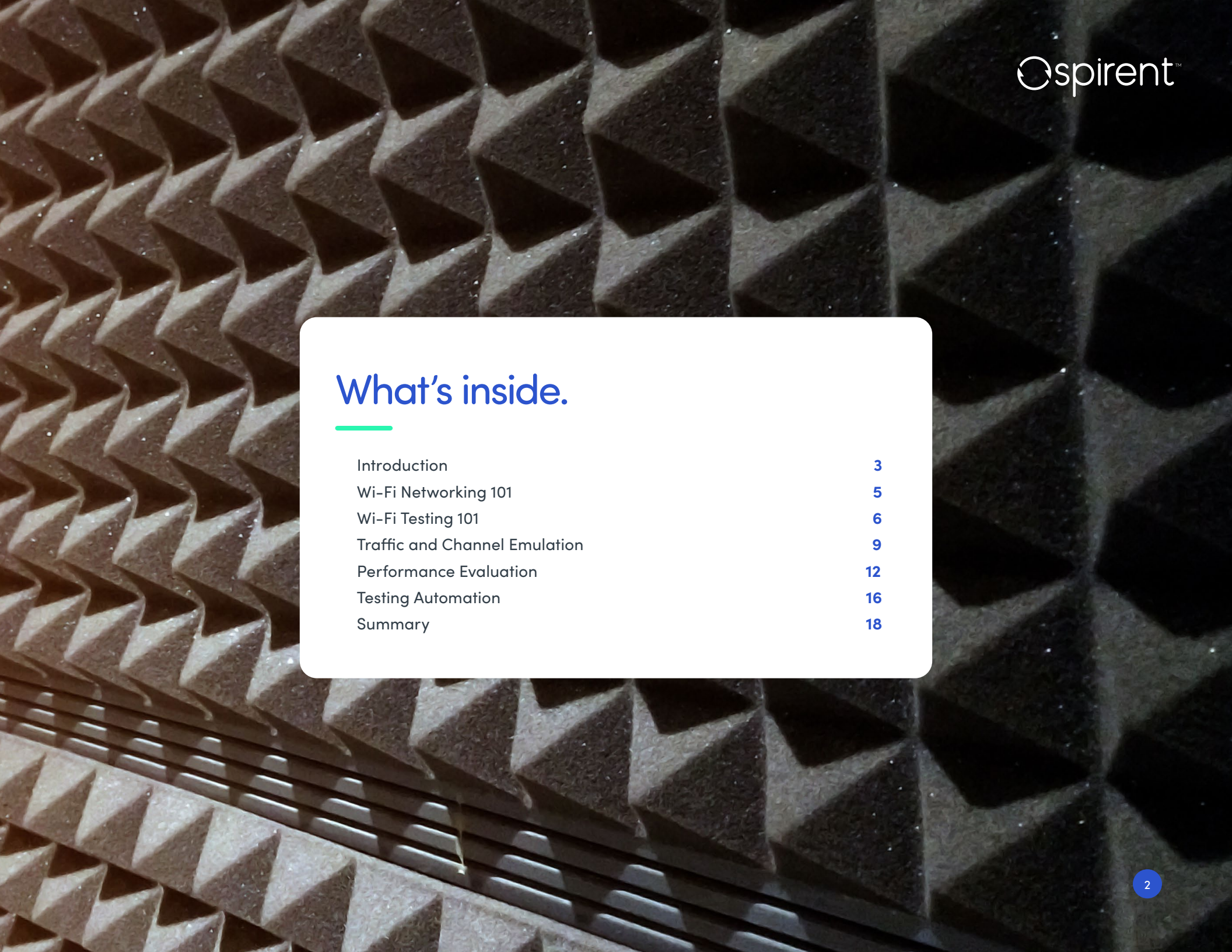
A SPIRENT EBOOK

Testing Wi-Fi for High-Performance Use Cases



What's inside.

Introduction	3
Wi-Fi Networking 101	5
Wi-Fi Testing 101	6
Traffic and Channel Emulation	9
Performance Evaluation	12
Testing Automation	16
Summary	18

Introduction

More than 16 billion wireless devices are in the world today[1], driving $3.3 trillion in global economic value.[2] The industry will ship an additional 4 billion Wi-Fi devices in 2021 alone. This juggernaut is driven by a wide range of existing and emerging use cases, including:

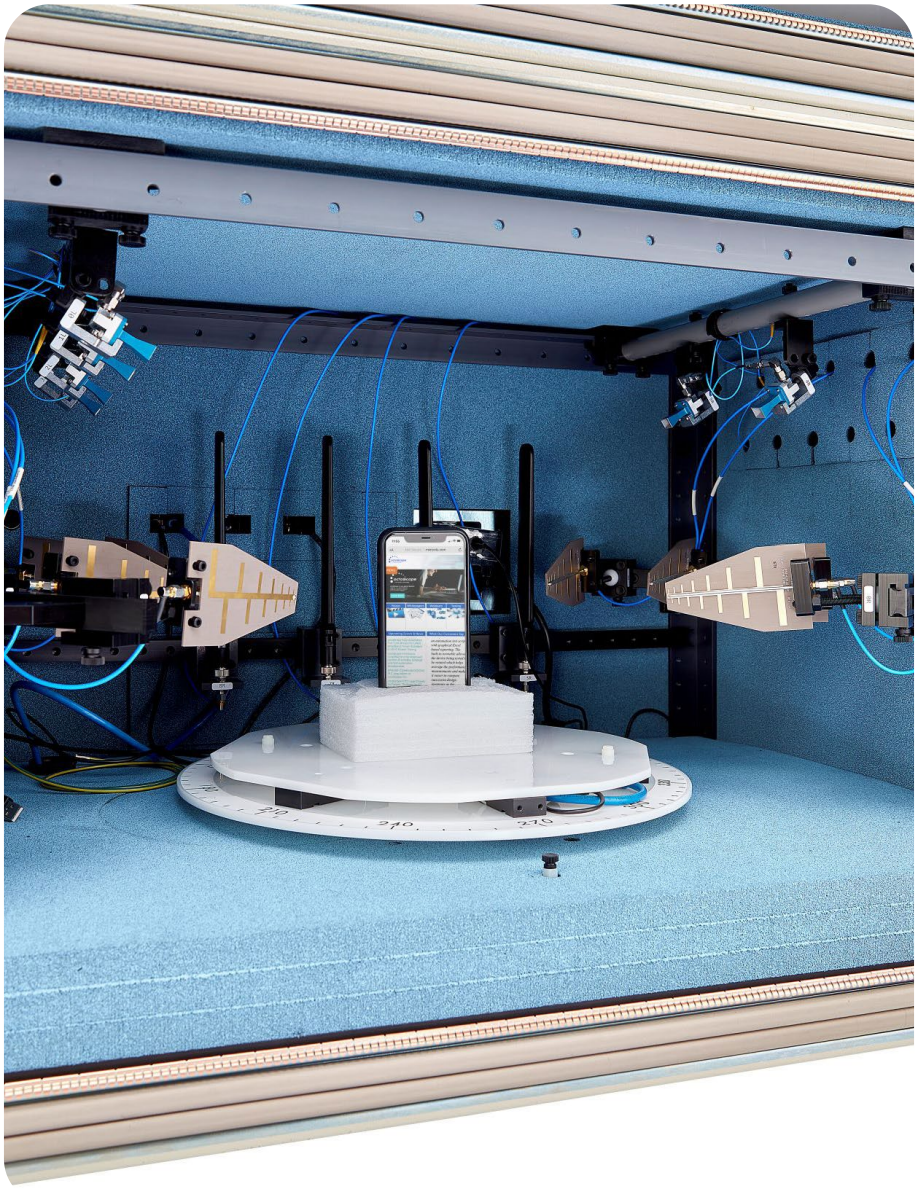
[1] IDC
[2] Wi-Fi Alliance

Whereas Wi-Fi was once a nice-to-have feature that allowed people to browse the internet and check email, today's Wi-Fi apps are becoming increasingly crucial. Telehealth, Factory 4.0 and eLearning are three examples of apps that require a much more exacting Quality of Experience (QoE). As these and other new apps emerge, the need for precise, comprehensive testing of Wi-Fi networks and devices becomes critical.

In these new Wi-Fi use cases, the stakes are high. The costs of letting undiagnosed product issues creep into the field are significant:

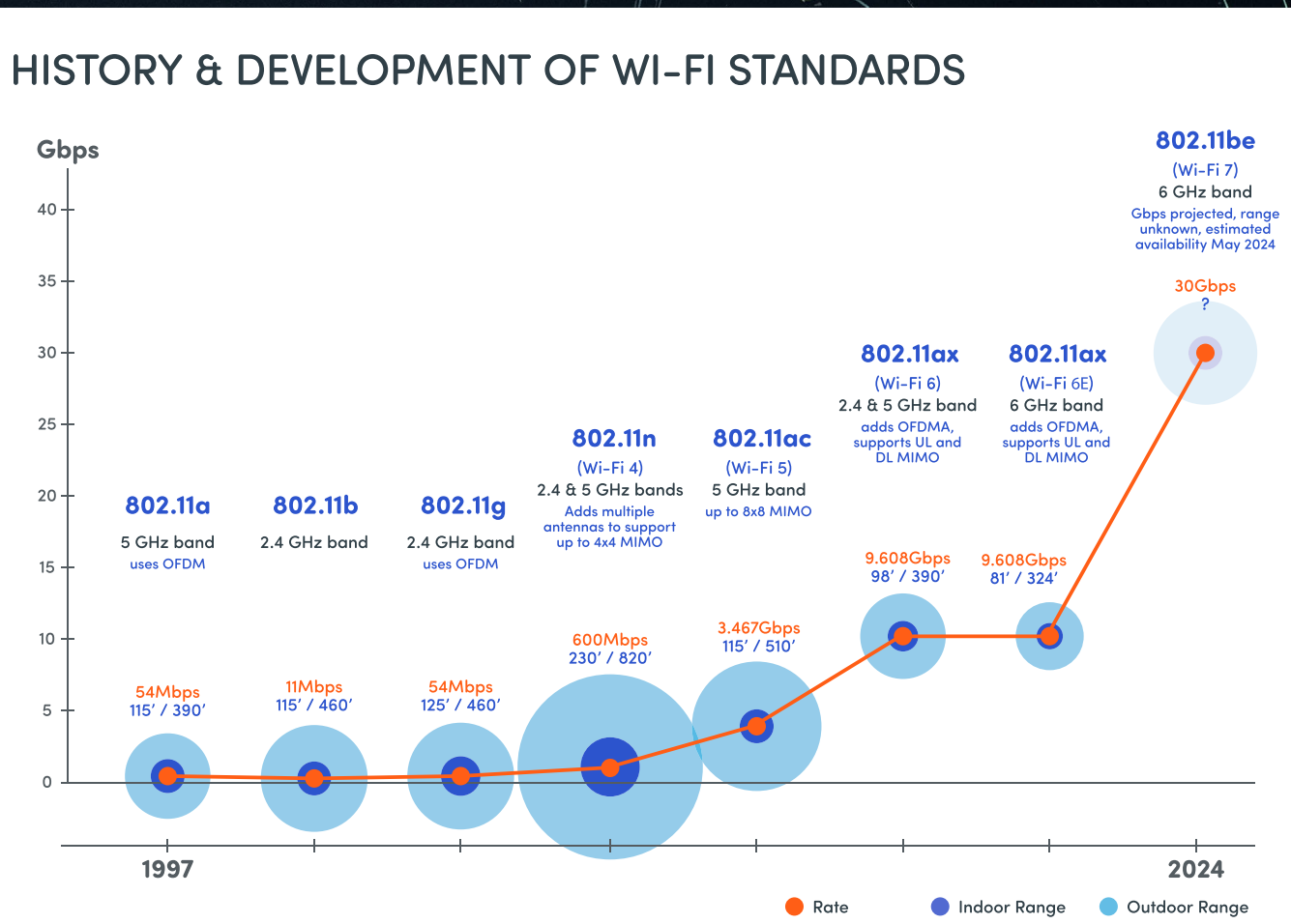
- Delayed revenue streams
- Angry customers
- High costs to fix problems (truck rolls, replacing equipment)
- In some cases, safety

As well, in the wake of Covid-19, with Wi-Fi taking on more of a workload in business and work-from-home (WFH) environments, an accelerating pressure to test Wi-Fi products accurately and comprehensively before they ship has reached a heightened priority. In this Ebook, we examine how best to achieve the caliber of testing required to ensure Wi-Fi networks and devices are performant and reliable enough for tomorrow's wireless world.

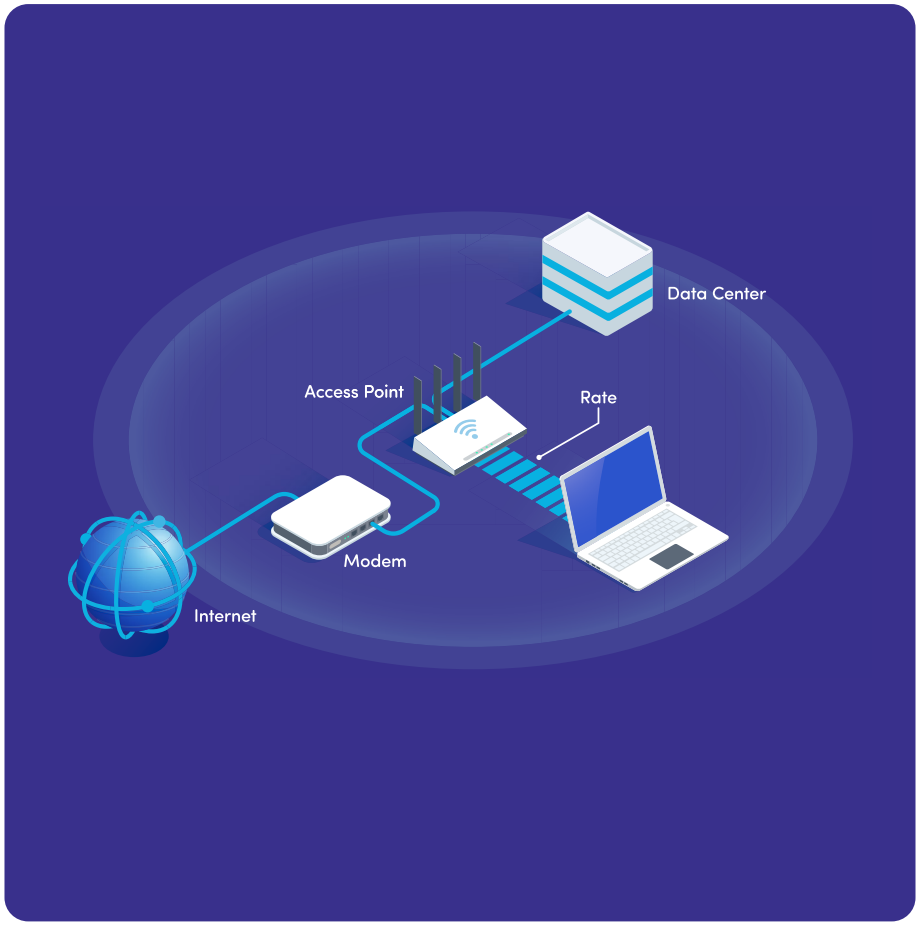


Wi-Fi Networking 101

Wi-Fi was born nearly a quarter-century ago (in 1997). It has progressed rapidly since then, with Wi-Fi 6 boasting 178X better throughput than the original 802.11a standard, at roughly the same range:



Conceptually, Wi-Fi's operation is simple. A Wi-Fi-enabled device, such as a laptop, smartphone or IoT device, connects with a Wi-Fi access point using radio waves operating in the 2.4, 5.0 or 6.0 Gigahertz spectrum. The access point then connects to the network the device is trying to reach – perhaps the internet for a home or public Wi-Fi network or a wired network in a business.



Wi-Fi Testing 101

Before examining the complexities of Wi-Fi testing, it is helpful to provide a simple overview of what's being tested. At the highest level, it involves testing three key aspects of Wi-Fi:

Conformance. Does the equipment meet standards? The Wi-Fi Alliance (WFA) provides standards to which vendors must conform.

Interoperability. Does the equipment work with other Wi-Fi equipment? For example, does a smartphone's Wi-Fi interface work with various Wi-Fi access points? WFA also provides interoperability standards to which vendors must conform.

Performance. Is the performance of the Wi-Fi equipment being tested sufficiently? For example, the Broadband Forum (BBF) has released the TR-398 Wi-Fi In-Premises Performance Testing standard.

Summing up, Wi-Fi testing answers three basic questions: Does specific Wi-Fi equipment work? Does it interoperate with other Wi-Fi equipment? And, is its performance sufficient? Put simply, performance testing involves a measurement of two key metrics:

- How fast is the connection (**rate**)?
- How far can the connection reach (**range**)?

These two qualities are interdependent – as the distance between the device and the access point (AP) increases, the connection speed decreases. The maximum **rate** will occur closest to the access point, while the maximum **range** will deliver the slowest rate.

There is much more to Wi-Fi testing in the real world than these basic descriptions. Let's dive into an overview of these nuances.

How is Wi-Fi testing accomplished?

In essence, Wi-Fi testing should be simple; just measure signal strength at every distance from the AP out to where you don't have enough signal to use Wi-Fi. That's called an RvR test (Rate versus Range). It's a basic idea but performing an RvR test is not as easy as it seems.

The problem is there are so many factors that can affect Wi-Fi signals, and these change from day-to-day, hour-to-hour and even minute-to-minute. A partial list of the dynamics affecting Wi-Fi signal strength and range include:

- Atmospheric conditions
- Physical obstructions (like walls)
- Interference from other wireless networks, electronic gadgets, etc.
- Signal reflection
- How Wi-Fi equipment is oriented

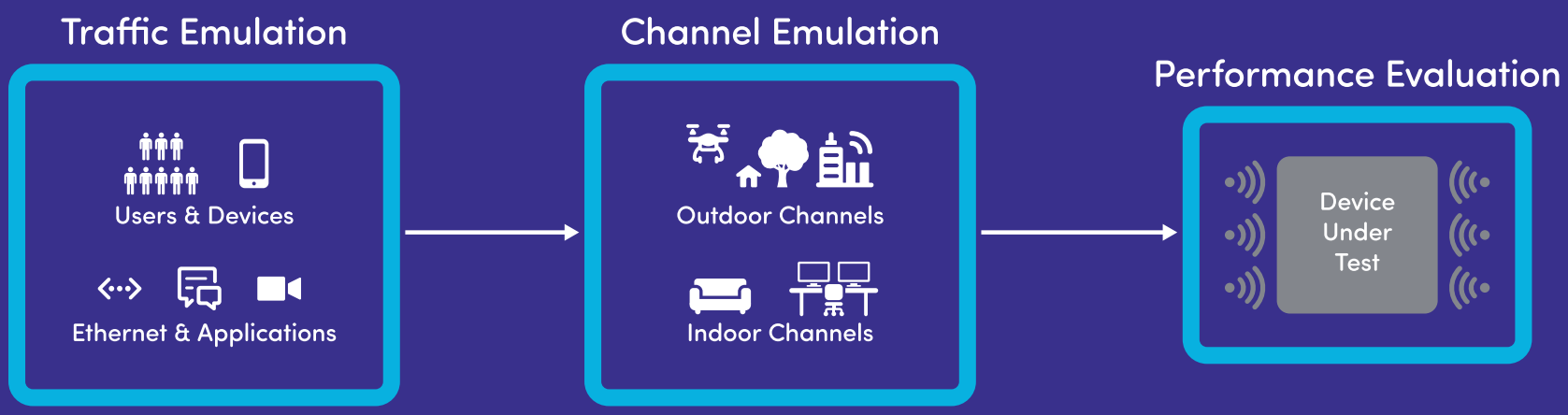
If you cannot control these variables, you'll find that your test is not repeatable. It might show great signal strength one minute, average the next, and poor the next test after that. The key to accurate and efficient Wi-Fi testing is using a test methodology that controls these variabilities.

Wi-Fi Signal Strength Explained

Wi-Fi signal strength is measured in decibel milliwatts. Why decibel? Wi-Fi signals are waves, and as is true with all waves, the signal strength decreases proportionally to the square of the distance the wave travels. For example, the signal at 2 feet is just a quarter of the signal at 1 foot and at 8 feet it is down to less than 2% of the signal at 1 foot (1/64th). The decibel scale is useful because it is logarithmic, which means it maps these massive changes into a simple scale. For similar reasons, sound waves and light intensity are also measured using a log scale.

Here is a simple guide to Wi-Fi signal strengths:

In a broad sense, Wi-Fi testing involves the following steps:



Traffic emulation is where the test generates realistic network traffic. Emulated traffic can be stateless or stateful. Stateless emulation typically focuses on generating huge volumes of layer 2/3 traffic for load testing. Stateful emulation covers the entire protocol stack, layers 2-7, and is used to characterize the end-user experience.

Channel emulation involves test methodologies that emulate the behavior of the various Wi-Fi channels. The emulation models real-world behavior by introducing delays and attenuation of the radio signal. It can be passive, where cables are used, or real-time digital signal processing (DSP) based, a more sophisticated channel emulation that can emulate a wider range of environments more accurately.

Performance evaluation validates the device under test (DUT) to assess how it responds to the emulated channels and traffic. There is a wide range of ways to do this, which we'll discuss in detail below.

Traffic Emulation

While there are low-level tests that don't require traffic, you will eventually need realistic network traffic to observe how your DUT performs under realistic conditions. There are two ways to generate it:

Stateless traffic emulation simply generates a stream of low-level network packets. Also known as "packet-blasting," stateless traffic emulation aims to validate lower-layer performance under load. It is helpful when measuring key metrics such as total throughput, packet loss, jitter, and latency.

While relatively simple and cost-effective, this testing method doesn't capture end-user experience or higher-layer performance.

Stateful traffic emulation generates a stream of layer 2-7 packets. This provides metrics that directly impact user experience such as dropped calls, lost connections, application-layer throughput and latency. It can directly measure perceptual quality for speech and video.

More useful than stateless traffic emulation, it is also more complex and expensive.

Channel Emulation

Once you are capable of generating network traffic, the DUT must be tested for performance under a wide variety of conditions. This involves varying distances and orientations between Wi-Fi devices and access points, introducing interference, modeling multipath, and dozens of other factors.

In the next section, we examine different ways to test the actual devices. In some approaches (such as walk testing), the methodology uses actual hardware which have real channels. But for reasons we explore in the next section, that has many disadvantages.

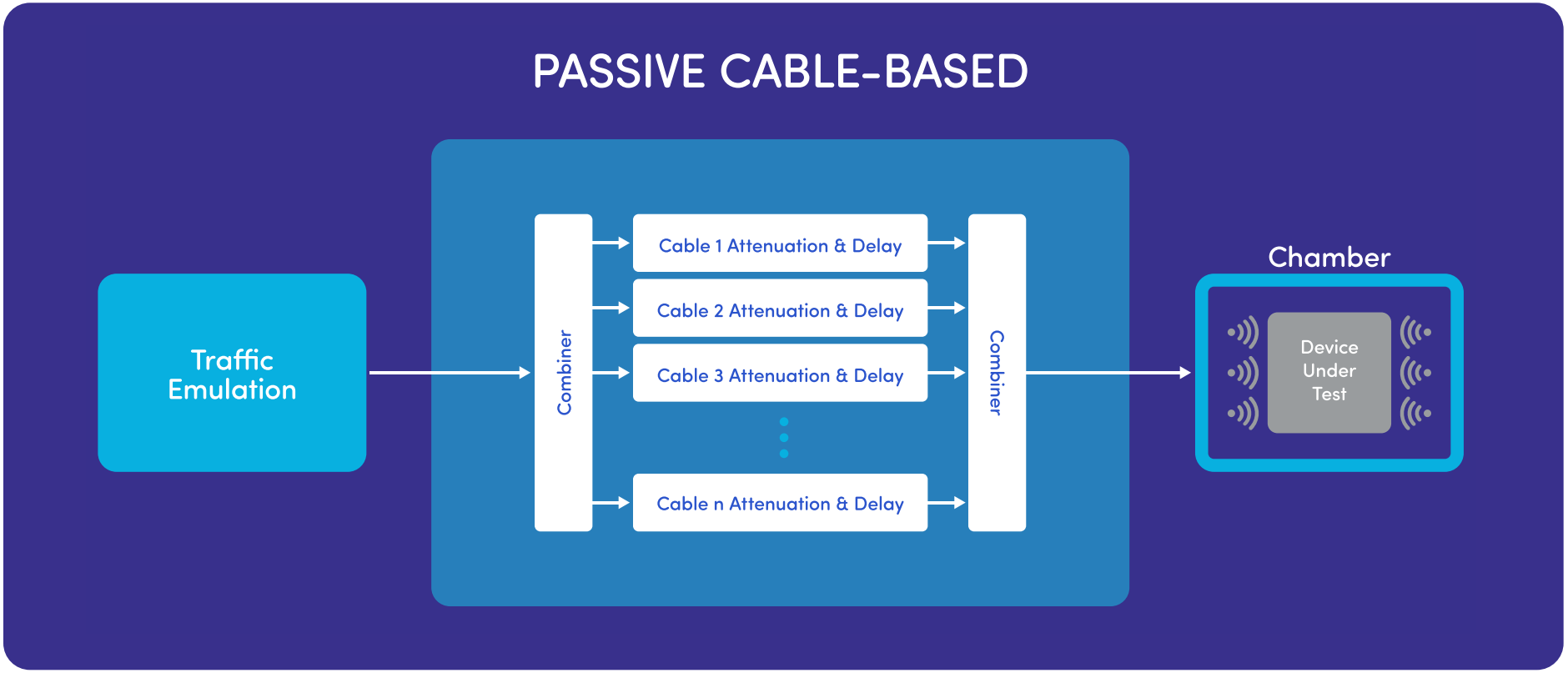
A channel emulator takes the network traffic from the previous step and emulates how that traffic flow would be affected by various real-world environments and test scenarios (interference, distance, etc.). This can lead to a more reliable, repeatable, efficient test.

There are two approaches to accomplish channel emulation:

Passive, cable-based channel emulation uses multiple cables that run between the traffic emulator and the test bed. These cables can introduce delays and attenuation to emulate what would happen in the real world based on test scenarios.

Passive cable-based channel emulation supports a wide range of frequency bands. It can be used with any technology (e.g., Wi-Fi 4, 5, 6 or 6E). This approach is suited to emulate simple channel models such as the IEEE Models A (line of sight) or B (indoor home or small office multipath). It is relatively cost-effective.

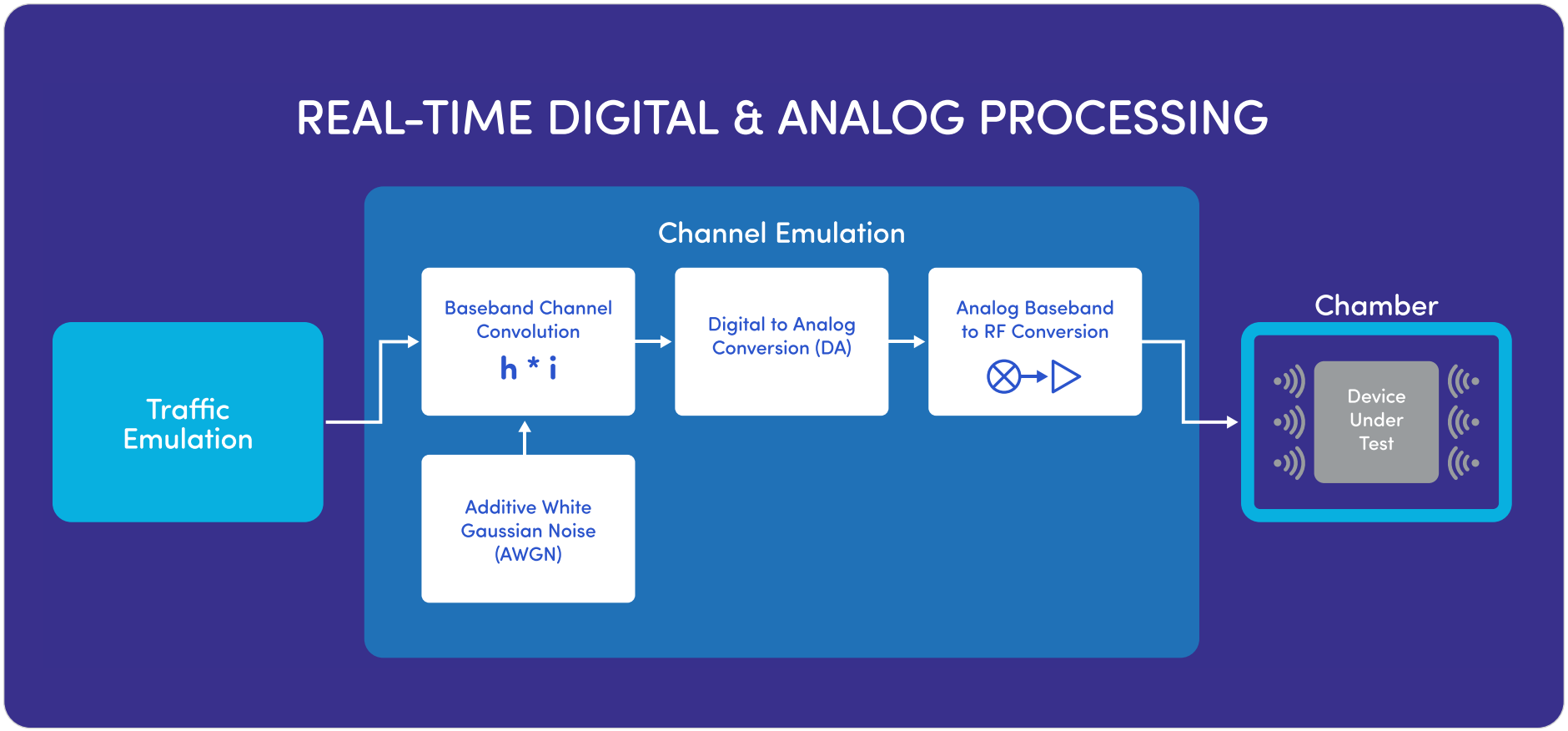
Passive, cable-based traffic emulation supports only a limited range of environments and doesn't model all aspects of multipath fading in a mobility environment.



Real-time DSP-based channel emulation is a much more sophisticated form of channel emulation that uses advanced DSP technology to emulate different channel scenarios. But real-time DSP-based channel emulation is more expensive and more complex to configure.

Real-time DSP-based channel emulation can emulate more comprehensive environments, such as large offices, small offices, homes, outdoor, outdoor to indoor, airborne, air to ground, etc.

It also supports all IEEE models (A-F). Furthermore, it more robustly emulates mobility (factors like multipath fading, etc.). Finally, it supports a broader range of frequencies (30MHz to 6GHz + millimeter wave).



Performance Evaluation

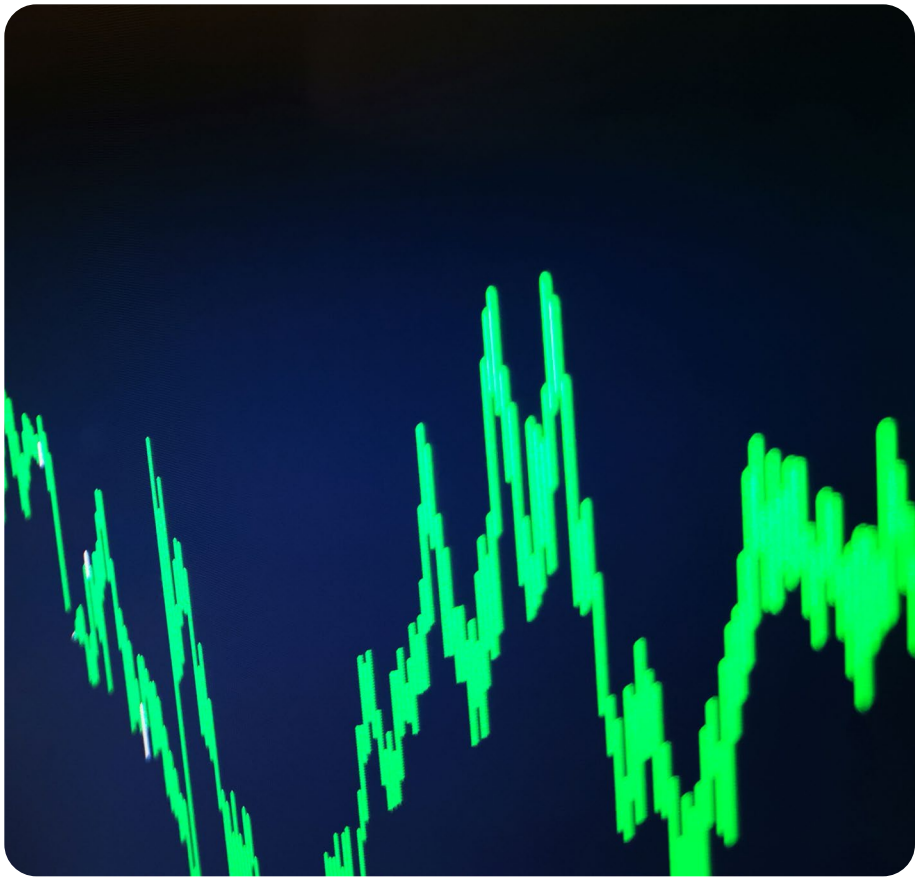
Once you have generated realistic network traffic and emulated the effects of channel scenarios, observing the performance of the DUT follows. For this, the DUT is configured for a wide range of testing. Each has its own advantages and disadvantages:

Walk (or drive) testing is where the test engineer walks/drives the Wi-Fi device around a real-world location. The goal is a realistic RvR test in an actual environment. Recalling the Verizon ad where the tester walked throughout a city saying, "Can you hear me now?" – that's the essence of this type of field testing.

Walk (or drive) testing is simple and generally inexpensive. It provides a straightforward way to perform RvR testing with the advantage of testing in a real-world environment.

It is susceptible, however, to virtually all the various interference sources we noted previously. For this reason, this testing exhibits practically zero repeatability.

Large anechoic chambers are large rooms fitted with materials that isolate the room from outside interference and significantly reduce wave reflections off the walls, ceiling, and floor. These are effective due to the lack of interference and reflection. Such large rooms are costly and complex to use. Due to the cost and size, they tend to be shared among various engineering and test teams, and thus are too often unavailable.



Testing in outdoor antenna ranges makes use of an open area where engineers can test various antennas and Wi-Fi equipment. Because these facilities are typically remote, there is less interference from other radio signals, but some still exists. Plus, the facilities suffer from other interferences, such as atmospheric conditions. In any case, these facilities are accessible and usable by only the most sophisticated users.

Conducted testing involves replacing actual "over-the-air" (OTA) radio transmissions with simulated radio signals. The signals are generated by channel emulators and are connected directly to the DUT. The best channel emulators can emulate real-world conditions, including interference, signal fading, multipath fading and so on.

However, as increasing numbers of antennas are added to access points, conducted testing is becoming impractical and cumbersome with the requirement of attaching a continuously growing number of cables to new antennas. In addition, as these antenna arrays grow, it is important to analyze the radiation patterns they produce, which is achieved more effectively in an over-the-air scenario.

Personal testbeds are a recent advancement and a novel variation to traditional anechoic test chambers. Personal testbeds make use of smaller anechoic chambers that can be connected to each other. Wireless devices (e.g., APs and STAs, eNodeBs and UEs, etc.) are isolated in their own individual chambers, where their OTA signals are connected to devices in other chambers via RF cables with specialized programmable attenuators to emulate different real-world configurations.

Personal testbeds are smaller, less expensive, and less complex. They are also very efficient, often reducing testing from weeks down to hours. With proper configuration, personal testbeds can emulate real-world challenges and interference, as well as all Wi-Fi and 5G spectrum bands.

Past Wi-Fi testing approaches were more geared to testing individual Wi-Fi components, which is sufficient for determining the performance level of a single instrument but cannot fully assess how that instrument will perform as a component in a system of multiple instruments. The personal testbed approach excels at system-level testing, which is of increasing importance as Wi-Fi is used for new use cases such as streaming video and real-time monitoring where end-to-end performance is critical.

A testbed with multiple small, isolated chambers can test complex configurations including new mesh systems, where the base Wi-Fi access point is extended with peripheral devices to increase signal range in larger spaces. Some of the challenges faced when using extenders in these system configurations are:

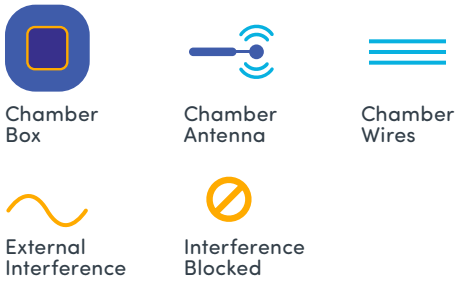
- Sending packets twice, which creates congestion and two times the exposure to interference
- Handovers – devices can sometimes get “stuck” on a particular extender rather than switching to a stronger signal source

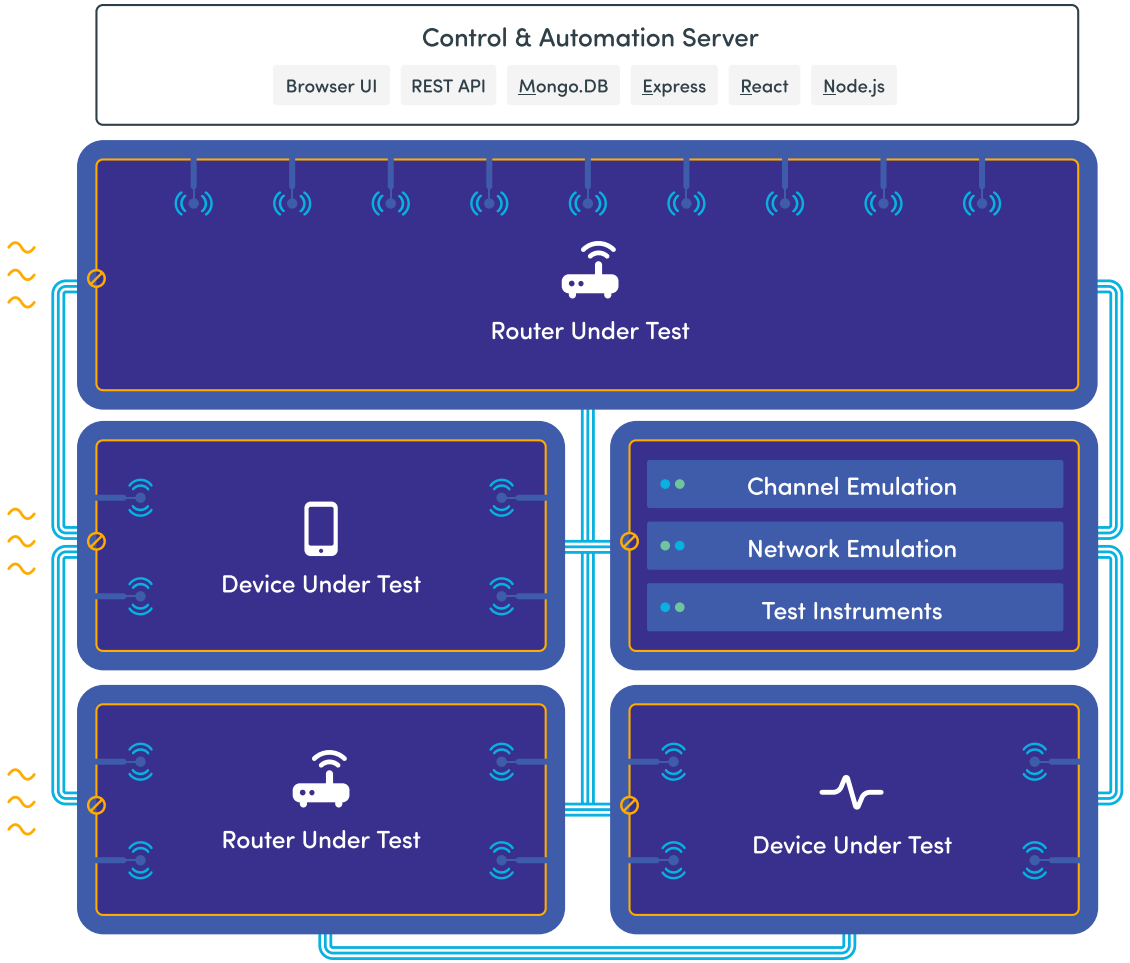
Mesh and band steering tests demonstrate how well an access point and range extenders maintain airlink efficiency to support demanding applications such as video and audio over Wi-Fi.

An important data capturing tool to observe the behavior of the system under test is sniffing. Traditional (pre-Wi-Fi 6) sniffers used to be able to look at all of the packets on the air using a sniffer in monitor mode, which is no longer possible in Wi-Fi 6/6E. OFDMA and MU-MIMO packets are sent using specific IDs (association IDs, or AIDs) that allow receivers to identify traffic even when multiple packets are being sent simultaneously. Without using these IDs, it is no longer possible to sniff the packets, so specialized synchronization tools within these testbeds have been designed to keep the association and capture results while a test is running.

Another key testbed feature is the ability to take captured real-world results, for example in a walked path through a home or office, and play back the walk in the testbed just as it was recorded. Replicating these highly repeatable test scenarios enables the user to look for behavior inconsistencies.

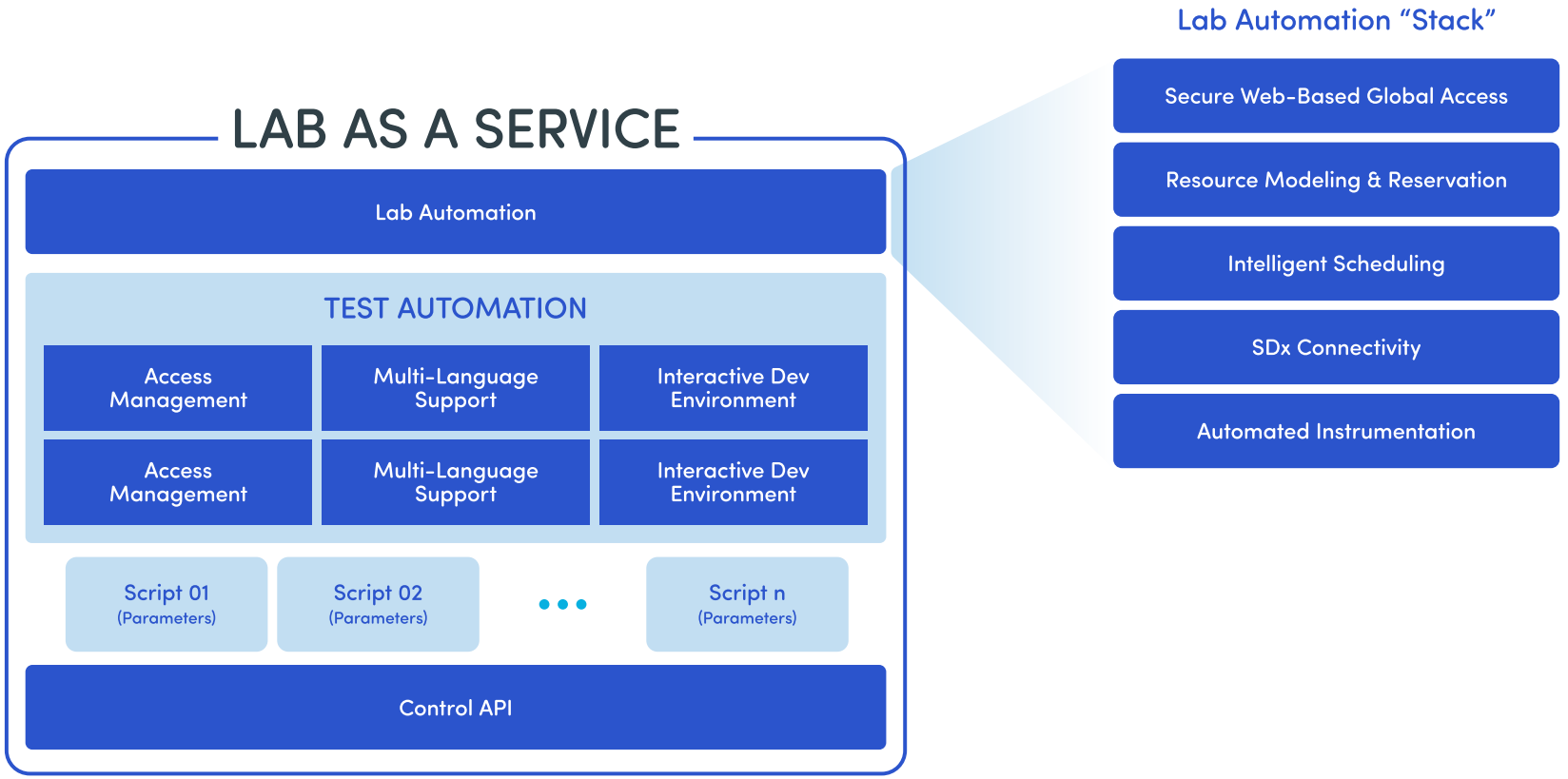
There are many choices to make when deciding on how to test your Wi-Fi equipment. But, once you've made these decisions, you'll need to find a way to accomplish your testing loads quickly, reliably, and effectively. For that, Wi-Fi testing automation is required, which we describe in the next section.





Testing Automation

The pace of Wi-Fi technology change has accelerated over the past decade. At the same time, the requirement to deliver next-generation products quickly has also increased. Wi-Fi 6E was recently released, yet articles are already coming out about Wi-Fi 7. 5G is also just reaching the masses and already 6G is being discussed. As well, Wi-Fi 6 and 5G are viewed by many experts to be headed for convergence.



At the same time, the importance of Wi-Fi has increased. Whereas Wi-Fi 10 years ago was useful for checking email and getting directions, today's Wi-Fi apps include Factory 4.0, remote telehealth, and edge computing applications such as autonomous vehicles or drone delivery, along with a massive increase in demand for supporting WFH users.

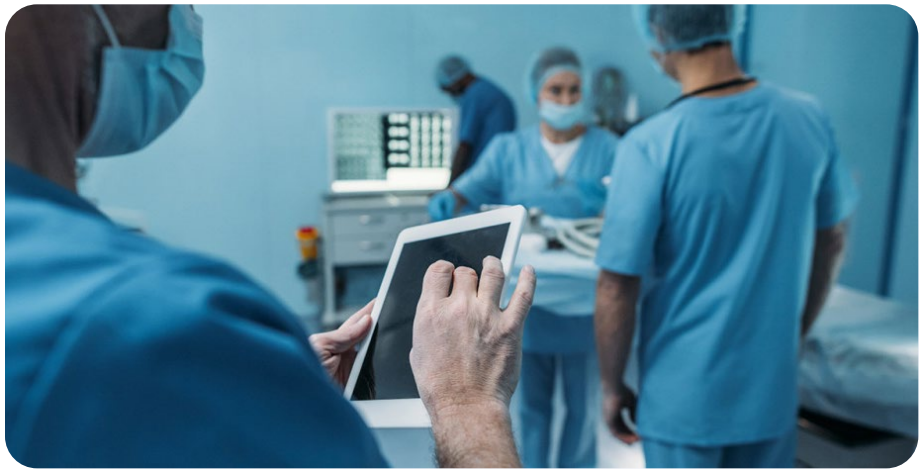
The bottom line is that testing Wi-Fi has moved from "nice-to-have" to "must-have" and the timeline for such testing has moved from "when possible" to "now."

But how can the industry keep up? The answer is Wi-Fi testing automation. Let's discuss the details of how to leverage automation for your Wi-Fi test needs.

Basic Test Automation (aka Script Management). Fundamentally, automation is as simple as running basic test scripts that automate test equipment and DUTs using a Control API. A primary Wi-Fi test automation solution comes with a suite of different standard tests to run. These are designed by qualified Wi-Fi experts, which means in-house test engineers don't need the most advanced degree of subject matter expertise. They can change key parameters using a user-friendly GUI, and easily run the tests as needed. During tests, automated capture of the packets running across the network is needed to provide essential feedback on network performance. Wireshark – an open-source packet capture solution – is a common choice here.

Advanced Test Automation. To get the full benefits of automation, additional capabilities beyond script management are required. Access management controls the permissions for creating, modifying, and executing test scripts, to ensure any changes to test scripts are carefully reviewed first and aren't accidentally introduced. Because automation is built over time, a full test automation framework should provide multi-language support including import, modification, and execution of the most popular languages such as Python and Robot. An interactive development environment (IDE) makes it easy to create, edit, and debug test scripts and links to rich results analyses including automated test execution reports. To accelerate the creation process, the IDE should enable users to record and play back manual testing activities such as using a command line interface (CLI) to configure a device under test.

Lab Automation. Building on advanced test automation, lab automation allows distributed teams to efficiently access automated testing environments. One key feature of lab automation is secure Web-based global access, which provides a single portal for users around the world to configure and spin-up testbeds and kickoff testing – in minutes. With resource modeling and reservations, all physical and virtual equipment in local, regional and global labs represented in a single screen GUI, teams easily share equipment and other resources needed to run their tests. Intelligent scheduling allows equipment to be powered up and accessed "just in time" to run tests, maximizing energy efficiency.



Absolutely critical to achieving full test lab automation, software-defined everything (SDx) connectivity links all automated instrumentation, lab networks and DUTs with layer 1 switches, which may be rapidly reconfigured based on test reservations.

Lab as a Service. When organizations don't have the time, resources, or upfront capital to deploy their own lab automation solution, a Lab as a Service (LaaS) model delivers these capabilities as a managed solution. Common options include a fully hosted solution or hybrid models where the LaaS service provider hosts a subset of lab infrastructure or manages a subset of lab workflows. Traditionally, a vendor offering this kind of solution should also provide the option of an accompanying Test as a Service (TaaS) solution.

Summary

Applications and new use cases are driving a need for more robust bandwidth (high speed, low-latency, high reliability). Wi-Fi is an obvious answer for many of these new applications. The questions many communication service providers (CSPs) face remains: Is our Wi-Fi ready for today's broadening demands and those in the future? After decades of being a nice-to-have, is our Wi-Fi ready for mission-critical, and sometimes life-and-death use cases?

Only with robust, efficient, effective, and continuous automated Wi-Fi testing will those questions be answered with confidence.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled. For more information visit: **www.spirent.com**

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com