Security: MFP and how it can affect your throughput

Few months ago, we faced a mysterious issue with a set up box under test. The box had the **QCA6174A** which is a 2x2 80MHz 802.11ac chipset. During some of the test the box exhibited an abnormal behavior. The max throughput would drop significantly even within LOS and a clean environment. Under these conditions the box should be able to achieve max TCP DL throughput of around 600-650Mbps with a PHY rate of 877Mbps. What we have seen is that in some cases the box max DL throughput would drop to as low as 30Mbps. The first step in our investigation was to ensure that the drop-in throughput was not accompanied by a drop in PHY rates. It turned out that was that was not the case. The PHY rate was a sold 877Mbps during those drops.

Further investigation revealed that this drop only happened while the box is connected to WPA2 secure SSID. The other thing that these investigations revealed was that it only occurred with Broadcom based AP. With these two pieces of information in mind we started our troubleshooting. We listed all the possible causes of a throughput drop and how they would play into our scenario. The first to be rolled out was PHY rate drop since we could monitor both AP and box PHY rates during the test. The second was Airtime and that was also rolled out due to the test being conducted in a clean environment. The third candidate was aggregation. For we had to run a packet capture and analyze the packet.

We started comparing packet capture from a case where the box was able to do around 650Mbps TCP on DL with capture from a case where the box was only able to do around 30Mbps. At this point we could tell what the reason for this drop was. It was aggregation. In the low throughput case, there were no BA frames. All packets were sent as single MPDUs frames rather being sent as A-MPDUs frames. Now the only thing left was to know why this was happening. To explain this, let's take a quick look how at how A-MPDU works, first the AP wins time slot, then it sends an ADDBA request to the client, the client acknowledges it and sends back an ADDBA response. Now that the BA frame work has been established the AP can send all MPDUs as an A-MPDU and the client can acknowledge all of them by a BA frame at the end of the transmission. Figure-1 shows how the process works.

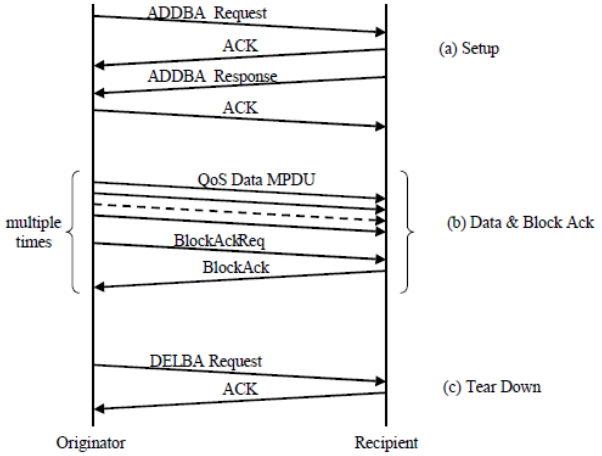

Figure 1

Filtering for ADDBA request and ADDBA response in the low throughout case packet capture revealed 2 issues:

- ADDBA requests from the AP but no ADDBA responses from the box.
- ADDBA requests from the box but no ADDBA responses from the AP.

Which led to a failure in establishing a BA frame work and packets being sent as single MPDUs. Since this only happened under a WPA2 secure SSID it led us to believe that it has to do with MFP. Both the AP and the box were capable of doing MFP. We set up a test with 4 scenarios:

- Scenario 1: MFP is enabled on both AP and the box.
  - Results: Failure to establish a BA frame work manifesting itself as low throughput issue.
- Scenario 2: MFP is enabled on the AP and disabled on the box.
  - Results: Successful establishment of BA frame work and high throughput achieved.
- Scenario 3: MFP is enabled on the box and disabled on the AP.
  - Results: Successful establishment of BA frame work and high throughput achieved.
- Scenario 4: MFP is disabled on both AP and the box.
  - Results: Successful establishment of BA frame work and high throughput achieved.

Now that we have established it was an MFP interoperability issue between a Qualcomm client and a Broadcom AP. The next step was to determine which one was the cause of the issue. A different client (a DELL XPS laptop) with the same **QCA6174A** was paired to the AP in a secure WPA2, MFP enabled SSID. To our surprise the client was successful in establishing a BA frame work with protected action frames and high throughputs were achieved. Comparing the wireless driver on the DELL laptop to the wireless on the box revealed the box was running a different and older driver version. Upgrading the box's wireless driver solved the interoperability issue.

As we migrate from WPA2 to WPA3 we lose the option to disable MFP since its MFP support is mandatory in WPA3. I believe further investigations are needed into interoperability between different vendors.