# Eliminating Interference

*Troubleshooting the Invisible*

Rowell Dionicio

In a campus environment, users are given a considerable amount of freedom to pursue their research and to foster innovation. This sometimes comes with issues relating to Wi-Fi. I was brought in to identify why users were unable to be productive using Wi-Fi.

The first task in troubleshooting is to find out the extent of the issue. Are one or more users affected and how are they impacted? Was a single application being affected or was it many? And when did the issue start occurring?

End users who rely on Wi-Fi were describing many symptoms including low throughput, loss of connectivity or not able to connect. I determined the issue to be widespread and began looking into the infrastructure. The symptoms pointed towards a Layer 1 issue but following my troubleshooting methodology I needed to confirm the infrastructure was working as configured.

Taking on a troubleshooting methodology will help provide an organized framework to finding a resolution.

The infrastructure saw no loss of access points in the area. The building had 100% coverage. Users had described being able to connect to Wi-Fi; a sign that they were able to authenticate and associate to an access point.

In order for a client device to get connectivity, it must first probe passively or actively for an SSID. This is the beginning of the 802.11 State Machine. An access point responds to a probe request and the client device begins open system authentication. After the access point determines the client device meets the requirements of joining the basic service set (BSS) it then moves into association. The final step is a frame indicating a successful association. This process was confirmed based on the number of devices successfully connected to Wi-Fi from our Cisco wireless controller.

Most affected clients were on channel 11 of the 2.4 GHz spectrum. In 2.4 GHz spectrum there are three non-overlapping channels.

A post-deployment site survey showed there was no co-channel interference with the existing deployment. Co-channel interference causes overlapping access points to essentially share the same spectrum in which communication between access points and devices must compete for air time thus lowering capacity.

Additionally, there was no adjacent channel interference shown on the post-deployment site survey. Adjacent channel interference is caused by two access points servicing the same area but on channels adjacent to each other. The spectral mask of one channel can bleed into the adjacent channel causing interference and triggering clear channel assessment of the neighboring access point and nearby devices.

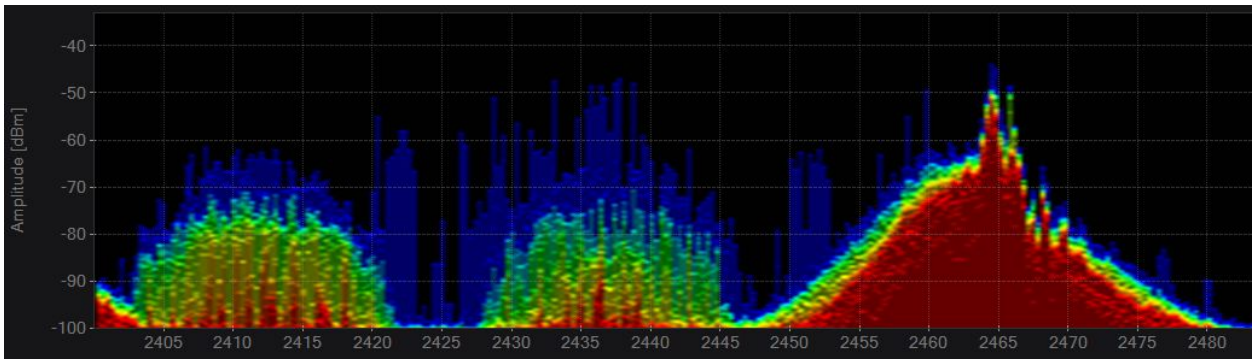
With protocol analysis, I was able to capture frames as they were transmitted through the air using a special USB adapter running in promiscuous mode. The adapter can capture frames up to 80 MHz channel widths.

Using my protocol analysis application, Metageek Eye P.A. and using a USB adapter capable of capturing wireless frames, I was able to visualize the types of frames transmitted in the air. The results showed excessive frame retransmissions.

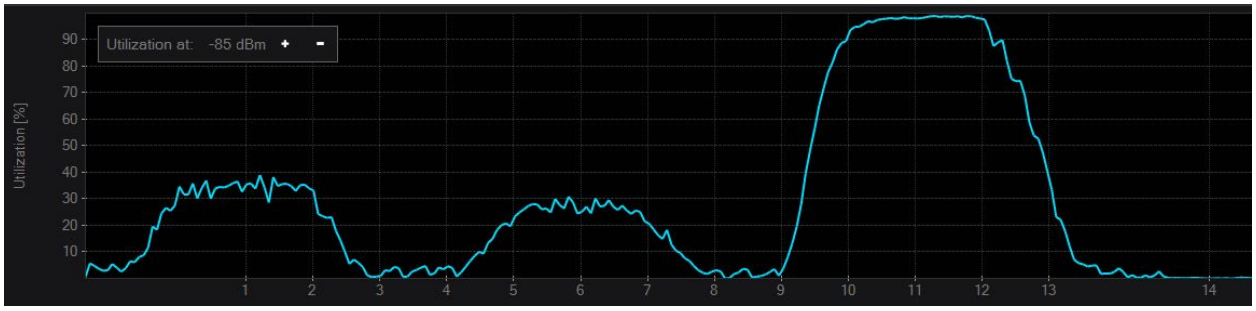
Frame retransmissions occur when a transmitting radio does not receive an acknowledgement from the destination radio. It is assumed that the frame was corrupted or not received.

My next step was to visualize the 2.4 GHz spectrum using Metageek's Chanalyzer with the Wi-Spy DBx USB adapter. The adapter gave the ability to view raw radio frequencies plotted on a graph with the respective amplitude and frequency of wireless signals.

An omni-directional antenna connected to the Wi-Spy DBx adapter showed a high powered device transmitting on channel 11, at 100% duty cycle. The RF pattern was not of an 802.11-compliant device. Chanalyzer's density graph displayed an amplitude (strength) signal peaking at -50 dBm, creating low SNR for client devices.




The source of interference had become a Layer 1 denial-of-service attack whether intentionally or unintentionally. Even though 802.11 devices used clear channel assessment (CCA) to detect energy, the interferer ignored 802.11 standards and continued to transmit regardless if a device was clear to send.




To narrow down the location of the interferer, I swapped out the omni-directional antenna with a directional antenna, which allowed me to see a better strength indicator of where the interference might be located. Splitting the building into four quad sections, I began narrowing the precise location of the interference. Metageek Chanalyzer showed the amplitude increasing as I approached a device sitting on a user's desk. To confirm my findings, I unplugged the device and began to see the signal decrease from my real-time graph.

The culprit was a consumer level device with Wi-Fi capabilities not operating properly or within 802.11 standards. After replacing the device there was no longer any interference and all complaints went away.

Troubleshooting this issue has shown how following the OSI model, and troubleshooting at Layer 1 first, would have shown the cause right away. The CWAP has provided me an incredible amount of knowledge in troubleshooting various Wi-Fi scenarios. In this case, protocol and spectrum analysis validated the issue was sourcing from an interfering device.