Application Report

SimpleLink Wi-Fi CC3x20, CC3x3x Test Strategy Overview

Benjamin Moore

ABSTRACT

The CC3x20 and CC3x3x devices are part of the SimpleLink™ microcontroller (MCU) platform, which consists of Wi-Fi®, *Bluetooth*® low energy, Sub-1 GHz and host MCUs. All share a common, easy-to-use development environment with a single core software development kit (SDK) and rich tool set. For more information, visit www.ti.com/simplelink.

This application report presents an overview of the strategy employed by TI to test the SimpleLink Wi-Fi CC3x20 and CC3x3x devices. The goal of the document is to help developers understand the scope of TI's internal Wi-Fi testing, which helps TI ensure the interoperability and reliability of its SimpleLink Wi-Fi products.

Table of Contents

List of Figures

List of Tables

Trademarks

1 Introduction

In the rapidly growing Internet of Things (IoT) market, many applications, from personal electronics to industrial machines and sensors, get wirelessly connected to the Internet. These applications span multiple use-cases, are deployed in various environments, and serve diverse sets of requirements. Among the important factors when selecting a connectivity device is the interoperability, security, and reliability of the solution. Using a device with a high level of interoperability, security, and reliability is an essential step in creating the most effective product and delivering the best user experience.

TI understands the importance of these factors and is making sure that the SimpleLink family of devices enable wireless connections with best-in-class stability and robustness for real-life scenarios. These investments include a comprehensive testing strategy with dedicated test labs and automated testing processes. TI's overall testing strategy is designed to cover all aspects of system performance in order to ensure devices will work properly in all environments and target use-cases.

This application report describes the specific test strategy employed for the SimpleLink Wi-Fi devices and includes information on the following test categories:

- Interoperability (IOP)
- Performance
- Robustness and Stability
- Networking Stack
- Functionality
- Pre-certification

2 Interoperability (IOP) Tests

Interoperability measures the ability of a device to work properly, or interoperate, with a wide range of devices from other vendors and provide consistent performance. TI understands the impact and cost of having an interoperability issue and, therefore, established a comprehensive IOP lab with automated testing capability to reduce the risk of interoperability issues occurring. The scope of these tests is beyond that of the standard Wi-Fi Alliance tests.

The TI IOP lab contains more than 200 access points (APs) from different vendors. The access points included in the lab are based on a wide range of different Wi-Fi chipsets and intended to provide a test coverage that is representative of most APs available in the market. A representation of the Wi-Fi IOP lab used at TI can be seen in Figure 2-1.

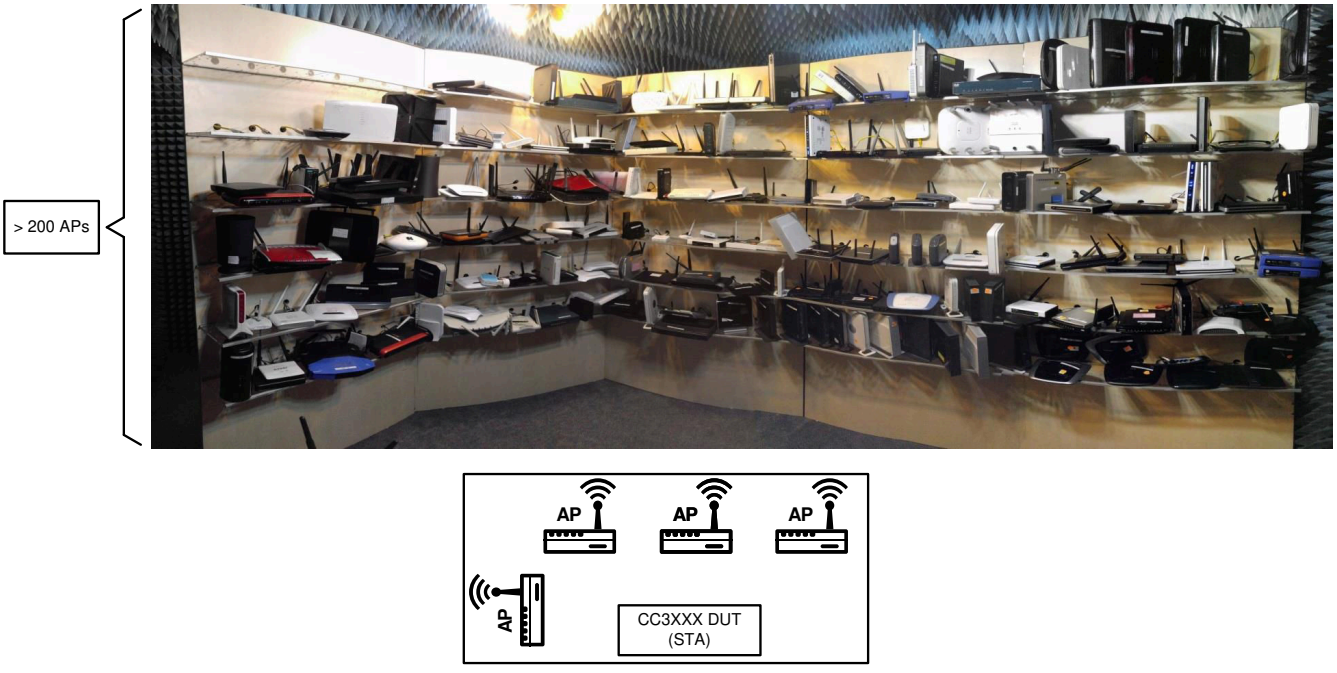

Figure 2-1. Wi-Fi IOP Lab

There are two major test case groups that are run as part of TI's Wi-Fi interoperability testing every SDK release:

- Basic Level
- Long Run

The **basic level** test cases are performed across all APs and include the following steps:

1. Connect the DUT (Wi-Fi STA) to the AP.
2. Acquire IPv4 and IPv6 address using DHCP.
3. Open a TCP/TLS connection to a server on the same network.
4. Run traffic for 5 minutes.
5. Measure current consumption.
6. Disconnect.

The **long run** test cases are performed with select APs and run over longer periods. The periods are defined per AP, with all tests being longer than 4 hours and some tests extended to longer than 12 hours. The APs selected for the long run test cases change over time and may be updated based on market share estimations.

These long run test cases include the following steps:

1. Connect the DUT (Wi-Fi STA) to the AP.
2. Acquire IPv4 and IPv6 address using DHCP.
3. Stay connected in power save mode for a defined period with no traffic.
4. Measure current consumption.
5. Send ping to the device from a peer on the same network and wait for a reply at the end of the period.
6. Disconnect.

2.1 Access Point List

The set of APs used for Wi-Fi testing is updated on a regular basis. Table 2-1 is a snapshot of the set of APs used in the TI lab as of December 2019 and organized by vendor.

Table 2-1. AP List from December 2019

Vendor	Models
3COM	WL-450
Actiontec	GT701-WG, MI424-WR, MI424-WR Rev. D, MI424-WR Rev. I, PK5000
Air	Live WL-5450AP
Airlink	AR570W Rev. A
Amped	R10000, RTA15, RTA1750
Apple	AirPort Express 2nd Gen A1392, AirPort Extreme 1st Gen A1034, AirPort Extreme 3rd Gen A1301, AirPort Extreme 5th Gen A1408, Time Capsule 3rd Gen A1355
Arris	TG1672G, TG1682G
Aruba	3200XM AP 105 PS, 800 Aruba AP 125
ASUS	RT-AC66U, RT-N10+, RT-N10E, RT-N12, RT-N13U, RT-N56U, WL-330g, WL-550gE
AT&T	2wire 2701HG-B
Belkin	F5D8230-4 v3000, F5D8231-4 v2, F5D8235-4 ver. 2033, F7D1301 v1, F7D5301 v3, F9K1002v5, F9K1102v1, N1 Vision F5D8232-4 v1000, N1 Vision F5D8232-4 v2000
BellAir	BA20E-11
Bergtek	WR150
BT	Home Hub 4, Home Hub 5
Buffalo	WCR-G54, WER-AM54G54, WHR-G301N, WHR-HP-GN, WZR-600HP2, WZR-D1800H, WZR-G300N, WZR-HP-AG300H
Cisco	AIR-AP1252AG-A-K924G, AIR-AP1252AG-A-K9 5G, AIR-AP1262N-I-K9 24G, AIR-AP1262N-I-K9 5G, AP1231, AP541N, AP541N-A-K9, DPC3825, M10
Cnet	CQR-980
Corega	CG-WLR300NM
Devicescape	24G

Table 2-1. AP List from December 2019 (continued)

Vendor	Models
D-Link	DIR-605L, DIR-618, DAP-1522, DAP-2690, DGL4500, DI-634M, DIR-300 A1, DIR-600 HW B1, DIR-601 HW A1, DIR-615 HW, DIR-615 HW C2, DIR-618 A1, DIR-625 HW C2, DIR-628 HW A2, DIR-635 HW B3, DIR-655 A3, DIR-655 HW A4 NA, DIR-655 HW A4 WW, DIR-655 HW A1, DIR-825 HW B1, DIR-868L, DIR-890L, DSL-G225, DWL-8600AP A1, DAP-2690
Edimax	BR-6428nS, BR-6478AC, BR-6574n
EnGenius	ERB9250, ESR9850, ESR9855G
eero	B010001
FAST	FW3030Rv2
Fritzbox	7390, 7490, 6842 LTE
Google	Asus OnHub8, TP-Link OnHub, NLS-1304-25
Hawking	HWABN1
Honeywell	WAP-PLUS
HP	V-M200
Huawei	WS322
ipTIME	N104Q, N604M
Levelone	WBR-6003
Linksys	E1000, E1500, E1550, E2100L, E2500, E3000, E3200, E4200, E900, EA3500 24G, EA3500 5G, EA6350, EA6700, EA7500 V2, EA8500, EA9200, WAP4400N v01, WAP55AG, WAP610N, WRT120N, WRT160NL, WRT160Nv3, WRT300Nv2, WRT310Nv2, WRT320N, WRT400N, WRT54G v5, WRT54G2, WRT54GL, WRT54GX ver. 2, WRT54G-TM, WRT600N, WRT610N, VLP01
Logitec	LAN-W300N/R
Medialink	MWN-WAPR300N
Meru	MC1500 AP300
MikroTik	hAP RB951Ui-2nD
Motorola	Netopia 33447-02, Arris SBG6580
MOXA	AWK-3131A
MSI	RG70A
NEC	Aterm WR7850S, Aterm WR8500N, Aterm WR8700N
Netgear	AC1900, R7000, B90-7550, DGND330v1, DGND3700, Nighthawk AX8 RAX80, orbi RBR50, orbi RBS50, R4500, R6120, R6200v2, R8000, R8500, VVG2000, WGR614v4, WGR614v9, WNDAP350, WNDR3300, WNDR3700 24G, WNDR3700 5G, WNDR3700v1, WNDR3700v3 24G, WNDR3700v3 5G, WNDR3800 24G, WNDR3800 5G, WNDR4000, WNHDE111, WNR2000, WNR2000 v4, WNR3500v1, WNR3500v2, WNR834B, WNR834Bv2, WPN824 v3, WPNT834
Netis	WF-2404
Pace	ATT 4111N-031
PCI	MZK-MF150, MZK-MF300N, MZK-WNH rev A
Proxim	Orinoco AP-4000, Orinoco AP-700
Ruckus	ZD1106, zoneFlex R510
Samsung	CY-SWR1100
Sapido	RB-1602
Securifi	Almond
SMC	WBRP-G
SonicWall	Sonicpoint-Ne
Speedport	W 921V
Tenda	N3, N30, W268R, W307R, W311R, W368R
TP-Link	AC1750 C7 v1.1, aD7200, Archer C9, Deco M5, N900 TL-WDR4900v1, TD-W89841N v4, TL-WDR4300, TL-WNR3500, TL-WR2041N, TL-WR641G, TL-WR702N, TL-WR740N v1, TL-WR740N v2.5, TL-WR740N v5.7, TL-WR740N v5.8, TL-WR741ND, TL-WR800N, TL-WR841N, TL-WR845N, TL-WR940N v2.1, TL-WVR450G, WDR7500 v2, WR541G v4, WR941N v6
Trendnet	TEW-625BRP v2.1R, TEW-625BRP v2.2, TEW-637AP, TEW-671BR, TEW-818DRU
Ubiquiti	UniFi AP AC

Table 2-1. AP List from December 2019 (continued)

Vendor	Models
US	Robotics USR5450, Robotics USR8054
Verizon	A90-750115-07, MI424WR Rev I
WD	N900-F2F
Xiaomi	Miwifi, XB6
ZIO	3300N v2

3 Performance Testing

Performance testing verifies that a device meets the expected performance level in all domains. These tests are not intended to find functional defects, but to validate that a new code version will provide consistent performance as compared to previous code versions. Some of the domains that are included in this testing category are throughput, RF performance, and power consumption.

Table 3-1. Performance Testing Domains

Domain	Description
Throughput	Throughput tests measure the maximum throughput over TLS, TCP, or UDP sockets in various configurations such as: • On different WLAN channels in each band (2.4GHz/5GHz) • With different cipher suites for TLS
RF Performance	RF performance tests verify transmit and receive characteristics using real life use-cases. The characteristics include: • Maximum transmit power in different channels and for all RF modulation rates • RX sensativity in different channels and for all RF modulations • Overall performance in congested environment
Power Consumption	Power consumption tests verify the average power consumption of the device in various real-life use-cases.
Coexistence	Coexistence tests check the performance of BLE and Wi-Fi devices in a coexistence environment.

4 Robustness and Stability

The reliability of a system is defined as the probability that a system, including all hardware, firmware and software, will satisfactorily perform the task for which it was designed over a specific time period and in a specific environment. TI believes that reliability is important for wireless connectivity devices and invests in running dedicated tests to ensure the reliability of its connectivity products. These reliability tests fall into two major categories:

- Robustness
- Stability

4.1 Robustness Tests

The Robustness tests validate the degree to which the device can function correctly with invalid inputs, in stressful environmental conditions, or over a large number of iterations. Some examples of robustness tests used by TI include:

- Opening the maximum number of simultaneous socket connections (TLS or TCP)
- Running different types of connections simultaneously with different traffic patterns or behaviors (for example, with maximum throughput, low throughput, bursts of traffic, no traffic)
- Running different types of connections in a congested environment
- Testing connections when the network is configured to be extremely dynamic (for example, very short DHCP lease time, very short key exchange interval, and so forth)

4.2 Stability Tests

Stability tests validate that the device can function as designed for long periods without degradation in performance or interruptions in service (for example, Wi-Fi disconnection). Some examples of stability tests include:

- Maintaining a connection with maximum throughput for long periods of time (10s of hours)
- Connecting and disconnecting from a network repeatedly for long periods of time (10s of hours)

The period of each stability test is selected per test case. All tests are longer than 12 hours and some test cases run for up to 168 hours (or 7 days). These tests run in environments that simulate real-life scenarios. For example, some tests run in a network that simulates a home network, which includes several other connected devices each using different traffic patterns.

5 Networking Stack

Testing a network stack and the associated protocols is complex and requires multiple test setups and test cases. These tests have to consider real-life scenarios such as handling multiple connections with different throughputs and latencies. Additionally, the tests must consider different behaviors within the network. The network stack tests are performed in each of the supported Wi-Fi roles (Station, Access Point, or P2P) and in different bands (2.4 GHz or 5 GHz).

TI invests in the following tests to maintain a reliable and trustworthy network stack.

Table 5-1. Network Stack Test Cases

Test Category	Description
IPv4/IPv6 Connectivity	Verifies IPv4/IPv6 behavior and connectivity of client and server sockets, including all the different supported options and capabilities.
Maximum Connections (sockets)	Tests the ability to open the maximum number of sockets (both open and secure) including combinations of different socket types. For example: • Connecting to 16 real webpages and downloading the homepage • Connecting to 6 secure webpages and 10 open webpages and downloading the homepage
Network Applications and Services	Verifies the behavior of internal network applications and services such as DHCP server, mDNS client and server, HTTP server, etc.

Some of tools and methods TI uses to test the embedded network stack of the CC31xx/CC32xx devices include:

- Using industry leading tools such as Ixia's IxANVL to validate protocol implementation
- Connecting and running traffic for several minutes on each of the supported TLS ciphers
- Connecting and downloading content from thousands of different websites
- Verifying standard BSD socket functionality

The TLS stack in the device allows it to establish secure connections to the cloud. As a result, the TLS stack must also be evaluated from a security perspective. TI maintains the embedded TLS stack and updates it to address known vulnerabilities using the following methods:

- Tracking common vulnerabilities/exposures and fix critical issues
- Maintaining a formal process for managing product incident reports. For more information, see: .

Fixes to identified issues are released by TI in service packs on a quarterly basis.

6 Functionality Tests

Functionality tests are designed to verify specific features that are included in the SimpleLink Wi-Fi device. In most cases, these are black-box tests that are designed to interact with the device through the host interfaces using software APIs. Automation tools are used to activate the different parts of the API and verify the response of the device. The functionality tests cover both positive and negative test cases for a specific feature based on the defined boundary. These tests cover a subset of all features and are often, but not exclusively, designed to leverage functionality that is not tested by the other test types.

Functional test are performed in two different ways:

- SDK Tests
- Dedicated Feature Tests

SDK tests verify the internal implementation of the Wi-Fi device, the driver for the embedded network processor, and the software libraries in the SDK. Dedicated feature tests use unique tools to verify functionality that cannot be covered with the standard SDK testing.

7 Pre-Certification Tests

Texas Instruments has obtained Wi-Fi Alliance certification for the SimpleLink Wi-Fi devices and modules. For more information, see the *Transfer of TI's Wi-Fi Alliance Certifications*. In order to verify that the devices meet certification requirements, TI maintains and runs its own testbeds for all of the certified features. These Pre-Certification Tests include the testbeds listed in Table 7-1.

Table 7-1. Pre-Certification Testbeds

Device Role	Testbeds
Station / Wi-Fi Direct	• TGN • P2P • WPS • IoT Low-power • WPA2 Security Improvments • PMF • SAE • WPA3 v2 • MBO
Access Point	• TGN

8 Testing Setup

The majority of the Wi-Fi tests described in this document all leverage a similar test setup. Figure 8-1 illustrates the typical test setup.

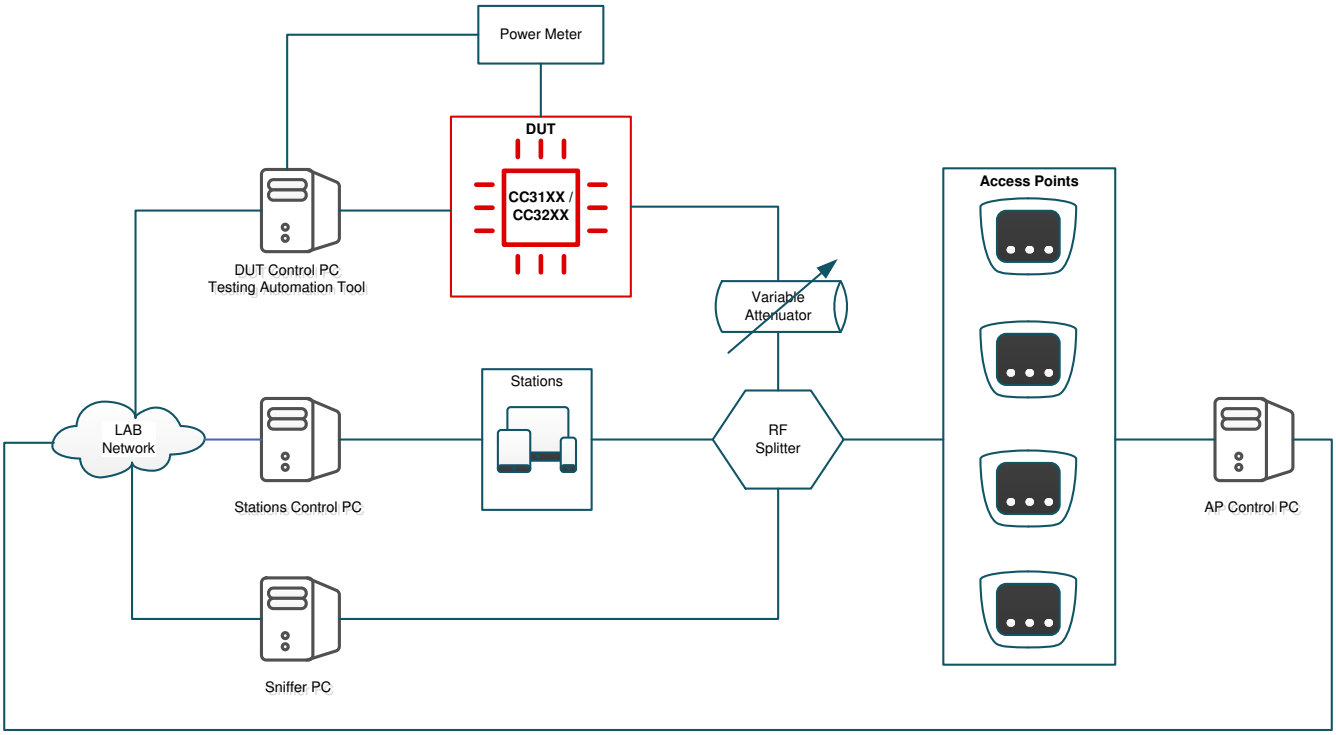

Figure 8-1. Wi-Fi Test Setup Diagram

Several of these test setups are used to run multiple test cases in parallel. Each setup may vary slightly from this illustration by including a different number of access points, stations, and measurement or logging tools.

9 Summary

A comprehensive test strategy is essential for ensuring that Wi-Fi devices have a high level of interoperability, security, and reliability. These factors impact the quality of a Wi-Fi solution and the user experience of a Wi-Fi based product. TI understands the importance of these factors, which is why TI invests in maintaining an extensive test strategy for its SimpleLink Wi-Fi devices comprised of interoperability, performance, robustness and stability, networking stack, functionality, and pre-certification tests.

10 References

- Texas Instruments: *Transfer of TI's Wi-Fi Alliance Certifications*

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265