GCN
Government Computer News
The online authority for government IT professionals

GCN LAB REVIEW Jul 29, 2011

Wireless access-point tracker cures headaches for network admins

By Greg Crowe

With more users needing to log in to networks with mobile devices, an administrator invariably needs to respond by making more wireless access points (APs) available. Unfortunately, that opens a can of worms — from user support to security problems. Keeping track of it all can be a real headache.

Well, here is your aspirin. The AirCheck Wi-Fi Tester from Fluke Networks is a handheld device that will tell you exactly what is out there from a wireless standpoint and give you the information you need to make sound decisions about your wireless implementation.

When we turned the AirCheck on, it immediately went through a scan of all the wireless channels in the 2.4 GHz and 5 GHz bands, and it displayed the total number of APs that it found. We found this to be nice information to have, but we were pleased to note that we could press on before the initial scan was completed if we so needed.

AirCheck Wi-Fi Tester

Pros: Small and light; can detect even the weakest signals.
Cons: Interface takes a little figuring out.
Performance: A
Ease of Use: B+
Features: B+
Value: A-
MSRP: $1,995.00
GSA Price: $1,844.00

The controls consist primarily of four directional keys that surround a Select button for navigating through menus and lists and two function keys that will do whatever the bottom of the 3-inch LCD screen says they will do at the time. These are more than adequate most of the time, but they could be a bit of a pain on the rare occasion in which you need to type something out.

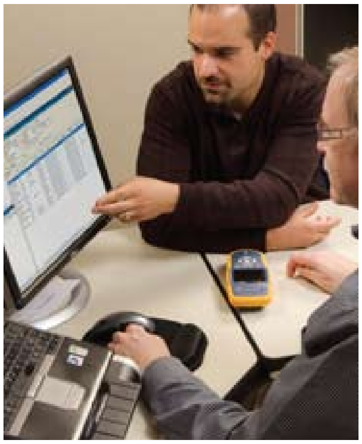
With a couple of button pushes, we were able to bring up a list of all the wireless networks that the AirCheck could detect, sorted by the Service-Set Identifier (SSID) of each network. For each network, it showed us signal strength; whether it was using security; the number of APs it contained; whether the network supports a, b, g or n clients; and any notes that had been made by this AirCheck device in the past.

Selecting one of the listed networks produced a list of the APs in that network. Selecting one of these individual nodes displayed more detailed information about that AP, such as the specific type of security used. Listing all of the APs from the home screen and selecting one of them also brought us to this detail screen. At this point, the function keys showed two actions: connect and locate. To connect to an AP with security, the log-in information had to be loaded through a profile, which we'll get into later.

When we activated the locate function, the AirCheck started beeping, and the screen showed a line graph indicating the latency of the signal to and from the AP. As we got closer to the device, the latency decreased and the beeps increased in frequency. This a vital tool for physically locating APs because they are not always put in memorable places. It can also help track down unauthorized APs that might reside in your building. And the beeping game was sort of fun, a bit of a digital treasure hunt, but that's beside the point.
The channel display shows all the legal channels on both the 2.4 GHz and 5 GHz bands, (11 and 24, respectively) and even shows activity on the three 2.4 GHz and four 5 GHz illegal channels. This screen told us which channels had the most 802.11 and non-802.11 traffic and how many APs were using each one.

Spotting APs

We were not surprised to find that the APs used by various organizations in our building and nearby buildings were primarily stacked up in the three factory-default channels (1, 6 and 11). We had wisely set the AP that we were primarily using for our testing to a nonstandard channel (4), but even there, we could see it was being shared with one other AP. Closer inspection of that AP through the AirCheck told us that it must be in the next building, as its latency would indicate. From this, we decided that the chance for interference between the two devices was in acceptable limits, and we kept our AP on its channel.



The AirCheck comes with AirCheck Manager software. We installed it on a Windows-based computer and connected the AirCheck through a USB 2.0 cable. The Manager program showed that the AirCheck was connected almost immediately. The Manager has two main functions. One is to create security profiles to upload to the AirCheck so that it can properly connect with secured APs. We just entered the SSID, authentication type, encryption and password/shared key. Once we saved it, we transferred it to the AirCheck. Once the Aircheck was disconnected, we then loaded the profile, and we were able to connect to our secure AP. The fact that you can only modify and create security profiles through the Manager software may seem like an inconvenience, but it is set up that way to make the AirCheck as secure as possible. This keeps your very powerful tool from becoming a security risk should it fall into the wrong hands.

The other purpose of the Manager is to generate reports from saved sessions of the AirCheck device. We saved a session into a file by clicking on the Save button and then the appropriate function button. Once the file was saved, we connected the AirCheck back up to the computer, and Manager created a report from it. This report had a detailed listing of all discovered networks and APs, a channel summary and usage graph, as well as any activity (such as network connections) that the AirCheck had been up to. This report is very detailed and well organized, and could easily fit into a list of periodic wireless network assessment tasks given how easy it was to generate.

Fluke Networks has set the retail price of the AirCheck Wi-Fi Tester at $1,995. We found this to be a bit more expensive than we would have liked, but it isn't outside the ballpark. Given how useful this device could be to a busy network administrator, it might be well worth the investment.

GSA Price: $1,844.00

Call for quote 1-888-665-2765