The Verification Experts

Air Expert Series

Why Your Hotspot Matters

By Eve Danel and Josh Sullivan, Product Marketing Manager

May 2019

Table of Contents

1. Cutting the Cord

It's hard to imagine a world today without mobile devices where communication, business, news and personal lives are all connected. As people connect to the Internet, gone are the days of wired technology. Most devices that we use don't even have an Ethernet LAN port anymore and the only way we communicate, work, or stream video and audio in our local networks is through WiFi.

WiFi-enabled devices connect to the Internet via a WLAN network and a wireless Access Point (AP), or hotspot. Americans today have an average of nine WiFi-enabled devices in their homes. With the implementation of Internet of Things and smart homes, the number of WiFi connected devices could skyrocket to fifty on average.

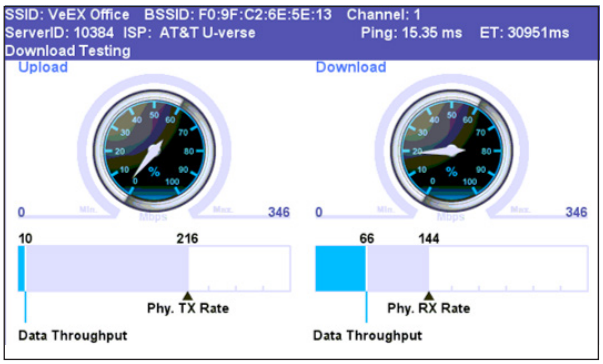
WiFi is the access technology of choice used not only in homes but in businesses and public spaces worldwide. It cannot be treated as a 'convenience' anymore, but as a Service, with all of the customer expectations that it entails. Yet very often this piece is overlooked during the installation process, leading to costly service calls and troubleshooting.

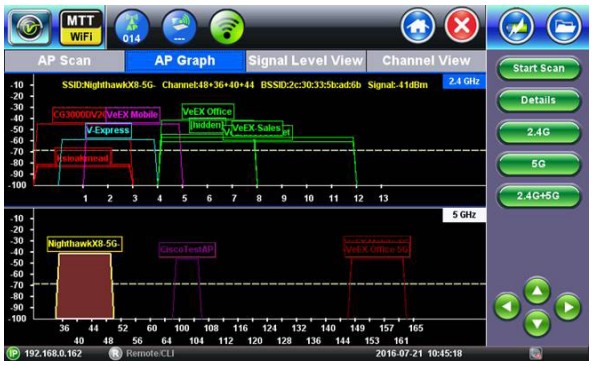
2. Not as Easy as It looks

It is true that WiFi is a very resilient technology that will connect in even the most adverse environments. But many wrongly assume that WiFi is a simple plug and play technology. Simply having a connection does not mean that it will perform optimally or reliably, and satisfy customer expectations. For this reason, a complete home installation plan should proactively survey the environment to ensure Quality of Experience (QoE) for the user. It should include audits for WiFi coverage, interference, performance and security.

3. Signal Coverage

The basis of a home installation plan is to survey signal coverage, in order to discover dead zones. When the WiFi signal's Radio Frequency waves travel through the air between the AP and the client, they will encounter many physical obstacles including walls, dressers and mirrors. These obstacles will degrade the signal's strength and make it harder for the receiver to decode. The amount of degradation depends on the obstacle's nature. For example, a concrete wall attenuates signals more than a drywall. This is one of the reasons why a signal's quality can drastically change from room to room and the QoE of two customers standing in the same room can differ significantly. In most cases there will be no control over the environment, but by surveying the signal levels throughout the home, coverage can easily be predicted. In areas of low coverage, you can adjust the AP location or add a wireless repeater (where an existing signal from the router is rebroadcasted to create a second network) ultimately improving signal range, coverage, and customer experience overall.

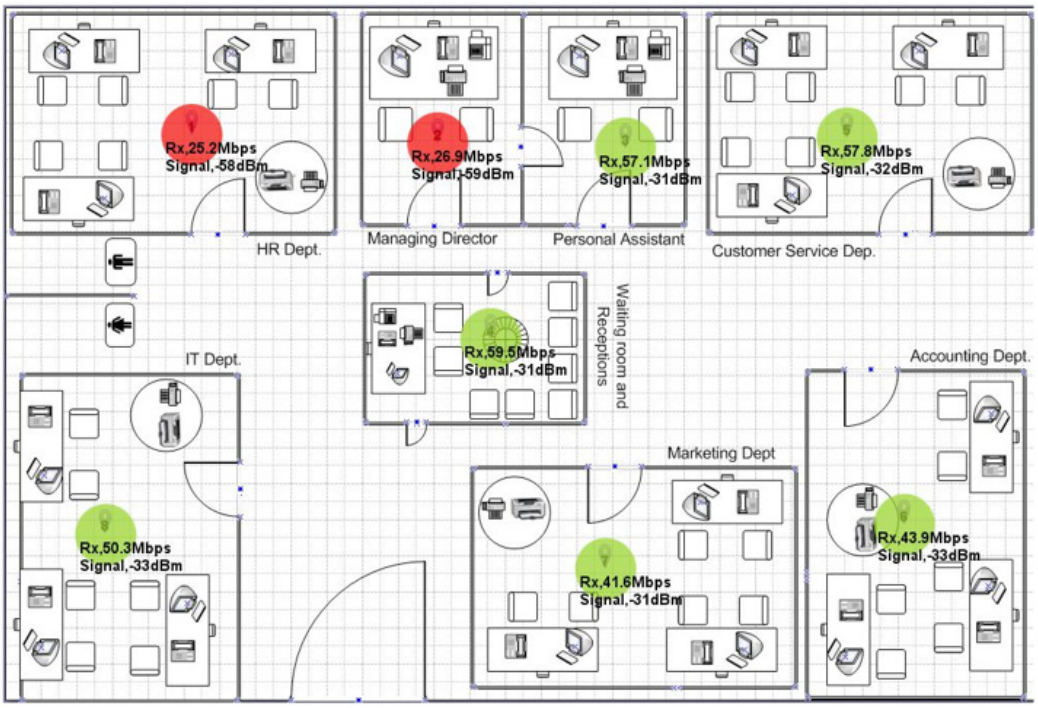


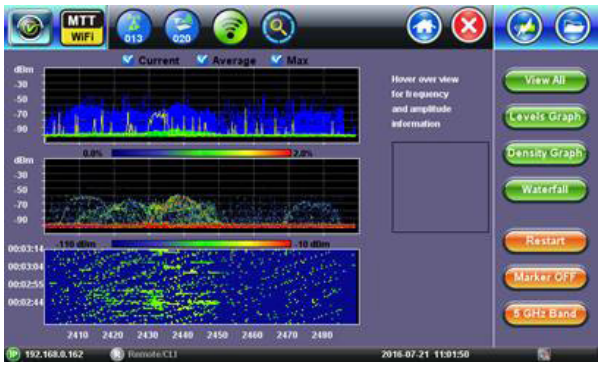


4. Interference from Neighbors and Other Devices

Neighbors often argue about overgrown trees or fence issues, but few would suspect that their neighbor's APs could be the cause of their poor WiFi performance. Most home users never change the settings on their routers, with most routers defaulting to the same WiFi channel. A neighbor's AP located on the same or an adjacent WiFi channel can crowd the default channel and reduce the available bandwidth. The WiFi RF channel is a shared medium, with each device only transmitting data when there is no other device transmitting, effectively dividing the available bandwidth between the number of devices attempting to transmit simultaneously. This sharing mechanism applies to devices connected to your own AP and to all devices connected to your neighbor's AP, which results in reduced speeds and higher latency for both you and your neighbor.

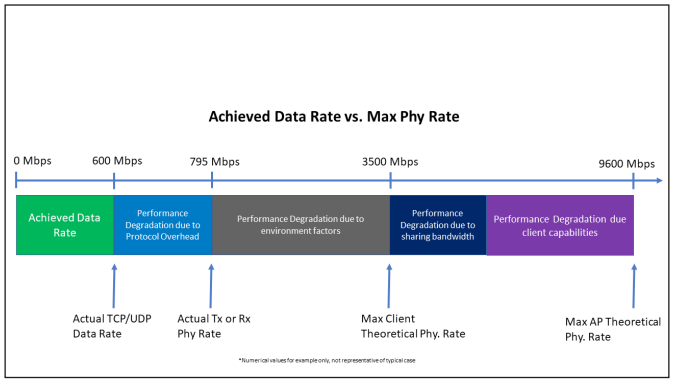
To make matters worse, other non-WiFi equipment like a microwave oven or a baby monitor could completely overpower the AP's signal and make it unintelligible to the receiver. With the rise of smart devices in the home, there has been an increasing need for identification and elimination of WiFi interferers. Unfortunately for WiFi users, the Federal Communications Commission (FCC) designates the 2.4 GHz and 5 GHz frequency spectrum for completely unlicensed use. Unlike AM or FM radio RF bands, where each transmitter is assigned a dedicated frequency, WiFi's frequency bands are available for anyone to use. The 2.4 GHz frequency band is one of the most heavily used and crowded bands available. It is used by many common devices including microwaves, cordless phones, Bluetooth® devices, wireless audio, security cameras, ZigBee devices and more. Interference by these competing devices degrade WiFi performance intermittently not necessarily continuously. This can cause frustration with the customer when the technician cannot duplicate the degraded WiFi performance. Surveying the home's WiFi environment is an important step for a successful home installation, firstly by discovering the neighboring APs channel allocation, signal strength and utilization, since this can guide optimal AP channel selection. It is also essential to monitor the full RF Spectrum in order to identify sources of non-WiFi interference that could have a destructive effect on the signal.





5. Performance

AP vendors advertise incredible data rates, but in practice those rates can only be achieved in specific testing situations. The further from the AP and the more obstacles in the way, the lower the speed at which the client device and AP will communicate. In addition, greater interference from WiFi or non-WiFi sources will cause more errors, resulting in more retransmissions. Protection mechanisms are built in the WiFi standards, to revert to the lowest speed when weak signal or errors are detected. The reality is that even with the latest WiFi 6 equipment capable of 9.6 Gbps, the client might end up connecting at a fraction of that speed. Beyond basic connectivity testing, the customer's QoE can only be evaluated by real data traffic transmission between the customer's AP and client device and educating the customer about true WiFi performance and shortcomings.



6. Security

Since WiFi data travels over the air, anyone in the vicinity, with simply a computer and the right sniffer software program, can capture and decode data or connect to your home network. WiFi security needs to be taken seriously and protection from intrusion and eavesdropping should be implemented. The home installation process should include verification of authentication and encryption and advanced troubleshooting capabilities, including detection and tracking of rogue APs and clients.

7. WiFi Air Expert Module

VeEX's WiFi Air Expert Module is the most complete and compact tool for WiFi networks discovery, survey, optimization, performance testing and troubleshooting. With an intuitive guided interface and ease-of-use, the WiFi Air Expert Module is the perfect test tool to ensure successful home WiFi installations.

- Supports detection and connection to 802.11a/b/g/n/ac devices
- Discovers the network and lists APs, Clients and Channels in table and graphical format
- AP detailed capabilities discovery including SSID, BSSID, channels, security, supported data rates, signal and noise levels, co-channel and adjacent APs and associated clients
- Site Survey functionality to create a physical representation of coverage and speed
- Speedtest® by Ookla® for quick QoE testing
- RFC 6349 test to verify TCP and UDP throughput performance through a WiFi AP or Router
- Locate rogue APs and clients with directional antenna
- Detect non-WiFi interference sources with built-in Spectrum Analyzer function and signature detection

Notes

About VeEX®

Located in the heart of Silicon Valley, VeEX develops next-generation test and monitoring solutions for telecommunication networks and services. Founded in April 2006 by test and measurement industry veterans, VeEX products blend advanced technology and vast technical expertise with the discerning measurement needs of customers.

VeEX products diligently address all stages of network deployment, maintenance, and field service turn-up and integrate service verification features across DSL, fiber optics, CATV/DOCSIS, mobile backhaul and fronthaul (CPRI/OBSAI), next-generation transport network, fiber channel, carrier and metro Ethernet technologies, WLAN, and synchronization. VeEX's multinational structure consists of several specialized business units operating in different parts of the world. VeEX has shipped more than 100,000 units since volume production began.

The VeEX team brings simplicity to tomorrow's networks.

The Verification Experts