Troubleshooting 4-way handshake initialization delay

Summary:

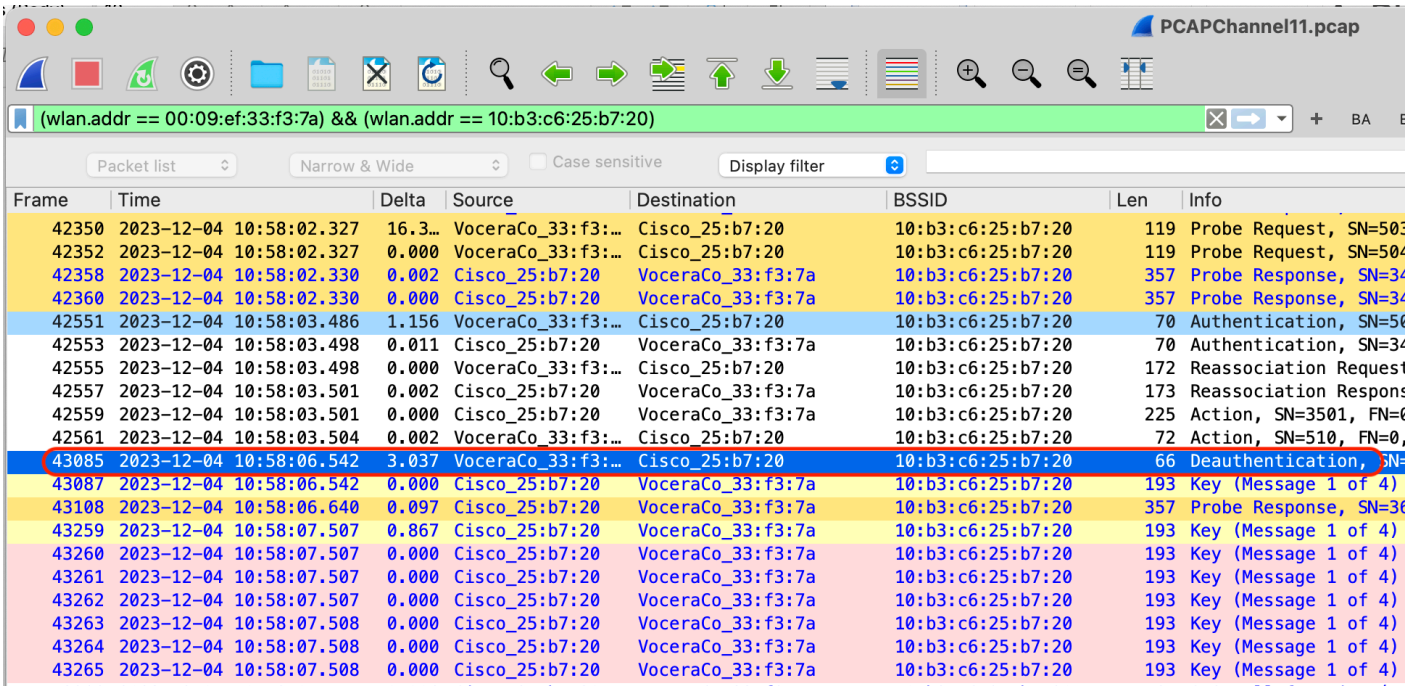
I currently work for a company that provides Voice Over WiFi services for large organizations. Customer reported an issue with extended roams with our wireless client – a badge. Wireless vendor was engaged and root cause appeared to bounce back and forth between client and wireless vendor as troubleshooting process continued. Ultimately it was found that the root cause was a Radio Measurement compatibility issue on the client side that was not being recognized by the wireless vendor's equipment. Once the particular feature was disabled on the WLC, the client experienced no further issues.

Analysis:

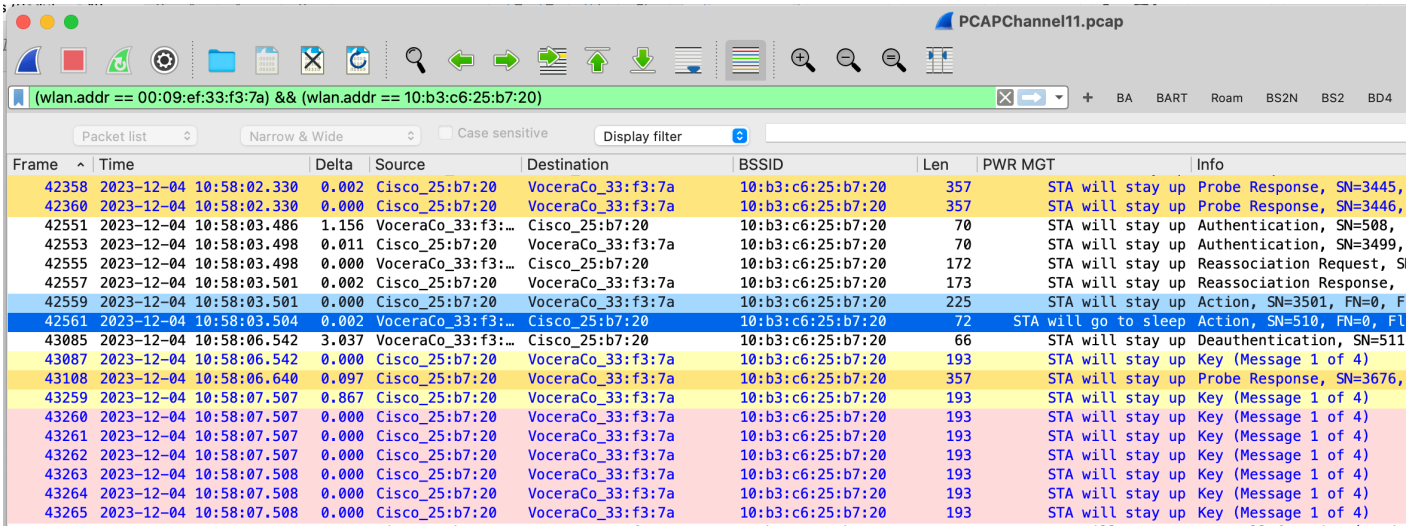
Customer was testing our wireless client in a dual-band environment. Upon testing they noticed extended roam times of a few seconds and were able to pin it down to when our badge roamed from 5GHz channel to 2.4GHz channel. Client logs and packet captures were taken of the issue.

Badge logs showed 4-way handshake timeout due to not receiving M1 within 3 seconds. Packet captures showed open authentication frame exchange, re-association request and response, followed by a client initiated deauthentication (deauth) 3 seconds later – without any M1 (message 1 of 4-way handshake) sent by AP. deauth presented with reason code 3 – sending station is leaving ESS. Almost immediately after deauth, Cisco AP started to send M1 repeatedly. These results were given to Cisco to review.

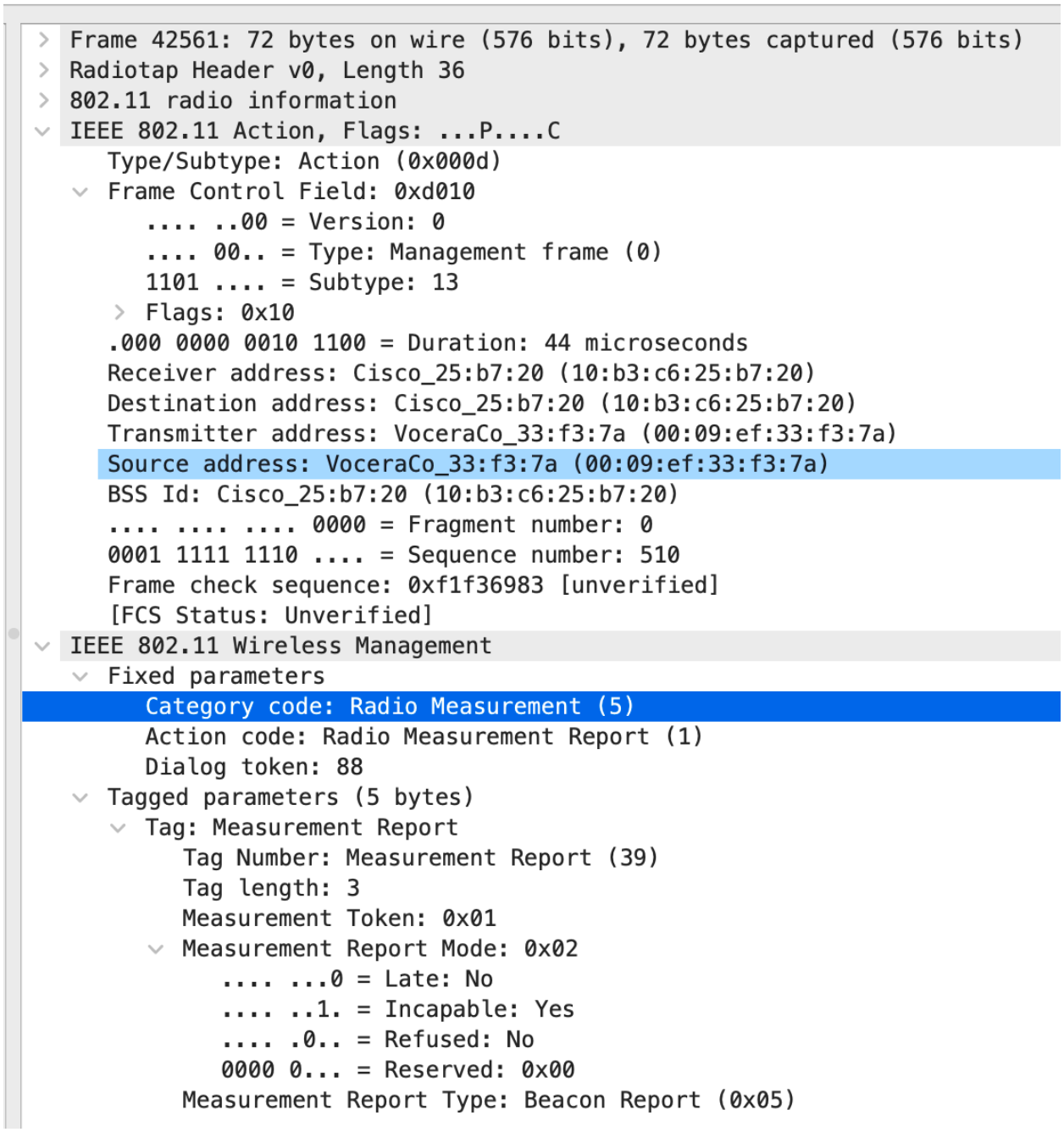
See next page for image of packet capture.



Cisco reviewed and got back to us. Their investigation showed that our badge was announcing it would go to sleep by setting its Power Save bit to '1' in an action frame response immediately preceding the deauth reason 3. The onus was back on us to figure out why this was happening.

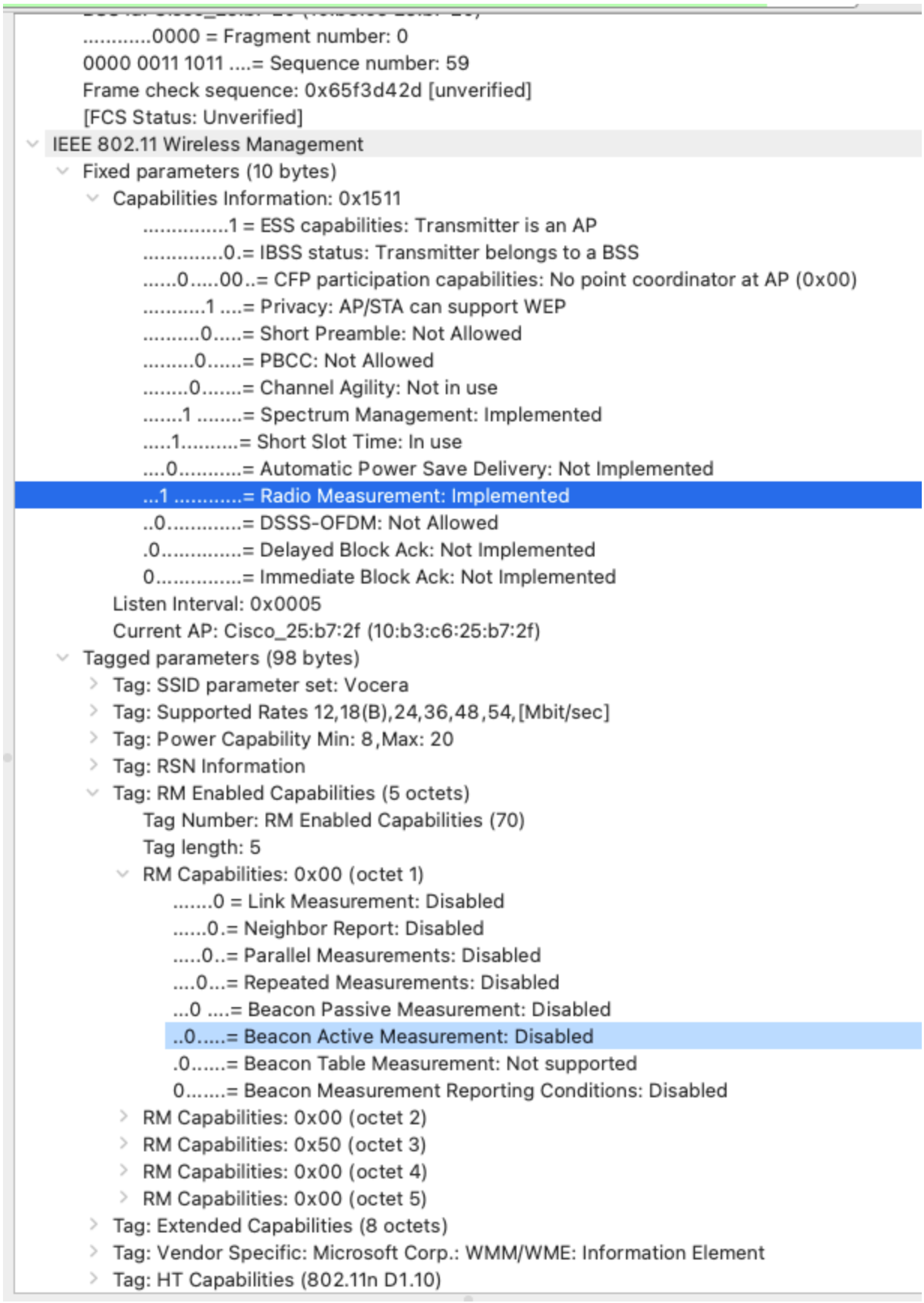


Action frame with sleep announcement was found to be a response to a Radio Measurement Request sent by the AP; specifically a Beacon Measurement Request. Why the deauth in response to this though? Looking at the details of the response, it started to become clear. Within the action frame response, the badge was announcing "Incapable: Yes" within the Measurement Report Mode of the Measurement Report.



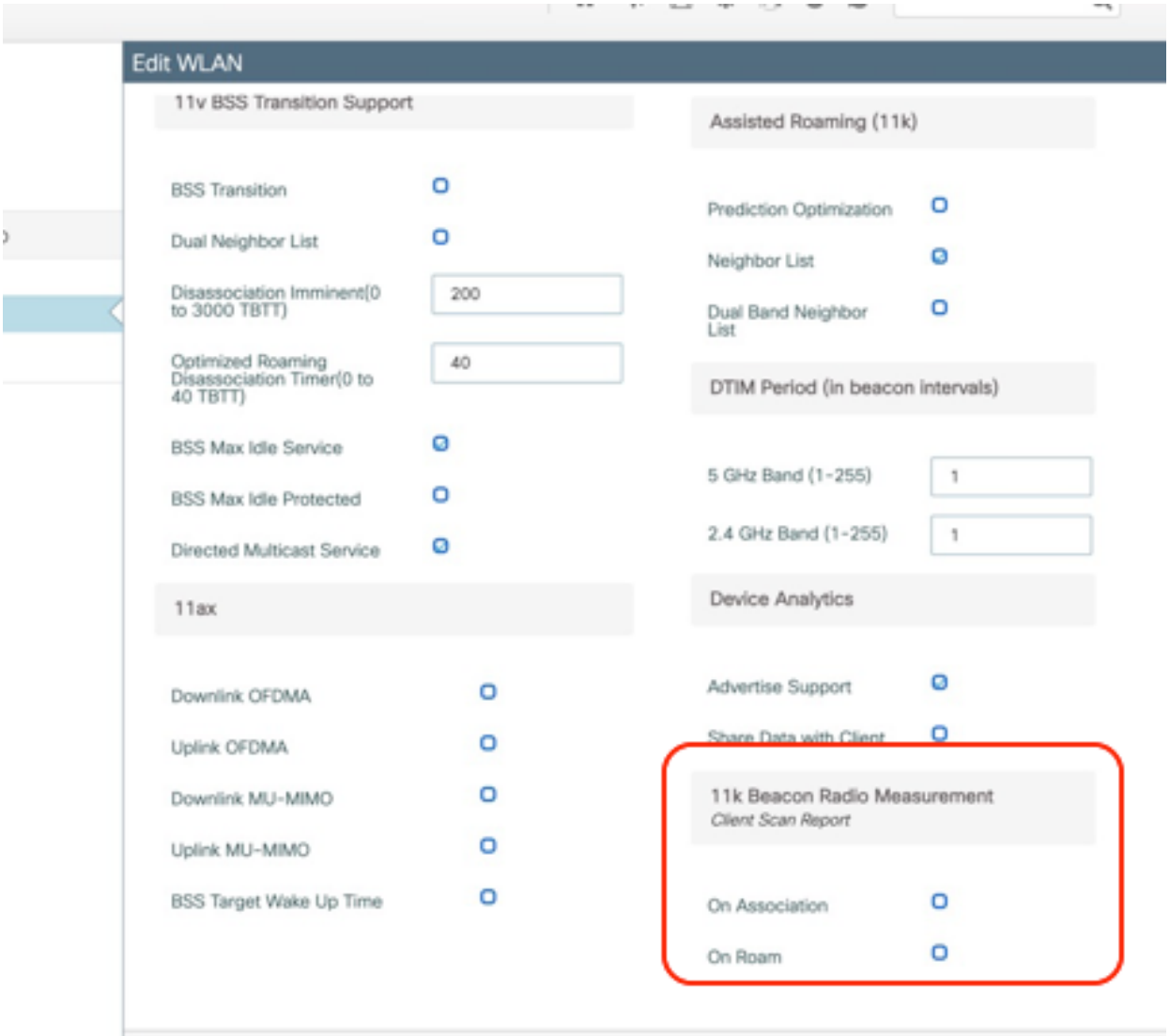
Our device engineering team was consulted, and they reviewed which items within Radio Measurement were supported. They reported the 802.11n chipset within our badge did not support Beacon Measurement Reports. It only supported 802.11k Neighbor Reports.

Now both vendors were investigating their side to ensure that the incompatibility was being communicated and honored. Looking at the reassociation request from the badge we noticed that Radio Measurement was announced to be “Implemented” within the Capabilities Information Element, however, within the more specific “RM Capabilities” Information Element all Beacon Measurement options were disabled.


.....0000 = Fragment number: 0
0000 0011 1011 ....= Sequence number: 59
Frame check sequence: 0x65f3d42d [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
Fixed parameters (10 bytes)
Capabilities Information: 0x1511
.....1 = ESS capabilities: Transmitter is an AP
.....0.= IBSS status: Transmitter belongs to a BSS
.....0.....00..= CFP participation capabilities: No point coordinator at AP (0x00)
.....1 ....= Privacy: AP/STA can support WEP
.....0.....= Short Preamble: Not Allowed
.....0.....= PBCC: Not Allowed
.....0.....= Channel Agility: Not in use
.....1 .....= Spectrum Management: Implemented
.....1.....= Short Slot Time: In use
....0.....= Automatic Power Save Delivery: Not Implemented
...1 .....= Radio Measurement: Implemented
..0.....= DSSS-OFDM: Not Allowed
.0.....= Delayed Block Ack: Not Implemented
0.....= Immediate Block Ack: Not Implemented
Listen Interval: 0x0005
Current AP: Cisco_25:b7:2f (10:b3:c6:25:b7:2f)
Tagged parameters (98 bytes)
Tag: SSID parameter set: Vocera
Tag: Supported Rates 12,18(B),24,36,48,54,[Mbit/sec]
Tag: Power Capability Min: 8,Max: 20
Tag: RSN Information
Tag: RM Enabled Capabilities (5 octets)
Tag Number: RM Enabled Capabilities (70)
Tag length: 5
RM Capabilities: 0x00 (octet 1)
.....0 = Link Measurement: Disabled
.....0.= Neighbor Report: Disabled
.....0..= Parallel Measurements: Disabled
....0...= Repeated Measurements: Disabled
...0 ....= Beacon Passive Measurement: Disabled
..0.....= Beacon Active Measurement: Disabled
.0.....= Beacon Table Measurement: Not supported
0.....= Beacon Measurement Reporting Conditions: Disabled
RM Capabilities: 0x00 (octet 2)
RM Capabilities: 0x50 (octet 3)
RM Capabilities: 0x00 (octet 4)
RM Capabilities: 0x00 (octet 5)
Tag: Extended Capabilities (8 octets)
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
Tag: HT Capabilities (802.11n D1.10)

This data was presented to Cisco. Cisco responded that they were able to send the Beacon Measurement Report Request to our badge since it was advertising Radio Measurement: Implemented within the Capabilities Information Element of its reassociation request frame. There was a little back and forth on this since the badge specifically announced Beacon Measurement Reports were disabled. Running the command “show wireless client <mac address>” on the WLC also showed Beacon Measurement Reports were announced as disabled by the client, and the WLC was aware.

We requested Cisco disable (or not send) this report as our badge was announcing it did not support it. We were told there was no way to disable this report without disabling Radio Measurement entirely. The customer was not agreeable to this. After some additional back and forth, it was found in the 9800 controller UI that this report could be disabled within the Edit WLAN -> Advanced tab. We were able to prove in our lab that the issue could no longer be reproduced with this setting disabled.



Conclusion:

There were a couple lessons learned from this experience.

First, the troubleshooting process between vendors is rarely complete after first analysis. It is a collaborative effort including several iterations and layers of analysis that need to take place before the final root cause is found. Through this process the ownership of the issue can change hands several times and it is important to keep an open mind until both sides have weighed in with their own feedback & analysis.

Second, the 802.11 Standard is not always specific on *how* its requirements get implemented. It can be gray on specifics. Throughout this troubleshooting process the standard was reviewed several times. Unfortunately this yielded no definitive answer as to whether or not the AP could solicit another station for a report of which that station advertised incompatibility for. Because neither side could find this scenario defined in the standards, that led to finger pointing between client and wireless vendor. Ultimately the solution was to disable the unsupported feature from being used by the WLC.