**Table of Contents**

**1** **Introduction**

[**1.1** **Purpose and Scope**](#h.1fob9te)

**1.2** **Glossary**

[**1.3** **References**](#h.2et92p0)

[**2** **Test Specification**](#h.3dy6vkm)

[**2.1** **Basic Test cases**](#h.4d34og8)

[**2.2** **Authentication and Encryption Test cases**](#h.3rdcrjn)

**2.3** **Reconnection test cases**

[**2.4** **Throughput Test cases**](#h.26in1rg)

[**2.5** **Mode 802.11(a/b/g/n) Test cases**](#h.1ksv4uv)

[**2.6** **Regression Test cases**](#h.2jxsxqh)

[**2.7** **API Test cases**](#h.z337ya)

1. **Introduction**
   1. **Purpose and Scope**

The purpose of this document is to describe the Software Test Specification for testing 8787 Wifi driver.. This document describes the detailed test cases for Testing Wifi device.

* 1. **Glossary**

|  |  |
| --- | --- |
| **Acronyms** | **Description** |
| AP | Access Point |
| STA | Station |
| WEP | Wired Equivalent Privacy |
| WPA | Wi-Fi Protected Access |
| WPA2 | Wi-Fi Protected Access II |
| PSK | Pre-Shared Key |
| TKIP | Temporal Key Integrity Protocol |
| AES | Advanced Encryption Standard |
| TCP | Transmission Control Protocol |

* 1. **References**
* ZSES150011 -RS-R1.2-REL1.0 – SoftwareRequirementSpecification

1. **Test Specification**

Following are the type of test,

* Basic Test cases
* Authentication and Encryption Test cases
* Reconnection test cases
* Throughput Test cases
* Mode 802.11(a/b/g/n) Test cases
* Regression Test cases

* 1. **Basic Test cases**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | Set authentication to OPEN. If device is connected to the network, ping the host IP address. |  |
| 2 | Set authentication to WEP. If device is connected to the network, ping the host IP address. |  |
| 3 | Set authentication to WPA. If device is connected to the network, ping the host IP address. |  |
| 4 | Set authentication to WPA2. If device is connected to the network, ping the host IP address. |  |
| 5 | Set authentication to WPA, WPA2 mixed mode. If device is connected to the network, ping the host IP address. |  |

* 1. **Authentication and Encryption Test cases**

**Open authentication test case**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | Auth=Open; Cipher=ClearText |  |
| 2 | Auth=Open; Cipher=WEP 40-bit key |  |
| 3 | Auth=Open; Cipher=WEP 104-bit key |  |

**Shared authentication test** **case**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | This test case should fail AP: Auth=Shared, Cipher=WEP STA: Auth=Shared, Cipher=ClearText |  |
| 2 | Auth=Shared; Cipher=WEP 40-bit key |  |
| 3 | Auth=Shared; Cipher=WEP 104-bit key |  |

**WPA-PSK authentication test cases**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | *Negative test*  AP: Auth=WPA\_PSK, Cipher=TKIP; STA: Auth=WPA\_PSK, Cipher=ClearText |  |
| 2 | Auth=WPA\_PSK; Cipher=TKIP 63-digit passphrase |  |
| 3 | Auth=WPA\_PSK; Cipher=TKIP 8-digit passphrase |  |
| 4 | *Negative test*  Auth=WPA\_PSK; Cipher=TKIP 7-digit passphrase |  |
| 5 | *Negative test*  Auth=WPA\_PSK; Cipher=TKIP 64-digit passphrase |  |
| 6 | Auth=WPA\_PSK; Cipher=AES 63-digit passphrase |  |
| 7 | Auth=WPA\_PSK; Cipher=AES 8-digit passphrase |  |
| 8 | *Negative test*  Auth=WPA\_PSK; Cipher=AES 7-digit passphrase |  |
| 9 | *Negative test*  Auth=WPA\_PSK; Cipher=AES 64-digit passphrase |  |

**WPA2-PSK authentication test case**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | *Negative test*  AP: Auth=WPA2\_PSK, Cipher=TKIP; STA: Auth=WPA2\_PSK, Cipher=ClearText. |  |
| 2 | *Negative test*  AP: Auth=WPA2\_PSK, Cipher=AES; STA: Auth=WPA2\_PSK, Cipher=ClearText |  |
| 3 | Auth=WPA2\_PSK; Cipher=TKIP 63-digit pass phrase |  |
| 4 | Auth=WPA2\_PSK; Cipher=TKIP 8-digit pass phrase |  |
| 5 | *Negative test*  Auth=WPA2\_PSK; Cipher=TKIP 7-digit pass phrase |  |
| 6 | *Negative test*  Auth=WPA2\_PSK; Cipher=TKIP 64-digit pass phrase |  |
| 7 | Auth=WPA2\_PSK; Cipher=AES 63-digit pass phrase |  |
| 8 | Auth=WPA2\_PSK; Cipher=AES 8-digit pass phrase |  |
| 9 | *Negative test*  Auth=WPA2\_PSK; Cipher=AES 7-digit pass phrase |  |
| 10 | *Negative test*  Auth=WPA2\_PSK; Cipher=AES 64-digit pass phrase |  |

**WPA, WPA2-PSK mixed mode authentication test case**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | *Negative test*  AP: Auth=WPA+WPA2\_PSK, Cipher=TKIP; STA: Auth=WPA+WPA2\_PSK, Cipher=ClearText. |  |
| 2 | *Negative test*  AP: Auth=WPA+WPA2\_PSK, Cipher=AES; STA: Auth=WPA+WPA2\_PSK, Cipher=ClearText. |  |
| 3 | Auth=WPA+WPA2\_PSK; Cipher=TKIP 63-digit pass phrase |  |
| 4 | Auth=WPA+WPA2\_PSK; Cipher=TKIP 8-digit pass phrase |  |
| 5 | *Negative test*  Auth=WPA+WPA2\_PSK; Cipher=TKIP 7-digit pass phrase |  |
| 6 | *Negative test*  Auth=WPA+WPA2\_PSK; Cipher=TKIP 64-digit pass phrase |  |
| 7 | Auth=WPA+WPA2\_PSK; Cipher=AES 63-digit pass phrase |  |
| 8 | Auth=WPA+WPA2\_PSK; Cipher=AES 8-digit pass phrase |  |
| 9 | *Negative test*  Auth=WPA+WPA2\_PSK; Cipher=AES 7-digit pass phrase |  |
| 10 | *Negative test*  Auth=WPA+WPA2\_PSK; Cipher=AES 64-digit pass phrase |  |

* 1. **Reconnection test cases**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | Connect the device to Wifi AP, Take the device far away from the AP. Device will be disconnected due to the lack of signal strength.  Bring back the device to the AP and see whether the device is connected back again to the AP. |  |
| 2 | Connect the device to Wifi AP, Switch off the AP. The device will be disconnected due to the complete drop of signal strength.  Switch ON the AP and see whether the device is connecting to the AP. |  |
| 3 | If the Station has been already configured with Wifi AP, but AP reaches maximum connection limit. In this case the station should automatically reconnect to Wifi AP, when the number of stations connected to AP become less than the maximum limit. |  |

* 1. **Throughput Test cases**

**Server :** PC

**Client :** Board

|  |  |  |  |
| --- | --- | --- | --- |
| **Test case** | **Server** | **Client** | **Results** |
| 1 | Server listening on client  TCP window size: 85.3 KByte (default) | Client Connecting to server  TCP window size: 16.0 KByte (default) |  |
| 2 | Server listening on client  TCP window size: 160 KByte (WARNING: requested 80.0 KByte) | Client connecting to server  TCP window size: 160 KByte (WARNING: requested 80.0 KByte) |  |
| 3 | Server listening on client  TCP window size: 200 KByte (WARNING: requested 100 KByte) | Client connecting to server  TCP window size: 200 KByte (WARNING: requested 100 KByte) |  |
| 4 | Server listening on client  TCP window size: 300 KByte (WARNING: requested 150 KByte) | Client connecting to server  TCP window size: 256 KByte (WARNING: requested 150 KByte) |  |
| 5 | Server listening on client  TCP window size: 400 KByte (WARNING: requested 200 KByte) | Client connecting to server  TCP window size: 256 KByte (WARNING: requested 200 KByte) |  |
| 6 | Server listening on client  TCP window size: 416 KByte (WARNING: requested 256 KByte) | Client connecting to server  TCP window size: 256 KByte (WARNING: requested 256 KByte) |  |

**Server :** Board

**Client :** PC

|  |  |  |  |
| --- | --- | --- | --- |
| **Test case** | **Server** | **Client** | **Results** |
| 1 | Server listening on client  TCP window size: 85.3 KByte (default) | Client connecting to server  TCP window size: 22.9 KByte (default) |  |
| 2 | Server listening on client  TCP window size: 160 KByte (WARNING: requested 80.0 KByte) | Client connecting to server TCP window size: 160 KByte (WARNING: requested 80.0 KByte) |  |
| 3 | Server listening on client  TCP window size: 200 KByte (WARNING: requested 100 KByte) | Client connecting to server  TCP window size: 200 KByte (WARNING: requested 100 KByte) |  |
| 4 | Server listening on client  TCP window size: 300 KByte (WARNING: requested 150 KByte) | Client connecting to server  TCP window size: 256 KByte (WARNING: requested 150 KByte) |  |
| 5 | Server listening on client  TCP window size: 400 KByte (WARNING: requested 200 KByte) | Client connecting to server  TCP window size: 256 KByte (WARNING: requested 200 KByte) |  |
| 6 | Server listening on client  TCP window size: 416 KByte (WARNING: requested 256 KByte) | Client connecting to server  TCP window size: 256 KByte (WARNING: requested 256 KByte) |  |

* 1. **Mode 802.11(b/g/n) Test cases**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | Check whether the 802.11b speed is around 11Mbps and its range is about 150 feet and frequency is at 2.4 GHz. |  |
| 2 | Check 802.11bg whether the speed is around 54Mbps and its range is about 50 feet and frequency is at 2.4 GHz. |  |
| 3 | Check whether the 802.11n speed is within the 54-600 Mbps and its range is about 175 feet and frequency is at 2.4/5 GHz. |  |

* 1. **Regression Test cases**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | Create five access points with different authentication modes like OPEN, WEP, WPA, WPA2 and WPA, WPA2 mixed mode. Connect the station to different access point one by one, by the below mentioned order.   1. Connect STA with OPEN mode to AP1 (OPEN mode) 2. Disconnect STA 3. Connect STA with WEP mode to AP2 (WEP mode) 4. Disconnect STA 5. Connect STA with WPA mode to AP3 (WPA mode) 6. Disconnect STA 7. Connect STA with WPA2 mode to AP4 (WPA2 mode) 8. Disconnect STA 9. Connect STA with WPA,WPA2 mixed mode to AP5 (WPA,WPA2 mixed mode) |  |
| 2 | Create five access points with different authentication mode like OPEN, WEP, WPA, WPA2 and WPA, WPA2 mixed mode. Connect the station to different access point one by one, by the below mentioned order.   1. Connect STA with WEP mode to AP2 (WEP mode) 2. Disconnect STA 3. Connect STA with OPEN mode to AP1 (OPEN mode) 4. Disconnect STA 5. Connect STA with WPA mode to AP3 (WPA mode) 6. Disconnect STA 7. Connect STA with WPA2 mode to AP4 (WPA2 mode) 8. Disconnect STA 9. Connect STA with WPA,WPA2 mixed mode to AP5 (WPA,WPA2 mixed mode) |  |
| 3 | Create five access points with different authentication mode like OPEN, WEP, WPA, WPA2 and WPA, WPA2 mixed mode. Connect the station to different access point one by one, by the below mentioned order.   1. Connect STA with WEP mode to AP2 (WEP mode) 2. Disconnect STA 3. Connect STA with WPA mode to AP3 (WPA mode) 4. Disconnect STA 5. Connect STA with OPEN mode to AP1 (OPEN mode) 6. Disconnect STA 7. Connect STA with WPA2 mode to AP4 (WPA2 mode) 8. Disconnect STA 9. Connect STA with WPA,WPA2 mixed mode to AP5 (WPA,WPA2 mixed mode) |  |
| 4 | Create five access points with different authentication mode like Open, WEP, WPA, WPA2 and WPA, WPA2 mixed mode. Connect the station to different access point one by one, by the below mentioned order.   1. Connect STA with WEP mode to AP2 (WEP mode) 2. Disconnect STA 3. Connect STA with WPA mode to AP3 (WPA mode) 4. Disconnect STA 5. Connect STA with WPA2 mode to AP4 (WPA2 mode) 6. Disconnect STA 7. Connect STA with OPEN mode to AP1 (OPEN mode) 8. Disconnect STA 9. Connect STA with WPA,WPA2 mixed mode to AP5 (WPA,WPA2 mixed mode) |  |
| 5 | Create five access points with different authentication mode like OPEN, WEP, WPA, WPA2 and WPA, WPA2 mixed mode. Connect the station to different access point one by one, by the below mentioned order.   1. Connect STA with WEP mode to AP2 (WEP mode) 2. Disconnect STA 3. Connect STA with WPA mode to AP3 (WPA mode) 4. Disconnect STA 5. Connect STA with WPA2 mode to AP4 (WPA2 mode) 6. Disconnect STA 7. Connect STA with WPA,WPA2 mixed mode to AP5 (WPA,WPA2 mixed mode) 8. Disconnect STA 9. Connect STA with OPEN mode to AP1 (OPEN mode) |  |

* 1. **API Test cases**

|  |  |  |
| --- | --- | --- |
| **Test case** | **Description** | **Results** |
| 1 | All User APIs will be tested individually. |  |