UM11567

WFA Certification Guide for NXP-based Wireless Modules on i.MX RT Platform Running RTOS

Rev. 5 — 29 June 2023 User manual

Document Information

Information	Content
Keywords	Wi-Fi Alliance (WFA), certification, NXP-based wireless modules, i.MX RT Platform
Abstract	Provides the step-by-step procedure of WFA certification for NXP-based wireless modules on i.MX RT platform running RTOS.

1 Revision history

Revision history

Rev	Date	Description
v.1	20210414	Initial version
v.2	20220110	**Modifications** • Section 4.6 "Wi-Fi 5 (802.11ac) certification program": added
v.3	20220314	**Modifications** • Figure 1 "Test setup" updated (removed APUT) • Section 3.3 "Most used commands": – Added a note in the introduction – Section 3.3.1 "wlan-version command": added – Replaced `psk` parameter with `passphrase` • Section 4.1.3 "Test case N-5.2.11": updated the section *Start iPerf traffic* • Section 4.2 "Protected management frame (PMF) certification program": – Removed the `pmfcfg` command from the procedure and added `mfpc mfpr` to `wlan-add` command – Added the Note about the use of QTT for some test cases • Section 4.3 "WPA3 (WPA3 SAE) certification program": removed the `pmfcfg` command from the procedure and added `mfpc mfpr` to `wlan-add` command • Section 4.5 "Security vulnerability detection (SVD) certification" modified a Wi-Fi profile by adding a static IP address • Section 6 "Acronyms and abbreviations" added WTS and QTT acronyms
v.4	20220915	**Modifications** • Section 2.1 "Purpose and scope": removed the reference to 88W8977 device
v.5	20230629	**Modifications** • Section 2.1 "Purpose and scope": added IW612 • Section 4.3 "WPA3 (WPA3 SAE) certification program": added a note about WPA3 SAE test cases • Section 4.5 "Security vulnerability detection (SVD) certification": added a note about SVD test cases • Section 7 "Note about the source code in the document": added

2 About this document

2.1 Purpose and scope

This document describes the test setup and procedure used for WFA certification of Wi-Fi features like 802.11n, protected management frames (PMF), WPA3, security enhancement, and security vulnerability detection of NXP wireless devices such as 88W8801, 88W8987, IW416 and IW612[1]. This document applies to NXP-based wireless modules connected to i.MX RT platform running RTOS.

The users should be familiar with the user manuals reference UM11441, UM11442, and UM11443.

2.2 References

Table 1. Reference documents

Document type	Document title
User manual	Getting Started with NXP-based Wireless Modules and i.MX RT Platform Running RTOS (UM11441)
User manual	Wi-Fi and Bluetooth Demo Applications for i.MX RT platforms (UM11442)
User manual	Wi-Fi Debug Feature Configuration Guide for MCUXpresso SDK (UM11443)

2.3 Considerations

The readers should have some knowledge of Wi-Fi terminologies and certification.

1 IW612 module support is available only in i.MX RT1170 EVKB and SDK version 2.13.2.

3 Pre-certification test procedure

The pre-certification test procedure is done for the purposes of the development, quality assurance and preparation for WFA certification test. The test procedure increases the probability and confidence for passing the tests successfully in the Wi-Fi Alliance certification lab.

3.1 Test setup

Figure 1 illustrates the test setup.

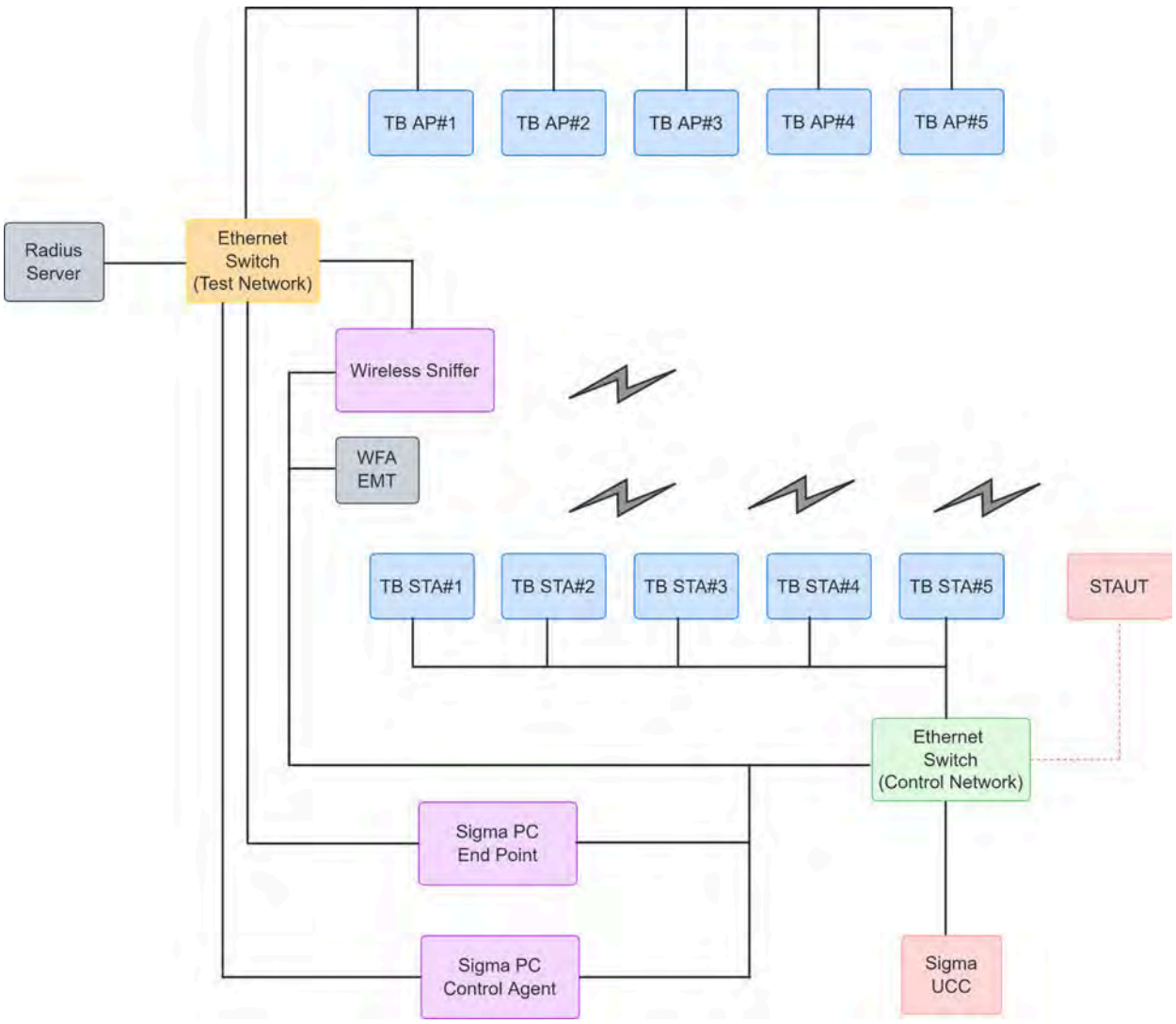

Figure 1. Test setup

3.2 Test procedure

The test procedure requires the setup based on the setup diagram and ensure that the test network and control network are up and running.

- Connect the DUT
  - Connect the DUT to the control network. The control network is the Ethernet switch, and the DUT will connect to it via Ethernet.
  - Assign the control network IP to the wired interface
- Configure the device
  - Open the device serial console
  - Configure the device as per the test case

3.3 Most used commands

This section describes the commands most used in the test programs.

Note: *For more details on the commands, refer to wifi_cert sample application in UM11442.*

3.3.1 `wlan-version` command

This command is used to get Wi-Fi firmware and driver version.

Syntax: `wlan-version`

Example:

```
wlan-version
WLAN Version : X-V0, RF878X, FP91, X.X.X
```

3.3.2 `wlan-scan` command

This command is used to scan the network.

Syntax: `wlan-scan`

3.3.3 `wlan-add` command

This command is used to add a network configuration.

Syntax: `wlan-add "profilename" ssid "ssid" ip:ipaddr,gateway,netmask wpa2 "passphrase"`

Where:

Command parameter	Description
`profilename`	Network profile name, with values of 0, 1,or 2
`ssid`	Service set identifier
`psk`	Password for the AP network

Note: *If DHCP IP is required in the test case, don't add the static IP address in the `wlan-add` command.*

3.3.4 `wlan-list` command

This command is used to list the profiles.

Syntax: `wlan-list`

3.3.5 `wlan-remove` command

This command is used to remove profiles.

Syntax: `wlan-remove "profilename"`

Where:

Command parameter	Description
`profilename`	Network profile name, with values of 0, 1,or 2

3.3.6 `wlan-disconnect` command

This command is used to disconnect.

Syntax: `wlan-disconnect`

3.3.7 `help` command

This command is used to for any command help.

Syntax: `help`

4 Certification program execution

This section shows how to execute the certification programs for the set of Wi-Fi features.

4.1 Wi-Fi 4 (802.11n) certification program

4.1.1 Test case N-5.2.3

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "WKV(*+8210" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "wpa2wpa2"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STAs

- Run the command to run *iPerf* in server mode for STAUT:

```
iperf -s
```

- Run the command to run *iPerf* in client mode for the AP back-end:

```
iperf -c <STAUT IP address> -t <number of seconds to transmit for>
```

- Run the command to run *iPerf* in server mode for the AP back-end:

```
iperf -s
```

- Run the command to run *iPerf* in client mode for STAUT:

```
iperf -c <AP backend IP address> -t <number of seconds to transmit for>
```

- Run the command to run *iPerf* in server mode for STAUT:

```
iperf -s
```

- Run the command to run *iPerf* in client mode and dual test mode for AP back-end during 30 seconds:

```
iperf -c <STAUT IP address> -d -t 30
```

- Run the command to run *iPerf* in server mode for the AP back-end:

```
iperf -s
```

- Run the command to run *iPerf* in client mode for STAUT:

```
iperf -c <AP backend IP address> -t <number of seconds to transmit for>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.2 Test case N-5.2.5

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "abcedfghijklmnopqrstuvwxyzABCDEF"
 ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "abcedfghijklmnopqrstuvwxyzABCDEF"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STAs

Traffic between the AP and STAs:

- DT1: iperf on STAUT and chriot for testbed sta, start at same time
- DT2: iperf on STAUT and chriot for testbed sta, start at same time
- DT3: iperf on STAUT and chriot for testbed sta, start at same time

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.3 Test case N-5.2.11

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "OBEW23@?+" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "OBEW23@?+"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Start iPerf traffic

- Run the command to run iPerf in server mode for the STAUT:

```
iperf –s -u
```

- Run the command to run iPerf in client mode for AP back-end:

```
iperf –c <server IP address> -d –u
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.4 Test case N-5.2.14

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Multicast" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "Multicast"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STAs

STAUT Tx of multicast traffic

- AP back-end:

```
iperf –s -u -B 224.0.0.5 -i 1
```

- STA1:

```
iperf –s -B 224.0.0.5 -u -i 1
```

- STAUT:

```
iperf -c 224.0.0.5 -u -t <number of seconds to transmit for>
```

STAUT Rx of multicast traffic

- AP back-end:

```
iperf -c 224.0.0.5 -u -i 1 -t <number of seconds to transmit for>
```

- STA1:

```
iperf –s -B 224.0.0.5 -u -i 1
```

- STAUT:

```
iperf -s -B 224.0.0.5 -u
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.5 Test case N-5.2.19

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Negative" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.6 Test case N-5.2.26

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "01234567890123456789012345678901"
 ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "01234567890123456789012345678901"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Start a continuous ping from STAUT to the AP back-end:

```
ping -s 1000 <ip address of backend>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.7 Test case N-5.2.28

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "12345678" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Use the script stored in *5.2.28* directory

- AP back-end:

```
iperf -s
```

- STAUT:

```
iperf -c <server IP> -t 30
```

- Start chariot traffic from STA1 to AP back-end

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.8 Test case N-5.2.29

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "5.2.29" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Use the script stored in *5.2.29* directory

- AP back-end:

```
iperf -s
```

- STAUT:

```
iperf -c <server IP> -t 30
```

- Start chariot traffic from STA1 to AP back-end

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.9 Test case N-5.2.35

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "%@^98jhB" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "%@^98jhB"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Start a continuous ping from STAUT to the AP:

```
ping -s 10000 <IP address of AP back-end>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.10 Test case N-5.2.36

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "5.2.36" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.11 Test case N-5.2.37

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "NONE0WPA2PSK" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "NONE0WPA2PSK"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

- STAUT:

```
iperf –s -u
```

- AP back-end:

```
iperf –c <STAUT IP> -u –b 60M -t 30
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.12 Test case N-5.2.38

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "5.2.38" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

- STAUT:

```
iperf –s -u
```

- AP back-end:

```
iperf –c <server IP> -u –b 60M -t 90
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.13 Test case N-5.2.39

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "AP1-5.2.39" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

- AP back-end:

```
iperf –s
```

- STAUT:

```
iperf –c <server IP> -t 60
```

- Start the traffic between STA1 and AP2 using chariot

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.14 Test case N-5.2.40

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "AP1-5.2.40" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Use the chariot script stored in 5.2.40 directory

- AP back-end:

```
iperf -s
```

- STAUT:

```
iperf -c <server IP> -t 60
```

- Start the traffic between STA1 and AP2 using chariot

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.15 Test case N-5.2.42

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "h0rtG7" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.16 Test case N-5.2.43

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "AP1-5.2.43" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Use the chariot script stored in 5.2.43 directory

- AP back-end:

```
iperf -s
```

- STAUT:

```
iperf -c <server IP> -t 60
```

- Start the traffic between STA1 and AP2 using chariot

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.17 Test case N-5.2.44

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "5.2.44" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.18 Test case N-5.2.46

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "5T8CRx%" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.19 Test case N-5.2.47

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "5.2.47" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the AP of 1000 bytes

```
ping -s 1000 <IP address of AP back-end>
```

Start the traffic between the AP and STA

- AP back-end:

```
iperf –s -u
```

- STAUT:

```
iperf –c <server IP> -u –b 60M -t <sec>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.20 Test case N-5.2.50

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "5.2.50" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the AP

```
ping -c 100 -s 10000 <IP address of AP back-end>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.1.21 Test case N-5.2.55

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Association" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "Association"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to STAUT

```
ping <IP address of STAUT>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2 Protected management frame (PMF) certification program

This section includes the test configuration to be used on the DUT when running WFA Protected Management Frames (PMF) test plan.

Refer to the test plan (v1.8) for the test procedure using WTS tool and WFA documents for the test procedure using QTT tool.

Note: *QTT was used for some test cases. QTT guides the user to execute the test commands with different parameters such as* `ssid` *and* `password`*.*

4.2.1 PMF test 5.1

See Note .

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.1" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
 mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping to the PC end point

```
ping <PC-end point ip> -t 20
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Repeat the above steps for all three APs

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.2 PMF test 5.2

See Note.

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.2" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
 mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping to the PC end point

```
ping <PC-end point ip>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Repeat the above steps for all three APs

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.3 PMF test 5.3.3.1

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.3.3.1" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "12345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping continuously from the AP back-end to STAUT

```
ping <ip address of STAUT>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.4 PMF test 5.3.3.2

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.3.3.2" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "12345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping continuously from the AP back-end to STAUT

```
ping <ip address of STAUT>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.5 PMF test 5.3.3.3

See Note.

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.3.3.3" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "12345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping continuously from the AP back-end to STAUT

```
ping <ip address of STAUT>
```

Send unicast de-auth to test the AP

Send a unicast de-auth./disassoc. frame to the AP:

```
wlan-disconnect <BSSID>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.6 PMF test 5.3.3.4

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.3.3.4" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "12345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping continuously from the AP back-end to STAUT

```
ping <ip address of STAUT>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.7 PMF test 5.3.3.5

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.3.3.5" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "12345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping continuously from the AP back-end to STAUT

```
ping <ip address of STAUT>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.8 PMF test 5.4.3.1

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.4.3.1" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "12345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping continuously from the AP back-end to STAUT

```
ping <ip address of STAUT>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.2.9 PMF test 5.4.3.2

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "PMF-5.4.3.2" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 "12345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping continuously from the AP back-end to STAUT

```
ping <ip address of STAUT>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.3 WPA3 (WPA3 SAE) certification program

This section includes the test configuration to be used on the DUT when running WFA WPA3-SAE test plan. Refer to the test plan (v2.19) for the test procedure.

Note: *The WPA3 SAE test cases are also applicable for WPA3 SAE (R3) certification.*

4.3.1 WPA3 SAE test 5.2.1

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.1" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "0123456789abcdef0123456789abcdef" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping to the PC end point IP

```
ping <PC end-point ip>
```

Re-association using PMK caching

Disconnect from the AP

```
wlan-disconnect
```

Re-associate to the AP

```
wlan-connect 1
```

Disconnect from the AP when the test case is finished

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

Note: *Reset the STAUT after every test case*

4.3.2 WPA3 SAE test 5.2.2

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.2"ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping to the PC end point IP

```
ping <PC end-point ip>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

Note: *Reset the STAUT after every test case*

4.3.3 WPA3 SAE test 5.2.3

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.3" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping to the PC end point IP

```
ping <PC end-point ip>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

Note: *Reset the STAUT after every test case*

4.3.4 WPA3 SAE test 5.2.4

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.4" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678123456781234567812345678" mfpc 1 mfpr 0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping to the PC end point IP

```
ping <PC end-point ip>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

Note: *Reset the STAUT after every test case*

4.3.5 WPA3 SAE test 5.2.6

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.6" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP. If associated then fail, otherwise pass.

```
wlan-connect 1
```

Disconnect from the AP

```
wlan-disconnect
```

Delete the profile

```
wlan-remove 1
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.6" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP. If associated then fail, otherwise pass.

```
wlan-connect 1
```

Disconnect from the AP

```
wlan-disconnect
```

Delete the profile

```
wlan-remove 1
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.6" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP. If associated then fail, otherwise pass.

```
wlan-connect 1
```

Disconnect from the AP

```
wlan-disconnect
```

Delete the profile

```
wlan-remove 1
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.6" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP. If associated then fail, otherwise pass.

```
wlan-connect 1
```

Disconnect from the AP

```
wlan-disconnect
```

Delete the profile

```
wlan-remove 1
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "Wi-Fi-5.2.6" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa3 sae
 "12345678" mfpc 1 mfpr 1
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP. If associated then fail, otherwise pass.

```
wlan-connect 1
```

Disconnect from the AP

```
wlan-disconnect
```

Delete the profile

```
wlan-remove 1
```

Note: *Reset the STAUT after every test case*

4.4 Security enhancement certification program

This section includes the test configuration to be used on the DUT when running WFA Security Enhancement test plan. Refer to the test plan (v2.19) for the test procedure.

4.4.1 Security enhancement test 5.2.2

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "WiFi-5.2.2" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping the PC end-point

```
ping <PC end-point IP>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

Note: *Repeat the above steps for each scenario.*

4.4.2 Security enhancement test 5.2.3

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "WiFi-5.2.3" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping the PC end-point

```
ping <PC end-point IP>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

Note: *Repeat the above steps for each scenario.*

4.4.3 Security enhancement test 5.2.4

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "WiFi-5.2.4" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping the PC end-point

```
ping <PC end-point IP>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

Note: *Repeat the above steps for each scenario.*

4.5 Security vulnerability detection (SVD) certification

This section includes the test configuration to be used on the DUT when running WFA Security Vulnerability Detection (SVD) test plan. Refer to the test plan (v2.19) for the test procedure.

Note: *The SVD test cases are also applicable for Full Function Device (FFD) certification.*

4.5.1 SVD all test cases

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "<SSID>" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

Disconnect from the AP after every run and associate again

```
wlan-disconnect
```

4.6 Wi-Fi 5 (802.11ac) certification program

4.6.1 Test case AC-5.2.2

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "wi-fi" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.2 Test case AC-5.2.9

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "wpa2" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STAs

- Run the command to run *iPerf* in server mode for STAUT:

```
iperf -s -u
```

- Run the command to run *iPerf* in client mode for the AP back-end:

```
iperf -c <STAUT IP address> -t <number of seconds to transmit for>
```

- Run the command to run *iPerf* in server mode for the PC end-point:

```
iperf -s -u -i1
```

- Run the command to run *iPerf* in client mode for STAUT:

```
iperf -c <IP of PCE> -u -t 60
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.3 Test case AC-5.2.9A

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "wpa2" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Start iPerf traffic

- Run the command to run *iPerf* in server mode for STAUT:

```
iperf -s -u
```

- Run the command to run *iPerf* in client mode for the PC end-point:

```
iperf -c <STAUT IP address> -u -i 1 -b 60M -t 60
```

- Run the command to run *iPerf* in server mode for the PC end-point:

```
iperf -s -u -i1
```

- Run the command to run *iPerf* in client mode for STAUT:

```
iperf -c <IP of PCE> -u -t 60
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.4 Test case AC-5.2.22

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "80211h" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Check from SM bit in capability info from sniffer

4.6.5 Test case AC-5.2.23

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "80211h" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the PC end-point to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.6 Test case AC-5.2.26

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "012345678901234567890123456789O1"
 ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Start a continuous ping from the STAUT to the AP back-end

```
ping -s 1000 -c 300 <IP address of back-end>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.7 Test case AC-5.2.28

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.28" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Step 5

The pre-requisite for STAUT is Tx UDP AP back-end.

- PC end-point:

```
iperf –s
```

- STAUT:

```
iperf -c 192.165.100.99 -B 192.165.100.40 -u -t 60
```

Step 6

The pre-requisite for STA1 is to use WTS to send traffic.

Step 7

STAUT: Tx of AC_BE

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c 192.165.100.99 -B 192.165.100.40 -S 0 -u -t 30
```

Step 8

STAUT: Tx of AC_VI

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c 192.165.100.99 -B 192.165.100.40 -S 160 -u -t 30
```

Step 9

STAUT: Tx of AC_BK

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c 192.165.100.99 -B 192.165.100.40 -S 70 -u -t 30
```

Step 10

STAUT: Tx of AC_VI

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c 192.165.100.99 -B 192.165.100.40 -S 160 -u -t 30
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.8 Test case AC-5.2.33

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.33" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Step 4

The pre-requisite for STAUT is Tx UDP.

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c 192.165.100.99 –B 192.165.100.40 -u -t 60
```

Step 5

STAUT: Tx of AC_VI

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c 192.165.100.99 -B 192.165.100.40 -S 160 -u -t 30
```

Step 7 and step 9

Same as step 5

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.9 Test case AC-5.2.34

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.34" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Start a continuous ping from the STAUT to the AP

```
ping -s 10000 -c 90 <IP address of PC end-point>
```

Start the traffic between the AP and STA

Step 5

STAUT: Tx of AC_VI

- STAUT:

```
iperf -s -u -B 192.165.100.40
```

- PC end-point:

```
iperf -c 192.165.100.40 -u -S 160 -b 70M -t 30 -i1
```

Step 7

Same as step 5

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.10 Test case AC-5.2.35

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid “VHT-5.2.35-AP1" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2
 “12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Start a continuous ping from the STAUT to the AP

```
ping -s 10000 -c 300 <IP address of back-end>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.11 Test case AC-5.2.36

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.36" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 “12345678”
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.12 Test case AC-5.2.37

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.37" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Step 4

- STAUT:

```
iperf -s -u -B 192.165.100.40
```

- PC end-point:

```
iperf -c 192.165.100.40 -u -S 160 -b 60M -t 30 -i1
```

Step 9

Same as step 4.

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.13 Test case AC-5.2.38

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.38" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Step 4

- STAUT:

```
iperf -s -u -B 192.165.100.40
```

- PC end-point:

```
iperf -c <IP of STAUT> -u -i 1 -b 60M -t 60
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.14 Test case AC-5.2.40

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.40-AP1" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Start the traffic between the AP and STA

Step 4

Tx from STAUT and STA1 to PC end-point

- PC end-point:

```
iperf -s -u -i1
```

- STAUT:

```
iperf -c <IP address of PC end-point> -u -t 60
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.15 Test case AC-5.2.42

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.42" ip:192.165.100.40,192.165.100.50,255.255.0.0
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.16 Test case AC-5.2.46

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.46" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 “12345678”
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the AP to the STAUT

```
ping <STAUT IP address>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.17 Test case AC-5.2.47

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.47" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 “12345678”
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the AP of 1000 bytes

```
ping -s 1000 <IP address of AP back-end>
```

Start the traffic between the AP and STA

Step 5

Tx of AC_BE from STAUT to PC end-point

- PC end-point:

```
iperf –s –u –i1
```

- STAUT:

```
iperf -c <IP of PCE>  -B <IP of wlan interface> -u -S 0  -t 60
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.18 Test case AC-5.2.50

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.50" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 “12345678”
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the AP

```
ping -c 100 –s 10000 <IP address of AP>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.19 Test case AC-5.2.54

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.54" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point

```
ping -c 100 -s 10000 <IP address of PC end-point>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.20 Test case AC-5.2.55

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.55" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point

```
ping <IP address of PC end-point>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.21 Test case AC-5.2.57

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.57" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point

```
ping <IP address of PC end-point>
```

Start the traffic between the AP and STA

- STAUT:

```
iperf -s -u
```

- PC end-point:

```
iperf -c <IP of STAUT> -u -i 1 -b 60M -t 60
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.22 Test case AC-5.2.58

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.58" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point

```
ping -s 1000 -c 90 <IP address of PC end-point>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.23 Test case AC-5.2.59

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.59" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point

```
ping -s 1000 -c 90 <IP address of PC end-point>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.24 Test case AC-5.2.60

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.60" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point

```
ping -s 1000 -c 90 <IP address of PC end-point>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.25 Test case AC-5.2.61

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.61" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point

```
ping -s 1000 -c 90 <IP address of PC end-point>
```

Start the traffic between the AP and STA

Step 3

Make this value as X

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c <IP of PC end-point> -u -t 60
```

Step 7

Make this value as X' which should be 23% > X

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c <IP of PC end-point> -u -t 60
```

Step 11

Make this value as X which should be 6% > X

- PC end-point:

```
iperf –s -u -i1
```

- STAUT:

```
iperf -c <IP of PC end-point> -u -t 60
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

4.6.26 Test case AC-5.2.62

Associate STAUT to AP

- Run the command to scan the network:

```
wlan-scan
```

- Run the command to add a Wi-Fi profile with a static IP address:

```
wlan-add 1 ssid "VHT-5.2.62" ip:192.165.100.40,192.165.100.50,255.255.0.0 wpa2 "12345678"
```

- Run the command to check the added profile:

```
wlan-list
```

- Run the command to associate the STAUT to the AP

```
wlan-connect 1
```

- Run the command to ping from the STAUT to the PC end-point (WTS should take care)

```
ping -s 1000 -c 90 <IP address of PC end-point>
```

Disconnect from the AP

Disconnect from the AP when the test case is finished.

```
wlan-disconnect
```

Delete the profile

Delete the profile when the test case is finished.

```
wlan-remove 1
```

5 Contact information

Use the following links for more product details, queries and support.

- Home page: www.nxp.com
- Web support: nxp.com/support
- NXP community: community.nxp.com

6 Acronyms and abbreviations

Table 2. Abbreviations

Acronym	Description
AP	Access point
PMF	Protected management frame
QTT	Quick track tool
SAE	Simultaneous authentication of equals
STAUT	Station under test
SVD	Security vulnerability detection
WFA	Wi-Fi alliance
WTS	Wi-Fi test suite

7 Note about the source code in the document

The example code shown in this document has the following copyright and BSD-3-Clause license:

Copyright 2021-2023 NXP Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials must be provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8 Legal information

8.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

8.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

8.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com

Date of release: 29 June 2023
Document identifier: UM11567