Quick Guide: How to Test 6 Crucial Parameters in Your WLAN

In this guide you will learn how to test six crucial parameters of your wireless local area network (WLAN): 1) Ability to connect and transfer data; 2) Interference; 3) Capacity and coverage; 4) Roaming and range; 5) Load and performance; and 6) Policies and quality of service.

Below, we have outlined how to perform a basic test of your WLAN on your own with no special equipment. We will also show you how to perform a more comprehensive test using specialized equipment made by Ixia®.

Testing your own WLAN

Basic testing: connections, interference, capacity, and range

Perform the following steps to do a quick "Sanity Check" of your WLAN:

1. Turn off all your WLAN access points except one. Connect to it with five different Wi-Fi–enabled devices of different types (iPhone, Android phone, laptop, etc). Experience the network on each of the devices.

2. Run a streaming video on a mobile device, and move close to sources of radio interference in your office, such as microwave ovens, cordless phones and other WLAN. See if video streaming is interrupted.

3. Find a time when the office or facility is relatively full. Invite everyone present to a conferencing session (using a tool like WebEx or GoToMeeting), and determine if everyone can hear the audio session well.

4. Measure from your WLAN access point to see where the reported range ends. Initiate a Skype call from a mobile device and walk toward a location outside the range. Watch the signal strength going down; what is the user experience at the fringes, and at what point you lose the signal completely?

5. If there is more than one access point, walk from one access point to another. See the signal strength going down and wait for roaming to occur—the signal will then begin to strengthen.

This test verifies that your WLAN setup is functioning. It also helps you determine if radio interference, increases in load on the network, and physical conditions in your office or facility are getting in the way of Wi-Fi connectivity.

Testing load and performance

Next, we will test how your WLAN access points deal with simulated network load and what performance they deliver under load.

1. Download a free program called iPerf, which is used for network load testing.

2. Install the server version on a laptop on the wired network, and the client version on five devices connected to the wireless network.

3. Run the following command from each of the five client devices:
   ```
   iperf -c 192.xxx.xxx.xxx -u -b 2m -P 5
   ```

   Where "-c" specifies client, "192.xxx" is the Internet Protocol (IP) address of your server on the wired network, "-u" specifies User Datagram Protocol (UDP), "-b 2m" specifies each device should use 2 MB of bandwidth, and "-P 5" specifies there should be five concurrent network connections from each device. So, we are testing 25 connections in total with 2 MB bandwidth each, which totals 50 MB.

4. iPerf will show output indicating the result of the test. The output should look like something like this:
   ```
   Server Report: 0.0-10.0 sec xx MBytes 1.9 Mbits/sec 0.167 ms
   49/69507 (0.07%)
   ```
   Mbits/sec is the actual bandwidth your device got from the WLAN access point for each connection.

If you are getting close to the full 2 MB of bandwidth for each of the 25 connections, your WLAN access point is operating reasonably well, and there does not seem to be a major performance problem.

Testing WLAN policies

1. Check in your WLAN access point documentation for information on how to block traffic for certain ports.

2. Using a mobile device that has mobile data turned off open a browser and try to view google.com. Make sure the website displays correctly on the device.

3. Now block port 80 on all your access points.

4. Try to refresh the website on the device. You should get an error saying the site is not available.

This test verifies, at a basic level, that your WLAN access point is capable of executing policies and blocking specific types of traffic.

It is also important to test quality of service (QoS)—that the access point is able to guarantee a certain level of network performance for specific types of devices. But, it is very difficult to test QoS without specialized equipment.

Testing your WLAN with Help from Ixia

As you read in the preceding section, it is possible to test some aspects of your network manually. However, these tests can be labor intensive and cover only basic aspects of WLAN functionality.

Ixia IxVeriWave™ is a hardware solution that simulates complex WLAN environments and enables custom testing that is virtually impossible to execute by any other means. Using multipurpose traffic generation modules, this tool can emulate a large variety of real devices and the traffic they send and receive on the network. So, you can test your WLAN without laboriously manipulating real user devices.

Most importantly, IxVeriWave can test at scale—it can simulate anywhere from dozens to **hundreds of thousands** of connections to your WLAN, and reports how the WLAN access points actually perform.

In addition, IxVeriWave tests **all** of your WLAN access points' functions and components by simulating real-world conditions, measuring performance and tracking device and access point behavior.

- **Measures radio transmitter and receiver quality** under a variety of ideal and real world test conditions.

- **Exercises the access points' processor and packet buffers** by running full line rate throughput tests to see if the access point can receive, process, and transmit large amounts of data.

- **Tests the client association manager** by connecting hundreds of client devices to the access point and making sure they can connect, disconnect, and send and receive traffic.

- **Tests the Transmission Control Protocol (TCP)/IP stack** and measures the access points' ability to handle web traffic.
- **Tests QoS capabilities** of the access point by generating different types of traffic with different QoS settings. This lets you assess access point performance for each type of device and each type of traffic in your network.
- **Fully tests the policy engine** on the access point by creating many different policies (blocking or preferring different types of traffic) and then sending relevant traffic. For example, with IxVeriWave you can automatically set a policy to block peer-to-peer (P2P) traffic, then simulate some P2P traffic, and make sure it does not get forwarded.
- **Tests the client session manager** on the access point to check the roaming of clients between WLAN cells.
- **Tests the radio resource management** capability of the access point—IxVeriWave generates different types of interference and checks the access points' ability to operate uninterrupted.
- **Tests the authentication and encryption** mechanisms supported on the access point, and ensures traffic is encrypted properly in all use cases.
- **Tests standards compliance** for dynamic frequency selection (DFS) and Federal Communications Commission (FCC) radar.

Benefits of testing with IxVeriWave

CRUCIAL PARAMETER	TESTING EQUIPMENT VERIFIES	
Ability to connect and transfer data	✓	All access point features are working as advertised
Interference	✓	Access points' ability to overcome any type of interference in any location
Capacity and coverage	✓	Access points' true maximum capacity
Load and performance	✓	The maximum number of connections and bandwidth advertised by the access point manufacturer
Policies	✓	All policies supported by the access point by simulating the appropriate traffic and ensuring policies are correctly enforced
Quality of Service	✓	Quality of service through scientific testing with different levels of device activity, different traffic types, network congestion, etc.
Quality of Service	✓	Quality of service through scientific testing with different levels of device activity, different traffic types, network congestion, etc.
Roaming and range	✓	Complete map of WLAN, exact range supported by access points, and where failure points lie

Critical Testing for a Critical Infrastructure

Wi-Fi is a critical business infrastructure and needs to be tested to ensure it will enable productivity for employers and convenience for visitors and customers with no disruption in service.

When you buy a car, you will want to take it for a test drive and investigate third-party measurements of important metrics, like fuel consumption and emissions. In the same way, when implementing Wi-Fi in your organization, you should perform independent tests of your equipment to prevent critical problems at the outset and understand how far your equipment will go in terms of load and capacity.

Learn more about how to test mobile apps and devices in different network conditions with ixia technology – By requesting a live demo

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES