

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.

Frame	Time	Delta	Source	Destination	BSSID	Len	Info
42350	2023-12-04 10:58:02.327	16.3...	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	119	Probe Request, SN=503
42352	2023-12-04 10:58:02.327	0.000	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	119	Probe Request, SN=504
42358	2023-12-04 10:58:02.330	0.002	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	357	Probe Response, SN=34
42360	2023-12-04 10:58:02.330	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	357	Probe Response, SN=34
42551	2023-12-04 10:58:03.486	1.156	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	70	Authentication, SN=50
42553	2023-12-04 10:58:03.498	0.011	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	70	Authentication, SN=34
42555	2023-12-04 10:58:03.498	0.000	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	172	Reassociation Request
42557	2023-12-04 10:58:03.501	0.002	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	173	Reassociation Response
42559	2023-12-04 10:58:03.501	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	225	Action, SN=3501, FN=0
42561	2023-12-04 10:58:03.504	0.002	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	72	Action, SN=510, FN=0
43085	2023-12-04 10:58:06.542	3.037	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	66	Deauthentication, SN=
43087	2023-12-04 10:58:06.542	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)
43108	2023-12-04 10:58:06.640	0.097	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	357	Probe Response, SN=36
43259	2023-12-04 10:58:07.507	0.867	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)
43260	2023-12-04 10:58:07.507	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)
43261	2023-12-04 10:58:07.507	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)
43262	2023-12-04 10:58:07.507	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)
43263	2023-12-04 10:58:07.508	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)
43264	2023-12-04 10:58:07.508	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)
43265	2023-12-04 10:58:07.508	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	Key (Message 1 of 4)

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 death reason 3. The onus was back on us to figure out why this was happening.

Frame	Time	Delta	Source	Destination	BSSID	Len	PWR MGT	Info
42358	2023-12-04 10:58:02.330	0.002	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	357	STA will stay up	Probe Response, SN=3445,
42360	2023-12-04 10:58:02.330	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	357	STA will stay up	Probe Response, SN=3446,
42551	2023-12-04 10:58:03.486	1.156	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	70	STA will stay up	Authentication, SN=508,
42553	2023-12-04 10:58:03.498	0.011	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	70	STA will stay up	Authentication, SN=3499,
42555	2023-12-04 10:58:03.498	0.000	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	172	STA will stay up	Reassociation Request, S
42557	2023-12-04 10:58:03.501	0.002	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	173	STA will stay up	Reassociation Response,
42559	2023-12-04 10:58:03.501	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	225	STA will stay up	Action, SN=3501, FN=0, F
42561	2023-12-04 10:58:03.504	0.002	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	72	STA will go to sleep	Action, SN=510, FN=0, Fl
43085	2023-12-04 10:58:06.542	3.037	VoceraCo_33:f3:...	Cisco_25:b7:20	10:b3:c6:25:b7:20	66	STA will stay up	Deauthentication, SN=511
43087	2023-12-04 10:58:06.542	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)
43108	2023-12-04 10:58:06.640	0.097	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	357	STA will stay up	Probe Response, SN=3676,
43259	2023-12-04 10:58:07.507	0.867	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)
43260	2023-12-04 10:58:07.507	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)
43261	2023-12-04 10:58:07.507	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)
43262	2023-12-04 10:58:07.507	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)
43263	2023-12-04 10:58:07.508	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)
43264	2023-12-04 10:58:07.508	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)
43265	2023-12-04 10:58:07.508	0.000	Cisco_25:b7:20	VoceraCo_33:f3:7a	10:b3:c6:25:b7:20	193	STA will stay up	Key (Message 1 of 4)

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.

```

> Frame 42561: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Action, Flags: ...P....C
  Type/Subtype: Action (0x000d)
  > Frame Control Field: 0xd010
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1101 .... = Subtype: 13
  > Flags: 0x10
    .000 0000 0010 1100 = Duration: 44 microseconds
  Receiver address: Cisco_25:b7:20 (10:b3:c6:25:b7:20)
  Destination address: Cisco_25:b7:20 (10:b3:c6:25:b7:20)
  Transmitter address: VoceraCo_33:f3:7a (00:09:ef:33:f3:7a)
  Source address: VoceraCo_33:f3:7a (00:09:ef:33:f3:7a)
  BSS Id: Cisco_25:b7:20 (10:b3:c6:25:b7:20)
  .... .... 0000 = Fragment number: 0
  0001 1111 1110 .... = Sequence number: 510
  Frame check sequence: 0xf1f36983 [unverified]
  [FCS Status: Unverified]
  > IEEE 802.11 Wireless Management
    > Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Radio Measurement Report (1)
      Dialog token: 88
    > Tagged parameters (5 bytes)
      > Tag: Measurement Report
        Tag Number: Measurement Report (39)
        Tag length: 3
        Measurement Token: 0x01
      > Measurement Report Mode: 0x02
        .... ...0 = Late: No
        .... ..1. = Incapable: Yes
        .... .0.. = Refused: No
        0000 0... = Reserved: 0x00
        Measurement Report Type: Beacon Report (0x05)

```

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.

The screenshot shows the 'Edit WLAN' configuration page in the Cisco 9800 controller UI, specifically the 'Advanced' tab. The page is divided into several sections with various settings. A red box highlights the '11k Beacon Radio Measurement Client Scan Report' section, which includes two sub-settings: 'On Association' and 'On Roam', both of which are currently disabled (indicated by blue circles with a diagonal line).

Section	Setting	Value / Status
11v BSS Transition Support	BSS Transition	<input type="checkbox"/>
	Dual Neighbor List	<input type="checkbox"/>
	Disassociation Imminent(0 to 3000 TBTT)	200
	Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
	BSS Max Idle Service	<input checked="" type="checkbox"/>
	BSS Max Idle Protected	<input type="checkbox"/>
	Directed Multicast Service	<input checked="" type="checkbox"/>
Assisted Roaming (11k)	Prediction Optimization	<input type="checkbox"/>
	Neighbor List	<input checked="" type="checkbox"/>
DTIM Period (in beacon intervals)	5 GHz Band (1-255)	1
	2.4 GHz Band (1-255)	1
11ax	Downlink OFDMA	<input type="checkbox"/>
	Uplink OFDMA	<input type="checkbox"/>
	Downlink MU-MIMO	<input type="checkbox"/>
	Uplink MU-MIMO	<input type="checkbox"/>
	BSS Target Wake Up Time	<input type="checkbox"/>
	Device Analytics	
11k Beacon Radio Measurement Client Scan Report	On Association	<input type="checkbox"/>
	On Roam	<input type="checkbox"/>

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.