Troubleshooting Intermittent WLAN Issues

Scott Lester

A few years ago, I was presented with an issue at a higher education customer that required in depth troubleshooting of the WLAN to determine the root cause of the problem. The issue reported was periodically WLAN users in a lecture hall would be connected to the wireless network, yet they were unable to browse any network resource including the Internet. Symptoms of the issue reported were that the access points were connected and broadcasting the correct SSIDs, users were still showing connected to the AP, and the AP was not being reported offline by the WNMS. The following describe the steps taken to troubleshoot the issue and find a resolution based on the information gathered during the troubleshooting period.

Since I was unfamiliar with the environment, I started the troubleshooting process by utilizing a WLAN discovery tool, inSSIDer, to confirm that the correct SSIDs were being broadcast in the service area where the issue was being reported. After confirming the correct networks were being broadcast, I decided to check for the presence of multiple access points in the service area since the customer required a minimum of 3 AP providing coverage to this high-density location. I again utilized the discovery tool to verify that the SSID was being broadcast by the minimum number of AP required in each of the 2.4 and 5 GHz bands. Once coverage had been verified, I attempted to connect to the WLAN and test for the issue that the customer had reported. As with any network issue, I needed to verify that the issue was not related to a specific client or wireless chipset. I also needed to verify that the data was being transmitted by the client device and received by the access point. To accomplish this, I utilized protocol analyzer software (Omnipeek) and a USB NIC that was capable of being placed into promiscuous mode so I could capture all 802.11 wireless frames in the air on the channels being used in the affected area. I also placed a protocol analyzer in front of the connections to the physical WLAN controller to verify that all frames being transmitted to the AP were making it onto the wired medium and to the controller. While testing, the reported issue was not observed and I determined that waiting to continue troubleshooting until the classroom was in use would be the best approach since the lecture period was when the issue was consistently reported.

While reviewing the packet captures taking during the lecture period, I was able to determine that control plane packets from the AP to the controller were being transmitted and received successfully. This explained why the AP continued to appear online and allowed clients to associate and maintain a L2 connection. However, the vendor equipment being used by the customer required that the AP have two UDP ports open between AP and WLAN controller, one for control plane traffic and one for data plane traffic. After more examination of the packet captures, I discovered that packets containing data plane information from the AP were not making it to the WLAN controller. After presenting this information to the customer, we worked with their security team to discover that a IPS appliance had been installed in the network, and configured to scan traffic between the two VLANs that the APs and controllers resided. A rule on the IPS was scanning traffic destined for the UDP port that handled WLAN data plane traffic, and since peer to peer traffic was detected in some packets the IPS was blocking the unpermitted traffic. Therefore, the cause of the issue was that data plane packets were never making it to the WLAN controller to be processed and placed onto the wired network. This denial of data plane traffic caused all clients connected on the access point attempting to pass the unpermitted traffic to be unable to communicate across the WLAN. After the IPS rules were modified to always allow traffic on the data plane UDP port, the issue was no longer seen in the network.

Since the wireless became the de facto medium of choice for users connecting to the network, many users commonly blame the wireless network for their issues. As professionals know, there are many pieces that makeup an enterprise wireless network and knowing where in the network architecture to gather the necessary information to troubleshoot the problem is critical.