AN13006

Compliance and Certification Considerations

Rev. 3 — 20 February 2024 Application note

Document information

Information	Content
Keywords	FCC, ETSI, EMC/RF emissions, adaptivity, DFS
Abstract	Provides general guidance and tips on how to test products based on NXP Wi-Fi devices for regulatory compliance (FCC, ETSI, etc.).

1 Introduction

This application note provides general guidance to test products based on NXP devices for regulatory compliance with standards like FCC and ETSI.

Users of this document work with the regulatory test labs and module vendors to achieve the certification of their product.

Read this document prior to going to the lab for compliance testing.

1.1 Using certified modules

If your product contains a wireless module that has already been regulatory certified, ask your module vendor for the regulatory certification.

We also strongly recommend that you use the same antenna as the one used by your module vendor, or an antenna with lower gain. Doing so can reduce the testing required to demonstrate compliance, which helps reduce costs and delays to the project schedule.

2 Certification process overview

The regulatory certification is a multiple-step process to be planned closely with the regulatory test lab.

Start by determining the countries in which you plan to market your product. Each country has its own regulations that can affect:

- The allowable frequencies (channels) and channel bandwidths that your product operates on.
- The maximum transmit power that is allowed for each channel.
- Specific requirements for each operating frequency/channel (for example, adaptivity or dynamic frequency selection (DFS).
- Test schedule. Some certifications, like DFS can require more time to get certified.

Typical standards related to regulatory compliance include:

- FCC: Part 15C, Part 15E
- ETSI EN 300 328, ETSI EN 301 893, ETSI EN 303 687, ETSI EN 301 489, ETSI EN 300 440

After determining the target certifications, work with the regulatory test lab to determine a test plan to demonstrate compliance with the relevant requirements.

3 EMC/RF emissions

This section provides some guidance for EMC/RF emissions tests. These tests measure the emissions transmitted at the antenna to determine if they exceed regulatory limits. The limits and test conditions for these tests:

- are defined in the regulatory domain (for example FCC versus ETSI)
- vary with the frequency/channel of operation (for example, 2.4 GHz band requirements differ from 5 GHz and 6 GHz band requirements)
- depend on antenna gain

The regulatory requirements can restrict both in-band (for example, power spectral density) and out-of-band (for example, harmonics of the signal) emissions.

3.1 Related parameters

For EMC/RF emissions testing, the key parameter that can be adjusted to meet compliance requirements is the RF transmit power. In general, the goal of compliance testing is to determine the highest transmit power level that can be used while meeting regulatory requirements.

If the regulatory requirements still cannot be met after reducing the transmit power level, consider using an antenna with lower gain. If you are using a certified module, contact your module vendor for assistance.

3.2 Test preparation

Prior to going to the lab for compliance testing, work with the regulatory test lab to put together a test plan. The test plan is based on:

- The countries (regulatory domains) that you plan to get certified for
- The frequencies/channels of operation (for example, 2.4 GHz, 5 GHz, and 6 GHz bands)
- The channel bandwidths of operation (for example 20 MHz, 40 MHz, and/or 80 MHz)

The test plan includes test cases, which specify the following:

- Bands, channels, channel bandwidths
- Transmit power levels
- Data rates

If you are using a wireless module that is already certified, we recommend obtaining the power table from the module vendor. The power table includes information on transmit power levels that are compliant for the specific module design and relevant regulatory domain. This transmit power table can be the initial starting point for compliance testing for your product.

3.3 General test procedure

The test procedures and limits are generally defined by the relevant regulatory standards issued by organizations such as FCC and ETSI. This section provides some general tips on how to configure the radio for these tests.

1. For each test case, configure the radio to the desired band, channel, channel bandwidth, transmit power level and data rate. Look up the transmit power level for that particular radio configuration in the module transmit power table.
2. Enable continuous frame transmission mode.
3. Measure the emissions as required by the relevant standard, and determine the margin compared to limits. If the emissions are surpassing the limits of the standard, adjust the power setting down by 1 dB and measure again. Continue until the emission levels are below the limits. Record the final power setting and margin for passing condition.
4. Repeat the above process for all test cases.
5. To set the target TX power of your device during normal operation, fill out the power table and calibration data files.

3.4 Wi-Fi TX power

The Wi-Fi TX power table is used to store the target transmit power level for your device during normal operation. The power table can be called as a parameter during driver loading and will override the firmware default TX power.

The method to store your device's TX power depends on your device. Refer to the appropriate power table application note of your device for guidance on how to update the power table. The list of power table application notes are below:

- AN13009 - Wi-Fi TX Power Table Management in Linux
  - This is a legacy method, and is not recommended.
- AN13384 - Regulatory Domain and TX Power Level Management V2
  - Compatible with:
    - 88W8977
    - 88W8987
    - 88W8997
    - 88W9098
    - 88Q9098
    - AW690
    - IW416
    - AW611
    - IW611
    - IW612
    - IW620
- AN13463 - Regulatory Flags and TX Power Management Method V3
  - Compatible with:
    - 88W9098

After compliance testing is completed, fill out the power table to ensure that the correct channels and transmit power levels are used. Adjust the values if needed.

3.5 Bluetooth TX power

The Bluetooth TX power and Bluetooth TX power class can be set in the Bluetooth calibration file of your device.

From the Bluetooth calibration example file below, the parameters `ForceClass2Op` and `Class1OpSupport` are used to configure Bluetooth TX power class operation. Your device limits its maximum Bluetooth TX power based on its power class.

BT Power Class Setting Parameters example:

```
[BT_Config]
ANNEX56_EXIST=0
Version=0x1
Xtal=0x79
InitPwrIndBm_Pwr=4
FELoss=0x4
ForceClass2Op=1
Class1OpSupport=0
…
```

Configure both parameters `ForceClass2Op` and `Class1OpSupport` such that it matches the structure of the power class shown in Table X below.

Table 1. Bluetooth TX Power Class Parameters

Bluetooth TX Power Class	Configuration Parameter
Class 1 (up to 20 dBm)	`ForceClass2Op=0 Class1OpSupport=1`
Class 1.5 (up to 13 dBm)	`ForceClass2Op=0 Class1OpSupport=0`
Class 2 (up to 4 dBm)	`ForceClass2Op=1 Class1OpSupport=0`

For example, if `ForceClass2Op=1` and `Class1OpSupport=0` are set in the Bluetooth calibration file, then your device is limited to Class 2 operation (up to 4 dBm).

The parameter `InitPwrIndBm_Pwr` is used to set both the initial Bluetooth BDR/EDR TX power and the max Bluetooth LE TX power in dBm.

Where:

Table 2. InitPwrIndBm_Pwr Parameter

Parameter	Configuration Parameter
InitPwrIndBm_Pwr	Initial Bluetooth BDR/EDR TX Power and max Bluetooth LE TX power in dBm

In the example Bluetooth calibration file below, the initial Bluetooth BDR/EDR TX power and the max Bluetooth LE TX power is set to 4 dBm.

BT initial power parameter example:

```
[BT_Config]
ANNEX56_EXIST=0
Version=0x1
Xtal=0x79
InitPwrIndBm_Pwr=4
FELoss=0x4
ForceClass2Op=1
Class1OpSupport=0
…
```

Bluetooth TX power during runtime is set using vendor-specific HCI commands. Refer to the Bluetooth Software User Manual of your device for more information on these commands.

3.6 802.15.4 TX power

The 802.15.4 TX power limit can be configured in the Cal15_4DataFile.txt calibration file of your device. Refer to the Calibration Structure application note of your device for more information on configuring the Cal15_4DataFile.txt.

Note: This feature is only compatible for devices that have an 802.15.4 radio.

The `_15_4_TxPowerLimit` parameter, as shown bolded in the example calibration file below, is used to set the max operating TX power for 802.15.4 in steps of 0.5 dB. If the TX power limit parameter is set to 0, there will be no limit on TX power.

Cal15_4DataFile.txt example file:

```
[_15_4_Config]
_15_4_Version=0x01
_15_4_TxPowerLimit=20
_15_4_Address=80.70.60.50.40.30.20.10
_15_4_SPIClk=0
```

Where:

Table 3. _15_4_TxPowerLimit parameter

Parameter	Configuration Parameter
_15_4_TxPowerLimit	802.15.4 TX Power in 0.5 dBm steps Input range of 1 to 44 (0.5 dBm to 22 dBm) **Note:** 0 = No TX power limit

In the example above, `_15_4_TxPowerLimit` = 20 sets the max 802.15.4 TX power to 10 dBm.

802.15.4 TX power during runtime is set using SPINEL vendor-specific commands. Refer to the 802.15.4 Software User Manual of your device for more information on these commands.

4 Adaptivity

European standards such as ETSI EN 300 328, EN 301 893, and ETSI EN 303 687 require adaptivity testing.

The adaptivity test confirms the ability of the radio to hold off transmitting when an interfering signal is present. Meeting this requirement proves that the radio can safely share the spectrum with other users.

For the 2.4 GHz band, if the transmit power is less than +10 dBm EIRP, the adaptivity requirements do not apply.

Note: *For applications using Bluetooth, reduce the transmit power to less than 10 dBm EIRP so that the adaptivity requirement does not apply.*

4.1 Related parameters

The key Wi-Fi radio parameter that can be adjusted to meet the adaptivity requirement is the ED-MAC threshold. The ED-MAC threshold determines the sensitivity of the radio to interfering signals.

The ED-MAC threshold must be tuned to pass the adaptivity test. However, avoid tuning the ED-MAC threshold to be sensitive, doing so can impact performance.

Note: *Prior to testing adaptivity, ensure that RSSI has been calibrated for accurate measurements. For more information, refer to the Calibration Structure application note of your device.*

4.2 Test preparation

Prior to going to the test lab, prepare a test plan and review the general test procedure in Section 5.3 to be familiar with the related commands.

The test requires that the unit under test (UUT) transmits data to a companion device. The purpose of the test is to demonstrate that the data transmissions are paused when an interfering signal is present. Therefore, it is recommended to have a companion device (such as an access point) and a tool to generate data traffic (such as iperf) available for the test.

4.3 General test procedure

The ETSI standard generally defines the test procedures and limits. Refer to the application note AN13756 - ETSI Adaptivity and Receiver Blocking Tests for guidance to configure your device for adaptivity testing.

4.4 After testing is completed

If the ED-MAC threshold required tuning to pass the compliance test, it is important to log the passing value of the threshold. There is one ED-MAC threshold for each Wi-Fi frequency band. If you tested multiple channels per band during the compliance test, choose the lowest passing value for that band.

The ED-MAC threshold is stored in a configuration file. The system software loads this configuration file and set the ED-MAC threshold when the device boots, to ensure compliance when the device is used during normal operation.

5 DFS

Dynamic Frequency Selection (DFS) is an IEEE 802.11h standard that allows wireless networks to operate in certain channels used by radar systems. FCC, ETSI, and other regulatory bodies require DFS compliance testing for devices capable of operating on 5GHz radar channels to avoid co-channel operation.

Per regulatory requirements, when a DFS leader detects radar on the current channel, it ceases operations on that channel and moves to a new channel. The DFS leader must also inform its DFS followers of this channel change.

Your DFS-enabled device operates either as a DFS leader or a DFS follower. The DFS leader is the role of the radar detecting device in a Wi-Fi network. Conversely, DFS followers are client devices operating on a network controlled by DFS leaders.

DFS channels can be enabled and disabled from within the power table of the Wireless Soc. Refer to Section 3.4 for more information.

Note: Prior to testing DFS, ensure that the RSSI of the Wireless SoC has been calibrated to ensure accurate signal detection. For more information, refer to the Calibration Structure application note of the Wireless SoC in use.

5.1 Related parameters

Some common DFS testing requirements are defined below:

Channel availability check (CAC): The DFS leader checks the target DFS channel for any radar activity before starting operation on that channel.

In-service monitoring: The DFS leader monitors, detects, and reacts to radar signals while operating on a DFS channel.

- Channel shutdown time: Timing requirements for a DFS leader to stop transmissions and instruct any connected DFS followers to move out of the DFS channel when radar is detected.
- Nonoccupancy period (NOP): When radar is detected, the DFS channel must be marked as unavailable for a specific period known as the nonoccupancy period (NOP). The DFS leader and DFS follower do not occupy the DFS channel until the NOP is complete.

Statistical Performance Check (DFS Radar Detection): This test confirms that the DUT can detect DFS radar signals at a minimum success rate over a given number of trials.

Note: Some of the above test requirements will only apply to devices operating in DFS leader mode.

5.2 General test procedure

This section provides an overview of how to configure your device for DFS testing, per FCC requirements. The requirements and test procedures vary by regulatory region. Refer to the test standards of the applicable regulatory agency for details on test procedures and compliance requirements.

Prepare a test plan by consulting the test lab prior to going to the lab for certification.

5.2.1 DFS leader mode

This section covers the general test procedure for performing DFS leader tests.

The hostapd daemon is used to enable and configure DFS operation in DFS leader mode. When configured correctly, your device automatically monitors and responds to detected radar signals. Ensure you are familiar with how to use hostapd to set up your device in AP mode. Refer to the Software User Manual of your device for further information.

Optionally, the dfstesting command can be used to set a user-defined CAC time, nonoccupancy period, and channel change parameters. This command overrides the DFS timing parameters set by hostapd. This command is recommended to override channel check and channel change mechanisms when performing radar detection tests that requirer many trials.

Note: Only use the dfstesting command for regulatory testing purposes. Do not enable this command during normal operation of your device.

The commands and parameters are detailed below:

```
./uaputl.exe dfstesting <CAC Period> <Non-Occupancy Period> <Channel Change>
 <Fixed Channel Num> <CAC Restart>
```

Where:

Table 4. Dfstesting parameters

Parameter	Description
`CAC Period`	CAC Period in seconds 0 = 60 seconds 1 to 1800 = Set CAC in seconds
`Non-Occupancy Period`	Non-Occupancy Period (NOP) in seconds 0 = 1800 seconds 1 to 65535 = Set NOP in seconds
`Channel Change`	Channel change upon radar detection 0 = Enable change channel upon radar detection 1 = Disable channel change upon radar detection
`Fixed Channel Num`	Channel to change to upon radar detection 0 = Channel change to automatic channel 1 to 255 = Channel change to the set channel Note: this parameter can only be enabled when <Channel Change> is set to 0
`CAC Restart`	Restart CAC again after CAC success Set to 0

5.2.1.1 CAC test example

Follow the example command sequence below to configure the DFS leader for CAC testing.

1. Load device drivers.

```
modprobe moal mod_para=nxp/wifi_mod_para.conf
```

2. (Optional) Configure the CAC parameter per regulatory requirements using the *dfstesting* command. In the below example, the CAC is set to 60 seconds. All other *dfstesting* parameters are set to default and/or disabled.

```
./mlanutl uap0 dfstesting 60 0 0 0 0
```

3. Configure the RF channel and country code. In this example, the channel is set to 100 and the country code is set to the US. It is also required to enable 80211d and 80211h in your hostapd.conf file to enable DFS support. The parameters in bold in the .conf file below indicate the changes required to configure for DFS.

```
interface=uap0
hw_mode=a
ieee80211n=1
ieee80211d=1
ieee80211h=1
channel=100
country_code=US
ssid=DFS-test
```

4. Bring up the AP interface and assign a static IP

```
ifconfig uap0 192.168.1.2 netmask 255.255.255.0 up
```

5. Start the hostapd daemon in the background

```
hostapd -B /etc/hostapd.conf
```

The DFS leader will immediately perform a CAC after starting the hostapd daemon, as shown by the dmesg output below:

```
11h: issuing DFS Radar check for channel=100.  Please wait for response...
11h: Ret ChanRptReq.  Set dfs_check_pending and wait for EVENT_CHANNEL_REPORT.
```

After the CAC period, the DFS leader will start normal operation, as shown by the dmesg output below:

```
wlan: Starting AP
IPv6: ADDRCONF(NETDEV_CHANGE): uap0: link becomes ready
wlan: AP started
wlan: HostMlme uap0 send deauth/disassoc
Set AC=3, txop=47 cwmin=3, cwmax=7 aifs=1
Set AC=2, txop=94 cwmin=7, cwmax=15 aifs=1
Set AC=0, txop=0 cwmin=15, cwmax=63 aifs=3
Set AC=1, txop=0 cwmin=15, cwmax=1023 aifs=7
```

6. Restart the CAC sequence

```
killall hostapd
hostapd -B /etc/hostapd.conf
```

7. Trigger a radar signal on channel 100 during the CAC period (initial 60 seconds of starting hostapd).

The DFS leader detects the radar signal and automatically move to another channel upon radar detection, as shown by the dmesg output below:

```
11h: Radar Detected – stopping host tx traffic
11h: Radar Detected – adding CHAN_SW IE to interfaces
11h: Radar Detected – restarting host tx traffic
CSA/ECSA: Switch to new channel 36 complete!
OLD BW = 1 NEW BW = 0
11h: channel 100 is under NOP – can’t use.
```

5.2.1.2 In-service monitoring, channel shutdown, and NOP test example

Follow the example command sequence below to configure the DFS leader for testing in-service monitoring, channel shutdown, NOP.

1. Load the device drivers.

```
modprobe moal mod_para=nxp/wifi_mod_para.conf
```

2. (Optional) Configure the CAC and NOP parameters per regulatory requirements using the *dfstesting* command. In the below example, the CAC is set to 60 seconds and the NOP is set to 1800 seconds (30 minutes). All other *dfstesting* parameters are set to default and/or disabled.

```
./mlanutl uap0 dfstesting 60 1800 0 0 0
```

3. Configure the RF channel and country code. In this example, the channel is set to 100 and the country code is set to the US. It is required to enable 80211d and 80211h in your hostapd.conf file to enable DFS support. The parameters in bold in below .conf file indicate the changes required to configure for DFS.

```
interface=uap0
hw_mode=a
ieee80211n=1
ieee80211d=1
ieee80211h=1
channel=100
country_code=US
ssid=uAP-DFS-test
```

4. Bring up the AP interface and assign a static IP

```
ifconfig uap0 192.168.1.2 netmask 255.255.255.0 up
```

5. Start the hostapd daemon in the background

```
hostapd -B /etc/hostapd.conf
```

The DFS leader will immediately perform a CAC after starting the hostapd daemon, as shown by the dmesg output below:

```
11h: issuing DFS Radar check for channel=100.  Please wait for response...
11h: Ret ChanRptReq.  Set dfs_check_pending and wait for EVENT_CHANNEL_REPORT.
```

After the CAC period, the DFS leader will start normal operation, as shown by the dmesg output below:

```
wlan: Starting AP
IPv6: ADDRCONF(NETDEV_CHANGE): uap0: link becomes ready
wlan: AP started
wlan: HostMlme uap0 send deauth/disassoc
Set AC=3, txop=47 cwmin=3, cwmax=7 aifs=1
Set AC=2, txop=94 cwmin=7, cwmax=15 aifs=1
Set AC=0, txop=0 cwmin=15, cwmax=63 aifs=3
Set AC=1, txop=0 cwmin=15, cwmax=1023 aifs=7
```

6. Associate an external-station (ex-STA) to the DFS leader and perform a channel-loading mechanism as per regulatory requirements. The ex-STA is the DFS follower.

7. Trigger a radar signal on channel 100 during the in-service monitoring period.

The DFS leader detects the radar signal, stop all transmissions, and automatically move to another channel upon radar detection, as shown by the dmesg output below:

```
11h: Radar Detected – stopping host tx traffic
11h: Radar Detected – adding CHAN_SW IE to interfaces
11h: Radar Detected – restarting host tx traffic
CSA/ECSA: Switch to new channel 36 complete!
OLD BW = 1 NEW BW = 0
11h: channel 100 is under NOP – can’t use.
```

8. Monitor the DFS channel and verify that there are no transmissions from the DFS leader or from the DFS follower during the NOP. In this example, the NOP is 30 minutes.

5.2.1.3 Example procedure for statistical performance checks

The dfstesting command is especially useful for expediating statistical performance check testing. The DFS leader can be set not to move out of the DFS channel when a radar is detected, allowing it to run repeated radar detection tests without having to wait for the NOP.

Follow the example command sequence below to configure the DFS leader for repeated statistical performance check testing.

1. Load the device drivers

```
modprobe moal mod_para=nxp/wifi_mod_para.conf
```

2. Configure the nonoccupancy period and disable channel change upon radar detection using the *dfstesting* command. In the below example, the nonoccupancy period is set to 10,000 seconds and channel change is disabled. All other *dfstesting* parameters are set to default and/or disabled.

```
./mlanutl uap0 dfstesting 0 10000 1 0 0
```

3. Configure the RF channel and country code. In this example, the channel is set to 100 and the country code is set to the US. It is required to enable 80211d and 80211h in your hostapd.conf file to enable DFS support. The parameters in bold in below .conf file indicate the changes required to configure for DFS.

```
interface=uap0
hw_mode=a
ieee80211n=1
ieee80211d=1
ieee80211h=1
channel=100
country_code=US
ssid=uAP-DFS-test
```

4. Bring up the AP interface and assign a static IP

```
ifconfig uap0 192.168.1.2 netmask 255.255.255.0 up
```

5. Start the hostapd daemon in the background

```
hostapd -B /etc/hostapd.conf
```

After the CAC period, the DFS leader will start normal operation, as shown by the dmesg output below:

```
wlan: Starting AP
IPv6: ADDRCONF(NETDEV_CHANGE): uap0: link becomes ready
wlan: AP started
wlan: HostMlme uap0 send deauth/disassoc
Set AC=3, txop=47 cwmin=3, cwmax=7 aifs=1
Set AC=2, txop=94 cwmin=7, cwmax=15 aifs=1
Set AC=0, txop=0 cwmin=15, cwmax=63 aifs=3
Set AC=1, txop=0 cwmin=15, cwmax=1023 aifs=7
```

6. Associate an external-station (ex-STA) to the DUT and perform a channel-loading mechanism per regulatory requirements.

7. Trigger a radar pulse on the DFS channel.

The DFS leader detects the radar signal, as shown by the dmesg output below:

```
11h: Radar Detected – stopping host tx traffic
11h: Radar Detected – adding CHAN_SW IE to interfaces
11h: Radar Detected – restarting host tx traffic
```

8. Repeat step 7 for the required number of radar detection trials

5.2.2 DFS follower mode

This section will cover the general test procedure for performing DFS follower tests.

DFS follower operation is enabled by default on NXP devices operating in station mode. Ensure you are familiar with how to use wpa_supplicant to set up your device in station (STA) mode. Refer to the Software User Manual of your device for more information.

5.2.2.1 Channel shutdown test example

Follow the example command sequence below to configure your device (DFS follower) for channel shutdown testing.

1. Load the device drivers

```
modprobe moal mod_para=nxp/wifi_mod_para.conf
```

2. Bring up the mlan0 interface

```
ifconfig mlan0 up
```

3. Configure the wpa_supplicant to connect the DFS follower to an external-AP. The example configuration below is used to associate to an AP with an SSID of “DFS-AP”in open security mode.

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
update_config=1
ap_scan=1
network={
ssid="DFS-AP"
key_mgmt=NONE
}
```

4. Configure the external-AP to operate on a DFS channel.

5. Run wpa_supplicant to connect the DFS follower to the ext-AP and perform channel-loading, per regulatory requirements.

```
wpa_supplicant -B -i mlan0 -c /etc/wpa_supplicant.conf
```

6. Perform a channel-loading mechanism per regulatory requirements.

7. Trigger a radar signal onto the DFS channel.

The DFS follower stops transmissions and moves out of the DFS channel, as shown by the dmesg output below:

```
CSA/ECSA: Switch to new channel 36 complete!
```

8. Monitor the DFS channel to ensure that no transmissions of any type has occurred during the NOP.

6 Adjacent channel selectivity

Adjacent channel selectivity is a measure of the ability of the receiver to operate satisfactorily in the presence of a strong unwanted signal in an adjacent channel. Adjacent channel selectivity is a requirement of ETSI EN 300 440.

The requirement applies only to as Receiver Category 1 (highly reliable SRD communication media) short range devices (SRD) operating from 1 GHz to 40 GHz.

In EN 300 440 v2.1.1, the k value range is 0 dB < k < 40 dBm. In EN 300 440 v2.2.1, the k value range has been updated to -40 dB < k < 0 dB. If you declare your device as a Receiver Category 1 device, NXP recommends using EN 300 440 v2.2.1.

Note: *The adjacent channel selectivity requirement does not apply to Receiver Category 2 or Receiver Category 3 devices.*

7 Acronyms and abbreviations

Table 5. Acronyms and abbreviations

Acronym	Definition
AP	Access point
CAC	Channel Availability Check
DFS	Dynamic frequency selection
ED-MAC	Energy detect - Media/medium access controller
EIRP	Effective isotropic radiated power
EMC	Electromagnetic compatibility
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
RF	Radio frequency
SRD	Short range device
STA	Station
UUT	Unit under test

8 References

[1] Application Note - AN13009 - Wi-Fi TX Power Table Management in Linux link
[2] Application Note - AN13384 - Regulatory Domain and TX Power Level Management V2 link
[3] Applicaton Note - AN13463 - Regulatory Flags and TX Power Management Method V3 link
[4] Application Note - AN13756 - ETSI Adaptivity and Receiver Blocking Tests link

9 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 2020-2024 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.

10 Revision history

Table 6. Revision history

Document ID	Release date	Description
AN13006 v.3	20 February 2024	• Section 2 "Certification process overview": updated • Section 4.1 "Related parameters": updated the list of typical standards • Section 4.2 "Test preparation": updated • Section 4.3 "General test procedure": updated • Section 5 "DFS": updated • Section 6 "Adjacent channel selectivity": added • Section 7 "Acronyms and abbreviations": updated • Section 8 "References": updated
AN13006 v.2	17 August 2023	• Section 2 "Certification process overview": updated the list of typical standards • Section 4.1 "Related parameters": updated • Section 4.2 "Test preparation": updated • Section 4.3 "General test procedure": updated • Section 6 "Adjacent channel selectivity": added • Section 7 "Acronyms and abbreviations": updated • Section 8 "References": updated
AN13006 v.1	03 November 2020	• Initial version

Legal information

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.

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.

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 https://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.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

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.

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.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

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.

Bluetooth — the Bluetooth wordmark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by NXP Semiconductors is under license.

i.MX — is a trademark of NXP B.V.

Tables

Contents

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

Date of release: 20 February 2024
Document identifier: AN13006