

WL1271 System Test Guidelines

User's Guide



Literature Number: SPRUGT7

February 2011



Contents

Contents	3
Revision History	6
Reference Documents	6
About This Document	6
Chapter 1	7
Test Strategy	7
1.1 7	
1.2 Tested System	8
Chapter 2	9
Test Setup	9
2.1 Recommended Test Setup	10
2.2 Testing Tools.....	10
2.3 Test Categories	11
Chapter 3	13
Test Plan	13
3.1 Security.....	14
3.1.1 WEP	15
3.1.2 WPA PSK.....	19
3.1.3 WPA2 PSK	19
3.1.3.1 Negative Security Test.....	20
3.2 Functionality.....	20
3.2.1 Scanning	20
3.2.1.1 Application Scan.....	21
3.2.1.2 Background Scan	24
3.2.2 Roaming.....	25
3.2.2.1 Roaming Trigger – BSS Loss.....	26
3.2.2.2 Roaming Trigger – Low RSSI.....	26
3.2.3 QoS.....	27
3.2.4 Ad Hoc (IBSS)	27
3.2.4.1 Create IBSS Network.....	27
3.2.4.2 Join IBSS Network.....	30
3.2.5 Hidden SSID.....	31
3.3 Performance	34
3.3.1 Range Test	34
3.4 BT Testing.....	35
3.4.1 A2DP Profile	35
3.4.2 Object Push Profile	41
3.4.3 BT Inquiry and Inquiry Scan.....	44
3.4.3.1 BT Inquiry	44

3.4.3.2 BT Inquiry Scan	45
3.5 BT – WLAN Coexistence.....	46
3.5.1 WLAN Scan While BT is Idle.....	46
3.5.2 WLAN Scan While BT is Connected to an A2DP Sink.....	46
3.5.3 WLAN Runs Traffic While BT Transfers a File	46
3.5.4 WLAN Runs Traffic While BT Configured to A2DP.....	47
3.5.5 WLAN Flight Mode While BT Configured to A2DP	47
3.5.6 WLAN with WPA2-PSK While BT Configured to A2DP.....	47
3.5.7 BT A2DP Connection While WLAN is Idle	47
3.5.8 BT OPP Connection While the WLAN Runs Traffic.....	48
3.5.9 BT Inquiry While the WLAN Runs Traffic	48
3.5.10 WLAN Traffic When a BT A2DP Connection is Lost.....	48
3.6 Reliability.....	49
3.6.1 Repeated Association.....	49
3.6.2 Repeated AP Activation.....	49
3.7 Stability	49
3.7.1 Stability Setup 1	49
3.7.2 Stability Setup 2	50
3.7.3 Stability Setup 3	50
Appendix A	51
QoS Support in Windows.....	51
Glossary of Terms	53

List of Figures

Figure 1: Recommended Test Setup	10
Figure 2: Registry Window	51
Figure 3: DWORD Right-click Option	51
Figure 4: Edit DWORD Value Window	52

List of Tables

Table 1: Test Categories	11
--------------------------------	----



Revision History

Version	Date	Description
1.0	May 2009	Release
1.1	February 2011	Update

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 AM3715 and the 1271 chipset with focus on the Windows Embedded CE release. 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, QoS Support in Windows**, page 51, describes how to add a key to the Windows registry to provide QoS support.

Note: Throughout this document, characters in **blue** represent output from 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

8

1.1

1.2 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™ platformWindows Embedded CE comes with a dedicated tool and interface to configure the wireless interface and perform connections to the accessible Access Points.

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

Test Setup

Topic		Page
2.1	Recommended Test Setup	10
2.2	Testing Tools	10
2.3	Test Categories	11

2.1 Recommended Test Setup

The following figure shows the recommended test setup.

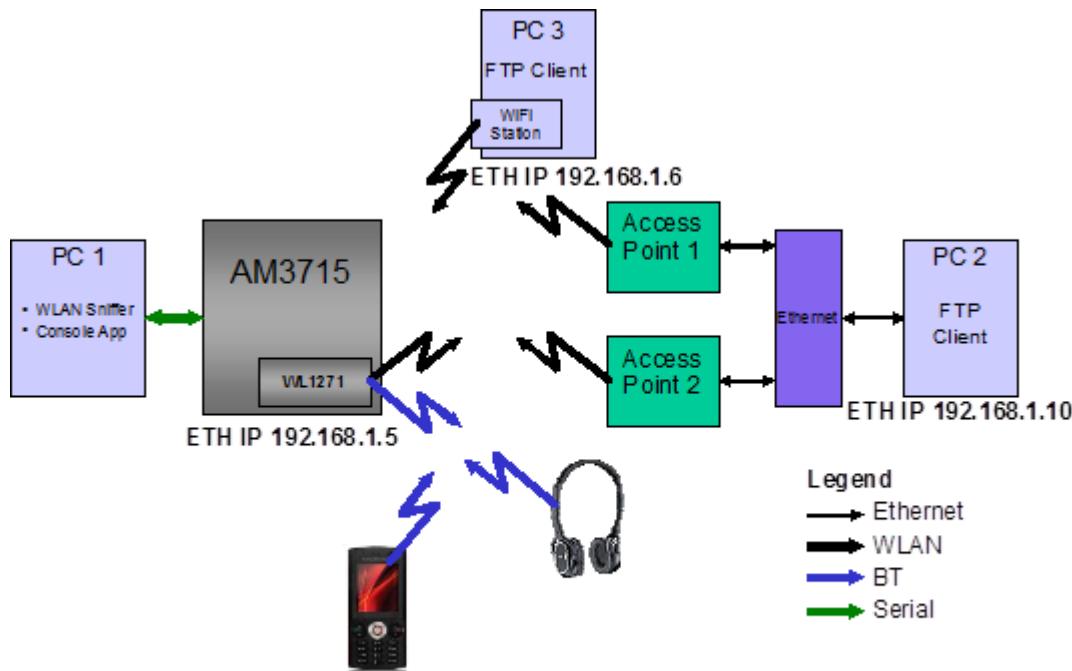


Figure 1: Recommended Test Setup

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.
- 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
1.1	7
1.2	Tested System
2.1	Recommended Test Setup
2.2	Testing Tools.....
2.3	Test Categories.....
3.1	Security.....
3.2	Functionality.....
3.3	Performance
3.4	BT Testing.....
3.5	BT – WLAN Coexistence
3.6	Reliability
3.7	Stability

3.1 Security

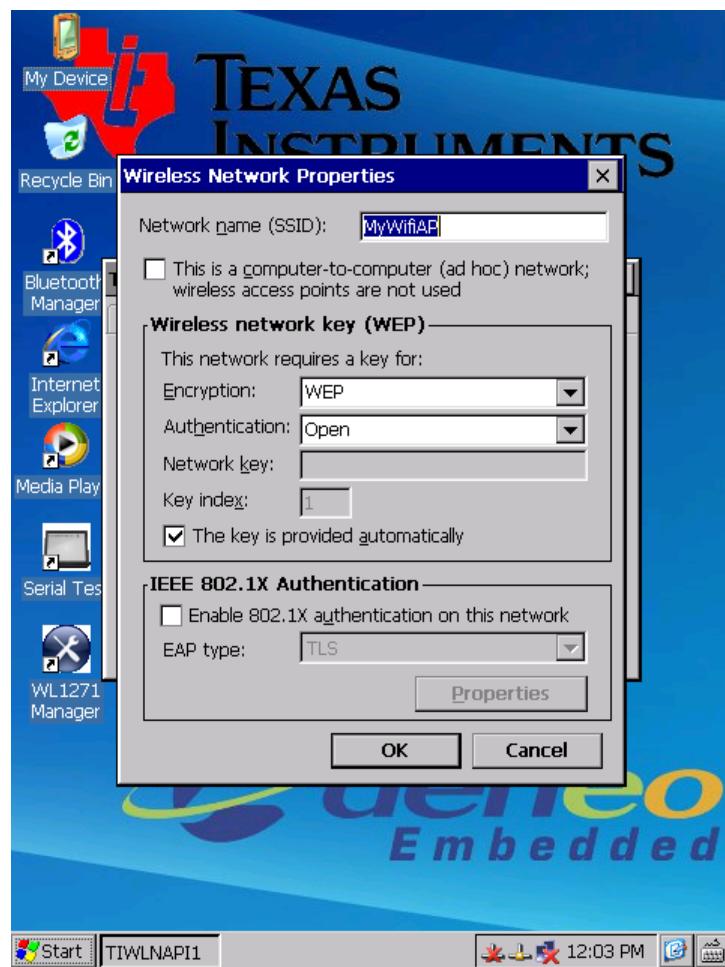
The Security test validates the use of security connections, including WEP, WPA-PSK and WPA2-PSK, as well as the behavior of the system under test (SUT) when attempting to connect with incorrect security settings.

3.1.1 WEP

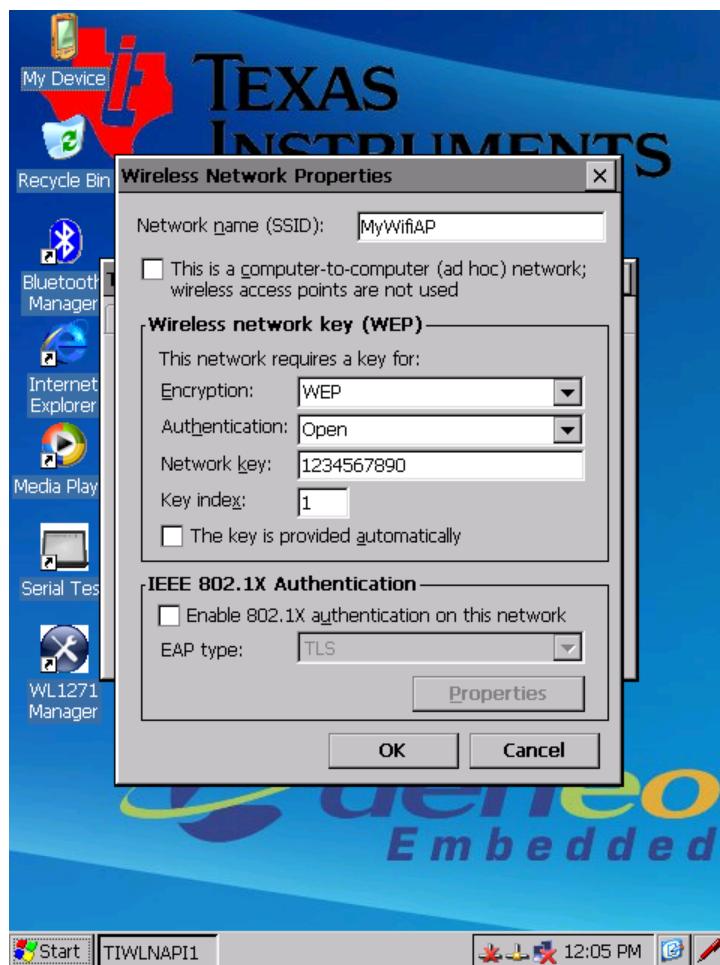
- Configure the AP and SUT to WEP with Open System authentication using a 64-bit key index 1. You may do the following actions:
 - Open the ZeroConfig window by clicking on the network icon located into the task bar at the bottom part of the screen.



- Select YourSSID in the list and hit Connect



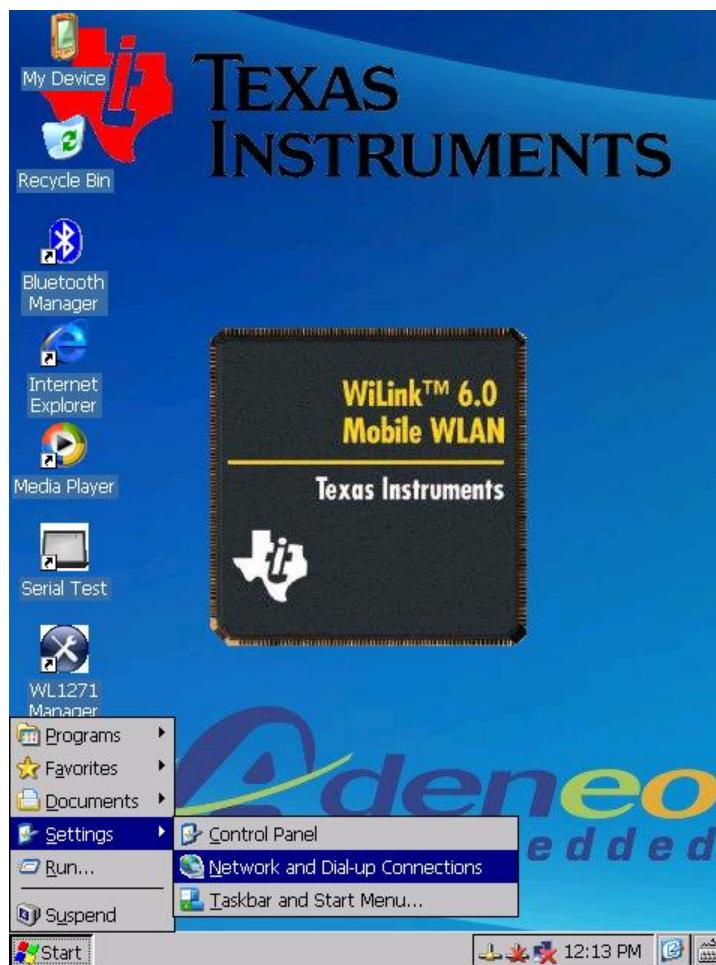
- Select network type and enter passkey



- Close connection window and wait for ZeroConfig to connect to the AP



- Configure the IP address on the SUT using the Network Connection Manager



- 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.

3.1.2 WPA PSK

- Configure the AP and SUT to WPA authentication with TKIP encryption. Refer to WEP configuration procedure above for the connection and configuration.
- 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.

3.1.3 WPA2 PSK

- Configure the AP and SUT to WPA2 authentication with AES encryption. Refer to WEP configuration procedure above for the connection and configuration.
- 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.

3.1.3.1 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.
- Use ZeroConfig window to establish and configure connection to the AP.
- 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 on top of the driver. This scan adds 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 WL1271 Manager application that can be launched from the control panel:



- Hit the Start Scan button
- On the WLAN sniffer, observes that the SUT sends probe requests when running the application scan.
- Reads the BSSID list.
- Turns off one of the APs and runs the scan command again.
- Reads the BSSID list.

This test performs the following operations from the GUI:

- Enables more than one AP to run in your environment.
- Runs an application scan on the SUT. You may use the WL1271 Manager application:



- Hit the Start Scan button
- Open the WLAN interface ZeroConfig window, by pointing on the network icon located in the task bar



- On the WLAN sniffer, observes that the SUT sends probe requests when running the application scan.
- Reads the BSSID list.
- 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 from the WL1271 Manager.



- Connects the SUT to one of the APs using the ZeroConfig GUI.
- Your SUT is configured by default to run a background scan. You may review it using the Application Scan and Other Scan Modes button from WL1271 Manager:
- 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:

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 WL1271 Manager application:



- Hit the Enable Roaming
- 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 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 51 for more details.

3.2.4 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.

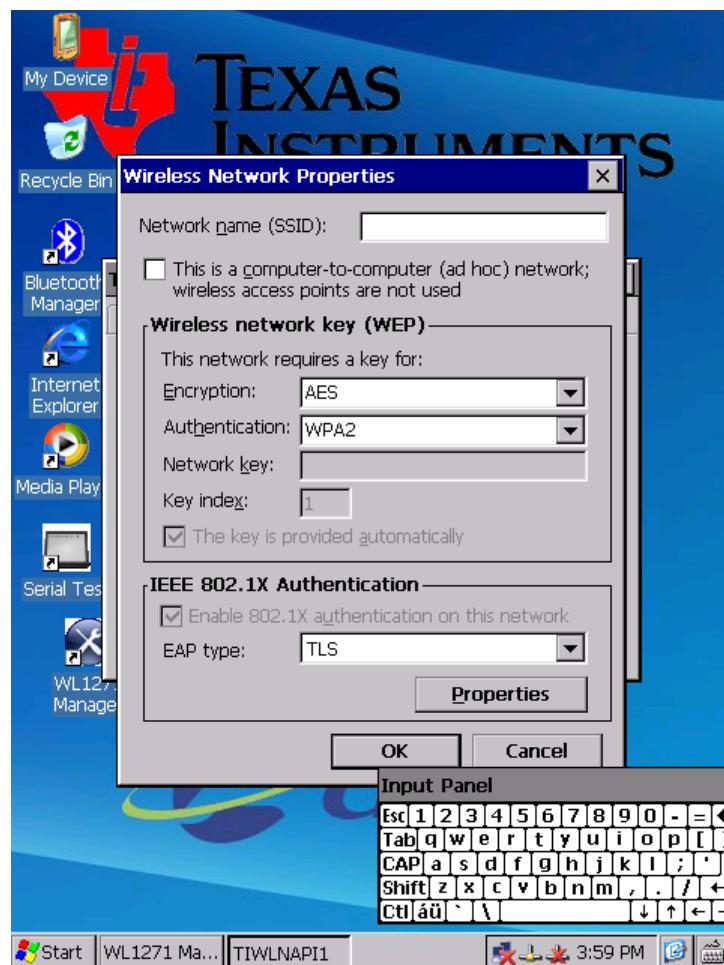
3.2.4.1 Create IBSS Network

Using the ZeroConfig GUI

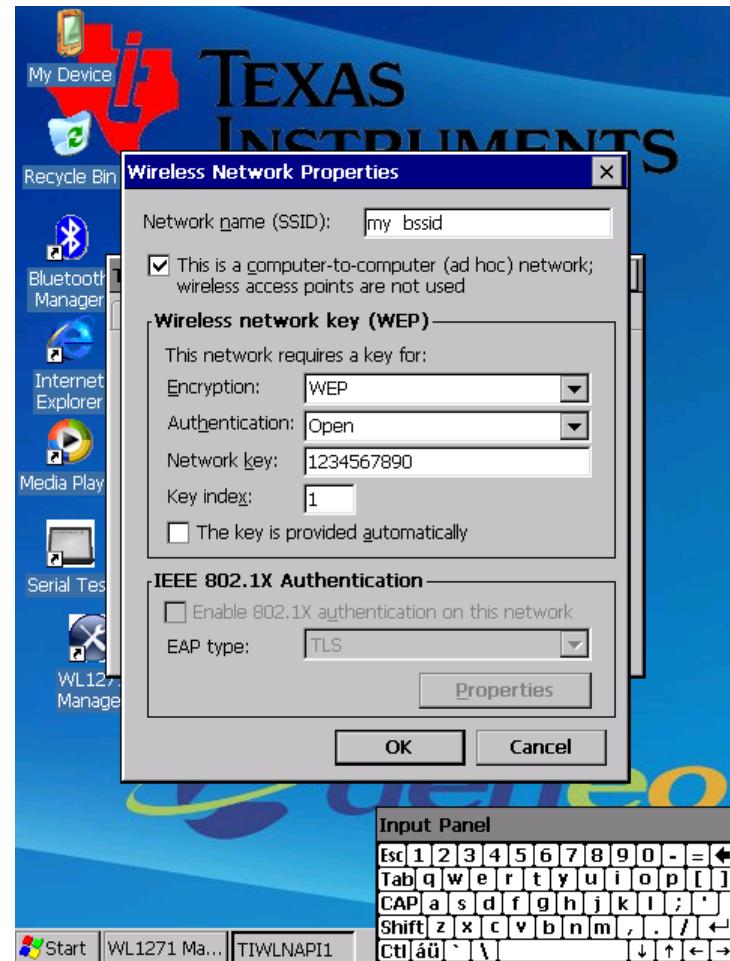
- Open the ZeroConfig application



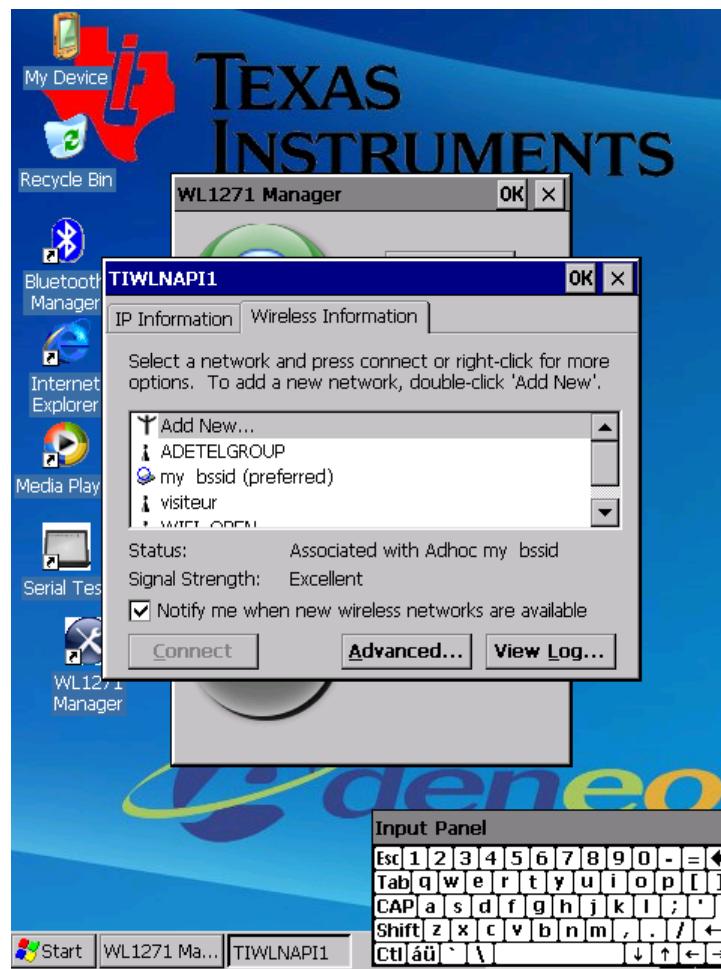
- Select the Add New in the list



- Configure the IBSS and name it my BSSID
 - Make sure that the checkbox 'This is a computer-to-computer (ad hoc) network....' is checked



- Connect other devices to the my bssid network



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.

3.2.4.2 Join IBSS Network

- Configure the WiFi station to create an IBSS network.
- Execute an Application Scan command from the ticon 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 ZeroConfig GUI
- Select the AP in the network list
- Hit connect button to connect to the target
- Configure a static IP address on both stations.
- Run a Ping command from the SUT to the WiFi station.

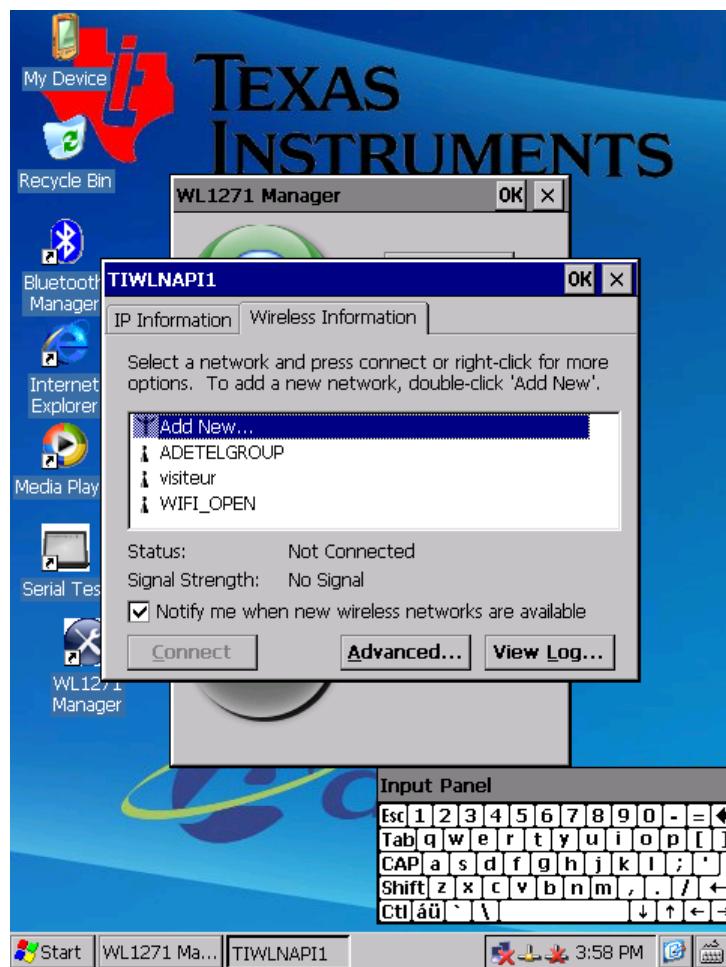
Expected result:

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

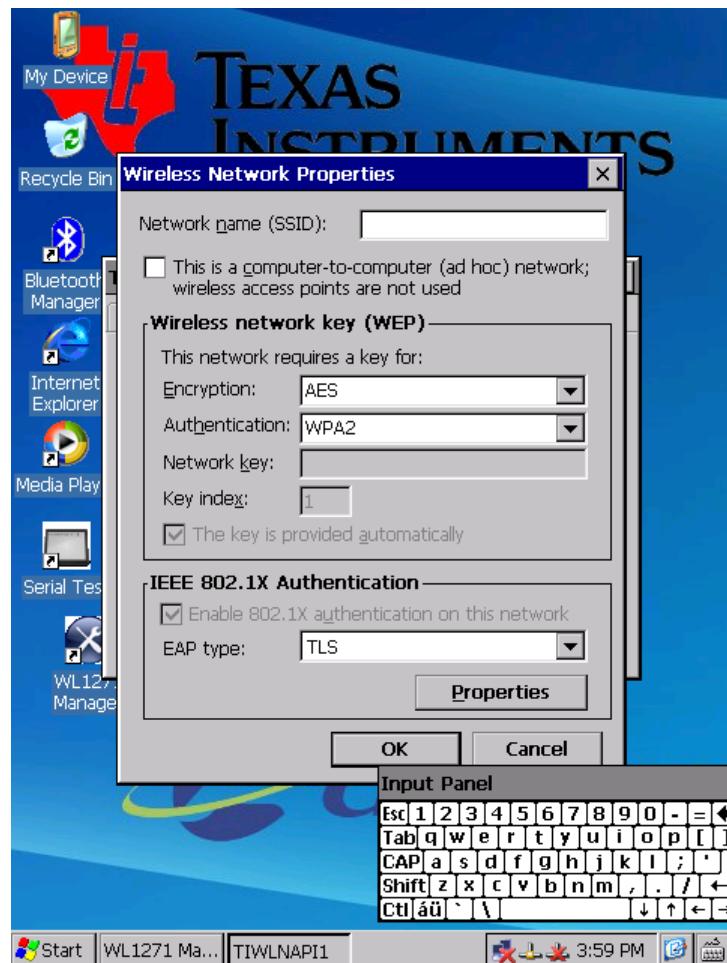
3.2.5 *Hidden SSID*

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

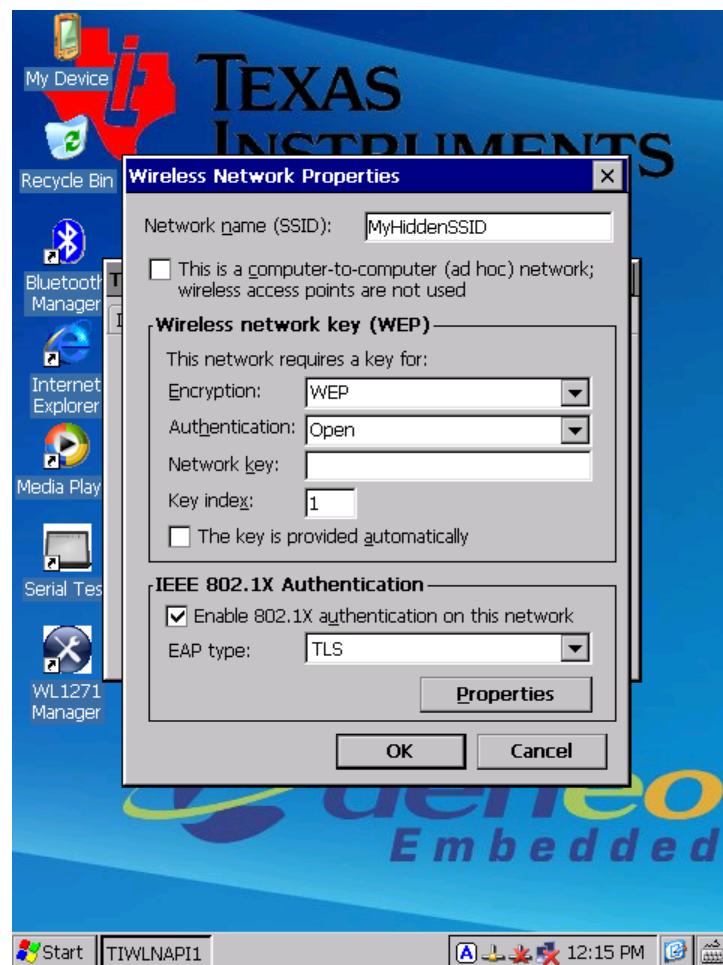
- Configure the AP to Hidden SSID mode with the SSID value **MyHiddenSSID**. In this state, the AP does not advertise the SSID in the beacons.
- Open the ZeroConfig application



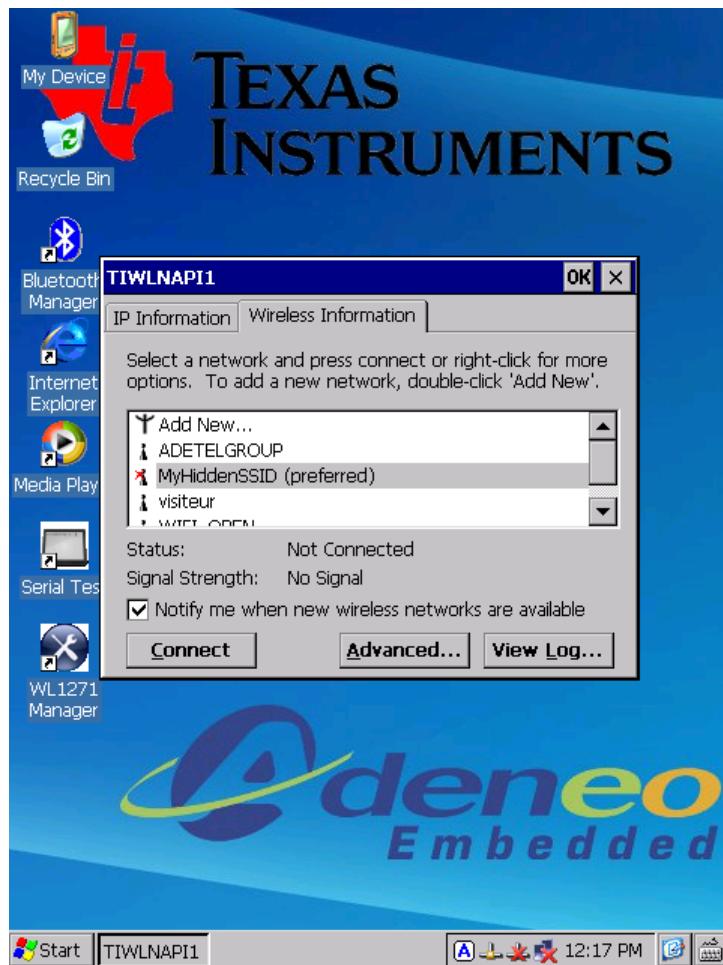
- Select the Add New in the list



- Configure the hidden network settings



- Connect the SUT to the AP. You may select **MyHiddenSSID** in the list and hit the connect button



- 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

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.

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.

3.4 BT Testing

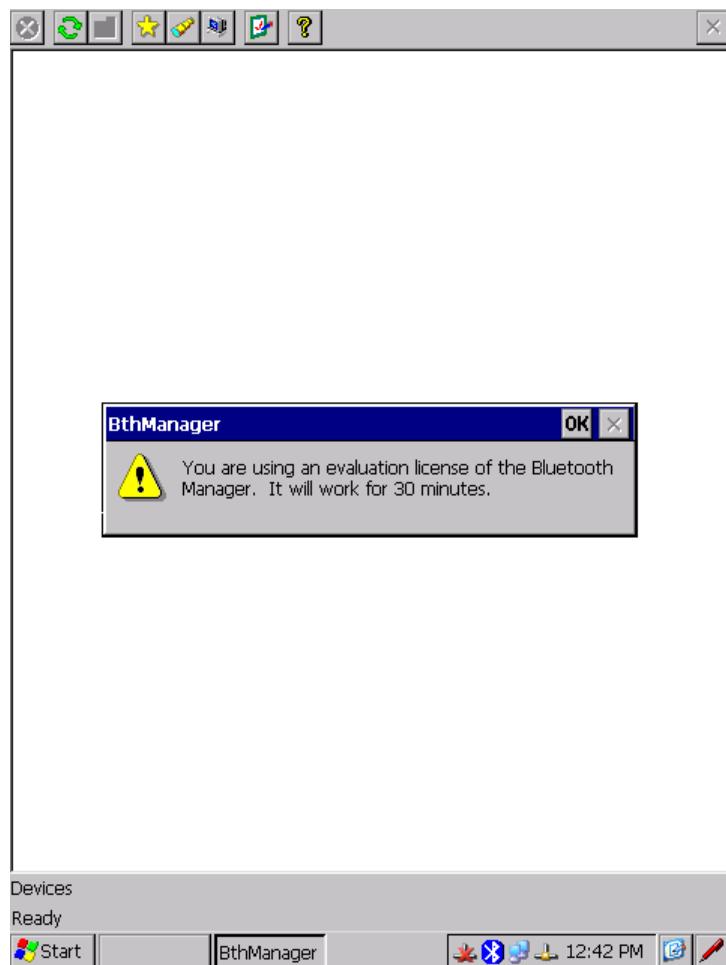
BT testing tests the basic operation of the BT stack and the functionality of the BT Device Under Test (DUT). The WLAN should be turned off during BT tests.

3.4.1 A2DP Profile

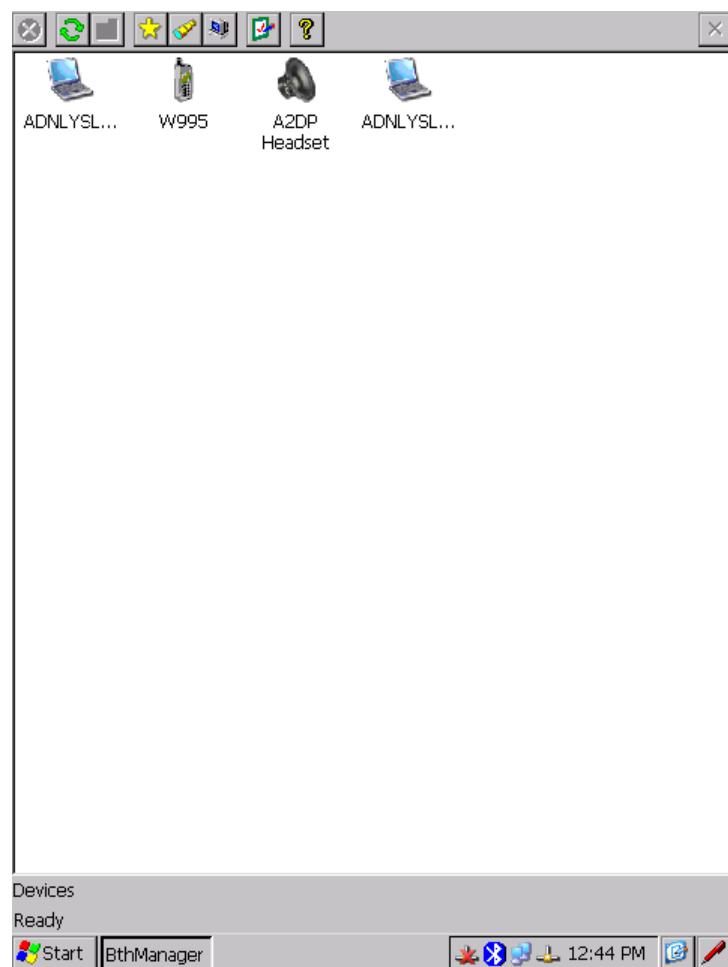
For this test, BT should be able to connect an A2DP-supported headset and an audio file should be played with high quality.

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

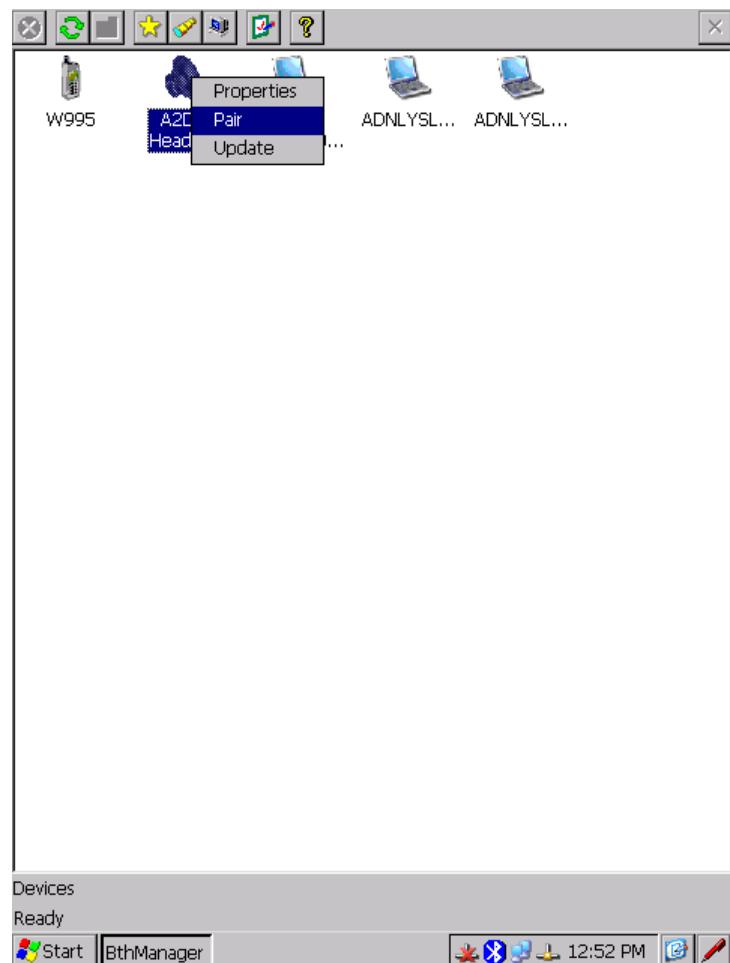
- After loading the device, Launch the Bluetooth Manager



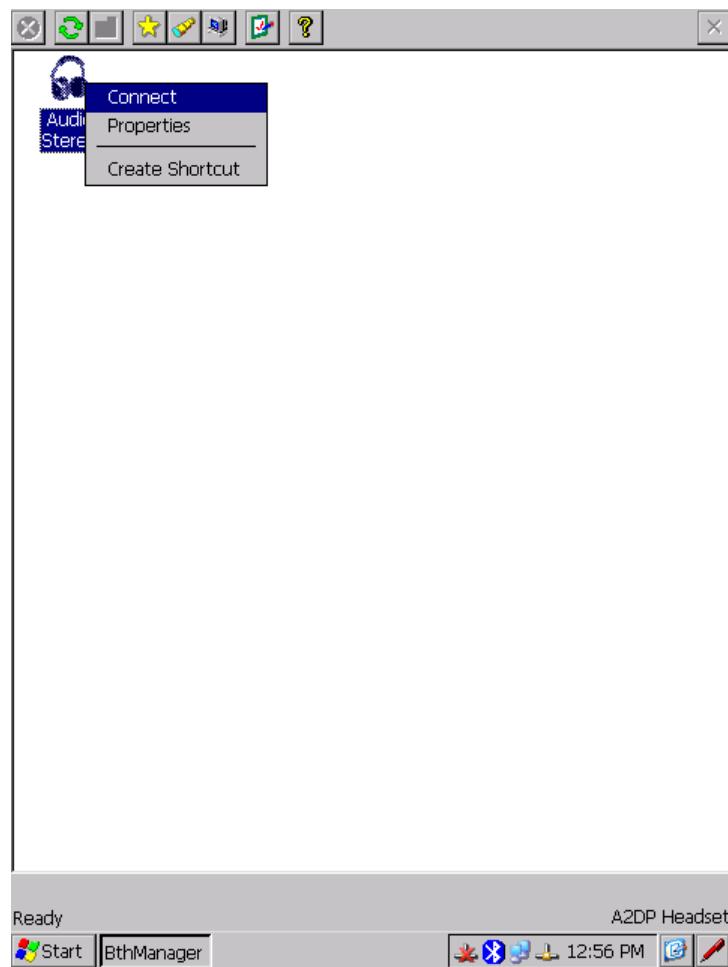
- Inquiry and pair with the A2DP headset



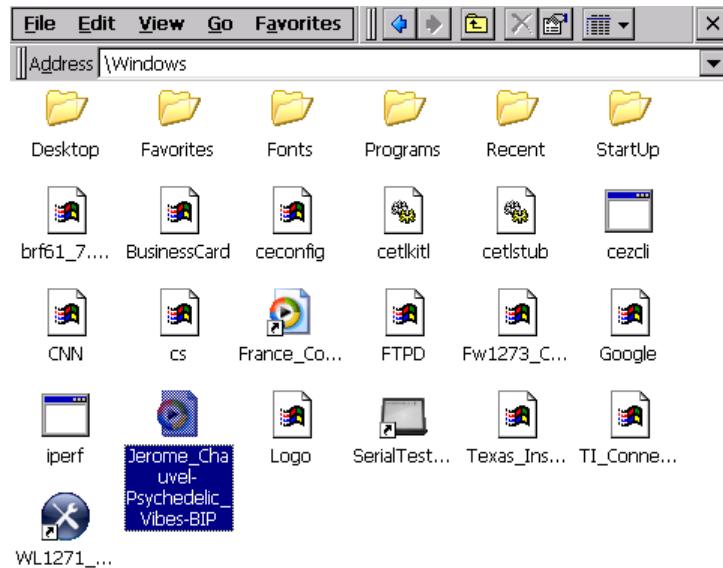
- Pair with the A2DP headset and enter pin code (see headset documentation for default pin code of your device)



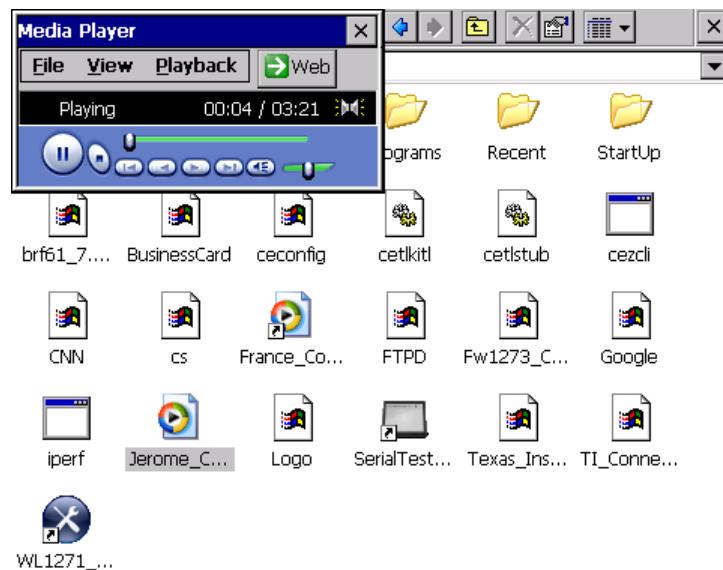
- List the A2DP device services and connect to A2DP service



- Switch to File Explorer without closing the Bluetooth Manager, otherwise you will lose the connection with the headset. And select the MP3 file located in the windows folder. If there is no MP3 in the windows folder, copy one to an SD card or USB flash drive and use it instead.



- Double click on it to launch the Media Player

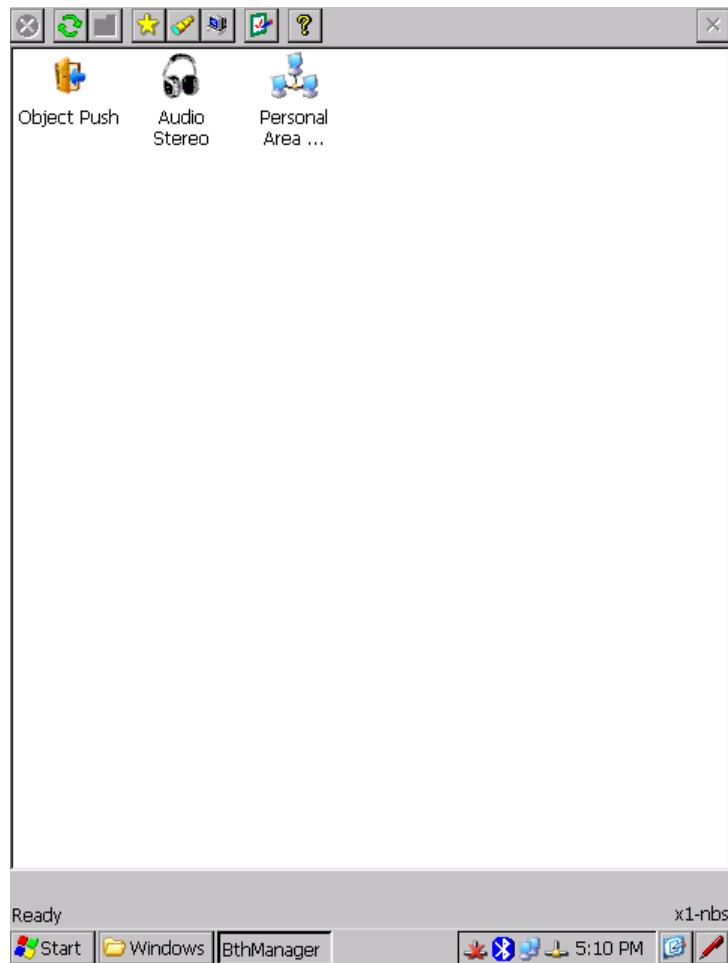
**Expected result:**

The file plays successfully and music sounds clear.

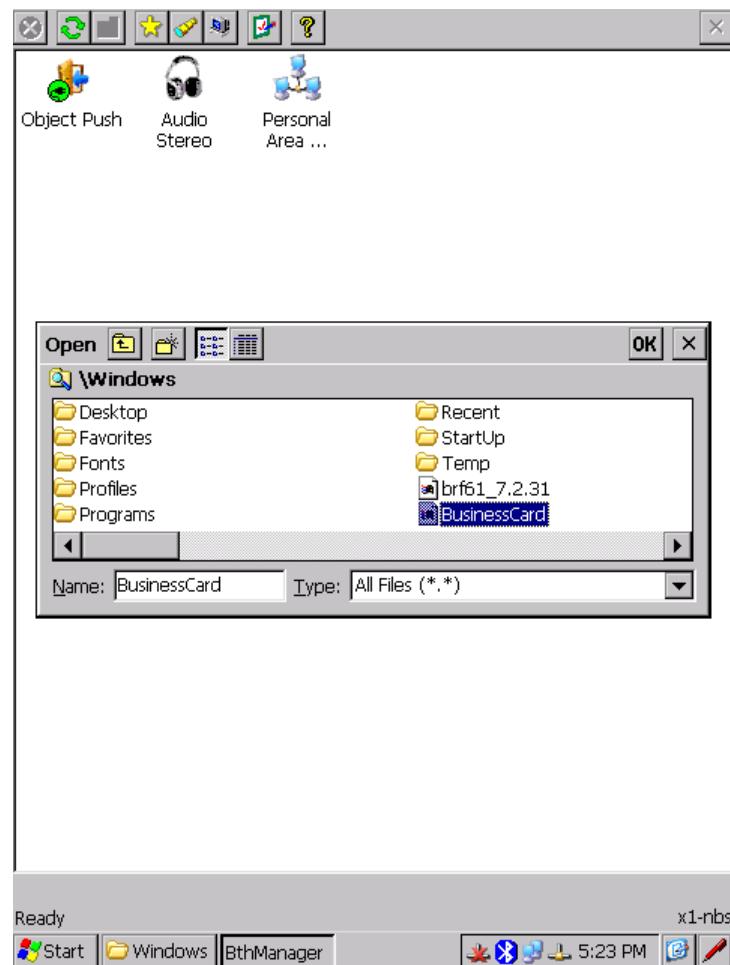
3.4.2 Object Push Profile

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).

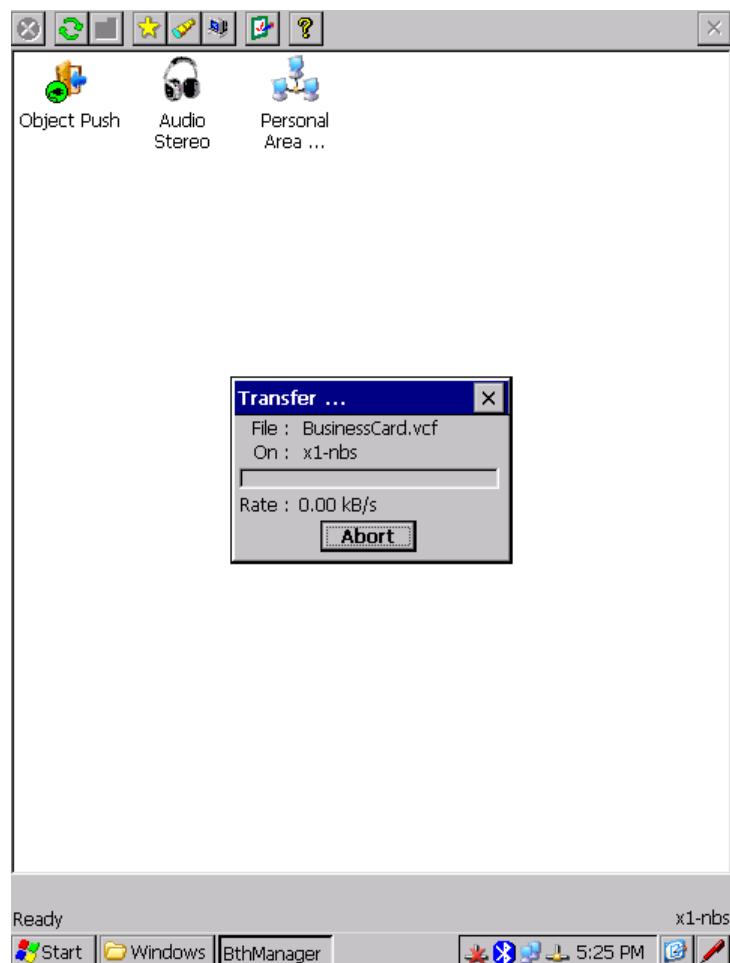
- From the Bluetooth Manager Launch inquiry; for the identified device (most common devices accepting vCards are Bluetooth Enable Phones), list the remote services



- Select Object Push service and push a file. You can select BusinessCard file located in Windows folder.



- Hit OK to start transfer

**Expected result:**

The file is received successfully and can be opened.

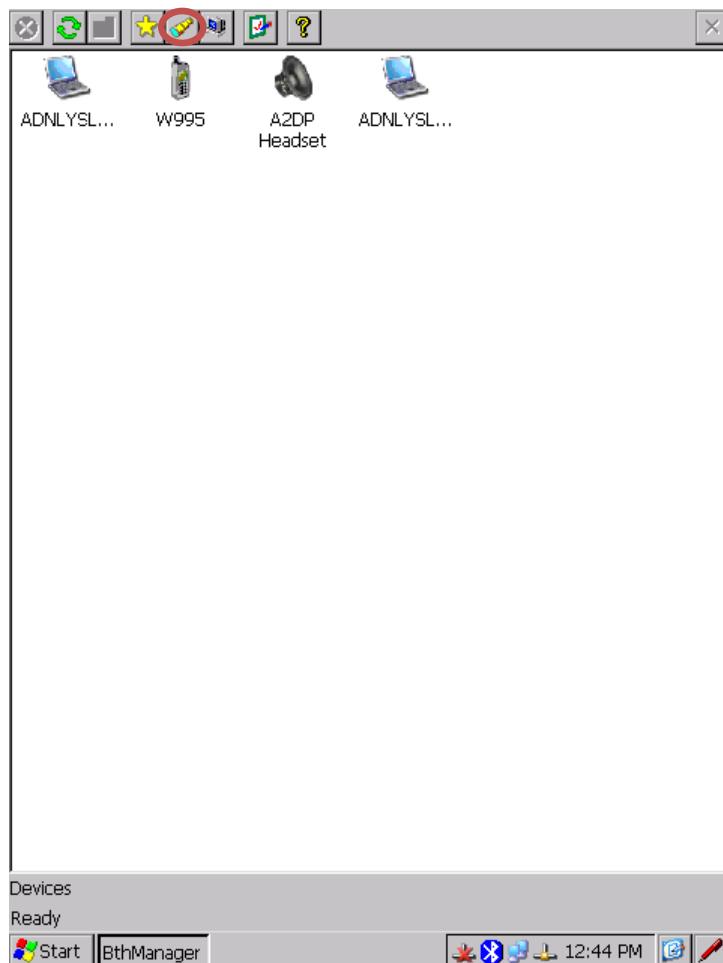
3.4.3 BT Inquiry and Inquiry Scan

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 Manager from the Windows CE desktop shell, and hit the long-view icon:



- Leave this configuration for the next step.

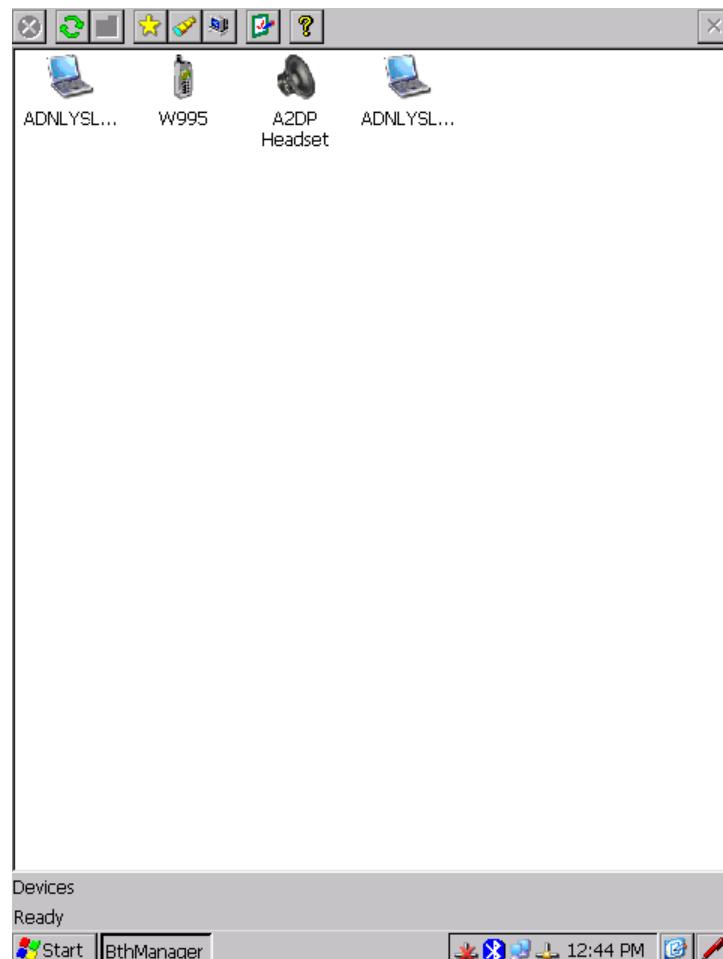
Expected result:

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:



- 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 WL1271 Manager application and read the BSSID List from the ZeroConfig window.
- 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 start an FTP transfer by downloading a 5Mbyte file from the SUT to the PC behind the AP.

Expected result:

The file is received successfully by the BT handset. The SUT runs the FTP transfer 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 launch an FTP transfer between the PC behind the AP and the SUT.

Expected result:

The music sounds clear. The SUT receives file through FTP 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.
- Start an FTP transfer between the SUT and 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.
- Start an FTP transfer between the PC behind the AP and 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.
- Start an FTP transfer between the PC behind the AP and 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 ZeroConfig window and the advanced menu:
- 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 FTP command from the PC to the SUT 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 FTP 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 FTP command from the PC behind the AP to the SUT.
- Connect the BT DUT to an A2DP device.
- Play a *.mp3 file repeatedly (use the Repeat option in the Playback menu of the Media Player).
- 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.

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 **regedit** and click **OK**. The **Registry Editor** window is displayed:

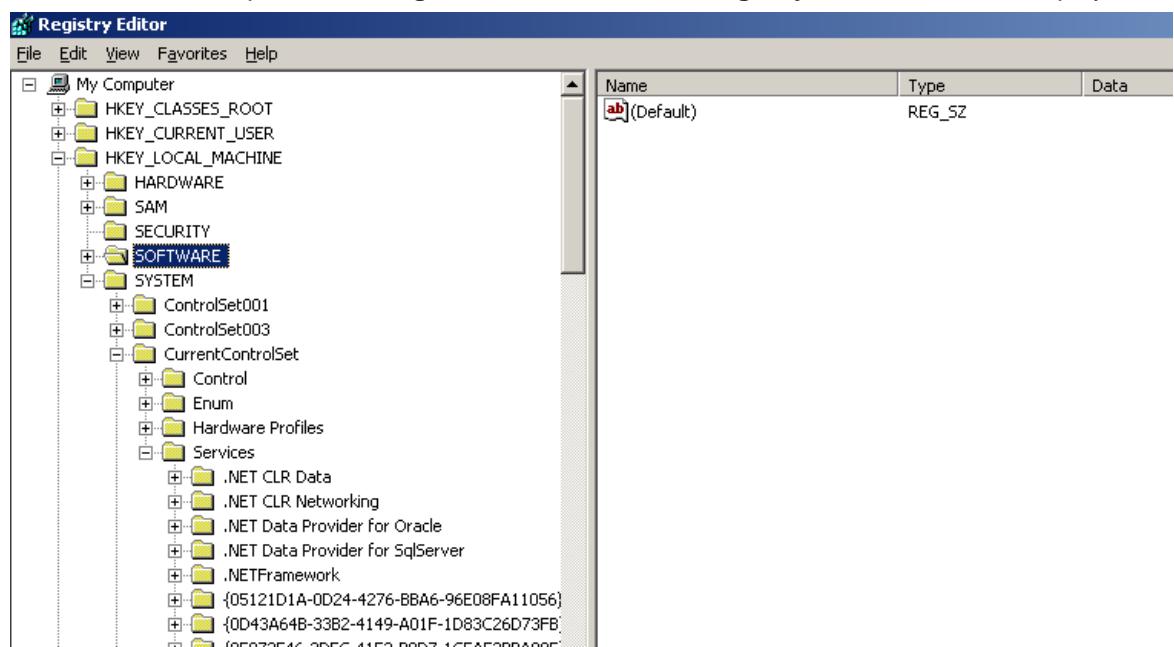


Figure 2: Registry Window

- 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:

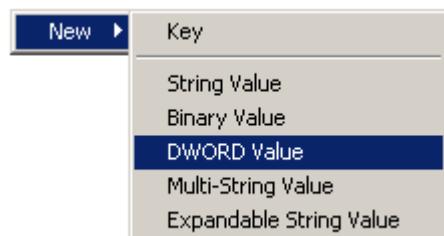


Figure 3: DWORD Right-click Option

The following window is displayed:

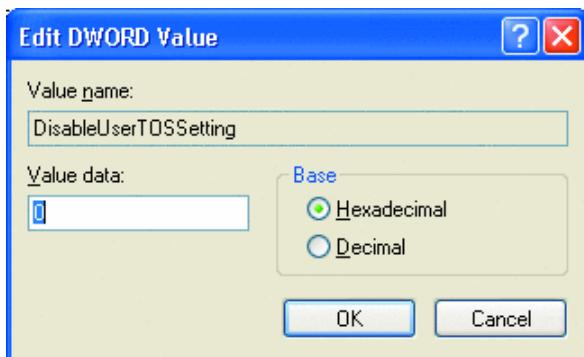


Figure 4: Edit DWORD Value Window

- 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