

Troubleshooting Common Wi-Fi Problems

Tom Resman - NetScout

It just has to work!

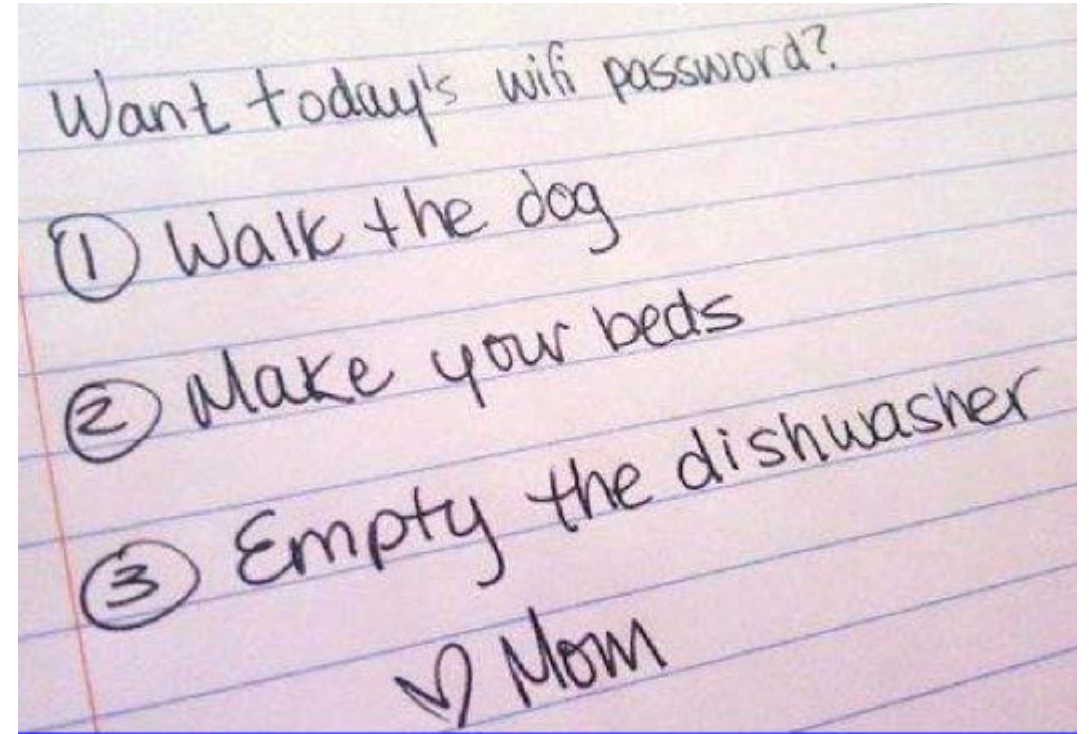


IT Professional Wi-Fi Trek 2016



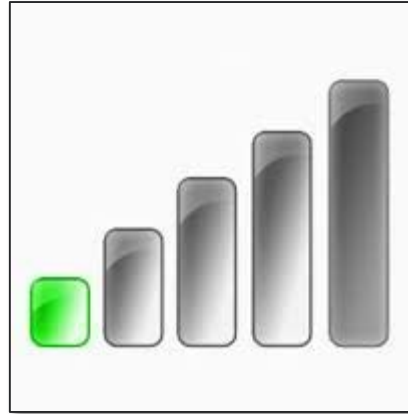
What Wi-Fi Complaints Do You Typically Get?

- The Wi-Fi is too slow
- I keep getting disconnected
- I can't roam
- I can't connect to the wireless network



What are the Causes Behind These Complaints?

- Mis-configuration
 - Access Points
 - Clients
- Coverage
- Capacity
- Co-Channel Interference
 - Your networks
 - Neighbor networks
 - Rogues
- Non Wi-Fi Interference
 - Persistent sources
 - Transient sources
- Security breaches and attacks



Finding Root Cause is Complex

- Complaints

Slow

Can't Connect

Get Disconnected

Can't Roam

- Causes

- Excessive Retries on channel
- Client connected at slow rate
- AP cell too big
- AP cell too small
- AP misconfigured
- Too many APs on channel
- Too many users on channel
- Interferers are present
- Too many SSIDs broadcasting
- Neighbor AP on same channel
- Too many users on same AP
- User's client misconfigured
- Legacy 802.11b clients present
- No secondary AP coverage



Finding Root Cause is Complex

- Complaints

Slow

Can't Connect

Get Disconnected

Can't Roam

- Causes

- Excessive Retries on channel
- Client connected at slow rate
- AP cell too big
- AP cell too small
- AP mis-configured
- Too many APs on channel
- Too many users on channel
- Interferers are present
- Too many SSIDs broadcasting
- Neighbor AP on same channel
- Too many users on same AP
- User's client misconfigured
- Legacy 802.11b clients present
- No secondary AP coverage

- Channel traffic congestion
- Channel device congestion
- Poor SNR



Finding Root Cause is Complex

- Complaints

Slow

Can't Connect

Get Disconnected

Can't Roam

- Causes

- Excessive Retries on channel
- Client connected at slow rate
- AP cell too big
- AP cell too small
- AP misconfigured
- Too many APs on channel
- Too many users on channel
- Interferers are present
- Too many SSIDs broadcasting
- Neighbor AP on same channel
- Too many users on same AP
- User's client misconfigured
- Legacy 802.11b clients present
- No secondary AP coverage

- Channel traffic congestion
- Channel device congestion
- Poor SNR
- Client mis-configured
- AP mis-configured
- ...



Key points

- Wi-Fi is location-dependent. Need portable tools to troubleshoot.
- Wi-Fi uses a time-shared medium... the channel.
- Signal Strength is important, but Signal/Noise Ratio is more-so.
- Critical KPIs include channel airtime utilization, SNR, retry rates.
- Client visibility is priceless.
- Every wireless network uses a wired network. Check for services.
- The right tools for the job makes all the difference.



- **So let's look at each complaint and how it can be addressed...**



“The Wi-Fi is too slow”



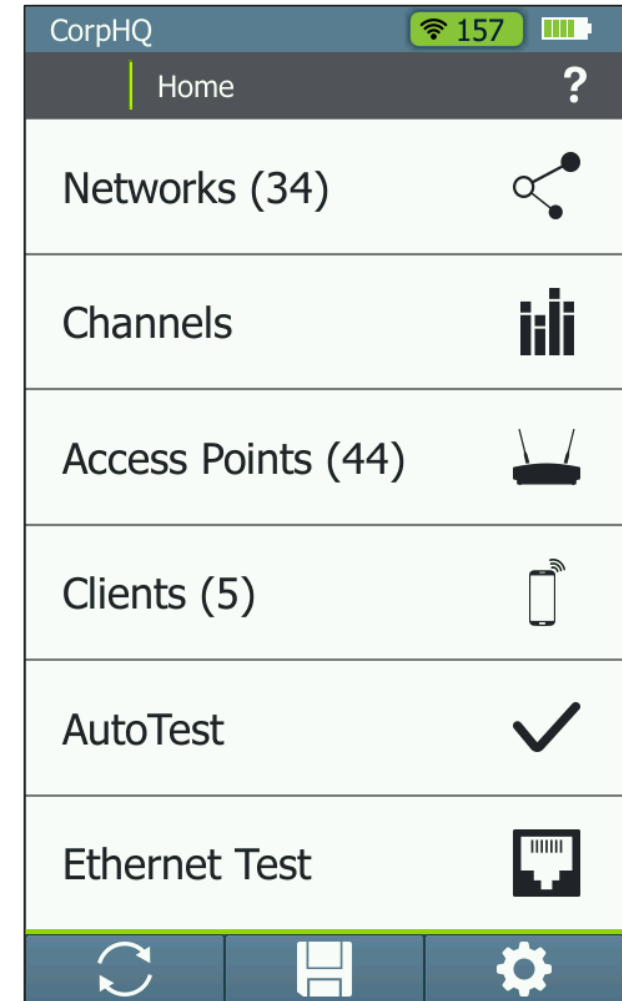
What To Check For

- How many APs on the channel?
- Airtime utilization of the channel for Wi-Fi devices
 - Are there legacy clients present?
- Airtime utilization of the channel for non Wi-Fi devices
 - Are there any non Wi-Fi interferers on that channel?
- What AP is the customer connected to, and what rates are supported?



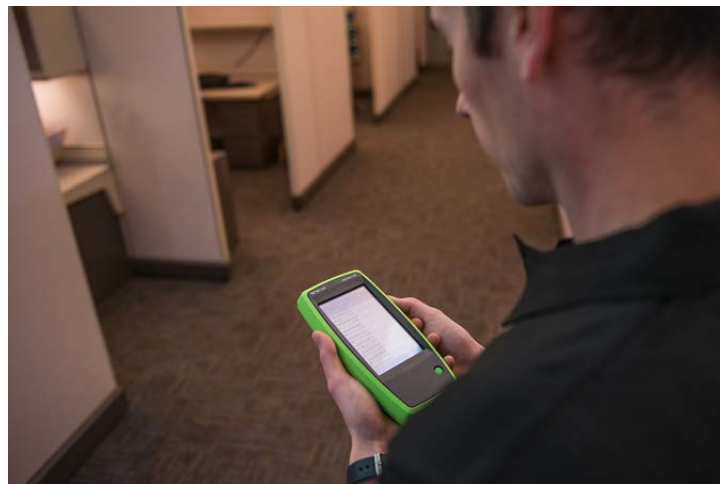
What Dave the IT Tech Did (v1)

- Grabbed his AirCheck Wi-Fi Tester and went to the location of the user.



What Dave the IT Tech Did

- Found the user's connection on his AirCheck Wi-Fi Tester, and identified its channel.

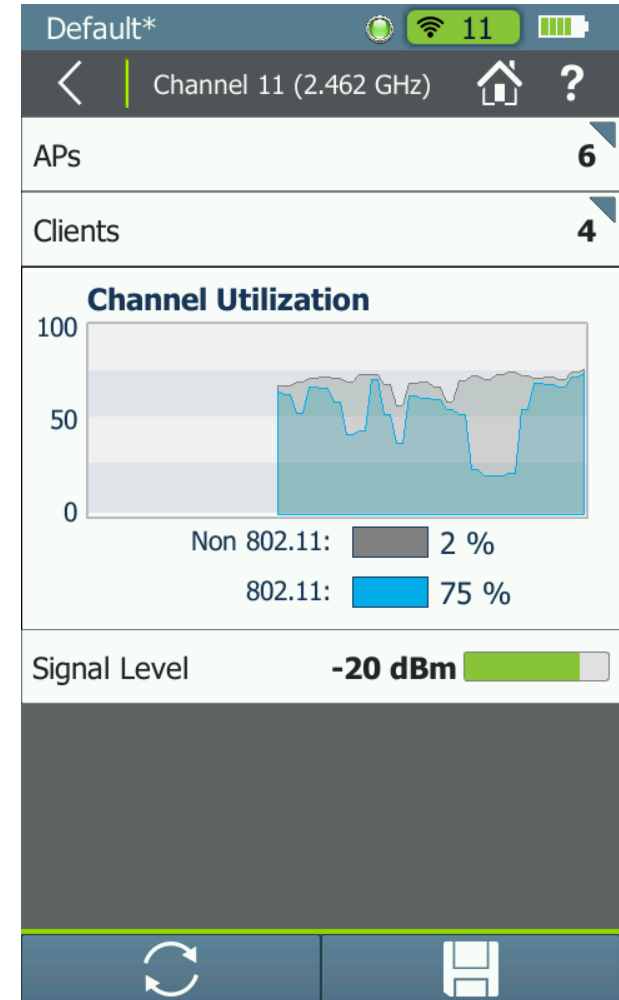


| Default* | |
|-----------------|-----------------|
| < | Apple:05:9f:d6 |
| Signal Strength | |
| Signal Level | -24 dBm |
| SSID | Flapjack-2 |
| AP Name | AsusTk:66:eb:08 |
| AP BSSID | AsusTk:66:eb:08 |
| Security | WPA2 |
| 802.11 Type | g |
| Band | 2.4 GHz |
| Channel | 11 |
| Last Seen | 0 seconds ago |
| Locate | |



What Dave the IT Tech Did

- Checked the channel and found too many APs on it.
- Corresponding 802.11 utilization was high.



What Dave the IT Tech Did

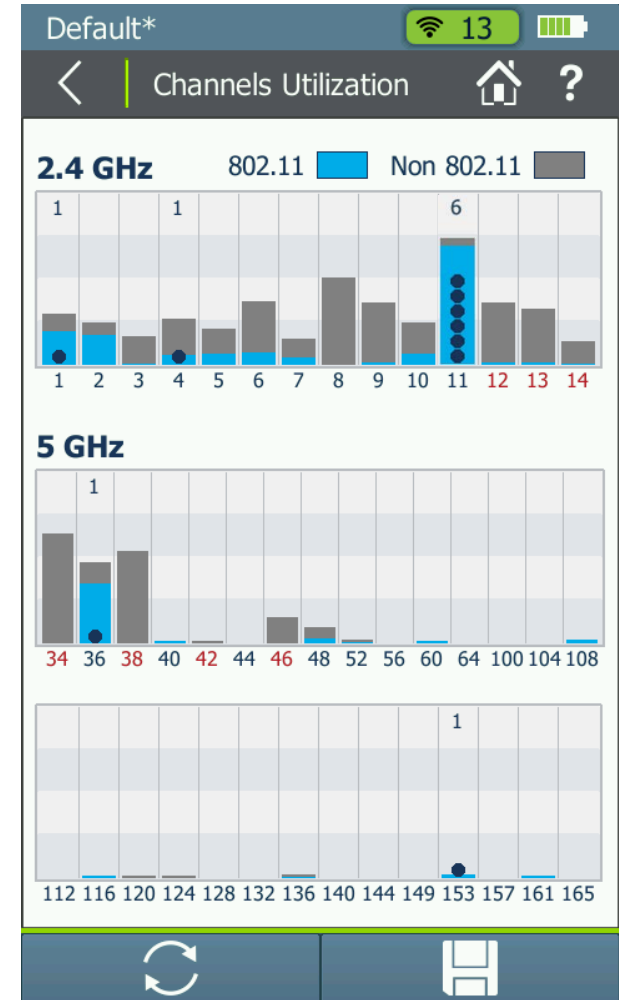
- Drilled to the APs on the channel and saw many neighbor network APs.

| AP Name | Signal Strength | SNR | Channel |
|-----------------|-----------------|-------|---------|
| AsusTk:66:eb:08 | -13 | 68 dB | 11 |
| Cisco1130-1Nort | -40 | 41 dB | 11 |
| Studio2020AP | -50 | 31 dB | 11 |
| Arris:53:b6:b7 | -62 | 19 dB | 11 |
| lap-cos-us-3 | -63 | 18 dB | 11 |
| lap-cos-us-9 | -70 | 11 dB | 11 |
| Cisco:84:aa:f0 | -74 | 7 dB | 11 |
| Cisco1130-2Sout | | | |



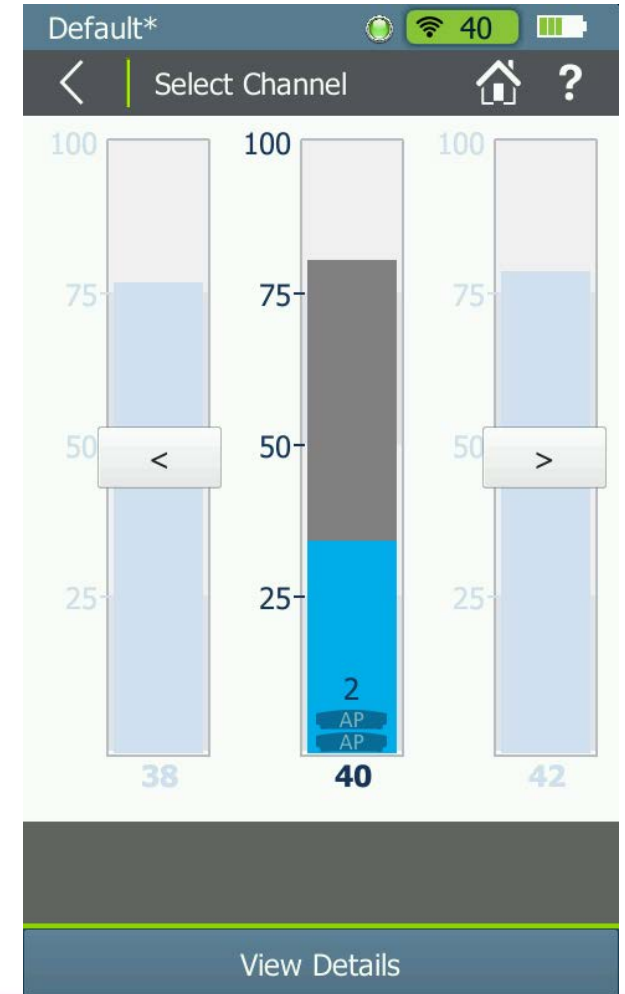
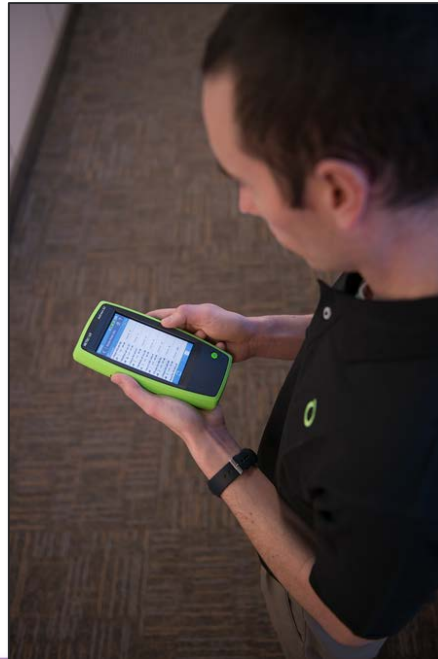
What Dave the IT Tech Did

- Viewed other channels and found one much less used.
- Moved the AP to that channel.



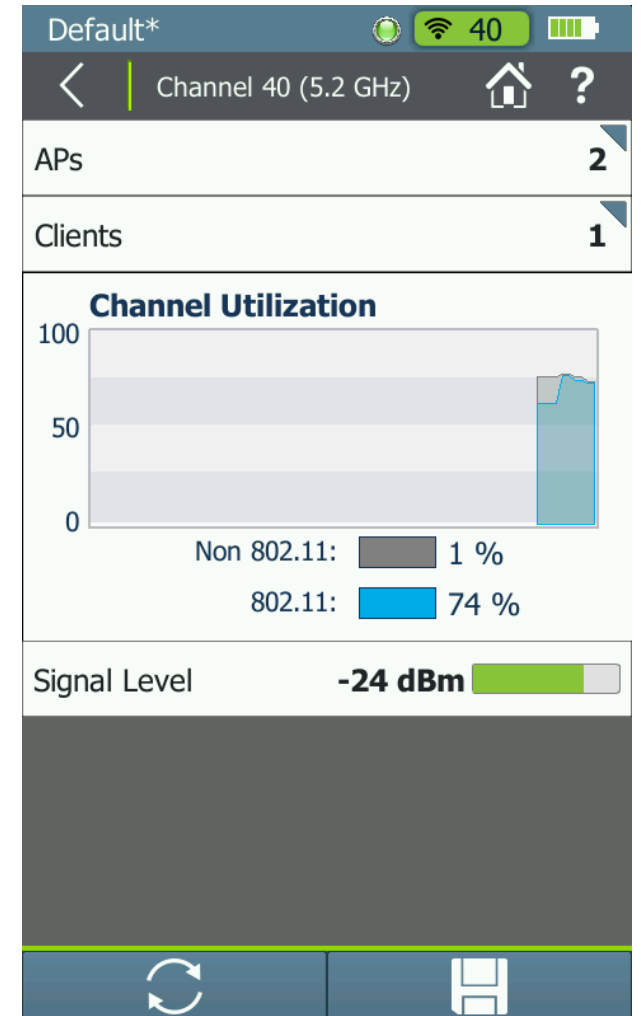
What Dave the IT Tech Did (v2)

- Checked the channel that the client was on.
- Found 2 APs on the channel; didn't seem too bad



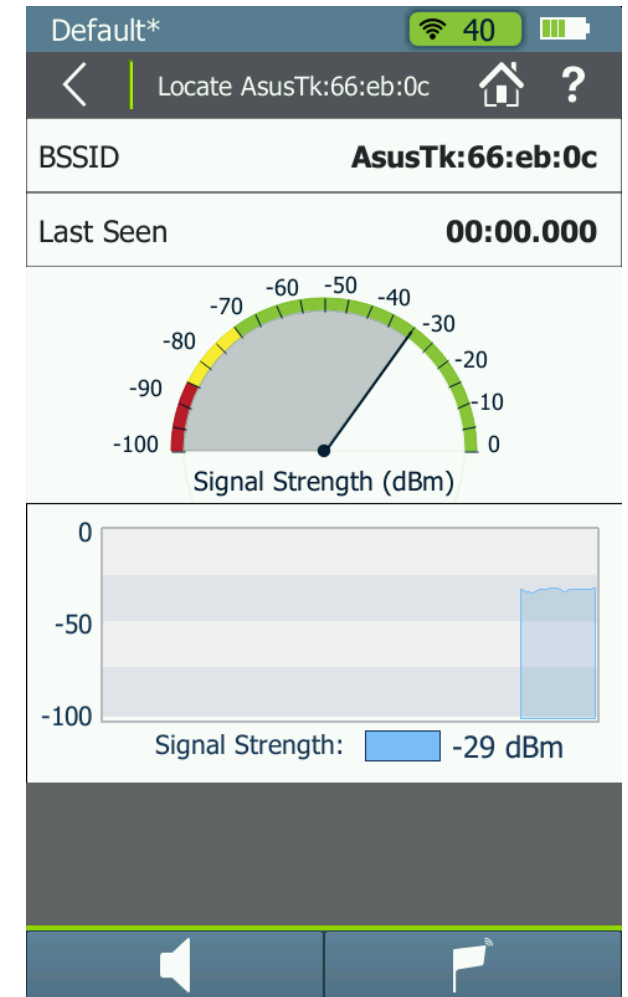
What Dave the IT Tech Did (v2)

- Checked channel utilization and saw it was very high



What Dave the IT Tech Did (v2)

- Checked the APs on the channel and found one was not familiar.
- He located it.



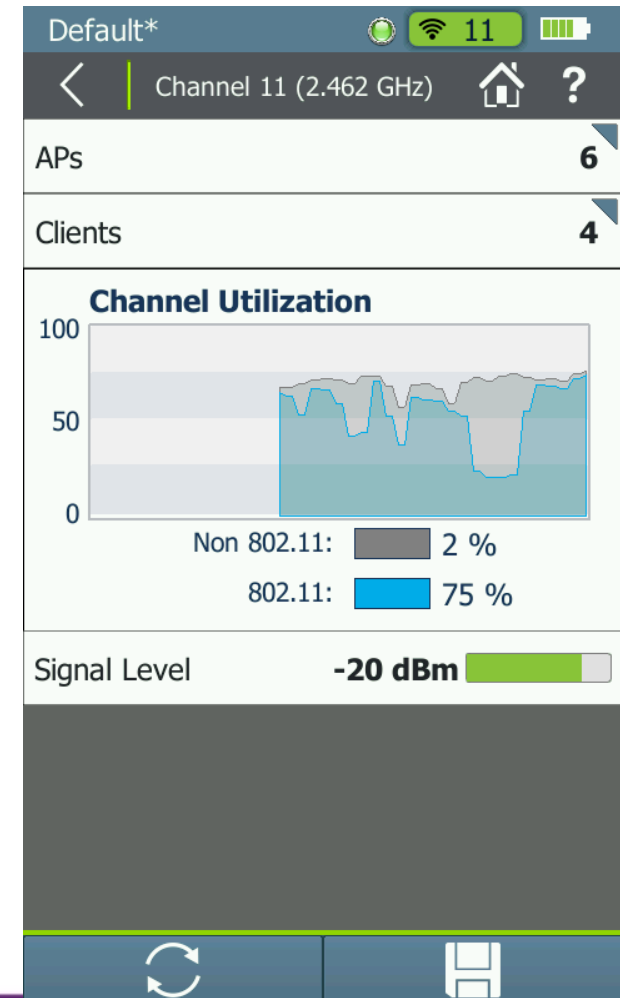
What Dave the IT Tech Did (v2)

- Found a rogue AP that was transmitting large files. One AP and client caused over-utilization of the channel.
- Removing the AP killed two problems with one swipe - Score!



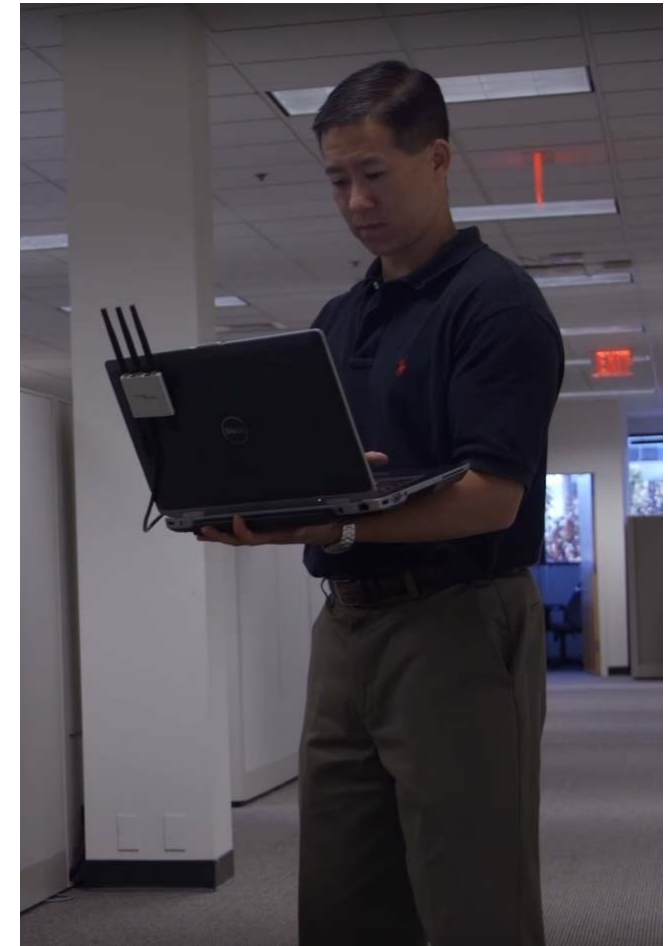
What Dave the IT Tech Did (v3)

- Checked the channel and found 802.11 utilization was high.
- Could not determine why
- Notified Tom the engineer



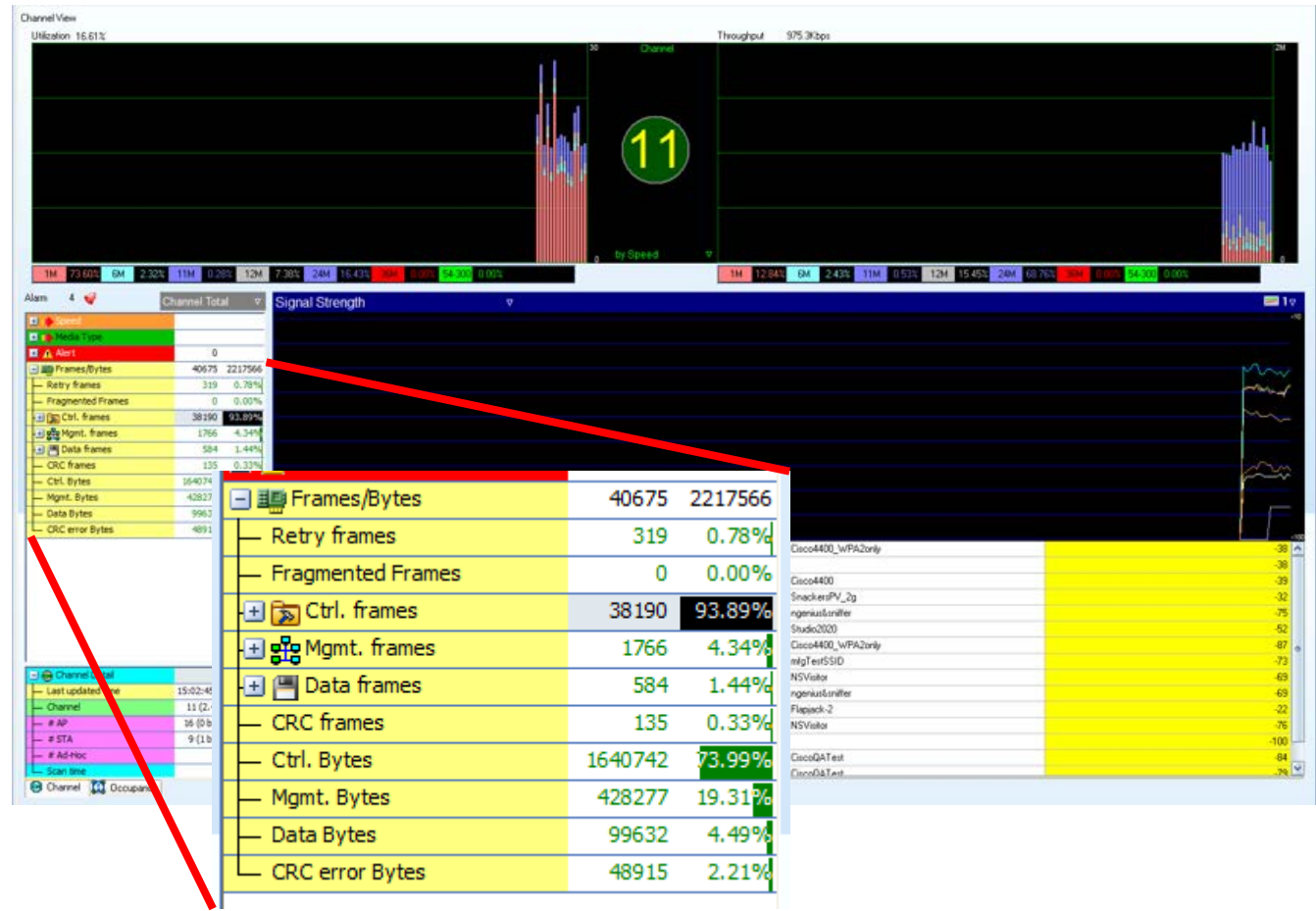
What Ed the engineer did

- Went to location of problem with the AirMagnet WiFi Analyzer PRO
- Scanned the channel



What Ed the engineer did

- Saw high channel utilization, and most of it was low speed transmissions
- Saw high utilization due to Control Frames, and within that, RTS and CTS frames



Diagnosis

- Excessive RTS/CTS frames often due to too many clients on a channel (not just an AP; it is the channel that is shared)
- Consider
 - Client load balancing
 - AP transmit power and cell size (clients connecting from too far away)
 - Another AP for capacity (if another channel is available)



“I keep getting disconnected”



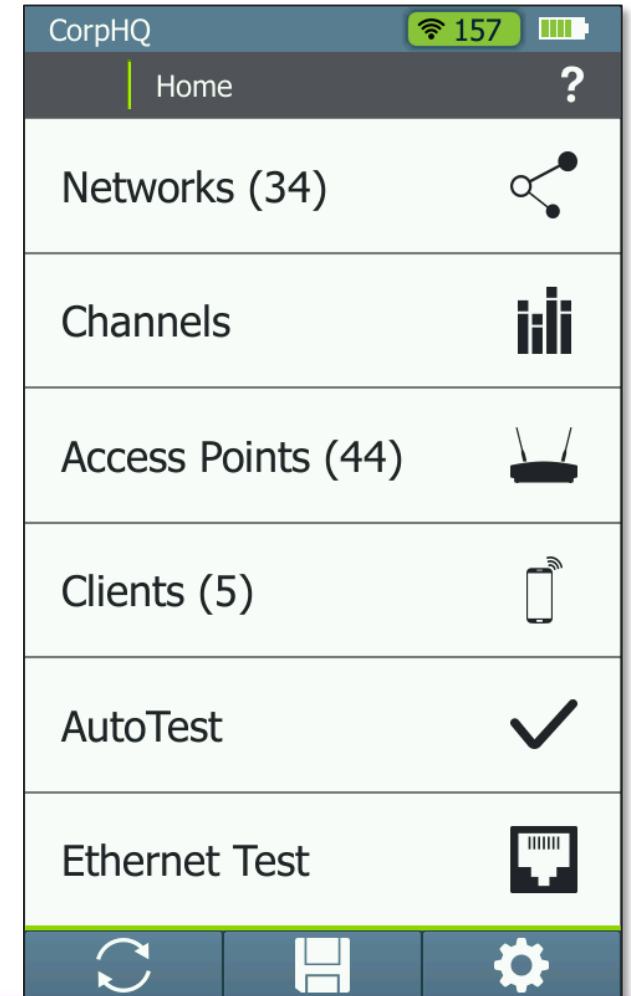
What To Check For

- Are there interference sources present?
 - Signal levels and duty cycles
- Weak SNR at client location
- Is the client device configured properly?



What Dave the IT Tech Did

- Grabbed his AirCheck Wi-Fi Tester and went to the location of the user



What Dave the IT Tech Did

- Found the AP that the user connects to, and identified its channel

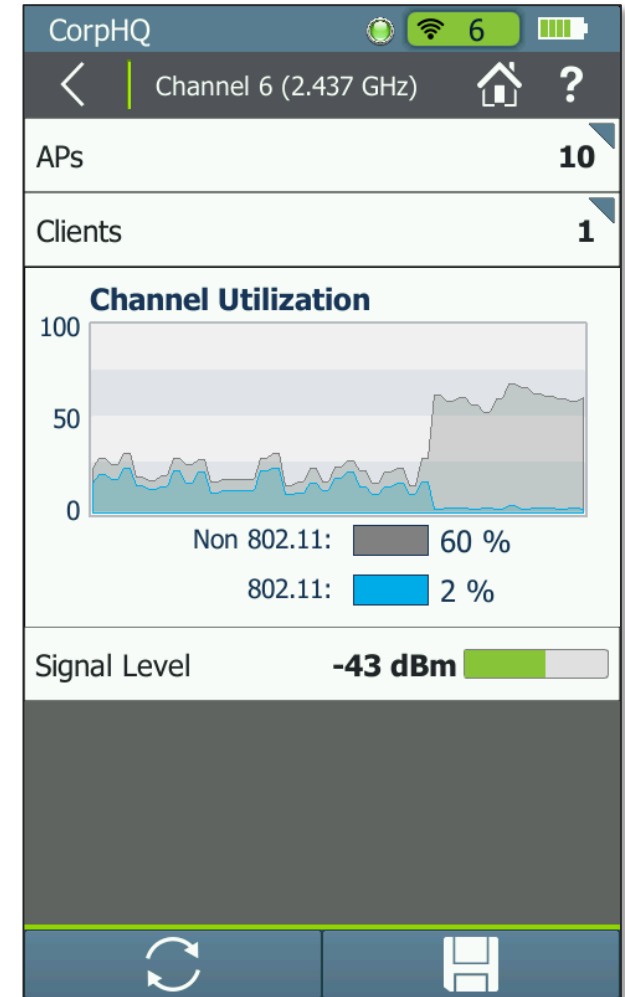
A screenshot of a mobile application interface showing Wi-Fi signal details. The interface is titled 'CorpHQ' and shows the following information:

| | |
|-----------------|----------------|
| Signal Strength | |
| Signal Level | -65 dBm |
| Noise Level | -82 dBm |
| SNR | 17 dB |
| SSID | NSVisitor |
| BSSID | Cisco:8e:cc:21 |
| Security | WPA2 |
| 802.11 Types | g n |
| Clients | 0 |
| Band | 2.4 GHz |
| Channels | 6 |

At the bottom, there are three buttons: 'Locate', 'Connect', and a save icon. A green arrow points from the 'Channels' row to the 'Locate' button.

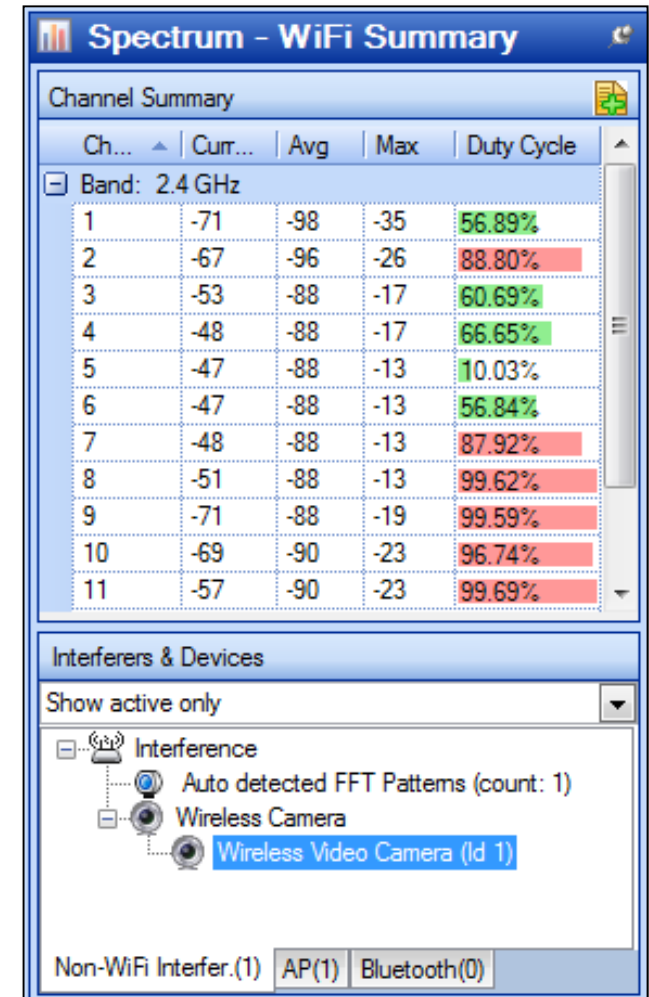
What Dave the IT Tech did

- Saw non-802.11 Wi-Fi channel utilization was high. Immediately knew there was a interferer issue and notified Tom the engineer



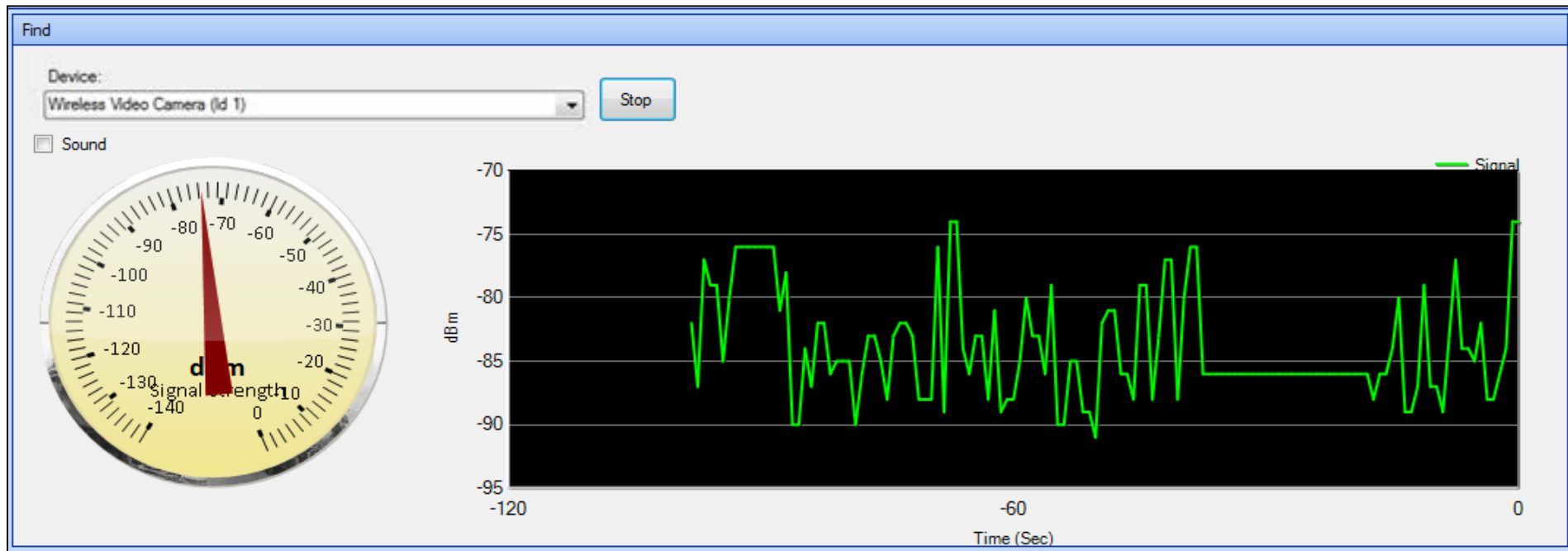
What Ed the engineer did

- Grabbed his AirMagnet[®] Spectrum XT[™] and identified the interference source
 - Only periodic transmissions
 - But duty cycle = 99% and across all 2.4GHz band



What Ed the engineer did

- Located the interference source



What Ed the engineer did

- Depending on the interference source:
 - Removed it
 - For unauthorized or unnecessary devices
 - Changed the Wi-Fi channels around it
 - For embedded devices like microwaves and security cameras
 - Move the AP or increase power to increase SNR
 - For low power devices like sensors



“I can’t roam”



What To Check For

- Secondary AP coverage
- AP cell sizes too big, Tx power too high
- Client overload on an AP
- AP misconfiguration



What Dave the IT Tech Did

- Grabbed his AirCheck Wi-Fi Tester and successfully connected to the network



Default 11* [Battery Icon]

< Connect to Cisco4400 [Home Icon] [Question Mark Icon]

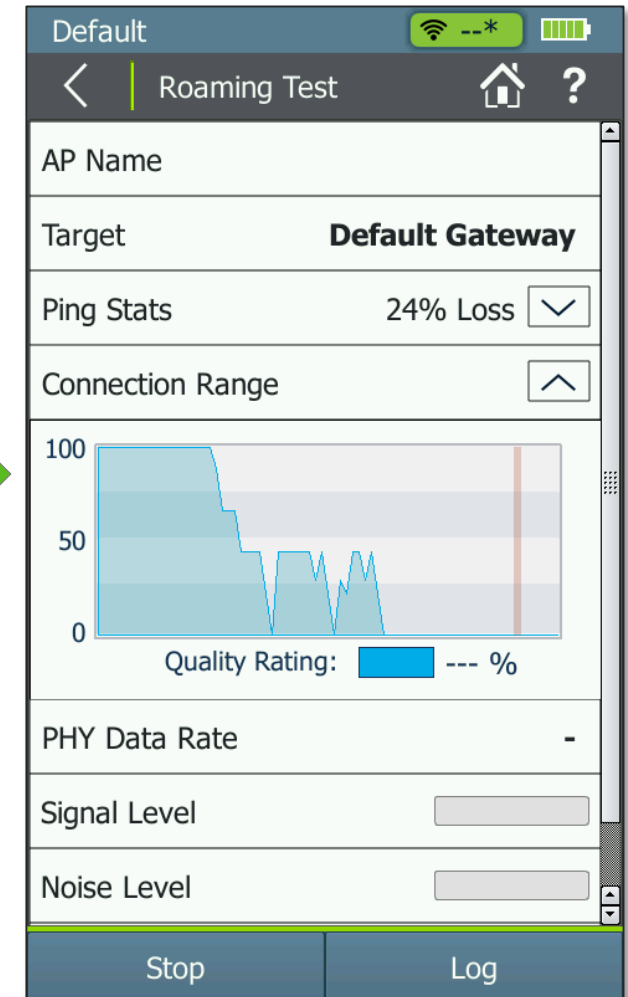
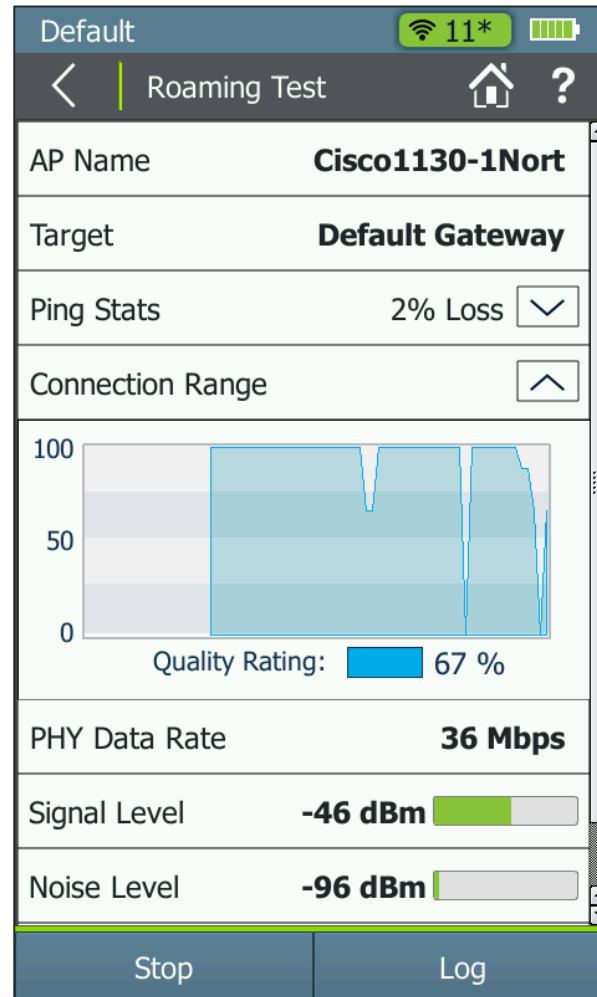
| | |
|-----------------------------|-------------------|
| SSID | Cisco4400 |
| BSSID | 00:17:0f:e7:9b:00 |
| Link Uptime | 0:00:30 |
| Connection Established | ▼ |
| IP Address | 10.250.9.247 ▼ |
| Gateway Found | 10.250.8.1 ▼ |
| DHCP Server Found | 10.250.8.2 ▼ |
| DNS 1 Found | 10.250.1.221 ▼ |
| DNS 2 Found | 129.196.196.25 ▼ |
| Target Found | www.google.com ▼ |
| Link-Live Upload Successful | ▼ |

Roaming Test Log [Save Icon]



What Dave the IT Tech Did

- Performed a roaming test. Roaming failed



What Dave the IT Tech Did

- AirCheck Wi-Fi Tester indicated the network had mixed security types. This is a misconfiguration of an access point

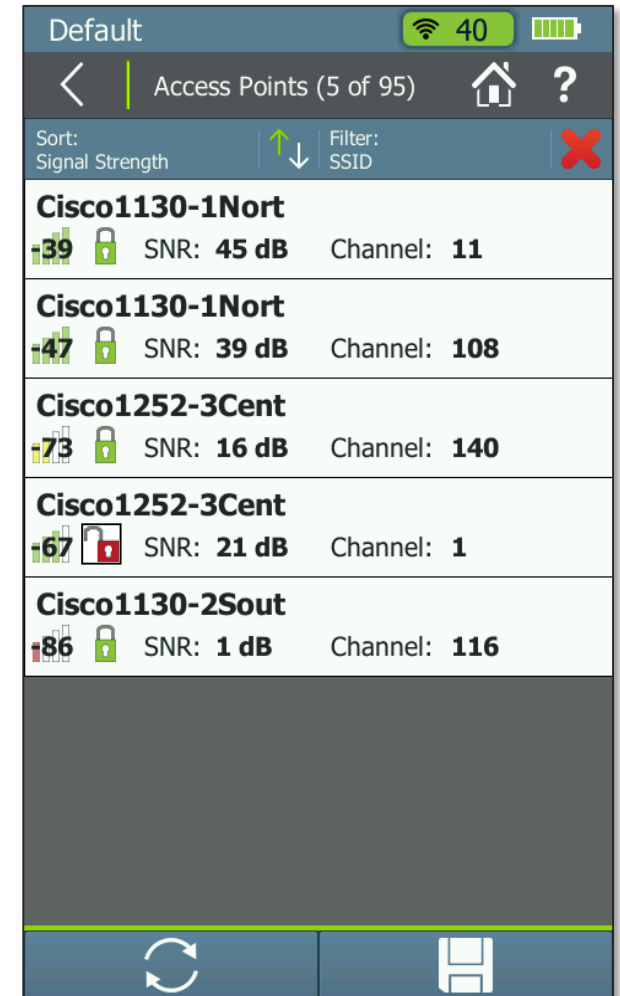


| Network Name | Signal Strength | Security | Devices | SNR |
|-------------------------------|-----------------|-------------------|---------|-------|
| Battle Mountain Crestron | -56 | WPA2 (Green Lock) | 1 | 32 dB |
| Chamber 5g | -64 | WPA (Red Lock) | 1 | 26 dB |
| Cisco4400 | -34 | WPA2 (Green Lock) | 5 | 50 dB |
| Cisco4400_WPA2only | -34 | WPA2 (Green Lock) | 5 | 50 dB |
| clh | -68 | WPA2 (Green Lock) | 1 | 18 dB |
| DIRECT-38-HP ENVY 7640 series | -47 | WPA2 (Green Lock) | 1 | 38 dB |
| DIRECT-PC-VIZIOTV | -79 | WPA2 (Green Lock) | 1 | 13 dB |
| EA6500 TAC 24G | | | | |



What Dave the IT Tech Did

- Immediately went to the list of APs on the network. Saw the AP he needed to roam to was set for the wrong security type



What Dave the IT Tech Did

- Fixed the AP security configuration issue, and roaming was restored

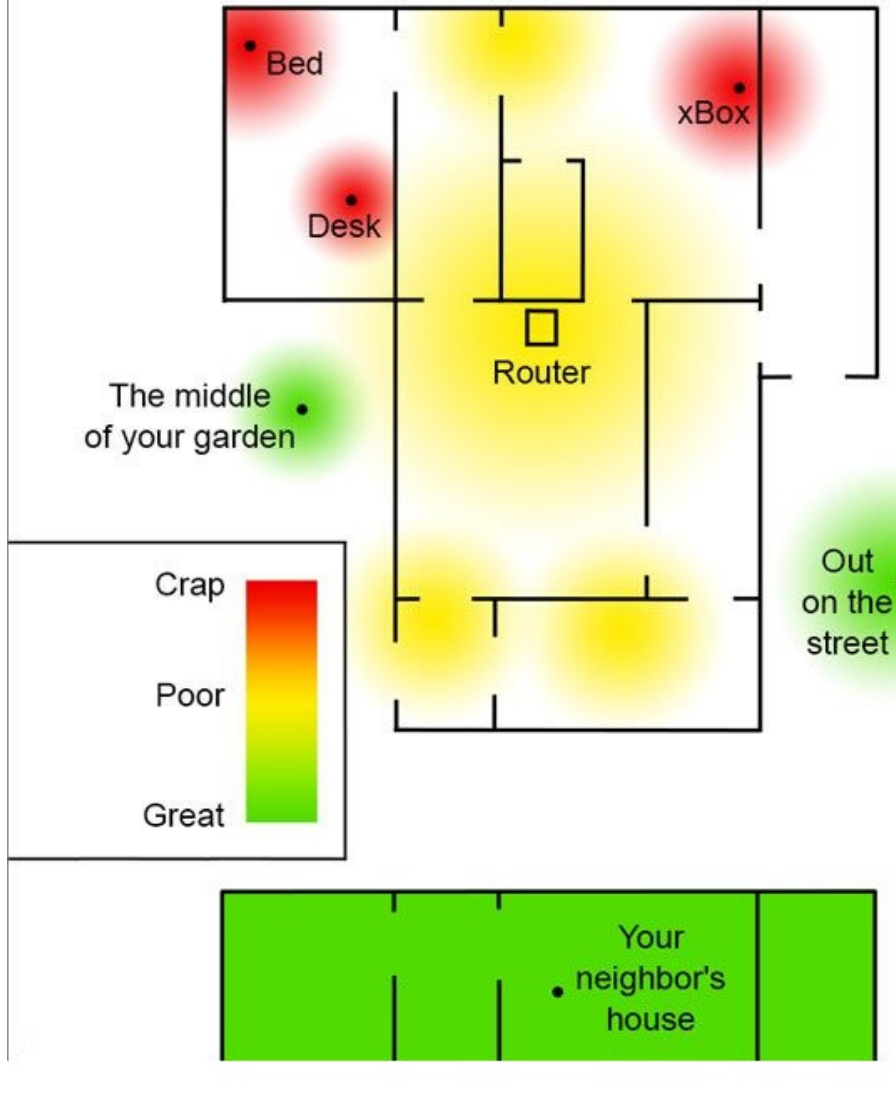


“I can't connect”

- “I can't connect”



Your wireless internet signal strength



What To Check For

- Network availability
- Proper signal coverage, and SNR
- Proper access point configuration
- Proper client configuration
- Channel utilization and interference
- Network services availability: DHCP, DNS, gateway route
- Security incidents



What Dave the IT Tech Did (v1)

- Grabbed his AirCheck Wi-Fi Tester and tried to connect to the network.



tom* 11* [Battery Icon]

< | Connect to Flapjack-2 [Home Icon] [Question Mark Icon]

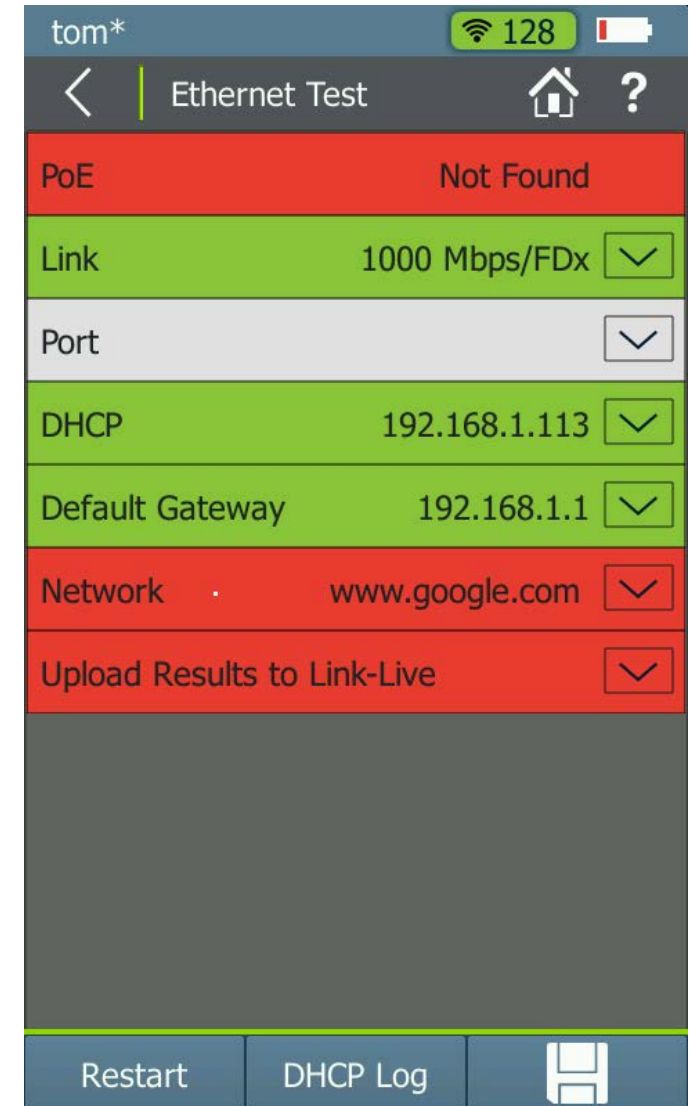
| | |
|-------------------------|-------------------|
| SSID | Flapjack-2 |
| BSSID | AsusTk:66:eb:08 |
| Link Uptime | 0:00:32 |
| Connection Established | ▼ |
| IP Address | 192.168.1.16 ▼ |
| DHCP Server Found | 192.168.1.1 ▼ |
| Gateway Found | 192.168.1.1 ▼ |
| DNS 1 Found | 192.168.1.1 ▼ |
| Find DNS 2 | ▼ |
| Target Not Found | www.google.c... ▼ |
| Link-Live Upload Failed | ▼ |

Roaming Test | Log | [Save Icon]



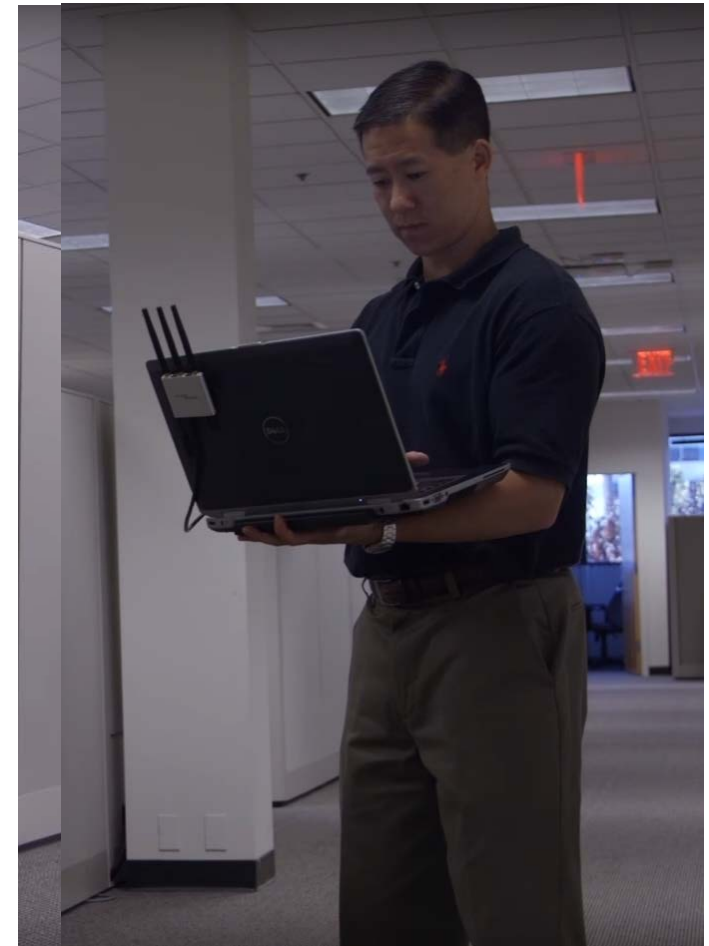
What Dave the IT Tech Did (v1)

- Checked the Ethernet connection at the AP and saw that he could not get out to the internet.
- Found that it was a misconfigured firewall.



What Ed the engineer did (v2)

- Grabbed AirMagnet WiFi Analyzer PRO and went to the location of the problem.



What Ed the Engineer Did

- Viewed AirWISE[®] alerts and immediately saw a DoS attack

The screenshot shows the AirMagnet WiFi Analyzer PRO interface. The main window displays an alert titled "DoS: De-Auth flood attack". The alert text reads: "There may have been a Denial-of-Service attack underway from the AP Cisco:43:11:55 (Name: QA-1200-7 ; SSID : QA-1200-7) . The system detected a number of out-of-order de-authentication frames sent from the AP's MAC address. This traffic pattern matches a form of Denial-of-Service attack that uses spoofed de-authentication frames to break the association between an AP and its client stations. You can use the Infrastructure screen to observe in real time the number of de-authentication frames sent by the AP Cisco:43:11:55 (Name: QA-1200-7 ; SSID : QA-1200-7) . Please note that these de-authentication frames may contain a spoofed source MAC address. In order to use the Find tool on the Mobile analyzers(AirMagnet WiFi Analyzer and Handheld)tool or the Triangulation feature on the Enterprise Console to locate the intruder, you may have to turn off the real AP Cisco:43:11:55 (Name: QA-1200-7 ; SSID : QA-1200-7) so that its signal strength is not mixed with the intruder's."

Below the alert text, there is a table with the following data:

| | Rx Total | Tx Total |
|------------|----------|----------|
| Speed | | |
| Media Type | | |
| Alert | 0 | 0 |
| Frames | 2955 | 5507 |
| 802.11d | | |
| 802.11h | | |
| AP Detail | | |

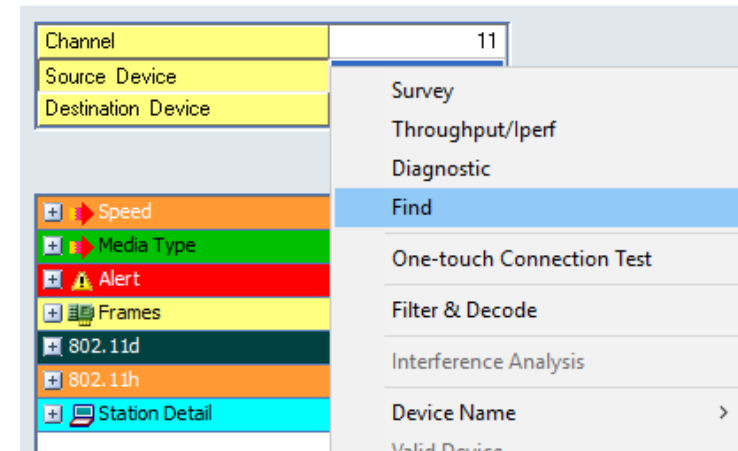
On the right side of the interface, there is a "Signal / Noise" section with a graph and a table:

| | Value |
|--------|-------|
| Signal | -45 |
| Noise | -100 |



What Ed the Engineer Did

- Selected the source and went to the Find screen.
- Located and disabled the device.
- Network connectivity was restored

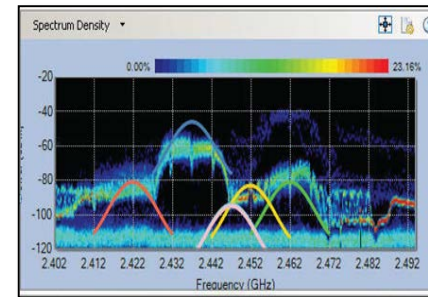


Wi-Fi Toolset for Troubleshooting

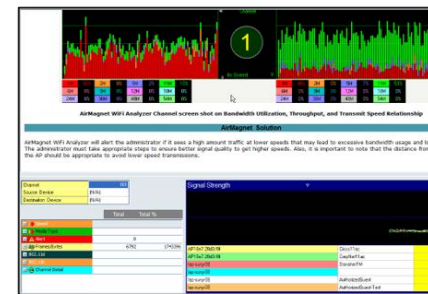
- FOR THE NETWORK ENGINEER

- FOR THE NETWORK TECHNICIAN

AirCheck Wi-Fi Tester G2



AirMagnet
Spectrum XT



AirMagnet Wi-Fi
Analyzer PRO



THANK YOU



IT Professional Wi-Fi Trek 2016

