LIBRARY_PATH=/WiLink_Demo_Target/lib:$LD_LIBRARY_PATH
/ # /WiLink_Demo_Target/sbin/hciattach /dev/ttyS1 texas 3000000
Found a Texas Instruments' chip!
Firmware file : /lib/firmware/TIInit_7.2.31.bts
Loaded BTS script version 1
texas: changing baud rate to 3000000, flow control to 1
Device setup complete
/ # /WiLink_Demo_Target/sbin/hciconfig
hci0:   Type: UART
        BD Address: 00:00:00:00:00:00 ACL MTU: 0:0 SCO MTU: 0:0
        DOWN
        RX bytes:0 acl:0 sco:0 events:0 errors:0
        TX bytes:0 acl:0 sco:0 commands:0 errors:0
/ # /WiLink_Demo_Target/sbin/hciconfig hci0 up
/ # /WiLink_Demo_Target/sbin/hciconfig hci0 piscan
/ # /WiLink_Demo_Target/sbin/hciconfig
hci0:   Type: UART
        BD Address: 00:21:BA:FA:BF:86 ACL MTU: 1021:4 SCO MTU: 180:4
        UP RUNNING PSCAN ISCAN
        RX bytes:359 acl:0 sco:0 events:11 errors:0
        TX bytes:50 acl:0 sco:0 commands:11 errors:0
```

- Run the Inquiry using the following command:

```
/ # /WiLink_Demo_Target/bin/hcitool scan
Scanning ...
        00:13:E7:48:3C:95       MCS-IL-X0052323 AVRCP Test APP
        00:03:C9:87:29:83       n/a
        00:12:62:02:22:5A       Yuval cell
        00:1C:A4:57:25:E8       K610i
        00:12:D2:96:99:EA       Nokia 6230i
        00:22:A5:B9:67:65       TI Android Bluetooth
        00:12:1C:BB:05:46       Parrot MK6000v1.01c
        00:16:41:B4:A8:C7       Shlomi_PC
        00:1A:6B:77:1D:F4       CBC0664
        00:12:62:26:0A:D6       Nokia 6230
        00:14:A4:DF:B0:3E       MCS086596
        00:10:C6:C2:D3:7F       CN
        00:17:E3:10:B9:6B       Assaf's cell.
        00:1F:5D:5D:3C:EA       Asher Golomb phone
        00:1D:28:6D:AD:0A       K610i ohad
```

- Leave this configuration for the next step.

Expected result:

An Inquiry command returns the list of BT devices in the range.

3.4.3.2 BT Inquiry Scan

Enable an Inquiry scan on the BT DUT using the script below.

- Run the following commands to enable an Inquiry Scan:

```
/ # /WiLink_Demo_Target/sbin/hciconfig hci0 piscan
/ # /WiLink_Demo_Target/sbin/hciconfig
hci0:   Type: UART
        BD Address: 00:21:BA:FA:BF:86 ACL MTU: 1021:4 SCO MTU: 180:4
        UP RUNNING PSCAN ISCAN
        RX bytes:359 acl:0 sco:0 events:11 errors:0
        TX bytes:50 acl:0 sco:0 commands:11 errors:0
```

- Run Inquiry command from the BT handset.

Expected result:

The Inquiry command from the BT handset returns the BT DUT Bluetooth device address.

3.5 BT – WLAN Coexistence

Coexistence tests validate the BT WLAN coexistence algorithm by mixing the WLAN and BT scenarios described below. Audio quality should not be affected from WLAN activity.

3.5.1 WLAN Scan While BT is Idle

- Enable the BT device.
- Run an Application Scan command using the wlan_cu and read the BSSID List.
- Repeat the previous step 10 times.

Expected result:

The BSSID list contains all APs in the range.

3.5.2 WLAN Scan While BT is Connected to an A2DP Sink

- Connect the BT device to an A2DP sink.
- Run an Application Scan command and read the BSSID List.
- Repeat the previous step 10 times.

Expected result:

The BSSID list contains all APs in the range. The BT connection remains active.

3.5.3 WLAN Runs Traffic While BT Transfers a File

- Connect the BT device to a BT handset.
- Start transferring a 5Mbyte file from the BT DUT to the BT handset using OPP.
- Connect the SUT to the AP and run Iperf TCP from the SUT to the PC behind the AP.

Expected result:

The file is received successfully by the BT handset. The SUT runs Iperf with no issue.

3.5.4 WLAN Runs Traffic While BT Configured to A2DP

- Connect the BT device to a BT A2DP sink.
- Start playing a music file from the BT DUT.
- While the music plays, connect the SUT to the AP and run Iperf TCP from the PC behind the AP to SUT.

Expected result:

The music sounds clear. The SUT receives Iperf with no issue.

3.5.5 WLAN Flight Mode While BT Configured to A2DP

- Connect the BT device to a BT A2DP sink.
- Start playing a music file from the BT DUT.
- Connect the SUT to the AP.
- Send a continuous ping from the PC behind the AP to the SUT.
- While the music plays, disable the WLAN driver and enable it again.
- Repeat the last action five times.

Expected result:

The music sounds clear during the entire test. The SUT replies to a ping each time the driver starts, and does not reply when the driver stops.

3.5.6 WLAN with WPA2-PSK While BT Configured to A2DP

- Connect the BT device to a BT A2DP sink.
- Start playing a music file from the BT DUT.
- Configure the AP to WPA2-PSK.
- Connect the SUT to the AP.
- Send a continuous ping from the PC behind the AP to the SUT.
- While the music plays, disconnect the SUT from the AP and reconnect it again.
- Repeat the last action five times.

Expected result:

The music sounds clear. The SUT replies to a ping each time it is connected to the AP.

3.5.7 BT A2DP Connection While WLAN is Idle

- Enable the SUT and leave it disconnected.
- Connect the BT device to a BT A2DP sink.
- Turn off the BT sink device, and turn it on again.
- Repeat the last action five times.

Expected result:

The BT DUT reconnects each time the BT handset is restarted.

3.5.8 BT OPP Connection While the WLAN Runs Traffic

- Connect the SUT to the AP.
- Run Iperf TCP from the SUT to the PC behind the AP.
- While traffic is running, connect the BT DUT to a BT handset using OPP.
- Disconnect the BT connection and reconnect it again. You can do so by shutting down the handset.
- Repeat the last action five times.

Expected result:

The BT DUT reconnects each time with the BT handset. The SUT handles the traffic for the entire test session.

3.5.9 BT Inquiry While the WLAN Runs Traffic

- Connect the SUT to the AP.
- Run Iperf TCP from the PC behind the AP to the SUT.
- Configure the BT A2DP sink device and the BT handset to run an Inquiry scan (*find me* state).
- While traffic is running over the WLAN, run an Inquiry command on the BT DUT.
- Repeat the last action five times.

Expected result:

The BT DUT performs an inquiry on the two BT devices. The SUT handles the traffic for the entire test session.

3.5.10 WLAN Traffic When a BT A2DP Connection is Lost

- Connect the BT device to a BT A2DP sink.
- Start playing a music file from the BT DUT.
- Connect the SUT to the AP.
- Run Iperf TCP from the PC behind the AP to the SUT.
- While the music plays, take the BT sink device far away from the BT DUT until the BT DUT disconnects from the BT sink.
- Return the BT A2DP sink device to the range of the BT DUT.
- Reconnect the BT device to the BT A2DP sink.

Expected result:

The SUT continues to handle traffic when the BT is disconnected. The BT A2DP sink reconnects to the BT DUT.

3.6 Reliability

The Reliability test category verifies system robustness and tests the response of system components to specific scenarios over time.

3.6.1 Repeated Association

- Configure the AP to WPA PSK.
- Connect the SUT to the AP.
- Run a ping from the SUT to the PC behind the AP.
- Disconnect the SUT from the AP. You may use the following command on the wlan_cu:
  - / Connection Disconnect
- Repeat the last three actions 20 times.

Expected result:

The SUT successfully reconnects 20 times and replies to a ping each time.

3.6.2 Repeated AP Activation

- Configure the AP to WEP 40 bits.
- Connect the SUT to the AP.
- Run a ping from the SUT to the PC behind the AP.
- Unplug the AP from power supply.
- Plug in the AP to the power supply.
- Repeat the last two actions 20 times.

Expected result:

The SUT reconnects to the AP each time it is up and replies to a ping.

3.7 Stability

The Stability test verifies system stability over time and verifies the robustness of the system. The test cases run over a long period in different system scenarios and configurations.

3.7.1 Stability Setup 1

- Configure the AP to WPA2 PSK.
- Connect the SUT to the AP.
- Run TCP traffic using an Iperf command from the SUT to the PC behind the AP.
- Leave the setup running for eight hours.

Expected result:

Traffic remains until the end of the test, and no major issue is observed. The SUT remains connected to the AP for the entire test.

3.7.2 Stability Setup 2

- Configure the AP to WPA PSK.
- Connect the SUT to the AP.
- Run UDP traffic using an Iperf command from the PC behind the AP to the SUT.
- Leave the setup running for eight hours.

Expected result:

Traffic remains until the end of the test, and no major issue is observed. The SUT remains connected to the AP for the entire test.

3.7.3 Stability Setup 3

- Configure the AP to WPA PSK security.
- Connect the SUT to the AP.
- Run TCP traffic using an Iperf command from the PC behind the AP to the SUT.
- Connect the BT DUT to an A2DP device.
- Play a *.mp3 file repeatedly.
- Leave the setup running for one hour.

Expected result:

Traffic remains until the end of the test, and no major issue is observed. Music plays clearly for the entire session.

Using Iperf

Iperf is a freeware traffic generation tool. It is a client/server application that should run on both peers, and generates UDP and TCP traffic from the client to the server, according to the configuration described in this appendix.

You should run the server before the client.

Topic **Page**

A.1 TCP Iperf Command

TCP Client Command: This command should be run on the peer the generates and transmits the data.

./Iperf –c ‘Destination IP’ –I ‘Interval’ –p ‘TCP Port’ –t ‘Time in Seconds’

For Example: Running a TCP client from the SUT to the PC behind the AP.

```
# ./Iperff--c 192.168.1.10--I 2--p 6000--t 90
Client connecting to 192.168.1.10, TCP port 6000
TCP window size: 16.0 kByte (default)
------------------------------------------------------------
```

TCP Server Command: This command should be run on the peer that receives the data.

./Iperf –s –I ‘Interval’ –p ‘TCP Port’

For Example: Running the TCP server to the SUT.

```
# ./Iperff--s--i2--p 6000
Server listening on TCP port 6000
TCP window size: 85.3 kByte (default)
------------------------------------------------------------
```

A.2 UDP Iperf Command

UDP Client Command: This command should be run on the peer the generates and transmits the data.

./Iperf –c ‘Destination IP’ –u –b ‘bandwidth’ –i ‘Interval’ –p ‘UDP Port’ –t ‘Time in Seconds’

For Example: Running UDP 1Mbps traffic from the SUT.

```
# ./Iperff--c 192.168.1.10--u--b 1M--i 2--p 6000--t 90
Client connecting to 192.168.1.10, UDP port 6000
Sending 1470 byte datagrams
UDP buffer size: 99.0 kByte (default)
------------------------------------------------------------
```

UDP Server Command: This command should be run on the peer that receives the data.

./Iperf –s –I –u ‘Interval’ –p ‘UDP Port’

For Example: Running the UDP server on the SUT.

```
# ./Iperff--s--i 2--p 6000--u
Server listening on UDP port 6000
Receiving 1470 byte datagrams
UDP buffer size: 99.0 kByte (default)
------------------------------------------------------------
```

A.3 Iperf with QoS Tagging

Tagging should be run only on the client side. The rest of the command is identical to that on the standard Iperf client. No server modification is required.

./Iperf –c ‘Destination IP’ –S ‘Tag’ –u –b ‘bandwidth’ –i ‘Interval’ –p ‘UDP Port’ –t ‘Time in Seconds’

For Example: Running 100K voice traffic from the SUT to the PC behind the AP.

```
# .□perff--c 192.168.1.10--S 224--u--b 100K--i 2--p 6000--t 90
Client connecting to 192.168.1.10, UDP port 6000
Sending 1470 byte datagrams
UDP buffer size: 99.0 kByte (default)
------------------------------------------------------------
```

This page was intentionally left blank.

QoS Support in Windows

In order to use the QoS on your Windows PC, you should add a key in the Windows registry. Follow the procedure below to do so.

To add a key to the Windows registry:

1 Select **Start ➔ Run**.

2 In the window that opens, enter r**egedit** and click **OK**. The **Registry Editor** window is displayed:

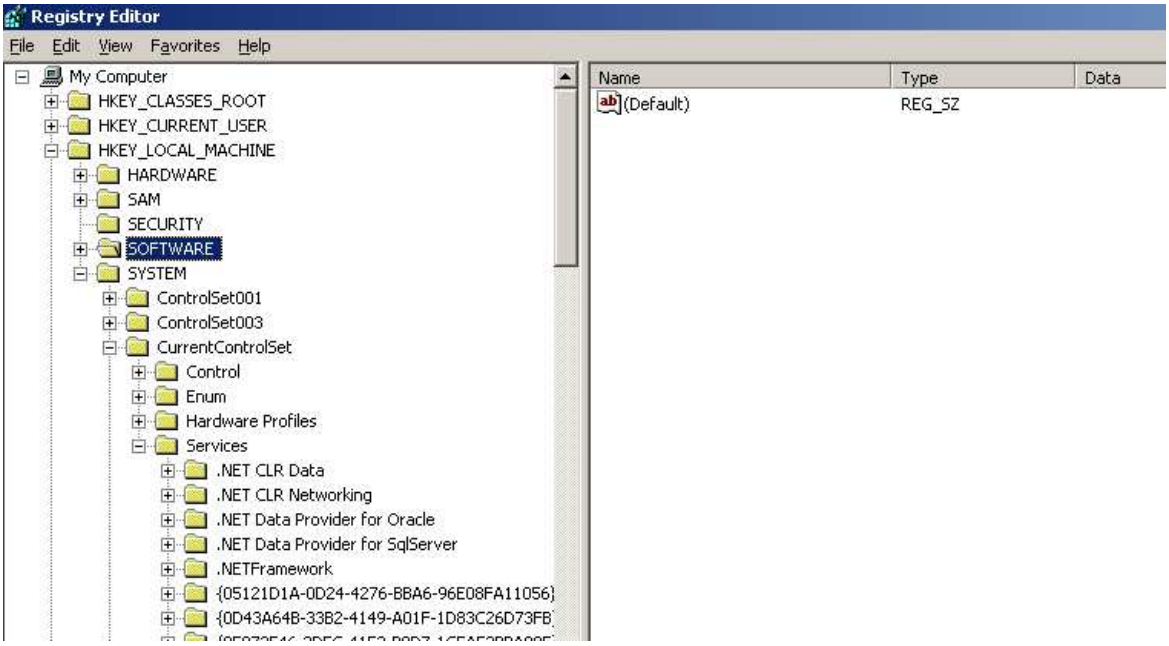

Figure 2: Registry Window

3 Locate the following path in the tree:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

4 Right-click in the right pane of the window and select **New > DWORD Value**, as shown below:

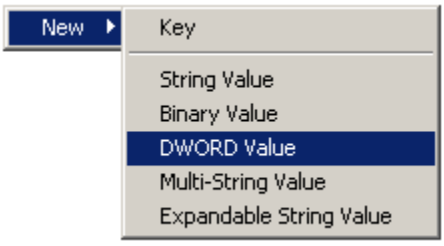

Figure 3: DWORD Right-click Option

The following window is displayed:

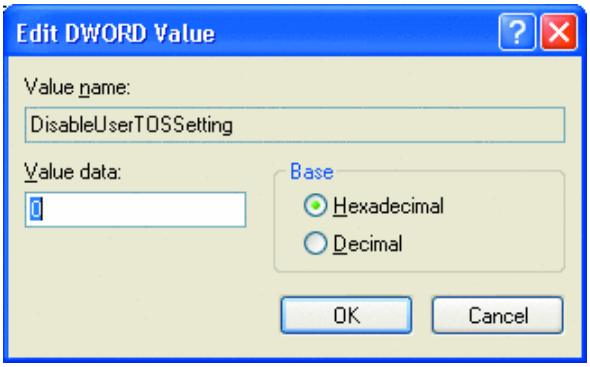

Figure 4: Edit DWORD Value Window

5 In the **Value name** field, enter **DisableUserTOSSetting**.

6 In the **Value data** field, enter 0.

7 **Restart the PC**.

Glossary of Terms

Term	Description
A2DP	Advanced Audio Distribution Profile
AC	Access Category
ACI	Adjacent Channel Interface
AP	Access Point
API	Application Program Interface
ARP	Address Resolution Protocol
BD Address	Bluetooth Device Address
BSS	Basic Service Set. A set of stations controlled by a single coordination function.
CLI	Command Line Interface
CCX	Cisco Compatible Extensions
DTIM	Delivery Traffic Indication Message
DUT	Device Under Test
DVP	Development platform
ELP	Enhanced Low Power
HW	Hardware
IBSS	Independent Basic Service Set
KVM	Keyboard Video Mouse
MOS	Mean Opinion Score
OBEX	Object Exchange
OPP	Object Push Profile
PER	Packet Error Rate
PS	Power Save
PLT	Production Line Test
PHY	Physical layer
QoS	Quality of Service
RF	Radio Frequency
RSSI	Receive Signal Strength Indication
RVR	Rate Versus Range
SDIO	Secure Digital Input Output
SSID	Service Set Identifier
STA	Station
SUT	System Under Test
TX	Transmit/transmitter
U-APSD	Unscheduled Automatic Power-Save Delivery

Term	Description
VoIP	Voice over Internet Protocol
WEP	Wired Equivalent Privacy
WIPP	Wireless IP Phone
WLAN	Wireless Local Area Network
WMM	Wireless Multimedia
WPA	Wireless Protected Access