DELL (BROADCOM) 15XX WIRELESS CARD; FOUR-WAY HANDSHAKE TIMEOUT

Almost two years ago now we ran into an issue where thousands of laptops in the school district had trouble connecting and/or maintaining a reliable connection to the wireless network. The laptops had issues which predated my employment and were a constant source of connectivity issues. After several attempts by Support to narrow down the issue, we (the Network Team) were brought in to further investigate with some of our colleagues from an adjacent support team (the Systems Team). After several long days of troubleshooting and testing it was determined that the common denominator was a rebranded Broadcom 15xx series wireless card that was the source of the issue. These cards came in several different models. For example, there was a 1504 which was a single band HT card and a 1530 which was a dual band HT card. There were a couple other iterations of the card and they all suffered from the same problem.

Early on in troubleshooting we discovered that there was no rhyme or reason to when the issue presented itself but it was more common with the affected card when it first came off the cart in the morning. As soon as the laptop would boot to the login screen a user could enter their credentials and immediately get a "No Logon Servers Available" error message. Eventually, after several attempts, the laptops were able to successfully login and maintain their connection for an indeterminate amount of time before disconnecting again (mostly after a roam). Several different troubleshooting methods were attempted such as driver updates, power management adjustments, wireless card setting changes, but none seem to prove a consistent fix for the problem.

Since the issue was somewhat consistent at initial login first thing in the morning, I decided to collect the MAC address from the wireless card of a few machines. I entered the MAC addresses into the CLI of the wireless controller and began collecting a station log so that I could monitor each step of the connection process. It did not take long to see that the issue was caused by a problem with the four-way handshake. We use WPA2-Personal (802.11i-2004; CCMP-AES) for our Robust Security Network which employs a lengthy and complex PSK to encrypt our wireless data. The problematic client would authenticate and associate to the AP without issue. Once the authentication and association process was complete the authenticator (AP) would send its ANonce (M1) to the supplicant. There would be no response (M2) from the supplicant and the authenticator would try three more times before timing out. It was clear in the logs that the authenticator was sending the ANonce but there was no response (SNonce) from the supplicant so the Pairwise Transient Key was not able to be produced. Since the PTK wasn't able to be produced the supplicant never sent the SNonce and Message Integrity Check back to the authenticator. Because of this failure, the authenticator was not capable of sending the Group Temporal Key with MIC, which obviously didn't allow for the supplicant to acknowledge and proceed on to the DHCP request. After a random period of time the client would attempt the process again and most of the time fail, but occasionally succeed. We tested this against several other clients with the same series card and each one suffered from the same problem. I was also able to confirm the four-way handshake failure by watching the process in Wireshark. Again it was clear that after the ANonce was sent, there were no subsequent frame exchange between the supplicant and authenticator thus producing a four-way handshake timeout.

After discussing the findings with members of the troubleshooting team we were able to gather up several Intel Dual Band Wireless-AC 7260 wireless cards for additional testing. We selected ten test machines with the Dell Broadcom 15xx card and replaced them with the Intel 7260 card. We found a suitable driver to use and installed it to the test machines. We then monitored each test machine's station log during the boot process. As soon as the radio on the machine was active we noticed a perfect authentication, association, and four-way handshake, followed by a successful DHCP process. Each laptop we tested was able to login immediately without issue.

In the end we reported our findings to the Support branch of our department who worked something out with Dell to have the (several thousand) Dell Broadcom 15xx cards replaced with Intel 7260 cards. We checked back with many of the school sites after the major replacement projects and found that they all had a much better user experience with the Intel 7260 cards installed.