Remote Troubleshooting Client Connection Issues

CWNE TECHNICAL ESSAY

JAMES JACKSON

PROBLEM:

Retail customer reported issues with client connectivity at one branch on a newly upgraded WLAN infrastructure utilizing Cisco FlexConnect with local switching. Cisco wireless phones as well as an Android tablet used as a timeclock were the client devices reported as having issues accessing the network.

MY ROLE:

Consultant working for a regional VAR. I had performed the WLAN infrastructure upgrade approximately 4 weeks earlier.

ANALYSIS AND TROUBLESHOOTING:

This particular store location was approximately a 4-hour drive from my office, and I was unable to go onsite to investigate the problem. Having to remotely troubleshoot wireless client connectivity without the ability to use specialty wireless tools (such as wireless protocol scanners and spectrum analyzers) would prove challenging. As a result, I needed to break down the troubleshooting process into sections that I could troubleshoot on my own and those that would require a "remote-hands" on-site.

AP CONNECTIVITY TROUBLESHOOTING:

With remote access to the WLC and switches, AP connectivity to the WLC was able to be troubleshot with no remote hands. Upon logging into the controller, I first noticed that one of the three APs was no longer connected to the controller. I logged into the local switch and noticed that the switchport that AP was connected to showed a Down status but with inline POE functioning. A subsequent shut/no shut was unsuccessful in restoring connectivity. At this point I had a suspicion that we were dealing with a bad cable due to issues encountered during the AP hardware upgrades at this site a few weeks prior. During the AP replacements two of the three new APs had refused to come online using the existing cabling (verified open pairs with built in switch TDR) and had required the use of spare runs. The third AP worked fine on its original run and so was not switched to a spare. Now though, that AP's TDR test was showing open pairs as well. Based on the close location of the affected clients to this AP, my initial hypothesis was that they couldn't connect to this AP and were too far away to connect to a different AP.

CLIENT CONNECTIVITY TROUBLESHOOTING:

This stage would require that I work with (non-IT) on-site staff and limited analysis tools. First step was to physically move the clients closer to an AP showing connected on the WLC. We first tried the basic steps of rebooting the client devices reporting issues – customer reported no change. Per the site contact the tablet showed full signal bars but was reporting no connectivity. I had the customer verify that the tablet was connected to the right SSID (it was) and that it had an IP (it did not). The controller though did not show this client connected nor was I unable to see any debug logs related to the client mac address. At this same time the controller was showing one connected wireless phone as a client at the site. I had the customer

make a test call and they confirmed that it was functioning properly. Since I was unable to see any debugs for the tablet, I attempted to do the same with the functional wireless phone. In particular I wanted to capture any (re)authentication/(re)association attempts to try and narrow down the likely root cause. Upon reboot the phone no longer showed up as a wireless client and the customer reported it was now exhibiting the same behavior as the other clients. The controller only showed debug logs up to the point of disassociation with no further debugs seen. Next I had the customer connect their personal cellphone to the internal SSID as a greenfield device in the hopes that we would see it connect. Unfortunately, it too exhibited the same connection behavior as well as the same issue with no logs being generated.

CONTROLLER INITIATED PACKET CAPTURE:

In an in-person troubleshooting session, I would turn to a packet capture at this point to again attempt to gather (re)authentication/(re)association frames from the client and AP. Without those tools available I next attempted to use a feature that is often handy for remote troubleshooting – using an AP to capture. Cisco offers a couple of ways to do this: AP Sniffer mode (AP is non-client serving) and AP packet capture (AP still serves clients). Both of these have a limitation however of only being able to capture on one channel at time: severely limiting the scope of traffic I could capture. Another limitation I encountered was that my APs were not compatible with the AP packet capture mode – leaving the non-client serving Sniffer mode as my only option. I placed one of the two working APs into sniffer mode and set it to consume frames on the channel my other AP was broadcasting on. Still though, I was unable to see any of the association/authentication traffic from my problem clients on that channel.

Resolution:

At this point I decided to review the known information again to see if there was something I was missing. I listed the symptoms out:

- Clients showed authenticated and associated to the correct SSID (from their perspective)
- Client showed no valid IP (just an APIPA 169.x.x.x address)
- Wireless controller showed no clients associating or attempting to associate
- Wireless debugs and packet captures showed no activity for client macs that should be associating with APs on the controller

As I went over those facts again, I realized that since the client was connecting to the correct SSID but not to the expected APs that there must be a rogue AP on site. Again, I had to turn to a different tool than I typically use to remotely determine if there were any rogues. Like all enterprise wireless vendors, Cisco maintains a list of potential rogue APs/SSIDs based on information gathered from when APs go off-channel to scan. I utilized this list to locate a device that was broadcasting both of this site's SSIDs. Looking at the BSSIDs I quickly realized that this "rogue" ap was actually the 3rd AP on site. At that point it became obvious that the 3rd AP was in fact powered up and broadcasting but simply unable to pass network traffic on the wired interface correctly due to the cabling issue. Since these APs were configured with FlexConnect

and local switching the problem AP had switched to a standalone state when it was unable to contact the controller via the uplink. The problem client devices were associating with this standalone ap and were able to successfully associate and authenticate to the wireless side but were subsequently unable to get IP addresses because of the wired uplink issues. To verify the root cause, I simply shutdown the port powering the 3rd AP and immediately saw the clients associate to the controller connected APs. Ultimately the customer ran a new drop to the affected AP to restore normal service.

POST-MORTEM:

Had I been able to be onsite, I likely would have used a wireless scanner like WiFi Explorer Pro very early on in the troubleshooting process to establish a baseline of what APs were online and sending beacons. It would have been almost immediately apparent that there were three APs broadcasting the SSIDs in question – negating the initial assumption that because the switch said the wired link was down that the AP in question was completely down. Understanding the alternative tools I had at my disposal (controller/AP packet captures, debugging commands, and ultimately rogue AP lists) allowed me to resolve the issue remotely without the need for an expensive and time-consuming on-site visit.