The bridge to possible

# TAC stories: WiFi networks that save lives… and your job

## And avoid escalations, losing hair and other undesirable effects

Nicolas Darchis, Sr Technical Leader, CX - @DarchisNicolas
Javier Contreras, Principal Engineer, Engineering

# Cisco Webex App

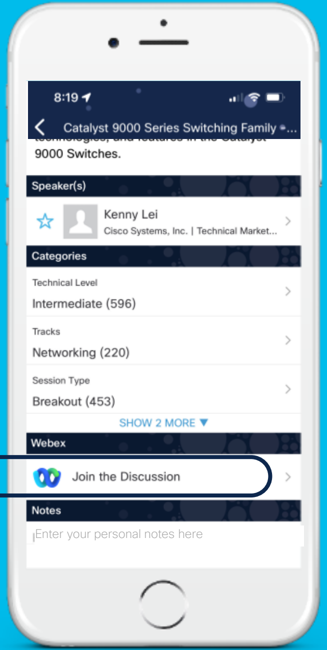
## Questions?

Use Cisco Webex App to chat
with the speaker after the session

## How

1. Find this session in the Cisco Live Mobile App
2. Click "Join the Discussion"
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

## Webex spaces will be moderated until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# About us - Nico

# Javier

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Agenda

- VoWifi in healthcare
- Of Mines and Men
- Throughput issues in a bank
- Multicast IPTV streaming
- If it walks like a duck...Could be an orange
- The Tale of the Three Defects
- Flapping around
- Tagging Etiquette
- The Real Thing

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# CISCO WIRELESS SOCIAL

with Food & Drinks and a Trivia Game

SPECIAL GIFT FOR EVERY REGISTERED ATTENDEE

SCAN QR CODE FOR REGISTRATION & DETAILS

Cisco Systems Netherlands

Haarlerbergweg 17-19
1101 CH Amsterdam-Zuidoost, Netherlands

Wednesday, FEBRUARY 8TH
AT 18:30-20:30

# Agenda

14.15 : start and intro

14.30 : Some stories from Nico

16.15 : coffee break

16.45 : Even More stories from Javier

18.45 : End !

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Agenda

- Story : the typical big escalation.
- The easy and the hard action plans
- Other gotchas and other short stories: tips to make sure you avoid bad escalations
- “Did you know ?” TAC tips about tools and troubleshooting techniques

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Disclaimer

- Nothing personal or negative intended
- Situations depicted can happen to anyone
- Objective is to hear a good story,  then to learn small tips to improve habits
- Situations depicted were full of great engineers. Sometimes, bad things happen due to circumstances that could not be avoided easily.

# Hospital + 8821 + WiFi network

# The story :  TAC case gets opened

- End users (nurses,doctors,..) are complaining about overall poor call performance
- Hard to know where, when and how : nurses and doctors' jobs are to take care of patients, not write down issue descriptions with timestamps
- This coincides with the beginning of COVID period (i.e., less staff, more activity, more stress)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Questions in the TAC engineer’s mind

And the logic behind them

- Are we talking about poor voice quality ? (i.e. robotic voice, muffled, hard to understand, …)
    - What it means: QoS, channel utilization
- Are we talking voice gaps ? Does the voice resume ?
    - What it means: One way voice could be ARP, voice gaps could be roaming issues
- How frequently does it happen ?
    - What it means:   is it easily reproducible or not ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Questions in the TAC engineer’s mind

And the logic behind them

- Does it happen in certain areas ? When roaming or standing still ?
  - What it means:  roaming issue ?
  - Specific area with interference or high CU ?
- Is it call manager disconnections or is it wifi instability ?

  No point on checking upper layers if lower is failing

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Questions in the TAC engineer’s mind

- TAC engineer :

Maybe it’s not the wifi

- Partner engineer :

🤨

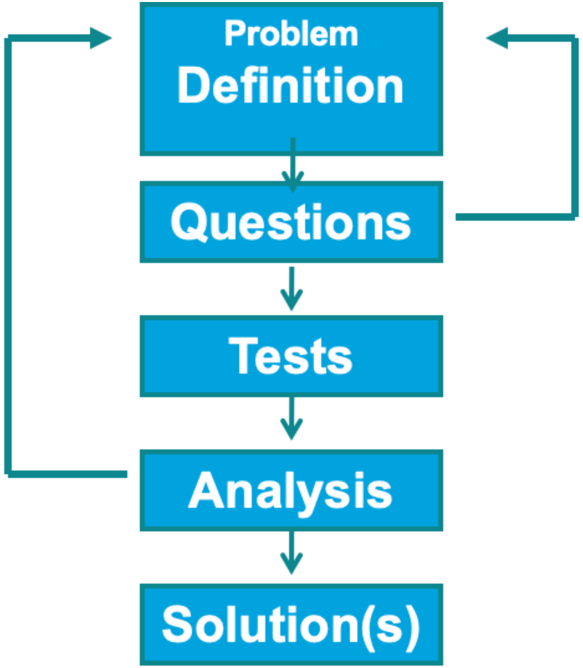
# Meanwhile the end users …

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Answers from the end users

- Are we talking about poor voice quality ?
  - Everything, bad voice and call drops
- Are we talking voice gaps ?
  - Sometimes a small voice gap, sometimes call drop
- How frequently does it happen ?
  - Some users report it every day
- Does it happen in certain areas ? When roaming or standing still ?
  - No particular area
- Is it call manager disconnections or is it wifi instability ?
  - ???

# Do you get vague problem descriptions?



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

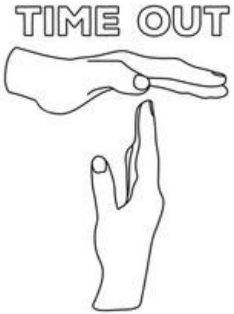
# What happened ? TAC initial plan

- Can you get an over the air capture of the problem ?
  - The partner is unable to capture/spot the problem
- Debugs are collected on the WLC. Do not seem to show anything strange.
  - WLC debugs are control-plane debugs. They only debug state machine events and not what happens to regular traffic
- Config adjustments : The wireless LAN config analyzer is a must !
  - https://cway.cisco.com/wireless-config-analyzer/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Wireless Config Analyzer Express

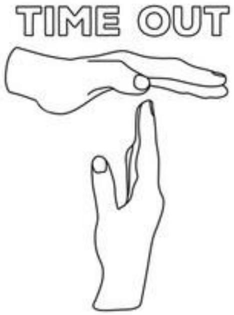
- Evolution from WLCCA
- Bring human years of learning and experience to you
- Case prevention
- Reduce case lifetime
- Single controller analysis
- Support for AireOS or 9800/EWC
  - Any model, any version



More in BRKEWN-3006

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

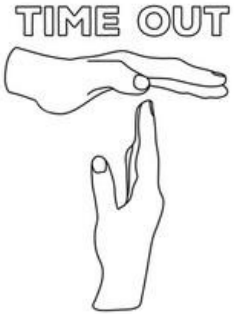
# Wireless Config Analyzer Express



- What it does:
  - Configuration Checks
  - RF Health Analysis
  - RF Stats Summarization
  - Upgrade Advisor
  - Channel Stats
  - Tag/Policy usage
  - RRM analysis
  - Log Message Summarization
  - Ap inventory
  - RF Graph Analysis
  - Client type list
  - NDP AP summarization
  - Controller config highlights
  - AP Config view
  - AP RF view
- New Client audits:
  - 8821, iPhone, Drager, Vocera, Spectralink

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Where?



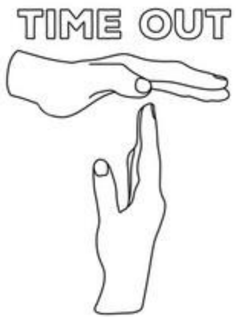
- Cloud Version:
  https://cway.cisco.com/tools/WirelessAnalyzer/
- Desktop Version:
  https://github.com/CiscoDevNet/wcae
- More info:
  https://developer.cisco.com/docs/wireless-troubleshooting-tools/
- Alias:
  wcae@cisco.com
- Webex Room:
  https://eurl.io/#R6RK2M73v

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# What happened ? The action plan

- Constant ping of 8821 phones to determine if there is wireless connectivity loss.
  - Phone regularly dropping pings
- Upgrade to latest stable release
  - https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html
  - https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/200046-tac-recommended-aireos.html
  - For 8821, latest is typically the recommended

# IOS-XE releases strategy



Long-term branches in bold

- Denali 16.1-**16.3**
- Everest 16.4 – **16.6**
- Fuji 16.7 – **16.9**
- Gibraltar 16.10-**16.12**
- Amsterdam 17.1-**17.3**
- Bengaluru 17.4-**17.6**
- Cupertino 17.7-**17.9**
- Dublin 17.10-**17.12**

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# What happened ? The action plan

- Debugs are enabled on selected phones.
- Users were asked to press a specific key when they just faced the problem
- Much smarter than asking user groups to note down timestamps on paper.

# Did it work ?

Phone logs didn’t seem to include any special key press to indicate issues. Nurses still have better to do than playing troubleshooting.

- Partner : I’m not hearing complains anymore from end users
- Hospital IT department : We have more urgent things cooking and no one screamed about this recently
- End users : I couldn’t tell you, I’m not using the wireless phones at all anymore, I’m using my cell phone.

# How did it end ?

- Case closed with:
  - Best practices tweaks
  - Verify the end-to-end QoS markings
  - Software update and an advice of making
  - New site survey based on a few suspicions from the show run-config (AireOS). More on this later

- Is it really the end ? No
- Was it actually solved ? No

# Situation goes nuclear

- Hospital leadership :

- There is the feeling that problems started a year ago
  - 5508s were replaced with 5520s
  - 1140 with 2800 APs and some 9115
- Site survey was done in emergency and does not find anything particular (apart from minor area-specific adjustment)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Engaging the Cisco A-team

Requirements :

- Solve it quick !
- Due to COVID, hardly anyone can go onsite
- End users were put to contribution enough, do not involve them

Partner/Customer feeling :

The new WLC or AP models transmit less/worse than the previous model

# Action plan :

Typical action plan involving multiple sniffer captures :

~~Can't~~

# Action plan : let’s go for quick and easy

Let’s go for quick and easy to collect:

- Fresh show run-config
- Someone (anyone) to walk around with  8821 and the “Site survey” feature on. Verify signal is always better than -67dBm
- Collect phone logs remotely after the person did the walkaround

# Clue number 1

Logs show low RSSI

No viable candidate

Problem : phone logs are many small text files in different zipped archives

```
DEB Feb 17 13:35:54.320313 wlanmgr-[vendor_get_rssi]: Curr
RSSI = -84
DEB Feb 17 13:35:54.320697 wlanmgr-[UpdateBSSList]: BSSID:
f4:db:e6:d6:13:08 RSSI: -84 Channel: 60 CU: 5
DEB Feb 17 13:35:54.320756 wlanmgr-[UpdateBSSList]: BSSID:
f4:db:e6:da:50:88 RSSI: -73 Channel: 40 CU: 11
DEB Feb 17 13:35:54.320808 wlanmgr-[UpdateBSSList]: BSSID:
f4:db:e6:dc:2c:a8 RSSI: -74 Channel: 48 CU: 4
DEB Feb 17 13:35:54.320859 wlanmgr-[UpdateBSSList]: BSSID:
f4:db:e6:d2:84:08 RSSI: -77 Channel: 48 CU: 3
DEB Feb 17 13:35:54.320910 wlanmgr-[UpdateBSSList]: BSSID:
f4:db:e6:dc:32:48 RSSI: -80 Channel: 52 CU: 2
DEB Feb 17 13:35:54.320986 wlanmgr-[rssi_update_ind]:
Update signal bar with rssi=-84
DEB Feb 17 13:36:10.496779 wpa_supplicant: wlan0: Event
DEAUTH (12) received
DEB Feb 17 13:36:10.496848 wpa_supplicant: wlan0:
Deauthentication notification
DEB Feb 17 13:36:10.496914 wpa_supplicant: wlan0: * reason 0
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Clue number 1

- How pervasive is this issue ?
- Enable “telephony” logging
- Write a quick python script
- Results: phone spends 50% of its time under too low RSSI

```
0568 DEB Feb 17 15:19:04.180825  call start
At time 15:19:08.986510, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-74 dbm
when connected to AP-402
At time 15:19:14.876540, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-72 dbm
when connected to AP-402
At time 15:19:19.106522, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-74 dbm
when connected to AP-402
At time 15:19:25.106515, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-75 dbm
when connected to AP-402
At time 15:19:33.106773, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-72 dbm
when connected to AP-402
At time 15:19:39.106963, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-71 dbm
when connected to AP-402
At time 15:19:45.106522, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-76 dbm
when connected to AP-402
At time 15:19:48.986657, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-81 dbm
when connected to AP-402
At time 15:19:55.106530, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-75 dbm
when connected to AP-402
At time 15:19:58.876568, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-75 dbm
when connected to AP-402
At time 15:20:05.106527, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-74 dbm
when connected to AP-402
At time 15:20:11.116511, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-76 dbm
when connected to AP-402
At time 15:20:15.116528, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-75 dbm
when connected to AP-402
At time 15:20:29.046698, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-76 dbm
when connected to AP-402
At time 15:20:34.374806, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-76 dbm
when connected to AP-402
At time 15:20:37.378521, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-77 dbm
when connected to AP-402
At time 15:21:09.368325, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-77 dbm
when connected to AP-402
At time 15:21:25.258186, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-73 dbm
when connected to AP-402
At time 15:22:53.138224, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-71 dbm
when connected to AP-402
At time 15:23:05.138630, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-74 dbm
when connected to AP-402
At time 15:23:23.767915, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-71 dbm
when connected to AP-402
At time 15:23:27.777954, SIGNAL STRENGTH TOO LOW while on call!  best neighbor at  :-74 dbm
when connected to AP-402
```

© 2023  Cisco and/or its affiliates. All rights reserved.   Cisco Public

# Clue number 1

- Panic scan is a sign of panic roaming, which is not good.

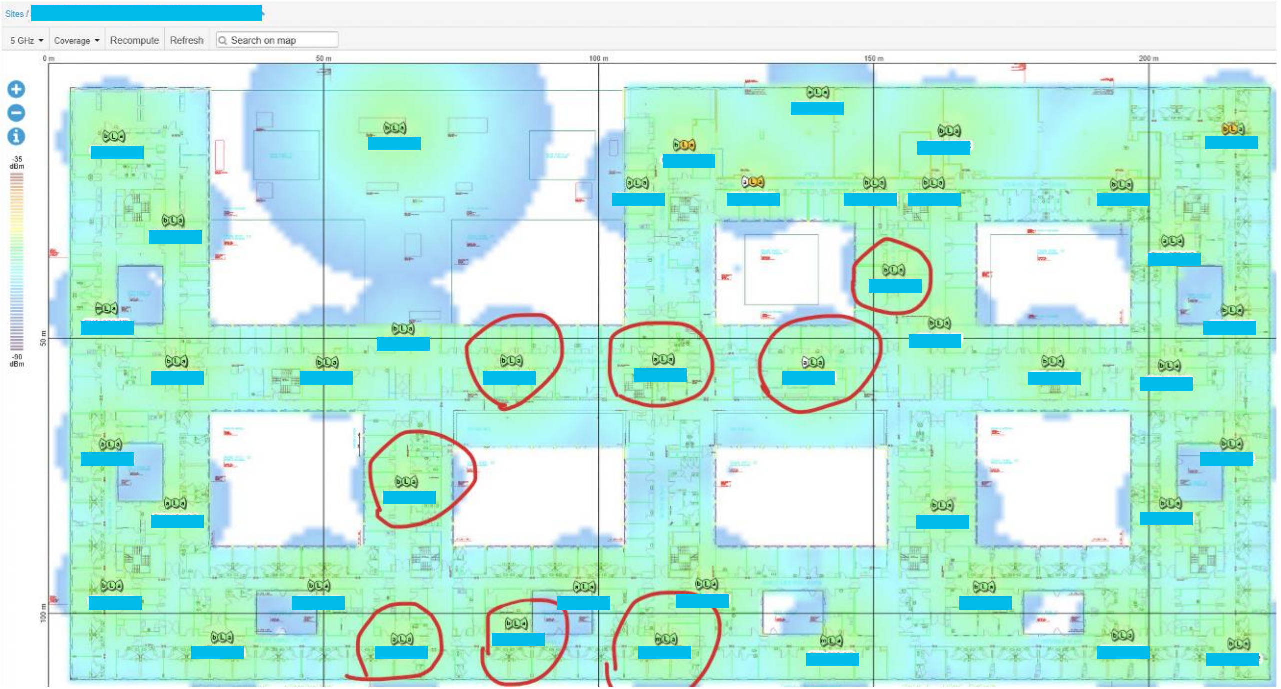
- Panic scan during the logs : 2748 (anything higher than 0 is concerning).
- Panic scans occur when the phone RSSI is below -70dbm
- It will definitely cause voice quality issues

- Number of successful roamings during the logs : 67

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Clue number 1

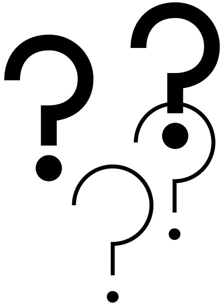
Where is the poor RSSI seen ?



# Clue number 2

The phone logs also indicate that downstream SIP messages are received with UP 0. It's doubtful QoS is correctly configured everywhere

```
DEB Feb 17 16:05:37.384171 kernel-[64500.311218] [dhd_sendpkt]: SIP [192.168.112.134:50481 -> 192.168.70.11:5060] [UP = 4] [len = 1047]

DEB Feb 17 16:05:37.384624 kernel-[64500.327453] [dhd_sendpkt]: SIP [192.168.112.134:53124 -> 192.168.70.12:5060] [UP = 4] [len = 1071]

DEB Feb 17 16:05:37.384668 kernel-[64500.330963] [dhd_rx_frame]: SIP [192.168.70.11:5060 -> 192.168.112.134:50481] [UP = 0] [len = 380]
```



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Clue number 3

- No evident problems in last site survey… why?

- What device was used to conduct the site survey ?
  - Proxim adapter on laptop

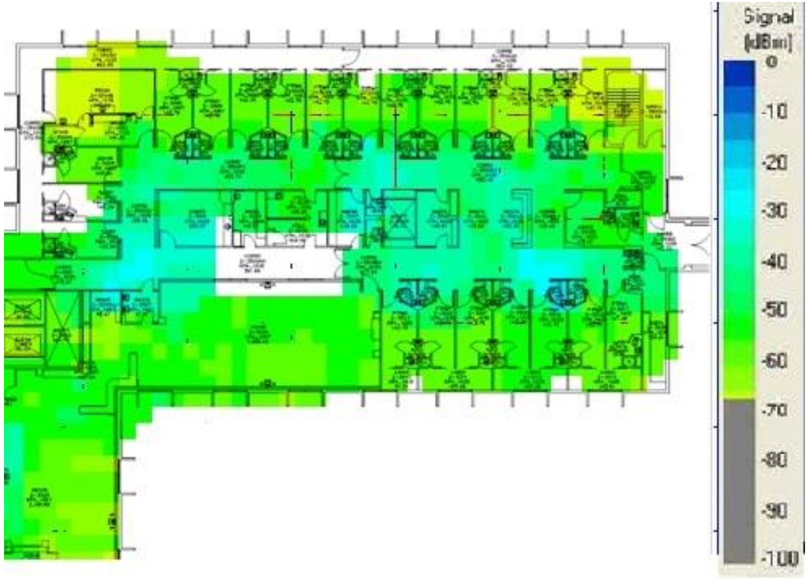
- No walk around with the device end users are using/complaining about (8821)

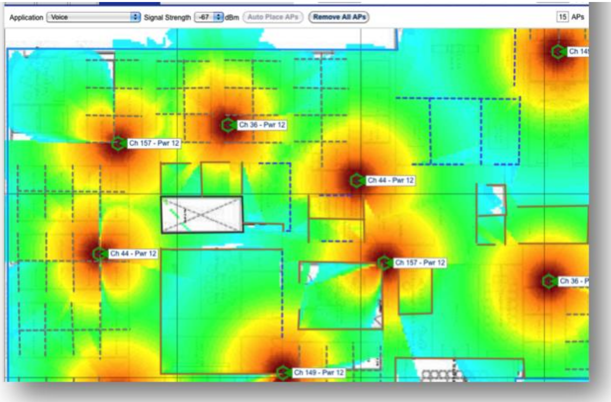
- Even if using 8821, holding it to your head gives very different result to holding in your hand

- Always test with the least capable device the customer will be using

# Clue number 3

- Site survey
  - No walking path showing in the printed report, all is green
  - When checking the original survey files, walking path indicate engineer did not enter any patient room
  - The “green” was extrapolated by the site survey software, not taking walls/attenuation into account
  - IT people could not reproduce the issue as they only walked in corridors too
  - All APs are placed in the corridors



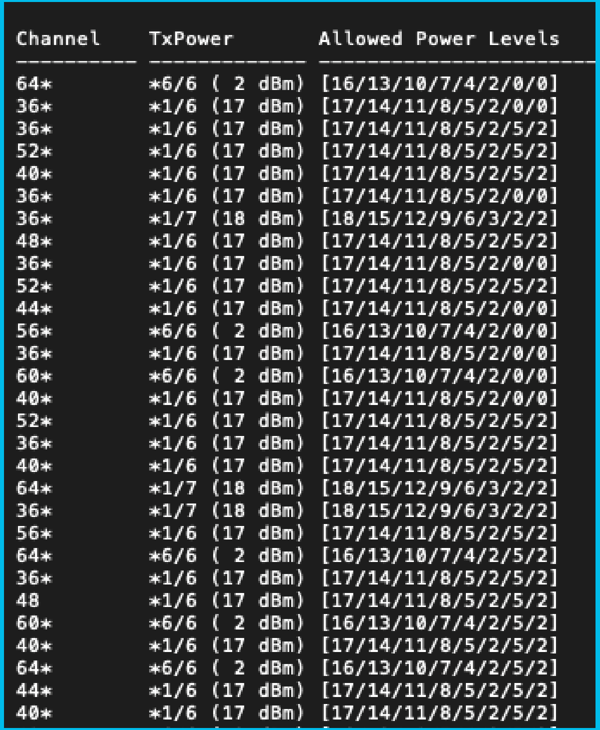

Application Voice Signal Strength -67 dBm Auto Place APs Remove All APs 15 APs

# Clue number 4

- WLC show run
- How come there was no problem before ?

- Before, people were using 7925s
- Some APs in default AP group not broadcasting voice SSID

# Clue number 4

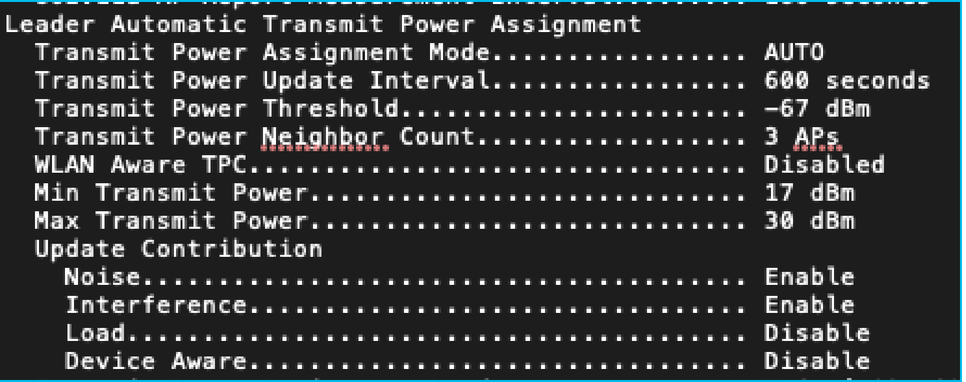


```
Channel       TxPower            Allowed Power Levels
-----------   ---------------   ---------------------------
64*           *6/6 ( 2 dBm)  [16/13/10/7/4/2/0/0]
36*           *1/6 (17 dBm)  [17/14/11/8/5/2/0/0]
36*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
52*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
40*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
36*           *1/6 (17 dBm)  [17/14/11/8/5/2/0/0]
36*           *1/7 (18 dBm)  [18/15/12/9/6/3/2/2]
48*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
36*           *1/6 (17 dBm)  [17/14/11/8/5/2/0/0]
52*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
44*           *1/6 (17 dBm)  [17/14/11/8/5/2/0/0]
56*           *6/6 ( 2 dBm)  [16/13/10/7/4/2/0/0]
36*           *1/6 (17 dBm)  [17/14/11/8/5/2/0/0]
60*           *6/6 ( 2 dBm)  [16/13/10/7/4/2/0/0]
40*           *1/6 (17 dBm)  [17/14/11/8/5/2/0/0]
52*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
36*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
40*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
64*           *1/7 (18 dBm)  [18/15/12/9/6/3/2/2]
36*           *1/7 (18 dBm)  [18/15/12/9/6/3/2/2]
56*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
64*           *6/6 ( 2 dBm)  [16/13/10/7/4/2/5/2]
36*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
48            *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
60*           *6/6 ( 2 dBm)  [16/13/10/7/4/2/5/2]
40*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
64*           *6/6 ( 2 dBm)  [16/13/10/7/4/2/5/2]
44*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
40*           *1/6 (17 dBm)  [17/14/11/8/5/2/5/2]
```

- Before, people were using 7925s
- Some APs in default AP group not broadcasting voice SSID
- All APs at power level 1 (or 2)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Clue number 4

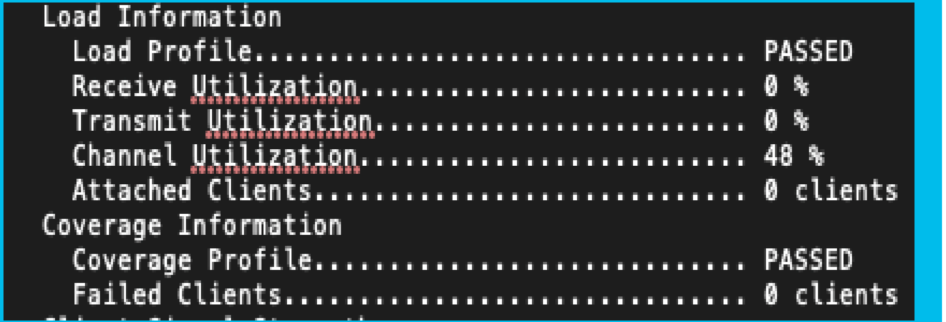


```
Leader Automatic Transmit Power Assignment
  Transmit Power Assignment Mode................. AUTO
  Transmit Power Update Interval................. 600 seconds
  Transmit Power Threshold....................... -67 dBm
  Transmit Power Neighbor Count.................. 3 APs
  WLAN Aware TPC................................. Disabled
  Min Transmit Power............................. 17 dBm
  Max Transmit Power............................. 30 dBm
  Update Contribution
    Noise........................................ Enable
    Interference................................. Enable
    Load......................................... Disable
    Device Aware................................. Disable
```

- Before, people were using 7925s
- Some APs in default AP group not broadcasting voice SSID
- All APs at power level 1 (or 2)
- Min TPC power is set to 17dbm in RRM settings

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

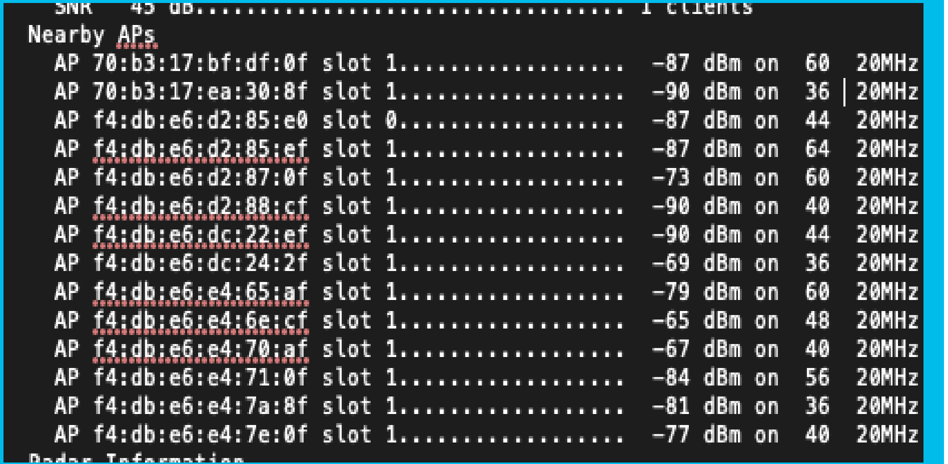
# Clue number 4



```
Load Information
  Load Profile................................ PASSED
  Receive Utilization......................... 0 %
  Transmit Utilization........................ 0 %
  Channel Utilization......................... 48 %
  Attached Clients............................ 0 clients
Coverage Information
  Coverage Profile............................ PASSED
  Failed Clients.............................. 0 clients
```

- Before, people were using 7925s
- Some APs in default AP group not broadcasting voice SSID
- All APs at power level 1 (or 2)
- Min TPC power is set to 17dbm in RRM settings
- Channel Utilization > 30% on 3 APs

# Clue number 4



```
  SNR    45 dB.................................. 1 clients
Nearby APs
   AP 70:b3:17:bf:df:0f slot 1..................  -87 dBm on  60  20MHz
   AP 70:b3:17:ea:30:8f slot 1..................  -90 dBm on  36 | 20MHz
   AP f4:db:e6:d2:85:e0 slot 0..................  -87 dBm on  44  20MHz
   AP f4:db:e6:d2:85:ef slot 1..................  -87 dBm on  64  20MHz
   AP f4:db:e6:d2:87:0f slot 1..................  -73 dBm on  60  20MHz
   AP f4:db:e6:d2:88:cf slot 1..................  -90 dBm on  40  20MHz
   AP f4:db:e6:dc:22:ef slot 1..................  -90 dBm on  44  20MHz
   AP f4:db:e6:dc:24:2f slot 1..................  -69 dBm on  36  20MHz
   AP f4:db:e6:e4:65:af slot 1..................  -79 dBm on  60  20MHz
   AP f4:db:e6:e4:6e:cf slot 1..................  -65 dBm on  48  20MHz
   AP f4:db:e6:e4:70:af slot 1..................  -67 dBm on  40  20MHz
   AP f4:db:e6:e4:71:0f slot 1..................  -84 dBm on  56  20MHz
   AP f4:db:e6:e4:7a:8f slot 1..................  -81 dBm on  36  20MHz
   AP f4:db:e6:e4:7e:0f slot 1..................  -77 dBm on  40  20MHz
Radar Information
```

- Before, people were using 7925s
- Some APs in default AP group not broadcasting voice SSID
- All APs at power level 1 (or 2)
- Min TPC power is set to 17dbm in RRM settings
- Channel Utilization > 30% on 3 APs
- Many channels in UNII2 are not enabled in DCA, on channel neighbor count is high for some APs
- APs were hearing each other fairly low

# Clue number 4

- Before, people were using 7925s
- Some APs in default AP group not broadcasting voice SSID
- All APs at power level 1 (or 2)
- Min TPC power is set to 17dbm in RRM settings
- Channel Utilization > 30% on 3 APs
- Many channels in UNII2 are not enabled in DCA, on channel neighbor count is high for some APs
- APs were not hearing each other very loudly
- 30% APs on Channel 36

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Clue number 4

- How about before ? How can we figure out if the problem is new ?

- Having stored show run-config or show tech wireless from “back in the days” is very useful
- All APs were already at power level 1 or 2 7 years before
- Even in absolute measure (i.e. dBm) the APs were at the same transmit power (17dBm)
- WLC shows how many clients are connected at low RSSI (worse than -75). That represented 35% of the clients back then

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Story conclusions

# Story conclusion

- Probably voice over Wifi was always a terrible experience
- Maybe the handsets were less used before, or parallel DECT system was in place
- Maybe it somewhat worked, but there is additional load wireless network
- Maybe it’s the nurse/doctor work pattern related to COVID, increasing failures

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Story summary

- Many healthcare voice escalations are related to suboptimal (or completely outdated) deployment
- Doing a basic verification costs less than letting things escalate
- Complex troubleshooting can be costly and require several skilled engineer on site, but a basic verification can be done remotely or easily with low involvement of people on site

# Key takeaways: Easy verification action plan

- Walk around with 8821 in site survey mode. Check there is -67 everywhere
- Check if QoS is in use on active calls (logs / OTA capture)
- Check phone logs to see if it stays within good RSSI range
- Check load and interference levels
- Wireless Config Analyzer Express !!!!

- If you have a good RSSI and are using QoS to get priority access to the medium, things shouldn’t be too bad already.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# The complicated action plan

- Simultaneous sniffer capture over the air (may require to remove encryption)
- Phone logs, client debugs from the WLC

# Design key takeaways

- Always design for the end device the customer will use
- Survey where and how the actual users use the network !
- Place APs where the users are, not where it’s convenient to place them
- Review your design every few years.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# But what exactly happened to that hospital ?

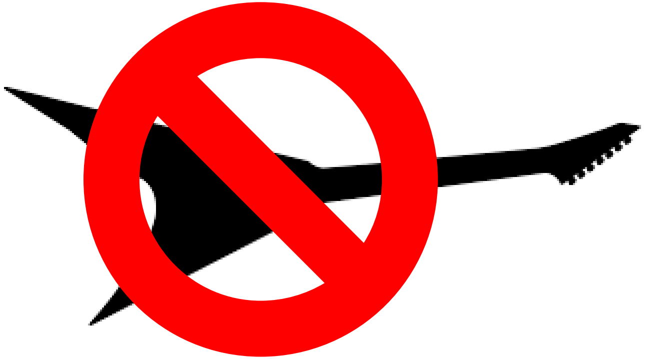
- New site survey advised:
  - increase of 30% of APs
  - overall AP repositioning
- Creates new problem: Not enough switchports per floor
- Creates new-new problem: no budget for network redesign

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Tips and tricks

If you are alone on site

- One end of the call is wired (Wired ip phone or laptop)
- Other end is your wireless handset
- Play music on the wired phone side
- Best is music you know the lyrics of. Lyrics get distorted first



# Tools covered

- WLCCA/WCAE
- TAC recommended releases documents
- Wireless sniffing tools

**Achievement Unlocked!**
Site survey expert

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Troubleshooting voice/encrypted streams

# The context

- Voice over Wi-FI
- 300 Iphone 7, few Iphone SE
- Cisco Jabber app
- Cisco Wi-Fi network

# The problem

- Various voice gaps during calls
- Some random
- Some at strangely regular intervals

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Capture 1 : iphone through USB

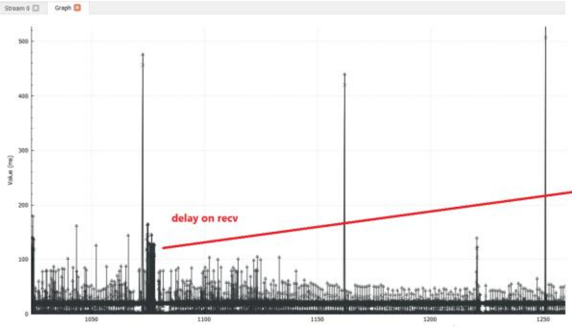
- Airtool allow you to capture on the iphone
  - Post 802.11 layer
  - Not OTA

- Shows unencrypted RTP traffic

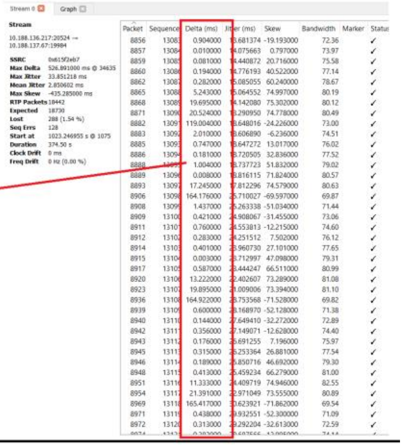
- Demo time!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Capture 1



Receiving side



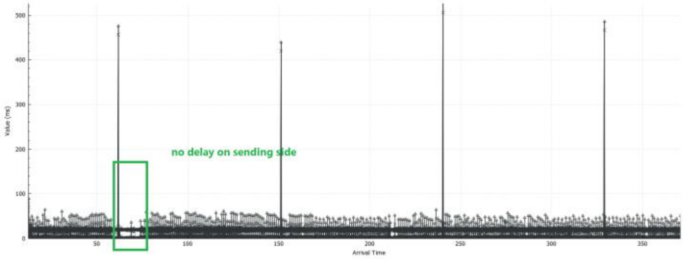
**Stream**

10.188.136.217:20524 →
10.188.137.67:19984

**SSRC** 0x615f2eb7
**Max Delta** 526.891000 ms @ 34635
**Max Jitter** 33.851218 ms
**Mean Jitter** 2.850602 ms
**Max Skew** -435.285000 ms
**RTP Packets** 18442
**Expected** 18730
**Lost** 288 (1.54 %)
**Seq Errs** 128
**Start at** 1023.246955 s @ 1075
**Duration** 374.50 s
**Clock Drift** 0 ms
**Freq Drift** 0 Hz (0.00 %)

| Packet | Sequence | Delta (ms) | Jitter (ms) | Skew | Bandwidth | Marker | Status |
|---|---|---|---|---|---|---|---|
| 8856 | 13083 | 0.904000 | 13.681374 | -19.193000 | 72.36 | | ✓ |
| 8857 | 13084 | 0.010000 | 14.075663 | 0.797000 | 73.97 | | ✓ |
| 8859 | 13085 | 0.081000 | 14.440872 | 20.716000 | 75.58 | | ✓ |
| 8860 | 13086 | 0.194000 | 14.776193 | 40.522000 | 77.14 | | ✓ |
| 8862 | 13087 | 0.282000 | 15.085055 | 60.240000 | 78.67 | | ✓ |
| 8865 | 13088 | 5.243000 | 15.064552 | 74.997000 | 80.19 | | ✓ |
| 8868 | 13089 | 19.695000 | 14.142080 | 75.302000 | 80.12 | | ✓ |
| 8871 | 13090 | 20.524000 | 13.290950 | 74.778000 | 80.49 | | ✓ |
| 8882 | 13091 | 119.004000 | 18.648016 | -24.226000 | 73.00 | | ✓ |
| 8883 | 13092 | 2.010000 | 18.606890 | -6.236000 | 74.51 | | ✓ |
| 8885 | 13093 | 0.747000 | 18.647272 | 13.017000 | 76.02 | | ✓ |
| 8886 | 13094 | 0.181000 | 18.720505 | 32.836000 | 77.52 | | ✓ |
| 8888 | 13095 | 1.004000 | 18.737723 | 51.832000 | 79.02 | | ✓ |
| 8889 | 13096 | 0.008000 | 18.816115 | 71.824000 | 80.57 | | ✓ |
| 8893 | 13097 | 17.245000 | 17.812296 | 74.579000 | 80.63 | | ✓ |
| 8906 | 13098 | 164.176000 | 25.710027 | -69.597000 | 69.87 | | ✓ |
| 8908 | 13099 | 1.437000 | 25.263338 | -51.034000 | 71.44 | | ✓ |
| 8909 | 13100 | 0.421000 | 24.908067 | -31.455000 | 73.06 | | ✓ |
| 8911 | 13101 | 0.760000 | 24.553813 | -12.215000 | 74.60 | | ✓ |
| 8912 | 13102 | 0.283000 | 24.251512 | 7.502000 | 76.12 | | ✓ |
| 8914 | 13103 | 0.401000 | 23.960730 | 27.101000 | 77.65 | | ✓ |
| 8915 | 13104 | 0.003000 | 23.712997 | 47.098000 | 79.31 | | ✓ |
| 8917 | 13105 | 0.587000 | 23.444247 | 66.511000 | 80.99 | | ✓ |
| 8920 | 13106 | 13.222000 | 22.402607 | 73.289000 | 81.08 | | ✓ |
| 8923 | 13107 | 19.895000 | 21.009006 | 73.394000 | 81.10 | | ✓ |
| 8936 | 13108 | 164.922000 | 28.753568 | -71.528000 | 69.82 | | ✓ |
| 8939 | 13109 | 0.600000 | 28.168970 | -52.128000 | 71.38 | | ✓ |
| 8940 | 13110 | 0.144000 | 27.649410 | -32.272000 | 72.89 | | ✓ |
| 8942 | 13111 | 0.356000 | 27.149071 | -12.628000 | 74.40 | | ✓ |
| 8943 | 13112 | 0.176000 | 26.691255 | 7.196000 | 75.97 | | ✓ |
| 8945 | 13113 | 0.315000 | 26.253364 | 26.881000 | 77.54 | | ✓ |
| 8946 | 13114 | 0.189000 | 25.850716 | 46.692000 | 79.30 | | ✓ |
| 8948 | 13115 | 0.413000 | 25.459234 | 66.279000 | 81.00 | | ✓ |
| 8951 | 13116 | 11.333000 | 24.409719 | 74.946000 | 82.55 | | ✓ |
| 8954 | 13117 | 21.391000 | 22.971049 | 73.555000 | 80.89 | | ✓ |
| 8969 | 13118 | 165.417000 | 30.623921 | -71.862000 | 69.54 | | ✓ |
| 8971 | 13119 | 0.438000 | 29.932551 | -52.300000 | 71.09 | | ✓ |
| 8972 | 13120 | 0.313000 | 29.292204 | -32.613000 | 72.59 | | ✓ |

Sending side



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

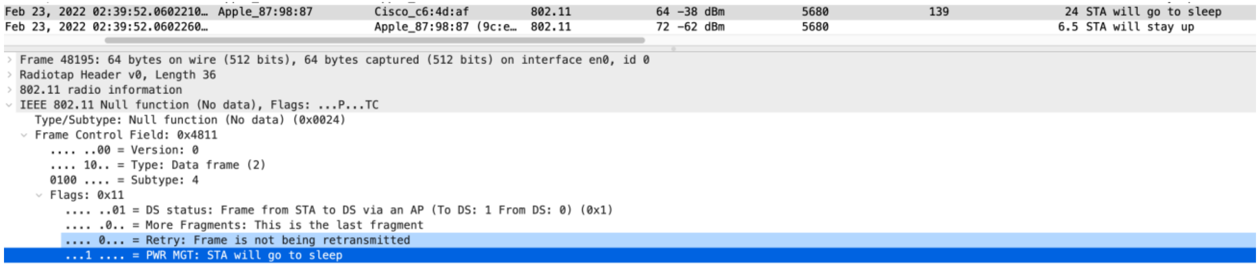
# Capture 2 – the OTA

- QOS in place?

wlan.addr == 9c:e6:5e:87:98:87 && (wlan.fc.type_subtype == 0x0028)  &&  (wlan.qos.tid==6)

- Sort by the delta column

Frame has a P flag ! One iphone goes to sleep, which causes voice traffic to be buffered



```
Feb 23, 2022 02:39:52.0602210…  Apple_87:98:87       Cisco_c6:4d:af       802.11          64 -38 dBm          5680            139                 24 STA will go to sleep
Feb 23, 2022 02:39:52.0602260…                       Apple_87:98:87 (9c:e…  802.11          72 -62 dBm          5680                               6.5 STA will stay up

> Frame 48195: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface en0, id 0
> Radiotap Header v0, Length 36
> 802.11 radio information
v IEEE 802.11 Null function (No data), Flags: ...P...TC
    Type/Subtype: Null function (No data) (0x0024)
  v Frame Control Field: 0x4811
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    v Flags: 0x11
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...1 .... = PWR MGT: STA will go to sleep
```

© 2023  Cisco and/or its affiliates. All rights reserved.   Cisco Public

# Wireshark name resolution

- Wireshark can optionally resolve IP addresses using your laptop DNS
- It can also resolve IP addresses using DNS requests that appear in the capture
- You can also add manual/static mappings IP-to-name on your laptop. Right-click on the packet -> Edit resolved names
- This can also be done with MAC addresses !
  - Go to $home/.config/wireshark/ and edit “ethers” on Mac OS
  - Go to %app data%/roaming/Wireshark on Windows and edit the “ethers” file

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Story conclusions

# Encrypted capture analysis

- Limited understanding on what it what
- No per-protocol analysis

But you CAN

- Guess traffic types
  - QoS-tagged traffic can be identified
  - Voice is a regular back-and-forth of small packets
  - DHCP is sent immediately after an association/WPA handshake
- Identify signal strength issues, roaming issues, unexpected disconnections
- Take a look at the retry rate

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Tools covered

- Wireshark
- RTP analysis
- Name resolution
- Filtering

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# What happened to that hospital ?

- One issue was a 500ms voice gaps every 90s, which was an interop issue between Jabber and Iphone 7.
- Iphone SEs did not have the problem, nor Webex app did not have the problem either.
- No issues on Wireless network
- Jabber developers were able to improve the experience and have the iPhone go to sleep mode much less while on call

**Achievement Unlocked!**

Voice WLAN expert

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Of Mines and Men (and WGBs)

# Underground mine : the context

# Underground mine : WGB losing connectivity

```
debug dot11 dot11Radio 1 trace print uplink
debug dot11 client debug dot11 dot11radio 0 print lines 0
debug dot11 dot11radio 0 monitor address XXXX.XXXX.XXXX
debug dot11 dot11radio 0 trace print cli mgmt key uplink xmt
rcv rates client
```

WGB is losing connectivity every now and then and reconnects quickly

```
Jun 12 12:48:20.463: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Received deauthenticate (7) not authenticated

Jun 12 12:48:20.647: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0, Associated To AP K1165-BL34-211 bc26.c78a.0a63 [None WPAv2 PSK]
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Underground mine : WGB losing connectivity

Interface Dot11Radio x
packet retries 32 drop

```
Jun 18 10:20:48.184: %DOT11-4-UPLINK_DOWN: Interface
Dot11Radio0, parent lost: Too many retries

Jun 18 10:20:48.184: 3D38D457-0 Uplink: Lost AP, Too many
retries

Jun 18 10:20:48.184: 3D38D4B8-0 Uplink: Setting No. of retries
in channel scan to 2

Jun 18 10:20:48.184: 3D38D4BD-0 Uplink: Wait for driver to stop

Jun 18 10:20:48.184: 3D38D6EF-0 Uplink: Enabling active scan
```

# Underground mine : WGB losing connectivity

```
config ap client-trace address add <wgb_MAC-address>
config ap client-trace filter all enable
config ap client-trace output console-log enable
config ap client-trace start term mon
```

Maybe the root AP is changing channel ?

Maybe the root AP channel is congested ? (carrier busy test)

Maybe root AP disconnects from WLC regularly ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

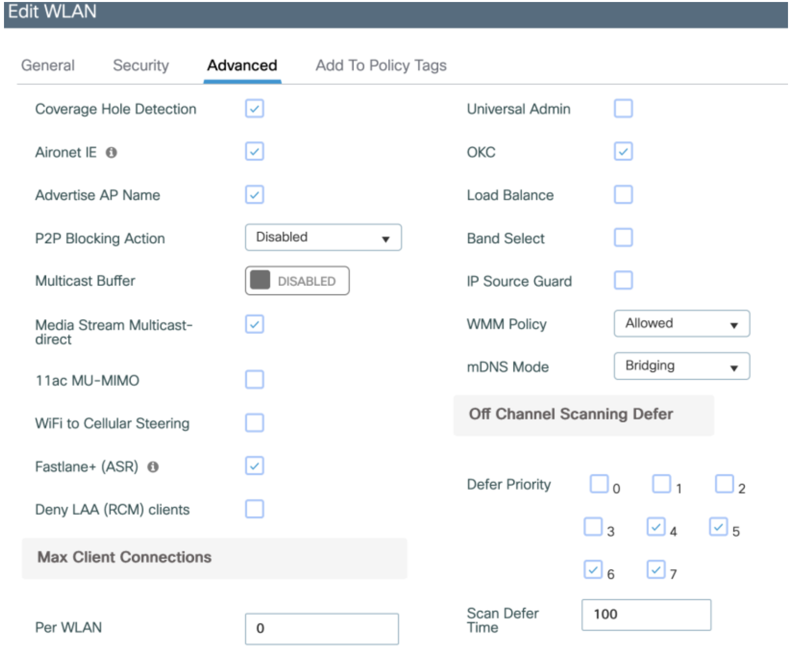
# Underground mine : WGB losing connectivity

## What is off-channel scan defer ?

Per User Priority

Postpones scan if frame is received on that UP

UP 0 would lead no more off-channel scan at all



Edit WLAN

Coverage Hole Detection ☑

Aironet IE ☑

Advertise AP Name ☑

P2P Blocking Action: Disabled

Multicast Buffer: DISABLED

Media Stream Multicast-direct ☑

11ac MU-MIMO □

WiFi to Cellular Steering □

Fastlane+ (ASR) ☑

Deny LAA (RCM) clients □

**Max Client Connections**

Per WLAN: 0

Universal Admin □

OKC ☑

Load Balance □

Band Select □

IP Source Guard □

WMM Policy: Allowed

mDNS Mode: Bridging

**Off Channel Scanning Defer**

Defer Priority: □ 0 □ 1 □ 2 □ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7

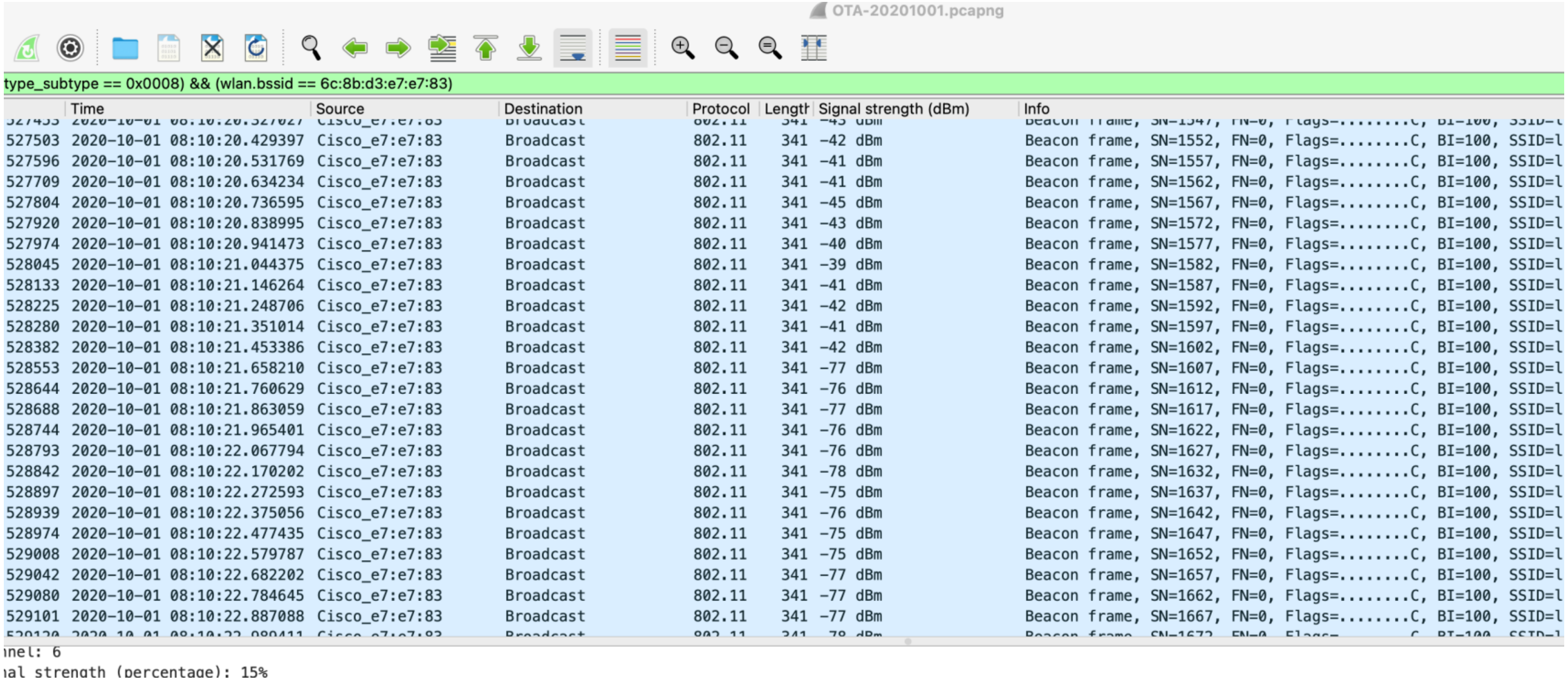
Scan Defer Time: 100

# Underground mine : WGB losing connectivity

1. Lost beacons (Interface Dot11Radio0, parent lost: Missed beacons)
2. Low power (Interface Dot11Radio0, parent lost: Signal strength too low

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Underground mine : WGB losing connectivity

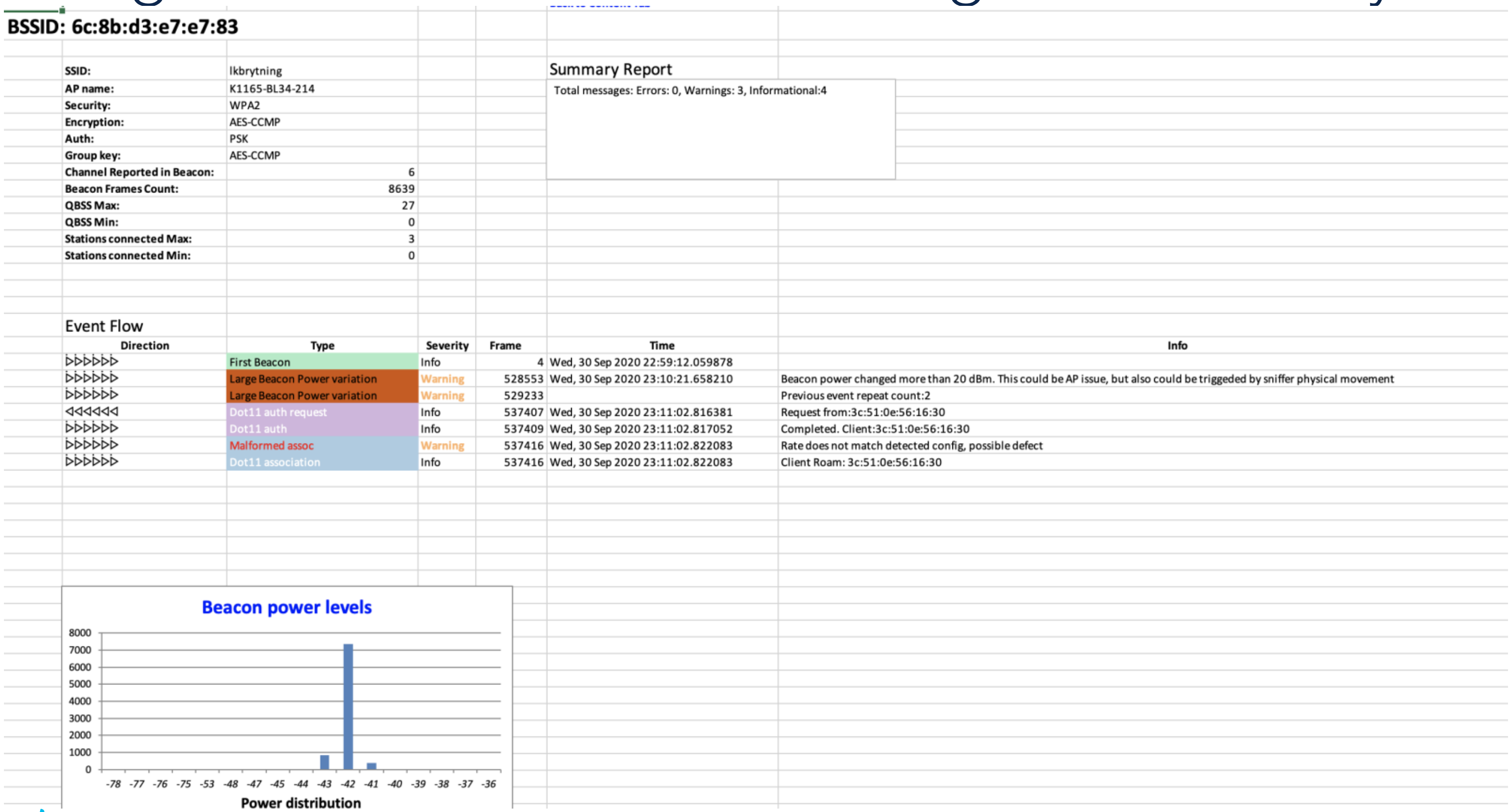


```
type_subtype == 0x0008) && (wlan.bssid == 6c:8b:d3:e7:e7:83)
```

```
       Time                          Source              Destination       Protocol  Length Signal strength (dBm)  Info
527453 2020-10-01 08:10:20.327027 Cisco_e7:e7:83 Broadcast 802.11 341 -43 dBm Beacon frame, SN=1547, FN=0, Flags=........C, BI=100, SSID=l
527503 2020-10-01 08:10:20.429397 Cisco_e7:e7:83 Broadcast 802.11 341 -42 dBm Beacon frame, SN=1552, FN=0, Flags=........C, BI=100, SSID=l
527596 2020-10-01 08:10:20.531769 Cisco_e7:e7:83 Broadcast 802.11 341 -41 dBm Beacon frame, SN=1557, FN=0, Flags=........C, BI=100, SSID=l
527709 2020-10-01 08:10:20.634234 Cisco_e7:e7:83 Broadcast 802.11 341 -41 dBm Beacon frame, SN=1562, FN=0, Flags=........C, BI=100, SSID=l
527804 2020-10-01 08:10:20.736595 Cisco_e7:e7:83 Broadcast 802.11 341 -45 dBm Beacon frame, SN=1567, FN=0, Flags=........C, BI=100, SSID=l
527920 2020-10-01 08:10:20.838995 Cisco_e7:e7:83 Broadcast 802.11 341 -43 dBm Beacon frame, SN=1572, FN=0, Flags=........C, BI=100, SSID=l
527974 2020-10-01 08:10:20.941473 Cisco_e7:e7:83 Broadcast 802.11 341 -40 dBm Beacon frame, SN=1577, FN=0, Flags=........C, BI=100, SSID=l
528045 2020-10-01 08:10:21.044375 Cisco_e7:e7:83 Broadcast 802.11 341 -39 dBm Beacon frame, SN=1582, FN=0, Flags=........C, BI=100, SSID=l
528133 2020-10-01 08:10:21.146264 Cisco_e7:e7:83 Broadcast 802.11 341 -41 dBm Beacon frame, SN=1587, FN=0, Flags=........C, BI=100, SSID=l
528225 2020-10-01 08:10:21.248706 Cisco_e7:e7:83 Broadcast 802.11 341 -42 dBm Beacon frame, SN=1592, FN=0, Flags=........C, BI=100, SSID=l
528280 2020-10-01 08:10:21.351014 Cisco_e7:e7:83 Broadcast 802.11 341 -41 dBm Beacon frame, SN=1597, FN=0, Flags=........C, BI=100, SSID=l
528382 2020-10-01 08:10:21.453386 Cisco_e7:e7:83 Broadcast 802.11 341 -42 dBm Beacon frame, SN=1602, FN=0, Flags=........C, BI=100, SSID=l
528553 2020-10-01 08:10:21.658210 Cisco_e7:e7:83 Broadcast 802.11 341 -77 dBm Beacon frame, SN=1607, FN=0, Flags=........C, BI=100, SSID=l
528644 2020-10-01 08:10:21.760629 Cisco_e7:e7:83 Broadcast 802.11 341 -76 dBm Beacon frame, SN=1612, FN=0, Flags=........C, BI=100, SSID=l
528688 2020-10-01 08:10:21.863059 Cisco_e7:e7:83 Broadcast 802.11 341 -77 dBm Beacon frame, SN=1617, FN=0, Flags=........C, BI=100, SSID=l
528744 2020-10-01 08:10:21.965401 Cisco_e7:e7:83 Broadcast 802.11 341 -76 dBm Beacon frame, SN=1622, FN=0, Flags=........C, BI=100, SSID=l
528793 2020-10-01 08:10:22.067794 Cisco_e7:e7:83 Broadcast 802.11 341 -76 dBm Beacon frame, SN=1627, FN=0, Flags=........C, BI=100, SSID=l
528842 2020-10-01 08:10:22.170202 Cisco_e7:e7:83 Broadcast 802.11 341 -78 dBm Beacon frame, SN=1632, FN=0, Flags=........C, BI=100, SSID=l
528897 2020-10-01 08:10:22.272593 Cisco_e7:e7:83 Broadcast 802.11 341 -75 dBm Beacon frame, SN=1637, FN=0, Flags=........C, BI=100, SSID=l
528939 2020-10-01 08:10:22.375056 Cisco_e7:e7:83 Broadcast 802.11 341 -76 dBm Beacon frame, SN=1642, FN=0, Flags=........C, BI=100, SSID=l
528974 2020-10-01 08:10:22.477435 Cisco_e7:e7:83 Broadcast 802.11 341 -75 dBm Beacon frame, SN=1647, FN=0, Flags=........C, BI=100, SSID=l
529008 2020-10-01 08:10:22.579787 Cisco_e7:e7:83 Broadcast 802.11 341 -75 dBm Beacon frame, SN=1652, FN=0, Flags=........C, BI=100, SSID=l
529042 2020-10-01 08:10:22.682202 Cisco_e7:e7:83 Broadcast 802.11 341 -77 dBm Beacon frame, SN=1657, FN=0, Flags=........C, BI=100, SSID=l
529080 2020-10-01 08:10:22.784645 Cisco_e7:e7:83 Broadcast 802.11 341 -77 dBm Beacon frame, SN=1662, FN=0, Flags=........C, BI=100, SSID=l
529101 2020-10-01 08:10:22.887088 Cisco_e7:e7:83 Broadcast 802.11 341 -77 dBm Beacon frame, SN=1667, FN=0, Flags=........C, BI=100, SSID=l
529120 2020-10-01 08:10:22.989411 Cisco_e7:e7:83 Broadcast 802.11 341 -78 dBm Beacon frame, SN=1672, FN=0, Flags=........C, BI=100, SSID=l
```

```
nel: 6
al strength (percentage): 15%
```

# Underground mine : WGB losing connectivity



## BSSID: 6c:8b:d3:e7:e7:83

| | |
|---|---|
| **SSID:** | lkbrytning |
| **AP name:** | K1165-BL34-214 |
| **Security:** | WPA2 |
| **Encryption:** | AES-CCMP |
| **Auth:** | PSK |
| **Group key:** | AES-CCMP |
| **Channel Reported in Beacon:** | 6 |
| **Beacon Frames Count:** | 8639 |
| **QBSS Max:** | 27 |
| **QBSS Min:** | 0 |
| **Stations connected Max:** | 3 |
| **Stations connected Min:** | 0 |

Summary Report

Total messages: Errors: 0, Warnings: 3, Informational:4

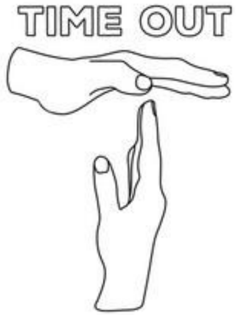
Event Flow

| Direction | Type | Severity | Frame | Time | Info |
|---|---|---|---|---|---|
| ▷▷▷▷▷▷ | First Beacon | Info | 4 | Wed, 30 Sep 2020 22:59:12.059878 | |
| ▷▷▷▷▷▷ | Large Beacon Power variation | Warning | 528553 | Wed, 30 Sep 2020 23:10:21.658210 | Beacon power changed more than 20 dBm. This could be AP issue, but also could be triggeded by sniffer physical movement |
| ▷▷▷▷▷▷ | Large Beacon Power variation | Warning | 529233 | | Previous event repeat count:2 |
| ◁◁◁◁◁◁ | Dot11 auth request | Info | 537407 | Wed, 30 Sep 2020 23:11:02.816381 | Request from:3c:51:0e:56:16:30 |
| ▷▷▷▷▷▷ | Dot11 auth | Info | 537409 | Wed, 30 Sep 2020 23:11:02.817052 | Completed. Client:3c:51:0e:56:16:30 |
| ▷▷▷▷▷▷ | Malformed assoc | Warning | 537416 | Wed, 30 Sep 2020 23:11:02.822083 | Rate does not match detected config, possible defect |
| ▷▷▷▷▷▷ | Dot11 association | Info | 537416 | Wed, 30 Sep 2020 23:11:02.822083 | Client Roam: 3c:51:0e:56:16:30 |

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Wifi Hawk

https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!features/wifi-hawk-features

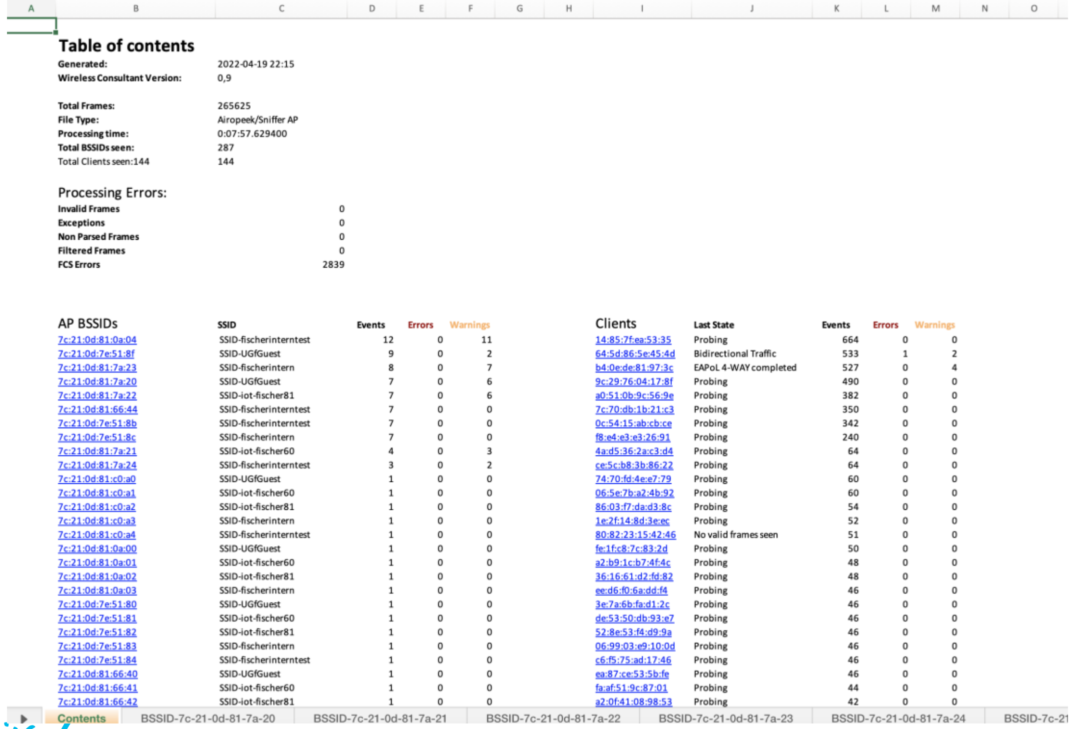


- Expert system to for wireless capture analysis
  - Identify hard to see issues found in huge files
  - Low level protocol analysis
  - Interoperability problems
- Event Flow: Generate a summary of events per client and AP WLANs
- Speed up event identification in a wireless capture
- Automated detection of 18 AP side problems and 16 client issues
- Highlight EAP authentication problems, EAP types
- 802.11 reason codes and status codes explained, including CCX and newer cisco extensions

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Wifi Hawk

https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!wifi-hawk-wireless-captures-analysis/key--features



## Table of contents

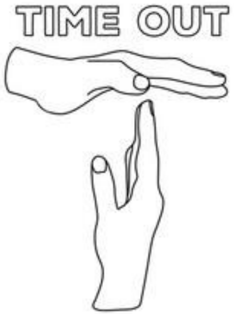
| | |
|---|---|
| **Generated:** | 2022-04-19 22:15 |
| **Wireless Consultant Version:** | 0,9 |
| | |
| **Total Frames:** | 265625 |
| **File Type:** | Airopeek/Sniffer AP |
| **Processing time:** | 0:07:57.629400 |
| **Total BSSIDs seen:** | 287 |
| Total Clients seen:144 | 144 |

Processing Errors:

| | |
|---|---|
| **Invalid Frames** | 0 |
| **Exceptions** | 0 |
| **Non Parsed Frames** | 0 |
| **Filtered Frames** | 0 |
| **FCS Errors** | 2839 |

| AP BSSIDs | SSID | Events | Errors | Warnings |
|---|---|---|---|---|
| 7c:21:0d:81:0a:04 | SSID-fischerinterntest | 12 | 0 | 11 |
| 7c:21:0d:7e:51:8f | SSID-UGfGuest | 9 | 0 | 2 |
| 7c:21:0d:81:7a:23 | SSID-fischerintern | 8 | 0 | 7 |
| 7c:21:0d:81:7a:20 | SSID-UGfGuest | 7 | 0 | 6 |
| 7c:21:0d:81:7a:22 | SSID-iot-fischer81 | 7 | 0 | 6 |
| 7c:21:0d:81:66:44 | SSID-fischerinterntest | 7 | 0 | 0 |
| 7c:21:0d:7e:51:8b | SSID-fischerinterntest | 7 | 0 | 0 |
| 7c:21:0d:7e:51:8c | SSID-fischerintern | 7 | 0 | 0 |
| 7c:21:0d:81:7a:21 | SSID-iot-fischer60 | 4 | 0 | 3 |
| 7c:21:0d:81:7a:24 | SSID-fischerinterntest | 3 | 0 | 2 |
| 7c:21:0d:81:c0:a0 | SSID-UGfGuest | 1 | 0 | 0 |
| 7c:21:0d:81:c0:a1 | SSID-iot-fischer60 | 1 | 0 | 0 |
| 7c:21:0d:81:c0:a2 | SSID-iot-fischer81 | 1 | 0 | 0 |
| 7c:21:0d:81:c0:a3 | SSID-fischerintern | 1 | 0 | 0 |
| 7c:21:0d:81:c0:a4 | SSID-fischerinterntest | 1 | 0 | 0 |
| 7c:21:0d:81:0a:00 | SSID-UGfGuest | 1 | 0 | 0 |
| 7c:21:0d:81:0a:01 | SSID-iot-fischer60 | 1 | 0 | 0 |
| 7c:21:0d:81:0a:02 | SSID-iot-fischer81 | 1 | 0 | 0 |
| 7c:21:0d:81:0a:03 | SSID-fischerintern | 1 | 0 | 0 |
| 7c:21:0d:7e:51:80 | SSID-UGfGuest | 1 | 0 | 0 |
| 7c:21:0d:7e:51:81 | SSID-iot-fischer60 | 1 | 0 | 0 |
| 7c:21:0d:7e:51:82 | SSID-iot-fischer81 | 1 | 0 | 0 |
| 7c:21:0d:7e:51:83 | SSID-fischerintern | 1 | 0 | 0 |
| 7c:21:0d:7e:51:84 | SSID-fischerinterntest | 1 | 0 | 0 |
| 7c:21:0d:81:66:40 | SSID-UGfGuest | 1 | 0 | 0 |
| 7c:21:0d:81:66:41 | SSID-iot-fischer60 | 1 | 0 | 0 |
| 7c:21:0d:81:66:42 | SSID-iot-fischer81 | 1 | 0 | 0 |

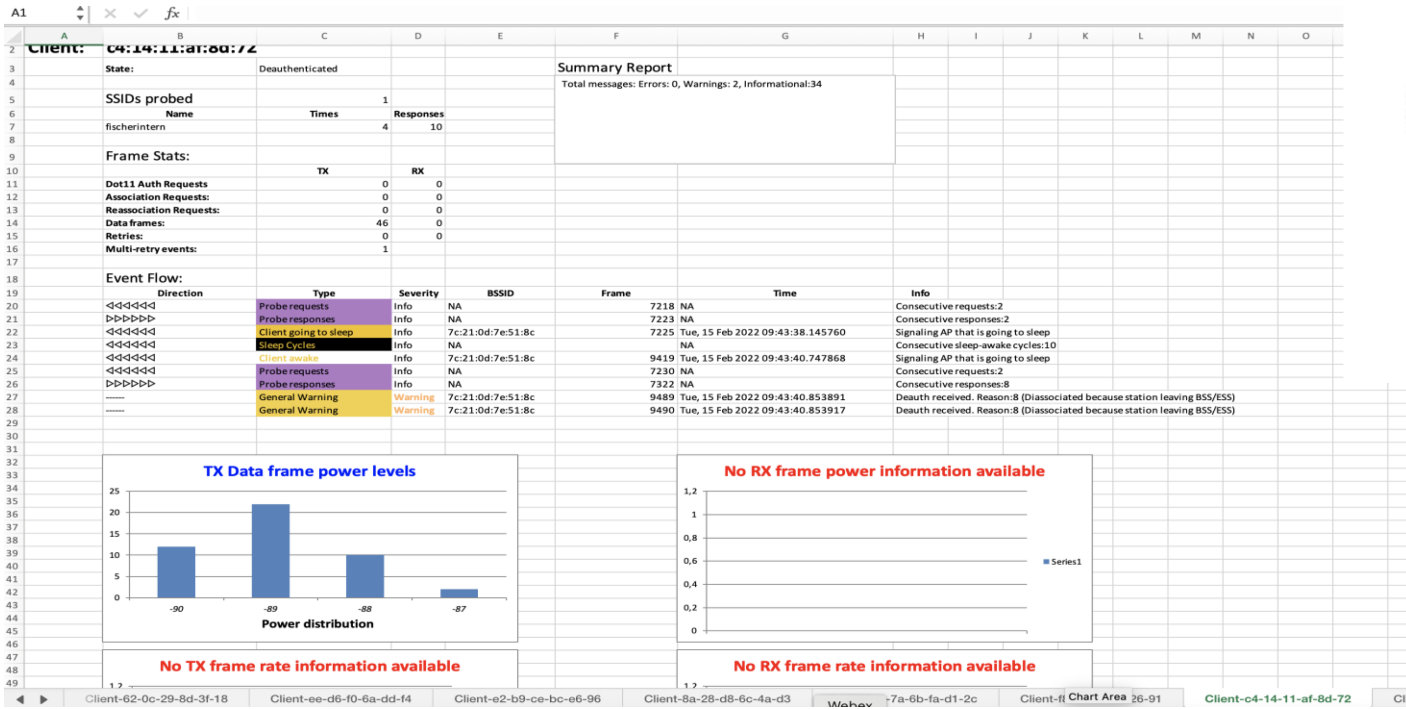
| Clients | Last State | Events | Errors | Warnings |
|---|---|---|---|---|
| 14:85:7f:ea:53:35 | Probing | 664 | 0 | 0 |
| 64:5d:86:5e:45:4d | Bidirectional Traffic | 533 | 1 | 2 |
| b4:0e:de:81:97:3c | EAPoL 4-WAY completed | 527 | 0 | 4 |
| 9c:29:76:04:17:8f | Probing | 490 | 0 | 0 |
| a0:51:0b:9c:56:9e | Probing | 382 | 0 | 0 |
| 7c:70:db:1b:21:c3 | Probing | 350 | 0 | 0 |
| 0c:54:15:ab:cb:ce | Probing | 342 | 0 | 0 |
| f8:e4:e3:e3:26:91 | Probing | 240 | 0 | 0 |
| 4a:d5:36:2a:c3:d4 | Probing | 64 | 0 | 0 |
| ce:5c:b8:3b:86:22 | Probing | 64 | 0 | 0 |
| 74:70:fd:4e:e7:79 | Probing | 60 | 0 | 0 |
| 06:5e:7b:a2:4b:92 | Probing | 60 | 0 | 0 |
| 86:03:f7:da:d3:8c | Probing | 54 | 0 | 0 |
| 1e:2f:14:8d:3e:ec | Probing | 52 | 0 | 0 |
| 80:82:23:15:42:46 | No valid frames seen | 51 | 0 | 0 |
| fe:1f:c8:7c:83:2d | Probing | 50 | 0 | 0 |
| a2:b9:1c:b7:4f:4c | Probing | 48 | 0 | 0 |
| 36:16:61:d2:fd:82 | Probing | 48 | 0 | 0 |
| ee:d6:f0:6a:dd:f4 | Probing | 46 | 0 | 0 |
| 3e:7a:6b:fa:d1:2c | Probing | 46 | 0 | 0 |
| de:53:50:db:93:e7 | Probing | 46 | 0 | 0 |
| 52:8e:53:f4:d9:9a | Probing | 46 | 0 | 0 |
| 06:99:03:e9:10:0d | Probing | 46 | 0 | 0 |
| c6:f5:75:ad:17:46 | Probing | 46 | 0 | 0 |
| ea:87:ce:53:5b:fe | Probing | 46 | 0 | 0 |
| fa:af:51:9c:87:01 | Probing | 44 | 0 | 0 |
| a2:0f:41:08:98:53 | Probing | 42 | 0 | 0 |



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Wifi Hawk

https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!wifi-hawk-wireless-captures-analysis/key--features



**Client:** c4:14:11:af:8d:72

| | | |
|---|---|---|
| State: | Deauthenticated | |

Summary Report

Total messages: Errors: 0, Warnings: 2, Informational:34

SSIDs probed 1

| Name | Times | Responses |
|---|---|---|
| fischerintern | 4 | 10 |

Frame Stats:

| | TX | RX |
|---|---|---|
| Dot11 Auth Requests | 0 | 0 |
| Association Requests: | 0 | 0 |
| Reassociation Requests: | 0 | 0 |
| Data frames: | 46 | 0 |
| Retries: | 0 | 0 |
| Multi-retry events: | 1 | |

Event Flow:

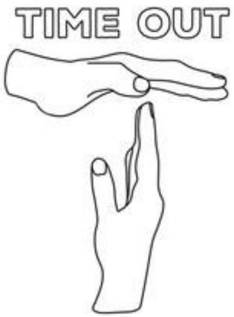
| Direction | Type | Severity | BSSID | Frame | Time | Info |
|---|---|---|---|---|---|---|
| ◁◁◁◁◁◁ | Probe requests | Info | NA | 7218 | NA | Consecutive requests:2 |
| ▷▷▷▷▷▷ | Probe responses | Info | NA | 7223 | NA | Consecutive responses:2 |
| ◁◁◁◁◁◁ | Client going to sleep | Info | 7c:21:0d:7e:51:8c | 7225 | Tue, 15 Feb 2022 09:43:38.145760 | Signaling AP that is going to sleep |
| ◁◁◁◁◁◁ | Sleep Cycles | Info | NA | | NA | Consecutive sleep-awake cycles:10 |
| ◁◁◁◁◁◁ | Client awake | Info | 7c:21:0d:7e:51:8c | 9419 | Tue, 15 Feb 2022 09:43:40.747868 | Signaling AP that is going to sleep |
| ◁◁◁◁◁◁ | Probe requests | Info | NA | 7230 | NA | Consecutive requests:2 |
| ▷▷▷▷▷▷ | Probe responses | Info | NA | 7322 | NA | Consecutive responses:8 |
| ------ | General Warning | Warning | 7c:21:0d:7e:51:8c | 9489 | Tue, 15 Feb 2022 09:43:40.853891 | Deauth received. Reason:8 (Diassociated because station leaving BSS/ESS) |
| ------ | General Warning | Warning | 7c:21:0d:7e:51:8c | 9490 | Tue, 15 Feb 2022 09:43:40.853917 | Deauth received. Reason:8 (Diassociated because station leaving BSS/ESS) |

TX Data frame power levels

No RX frame power information available

No TX frame rate information available

No RX frame rate information available



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Story conclusions

# Story conclusion

- Issues are not always easy to see.

- You need to understand what can your output prove for a fact or not

- In this case :
  - Randomly some beacons of the AP dropping by over 30 to 40dbm,
  - Sniffer not moving.
  - AP side issue, regardless of logs

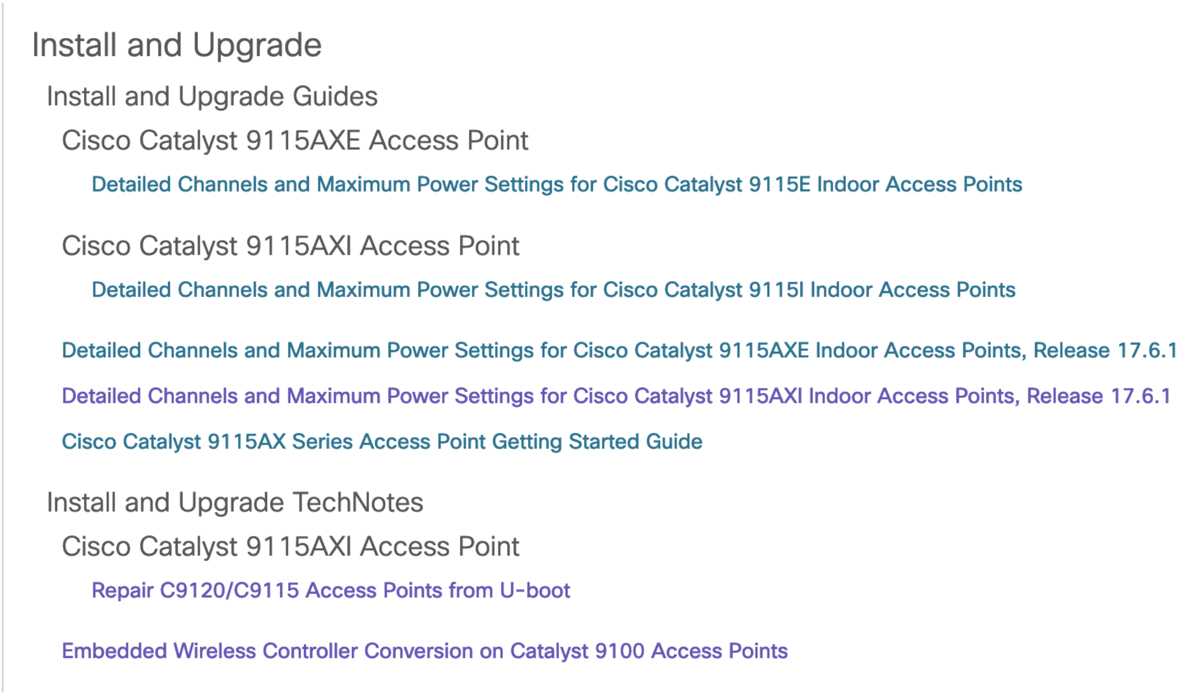
- This got solved through a fix on the 2800 infrastructure AP.

**Achievement Unlocked!**

PCAP or it didn't happen

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Which transmit power and channel to expect ?



## Install and Upgrade

### Install and Upgrade Guides

Cisco Catalyst 9115AXE Access Point

- Detailed Channels and Maximum Power Settings for Cisco Catalyst 9115E Indoor Access Points

Cisco Catalyst 9115AXI Access Point

- Detailed Channels and Maximum Power Settings for Cisco Catalyst 9115I Indoor Access Points

Detailed Channels and Maximum Power Settings for Cisco Catalyst 9115AXE Indoor Access Points, Release 17.6.1

Detailed Channels and Maximum Power Settings for Cisco Catalyst 9115AXI Indoor Access Points, Release 17.6.1

Cisco Catalyst 9115AX Series Access Point Getting Started Guide

### Install and Upgrade TechNotes

Cisco Catalyst 9115AXI Access Point

- Repair C9120/C9115 Access Points from U-boot

Embedded Wireless Controller Conversion on Catalyst 9100 Access Points

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Throughout issues in bank

# Throughput issues : context

- A bank moves their HQ a few buildings further down the block in a new state-of-the-art office right after COVID

Not the actual building but you get the idea =>

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Throughput issues : context

- They had a 5520 and 2800s in the old building and move to a 9800 with 9120s on the new building
- “More or less” the same configuration

- Old office still works great
- New office reports speed problems

# What probably happened

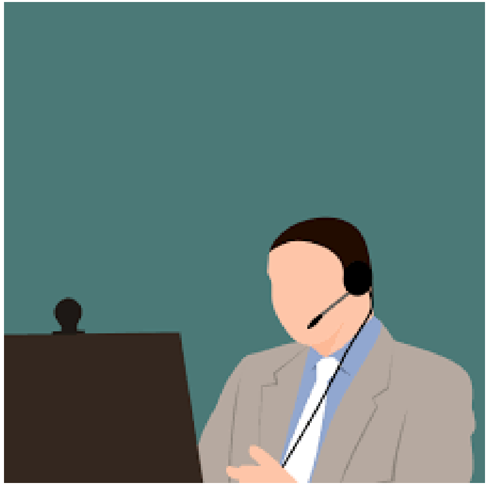
- Probably one engineer with their laptop went to the new office, tested connectivity and declared the new office was fit for purpose
- There was no clear report of the validation testing done
  - Same client type as the end users ?
  - Same type of applications in use ?
  - Same type of client density ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Throughput issues : the troubleshooting

Can you define what you mean with slow ?

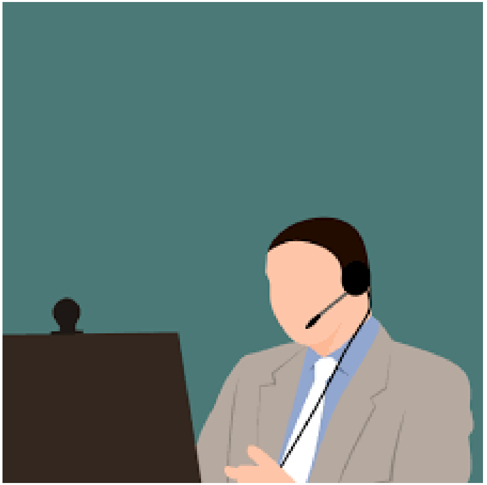
Very slow



# Throughput issues : the troubleshooting

Can you collect some Iperf tests ?

130Mbps



# What is slow ?

Slow can be : few kbps, few Mbps or “just 100Mbps instead of 800”

Step 1 : define

- Is everything equally slow ? Speedtest ? Local file transfer ? FTP ?
- Are all laptops affected equally ?
- Is it just browsing that’s giving a slow “feel” ?

# What is slow ?

- Customers may say the wifi is slow but in reality they mostly use one application (Citrix or similar)
- Different applications work in different way. A FTP transfer is a very simple TCP throughput test. Iperf is also your friend. Test TCP/UDP
- Browsing maybe be impacted by over fragmentation (adjust MSS) or latency
- If some clients are affected way more than others, you may be facing a driver-specific issue

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# What is slow ?

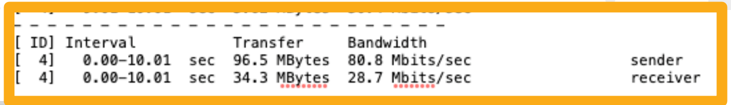
If the speed is objectively terrible (few kbps to few Mbps), it should be easy to observe

An over the air capture will show if there is any problem over the air. Examples :

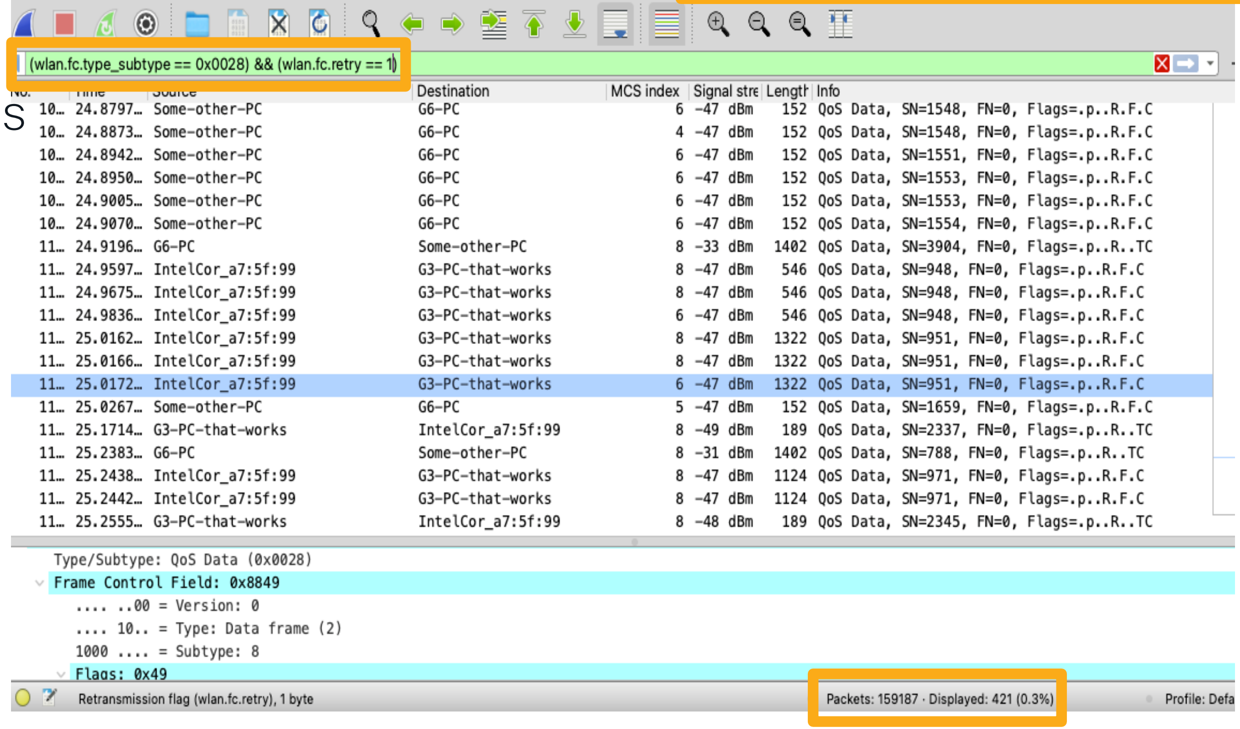
- Number of retried frames (as a ratio)
- Periods of gaps where AP or client is not answering
- Reconnections ?
- MCS data rates used

# Checking for possible reasons

- ☒ Bad RF
- ☒ Retransmissions



```
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  96.5 MBytes  80.8 Mbits/sec                  sender
[  4]   0.00-10.01  sec  34.3 MBytes  28.7 Mbits/sec                  receiver
```



```
(wlan.fc.type_subtype == 0x0028) && (wlan.fc.retry == 1)
```

| No. | Time | Source | Destination | MCS index | Signal stre | Length | Info |
|---|---|---|---|---|---|---|---|
| 10… | 24.8797… | Some-other-PC | G6-PC | 6 | -47 dBm | 152 | QoS Data, SN=1548, FN=0, Flags=.p..R.F.C |
| 10… | 24.8873… | Some-other-PC | G6-PC | 4 | -47 dBm | 152 | QoS Data, SN=1548, FN=0, Flags=.p..R.F.C |
| 10… | 24.8942… | Some-other-PC | G6-PC | 6 | -47 dBm | 152 | QoS Data, SN=1551, FN=0, Flags=.p..R.F.C |
| 10… | 24.8950… | Some-other-PC | G6-PC | 6 | -47 dBm | 152 | QoS Data, SN=1553, FN=0, Flags=.p..R.F.C |
| 10… | 24.9005… | Some-other-PC | G6-PC | 6 | -47 dBm | 152 | QoS Data, SN=1553, FN=0, Flags=.p..R.F.C |
| 10… | 24.9070… | Some-other-PC | G6-PC | 6 | -47 dBm | 152 | QoS Data, SN=1554, FN=0, Flags=.p..R.F.C |
| 11… | 24.9196… | G6-PC | Some-other-PC | 8 | -33 dBm | 1402 | QoS Data, SN=3904, FN=0, Flags=.p..R..TC |
| 11… | 24.9597… | IntelCor_a7:5f:99 | G3-PC-that-works | 8 | -47 dBm | 546 | QoS Data, SN=948, FN=0, Flags=.p..R.F.C |
| 11… | 24.9675… | IntelCor_a7:5f:99 | G3-PC-that-works | 8 | -47 dBm | 546 | QoS Data, SN=948, FN=0, Flags=.p..R.F.C |
| 11… | 24.9836… | IntelCor_a7:5f:99 | G3-PC-that-works | 6 | -47 dBm | 546 | QoS Data, SN=948, FN=0, Flags=.p..R.F.C |
| 11… | 25.0162… | IntelCor_a7:5f:99 | G3-PC-that-works | 8 | -47 dBm | 1322 | QoS Data, SN=951, FN=0, Flags=.p..R.F.C |
| 11… | 25.0166… | IntelCor_a7:5f:99 | G3-PC-that-works | 8 | -47 dBm | 1322 | QoS Data, SN=951, FN=0, Flags=.p..R.F.C |
| 11… | 25.0172… | IntelCor_a7:5f:99 | G3-PC-that-works | 6 | -47 dBm | 1322 | QoS Data, SN=951, FN=0, Flags=.p..R.F.C |
| 11… | 25.0267… | Some-other-PC | G6-PC | 5 | -47 dBm | 152 | QoS Data, SN=1659, FN=0, Flags=.p..R.F.C |
| 11… | 25.1714… | G3-PC-that-works | IntelCor_a7:5f:99 | 8 | -49 dBm | 189 | QoS Data, SN=2337, FN=0, Flags=.p..R..TC |
| 11… | 25.2383… | G6-PC | Some-other-PC | 8 | -31 dBm | 1402 | QoS Data, SN=788, FN=0, Flags=.p..R..TC |
| 11… | 25.2438… | IntelCor_a7:5f:99 | G3-PC-that-works | 8 | -47 dBm | 1124 | QoS Data, SN=971, FN=0, Flags=.p..R.F.C |
| 11… | 25.2442… | IntelCor_a7:5f:99 | G3-PC-that-works | 8 | -47 dBm | 1124 | QoS Data, SN=971, FN=0, Flags=.p..R.F.C |
| 11… | 25.2555… | G3-PC-that-works | IntelCor_a7:5f:99 | 8 | -48 dBm | 189 | QoS Data, SN=2345, FN=0, Flags=.p..R..TC |

```
    Type/Subtype: QoS Data (0x0028)
  ⌄ Frame Control Field: 0x8849
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ⌄ Flags: 0x49
```

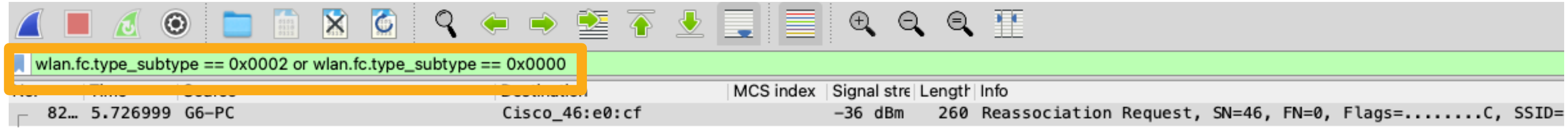
Retransmission flag (wlan.fc.retry), 1 byte

Packets: 159187 · Displayed: 421 (0.3%)

Profile: Defa

# Checking for possible reasons

❌ Reconnections

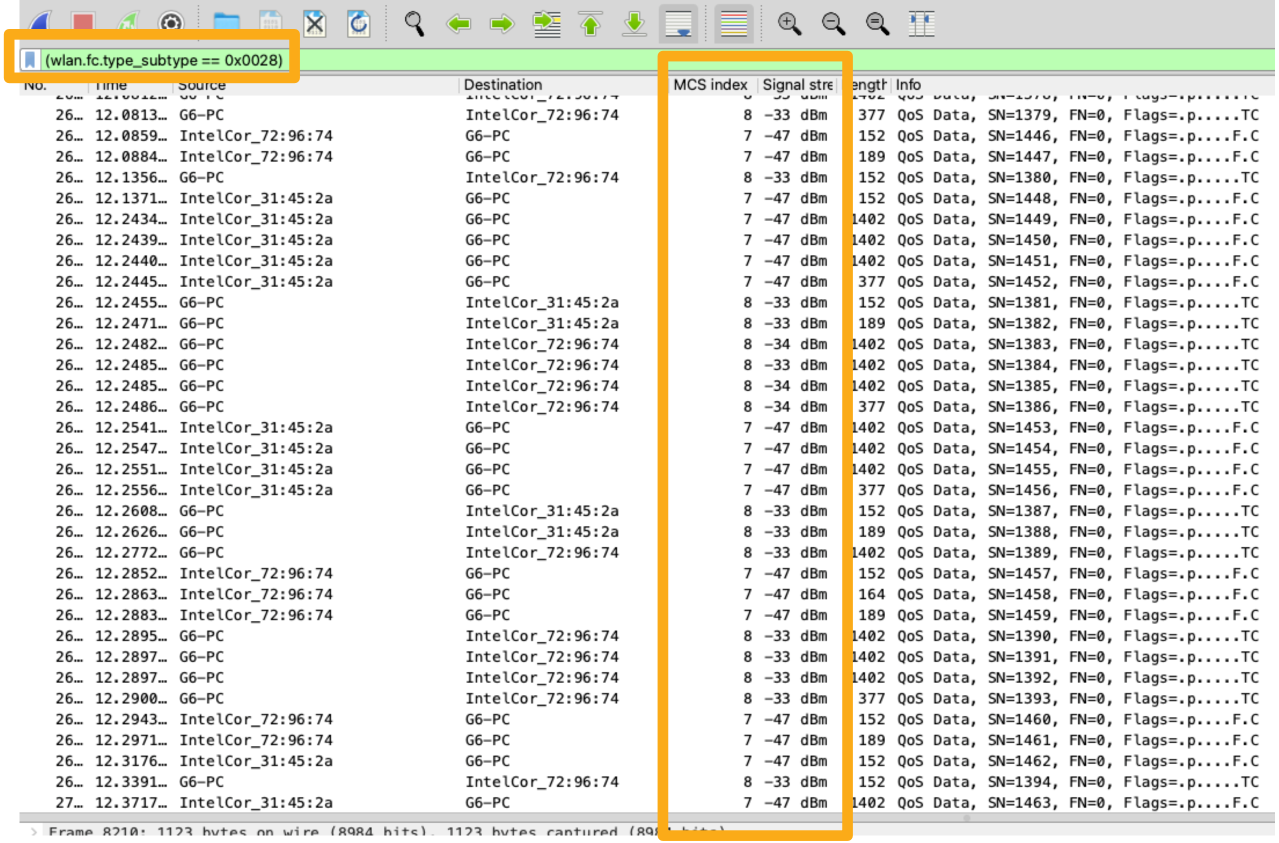


```
wlan.fc.type_subtype == 0x0002 or wlan.fc.type_subtype == 0x0000
```

```
                                                  MCS index  Signal stre  Lengtl  Info
82…  5.726999  G6-PC          Cisco_46:e0:cf                 -36 dBm        260   Reassociation Request, SN=46, FN=0, Flags=........C, SSID=
```

# Checking for possible reasons

- ❌ Bad data rate
- ❌ Bad RSSI



(wlan.fc.type_subtype == 0x0028)

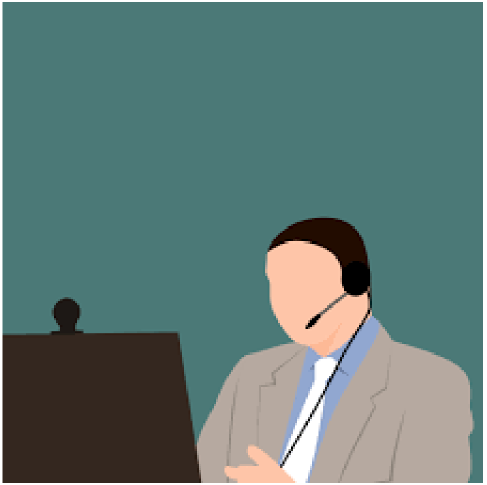
```
No.  Time      Source              Destination         MCS index  Signal stre  Length Info
26…  12.0813…  G6-PC               IntelCor_72:96:74           8  -33 dBm       377  QoS Data, SN=1379, FN=0, Flags=.p.....TC
26…  12.0859…  IntelCor_72:96:74   G6-PC                       7  -47 dBm       152  QoS Data, SN=1446, FN=0, Flags=.p....F.C
26…  12.0884…  IntelCor_72:96:74   G6-PC                       7  -47 dBm       189  QoS Data, SN=1447, FN=0, Flags=.p....F.C
26…  12.1356…  G6-PC               IntelCor_72:96:74           8  -33 dBm       152  QoS Data, SN=1380, FN=0, Flags=.p.....TC
26…  12.1371…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm       152  QoS Data, SN=1448, FN=0, Flags=.p....F.C
26…  12.2434…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm      1402  QoS Data, SN=1449, FN=0, Flags=.p....F.C
26…  12.2439…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm      1402  QoS Data, SN=1450, FN=0, Flags=.p....F.C
26…  12.2440…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm      1402  QoS Data, SN=1451, FN=0, Flags=.p....F.C
26…  12.2445…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm       377  QoS Data, SN=1452, FN=0, Flags=.p....F.C
26…  12.2455…  G6-PC               IntelCor_31:45:2a           8  -33 dBm       152  QoS Data, SN=1381, FN=0, Flags=.p.....TC
26…  12.2471…  G6-PC               IntelCor_31:45:2a           8  -33 dBm       189  QoS Data, SN=1382, FN=0, Flags=.p.....TC
26…  12.2482…  G6-PC               IntelCor_72:96:74           8  -34 dBm      1402  QoS Data, SN=1383, FN=0, Flags=.p.....TC
26…  12.2485…  G6-PC               IntelCor_72:96:74           8  -33 dBm      1402  QoS Data, SN=1384, FN=0, Flags=.p.....TC
26…  12.2485…  G6-PC               IntelCor_72:96:74           8  -34 dBm      1402  QoS Data, SN=1385, FN=0, Flags=.p.....TC
26…  12.2486…  G6-PC               IntelCor_72:96:74           8  -34 dBm       377  QoS Data, SN=1386, FN=0, Flags=.p.....TC
26…  12.2541…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm      1402  QoS Data, SN=1453, FN=0, Flags=.p....F.C
26…  12.2547…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm      1402  QoS Data, SN=1454, FN=0, Flags=.p....F.C
26…  12.2551…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm      1402  QoS Data, SN=1455, FN=0, Flags=.p....F.C
26…  12.2556…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm       377  QoS Data, SN=1456, FN=0, Flags=.p....F.C
26…  12.2608…  G6-PC               IntelCor_31:45:2a           8  -33 dBm       152  QoS Data, SN=1387, FN=0, Flags=.p.....TC
26…  12.2626…  G6-PC               IntelCor_31:45:2a           8  -33 dBm       189  QoS Data, SN=1388, FN=0, Flags=.p.....TC
26…  12.2772…  G6-PC               IntelCor_72:96:74           8  -33 dBm      1402  QoS Data, SN=1389, FN=0, Flags=.p.....TC
26…  12.2852…  IntelCor_72:96:74   G6-PC                       7  -47 dBm       152  QoS Data, SN=1457, FN=0, Flags=.p....F.C
26…  12.2863…  IntelCor_72:96:74   G6-PC                       7  -47 dBm       164  QoS Data, SN=1458, FN=0, Flags=.p....F.C
26…  12.2883…  IntelCor_72:96:74   G6-PC                       7  -47 dBm       189  QoS Data, SN=1459, FN=0, Flags=.p....F.C
26…  12.2895…  G6-PC               IntelCor_72:96:74           8  -33 dBm      1402  QoS Data, SN=1390, FN=0, Flags=.p.....TC
26…  12.2897…  G6-PC               IntelCor_72:96:74           8  -33 dBm      1402  QoS Data, SN=1391, FN=0, Flags=.p.....TC
26…  12.2897…  G6-PC               IntelCor_72:96:74           8  -33 dBm      1402  QoS Data, SN=1392, FN=0, Flags=.p.....TC
26…  12.2900…  G6-PC               IntelCor_72:96:74           8  -33 dBm       377  QoS Data, SN=1393, FN=0, Flags=.p.....TC
26…  12.2943…  IntelCor_72:96:74   G6-PC                       7  -47 dBm       152  QoS Data, SN=1460, FN=0, Flags=.p....F.C
26…  12.2971…  IntelCor_72:96:74   G6-PC                       7  -47 dBm       189  QoS Data, SN=1461, FN=0, Flags=.p....F.C
26…  12.3176…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm       152  QoS Data, SN=1462, FN=0, Flags=.p....F.C
26…  12.3391…  G6-PC               IntelCor_72:96:74           8  -33 dBm       152  QoS Data, SN=1394, FN=0, Flags=.p.....TC
27…  12.3717…  IntelCor_31:45:2a   G6-PC                       7  -47 dBm      1402  QoS Data, SN=1463, FN=0, Flags=.p....F.C
> Frame 8210: 1123 bytes on wire (8984 bits), 1123 bytes captured (89
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Throughput issues : the troubleshooting

Can you be more specific ?

Files transfers are slow and meetings are bad as well

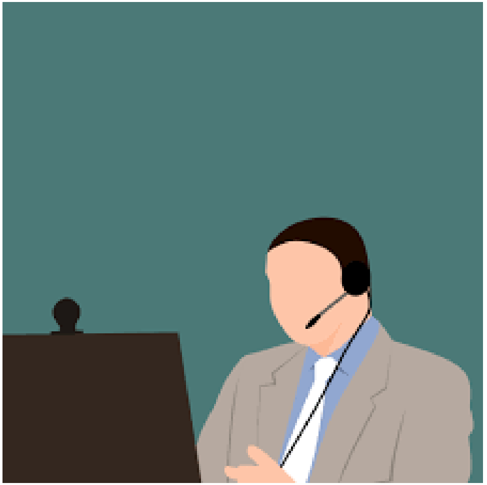


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Throughput issues : the troubleshooting

Can you really please be more specific ?

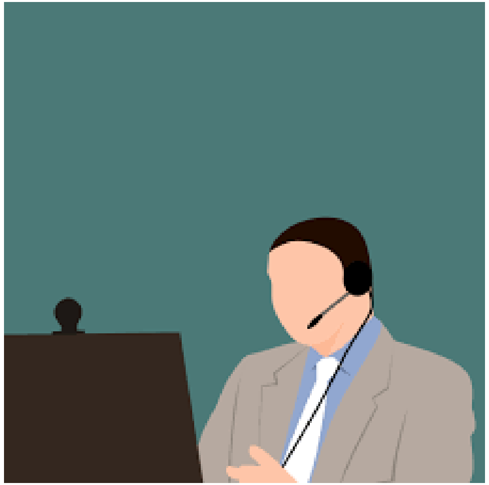
Well, actually, large commits by our developers take a while and people around our devs complain their Teams meeting are bad



# Throughput issues : the troubleshooting

Let’s run some tests with all the laptop variations you have

Older Dell G3 work great but newer Dell G6 don’t.

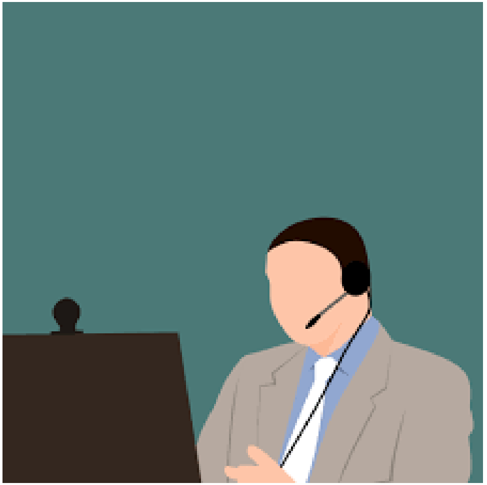


Ah !

# Throughput issues : the troubleshooting

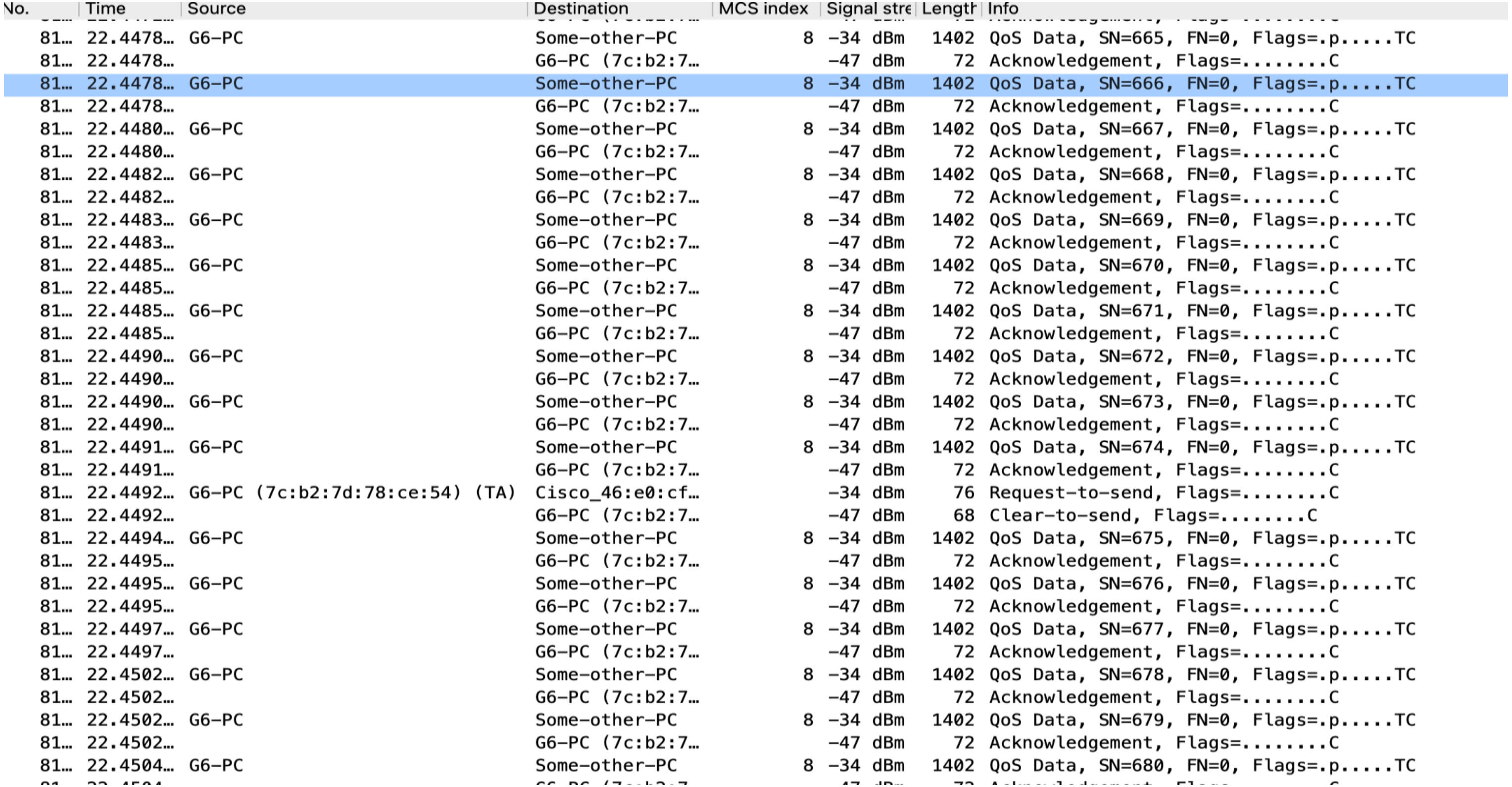
Is the issue only present on one SSID ?

We made a test PSK SSID and all works great there.



??!?!?? *visible confusion*

# Can you find the problem ?



| No. | Time | Source | Destination | MCS index | Signal stre | Length | Info |
|---|---|---|---|---|---|---|---|
| 81… | 22.4478… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=665, FN=0, Flags=.p.....TC |
| 81… | 22.4478… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4478… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=666, FN=0, Flags=.p.....TC |
| 81… | 22.4478… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4480… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=667, FN=0, Flags=.p.....TC |
| 81… | 22.4480… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4482… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=668, FN=0, Flags=.p.....TC |
| 81… | 22.4482… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4483… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=669, FN=0, Flags=.p.....TC |
| 81… | 22.4483… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4485… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=670, FN=0, Flags=.p.....TC |
| 81… | 22.4485… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4485… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=671, FN=0, Flags=.p.....TC |
| 81… | 22.4485… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4490… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=672, FN=0, Flags=.p.....TC |
| 81… | 22.4490… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4490… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=673, FN=0, Flags=.p.....TC |
| 81… | 22.4490… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4491… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=674, FN=0, Flags=.p.....TC |
| 81… | 22.4491… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4492… | G6-PC (7c:b2:7d:78:ce:54) (TA) | Cisco_46:e0:cf… | | -34 dBm | 76 | Request-to-send, Flags=........C |
| 81… | 22.4492… | | G6-PC (7c:b2:7… | | -47 dBm | 68 | Clear-to-send, Flags=........C |
| 81… | 22.4494… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=675, FN=0, Flags=.p.....TC |
| 81… | 22.4495… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4495… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=676, FN=0, Flags=.p.....TC |
| 81… | 22.4495… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4497… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=677, FN=0, Flags=.p.....TC |
| 81… | 22.4497… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4502… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=678, FN=0, Flags=.p.....TC |
| 81… | 22.4502… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4502… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=679, FN=0, Flags=.p.....TC |
| 81… | 22.4502… | | G6-PC (7c:b2:7… | | -47 dBm | 72 | Acknowledgement, Flags=........C |
| 81… | 22.4504… | G6-PC | Some-other-PC | 8 | -34 dBm | 1402 | QoS Data, SN=680, FN=0, Flags=.p.....TC |

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

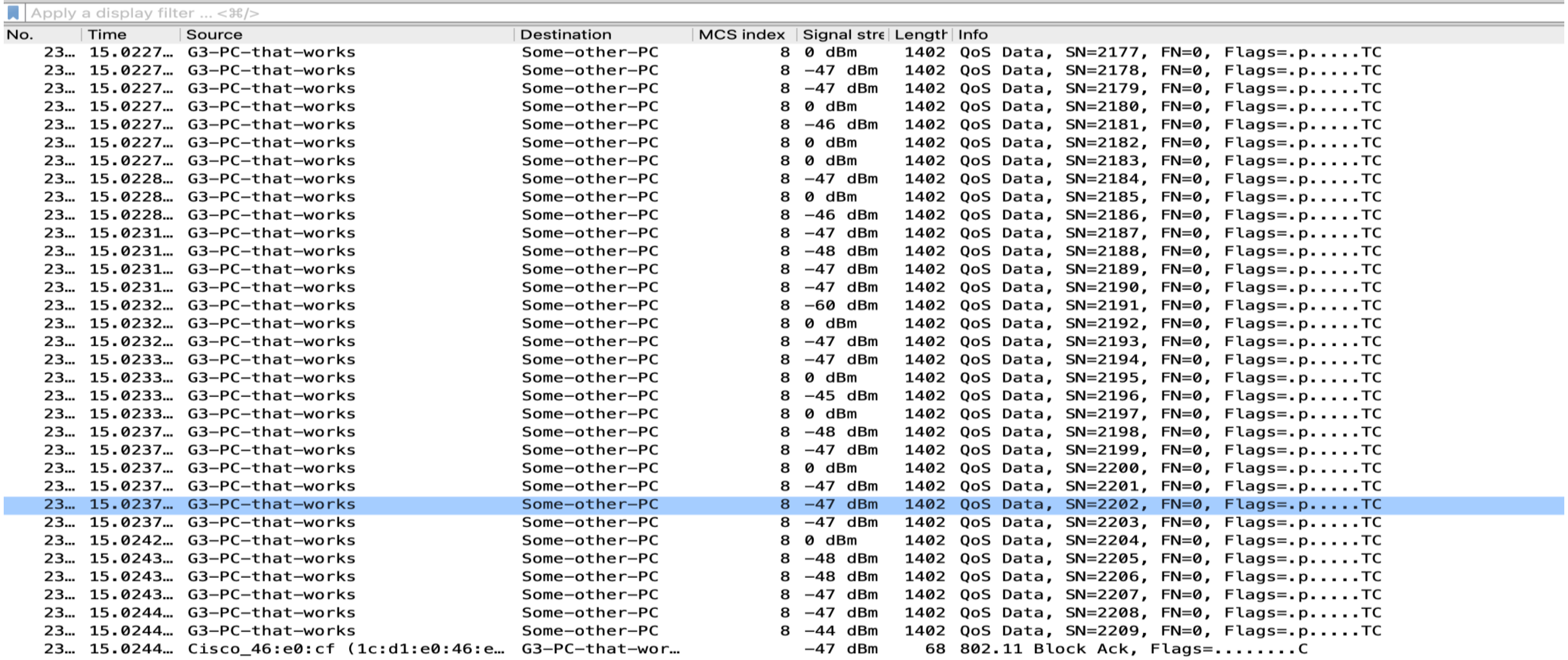
# What is slow ?

If the speed “could be better”, keep in mind that to go over 54Mbps

- You need open/WPA2-AES or better
- You need WMM
- Frame aggregation. Block ACKing 64 frames gives HUGE boost over acking each frame or ACKing 3-4 frames
- MCS Data rate
- Spatial streams

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# The working scenario



```
Apply a display filter ... <⌘/>
No.   Time       Source                          Destination      MCS index  Signal stre  Length  Info
 23…  15.0227…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2177, FN=0, Flags=.p.....TC
 23…  15.0227…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2178, FN=0, Flags=.p.....TC
 23…  15.0227…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2179, FN=0, Flags=.p.....TC
 23…  15.0227…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2180, FN=0, Flags=.p.....TC
 23…  15.0227…   G3-PC-that-works                Some-other-PC            8  -46 dBm      1402  QoS Data, SN=2181, FN=0, Flags=.p.....TC
 23…  15.0227…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2182, FN=0, Flags=.p.....TC
 23…  15.0227…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2183, FN=0, Flags=.p.....TC
 23…  15.0228…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2184, FN=0, Flags=.p.....TC
 23…  15.0228…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2185, FN=0, Flags=.p.....TC
 23…  15.0228…   G3-PC-that-works                Some-other-PC            8  -46 dBm      1402  QoS Data, SN=2186, FN=0, Flags=.p.....TC
 23…  15.0231…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2187, FN=0, Flags=.p.....TC
 23…  15.0231…   G3-PC-that-works                Some-other-PC            8  -48 dBm      1402  QoS Data, SN=2188, FN=0, Flags=.p.....TC
 23…  15.0231…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2189, FN=0, Flags=.p.....TC
 23…  15.0231…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2190, FN=0, Flags=.p.....TC
 23…  15.0232…   G3-PC-that-works                Some-other-PC            8  -60 dBm      1402  QoS Data, SN=2191, FN=0, Flags=.p.....TC
 23…  15.0232…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2192, FN=0, Flags=.p.....TC
 23…  15.0232…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2193, FN=0, Flags=.p.....TC
 23…  15.0233…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2194, FN=0, Flags=.p.....TC
 23…  15.0233…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2195, FN=0, Flags=.p.....TC
 23…  15.0233…   G3-PC-that-works                Some-other-PC            8  -45 dBm      1402  QoS Data, SN=2196, FN=0, Flags=.p.....TC
 23…  15.0233…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2197, FN=0, Flags=.p.....TC
 23…  15.0237…   G3-PC-that-works                Some-other-PC            8  -48 dBm      1402  QoS Data, SN=2198, FN=0, Flags=.p.....TC
 23…  15.0237…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2199, FN=0, Flags=.p.....TC
 23…  15.0237…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2200, FN=0, Flags=.p.....TC
 23…  15.0237…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2201, FN=0, Flags=.p.....TC
 23…  15.0237…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2202, FN=0, Flags=.p.....TC
 23…  15.0237…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2203, FN=0, Flags=.p.....TC
 23…  15.0242…   G3-PC-that-works                Some-other-PC            8  0 dBm        1402  QoS Data, SN=2204, FN=0, Flags=.p.....TC
 23…  15.0243…   G3-PC-that-works                Some-other-PC            8  -48 dBm      1402  QoS Data, SN=2205, FN=0, Flags=.p.....TC
 23…  15.0243…   G3-PC-that-works                Some-other-PC            8  -48 dBm      1402  QoS Data, SN=2206, FN=0, Flags=.p.....TC
 23…  15.0243…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2207, FN=0, Flags=.p.....TC
 23…  15.0244…   G3-PC-that-works                Some-other-PC            8  -47 dBm      1402  QoS Data, SN=2208, FN=0, Flags=.p.....TC
 23…  15.0244…   G3-PC-that-works                Some-other-PC            8  -44 dBm      1402  QoS Data, SN=2209, FN=0, Flags=.p.....TC
 23…  15.0244…   Cisco_46:e0:cf (1c:d1:e0:46:e…  G3-PC-that-wor…             -47 dBm        68  802.11 Block Ack, Flags=........C
```

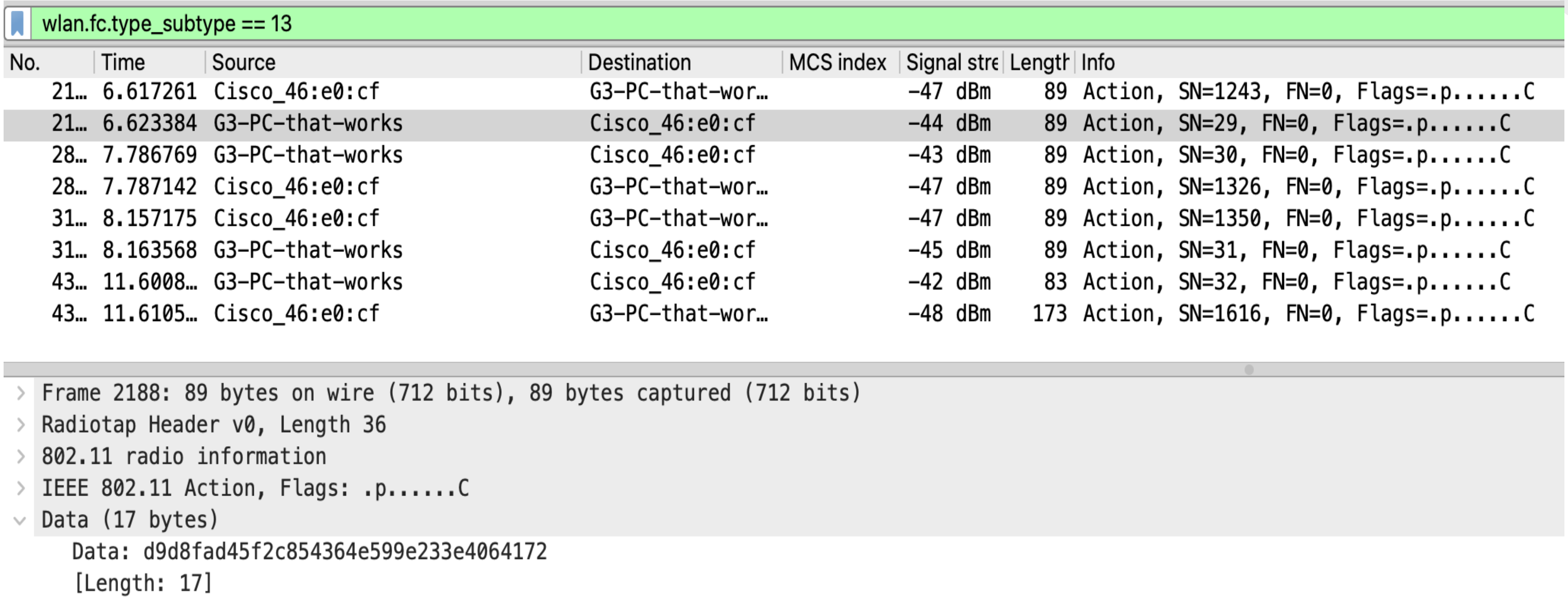
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Root cause?

Working situation shows lots of frames before a block ACK while problematic situation shows 1 frame 1 ACK, or few frames only with block ACK

- PSK SSID works
- Only certain laptop types are affected
- Previous network is not affected

# Root cause : exhibit A

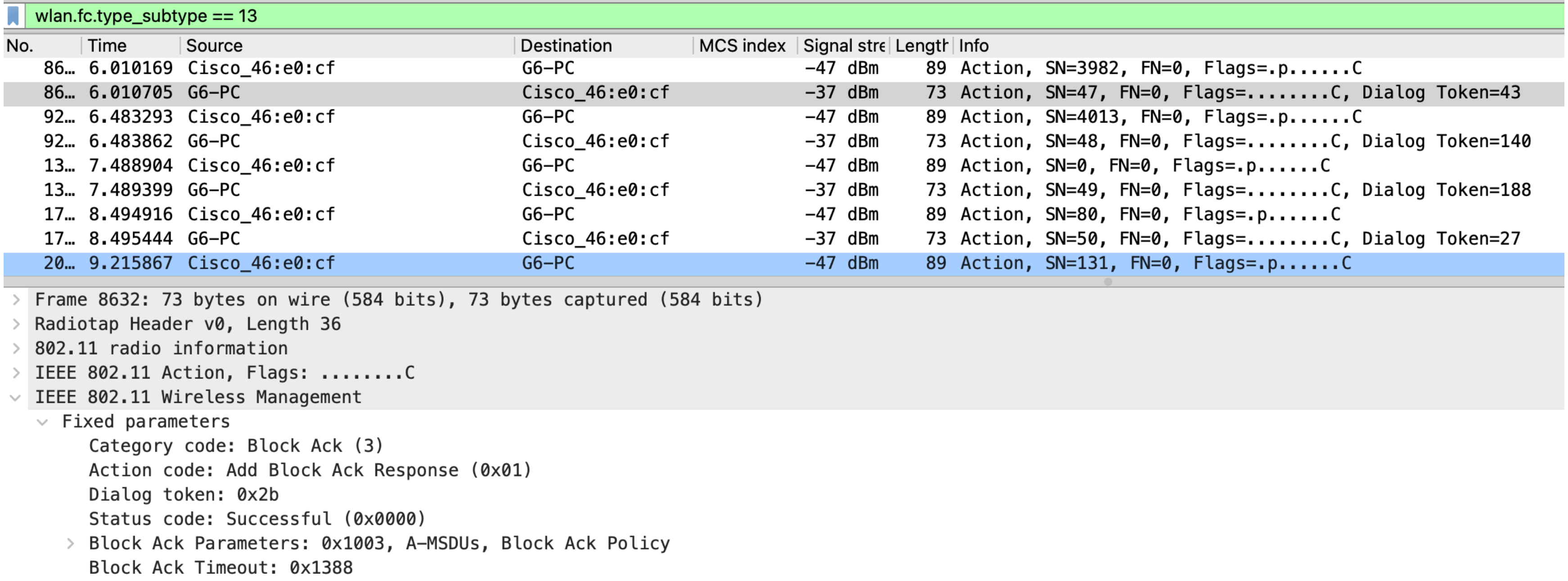


wlan.fc.type_subtype == 13

| No. | Time | Source | Destination | MCS index | Signal stre | Lengtł | Info |
|---|---|---|---|---|---|---|---|
| 21… | 6.617261 | Cisco_46:e0:cf | G3-PC-that-wor… | | -47 dBm | 89 | Action, SN=1243, FN=0, Flags=.p......C |
| 21… | 6.623384 | G3-PC-that-works | Cisco_46:e0:cf | | -44 dBm | 89 | Action, SN=29, FN=0, Flags=.p......C |
| 28… | 7.786769 | G3-PC-that-works | Cisco_46:e0:cf | | -43 dBm | 89 | Action, SN=30, FN=0, Flags=.p......C |
| 28… | 7.787142 | Cisco_46:e0:cf | G3-PC-that-wor… | | -47 dBm | 89 | Action, SN=1326, FN=0, Flags=.p......C |
| 31… | 8.157175 | Cisco_46:e0:cf | G3-PC-that-wor… | | -47 dBm | 89 | Action, SN=1350, FN=0, Flags=.p......C |
| 31… | 8.163568 | G3-PC-that-works | Cisco_46:e0:cf | | -45 dBm | 89 | Action, SN=31, FN=0, Flags=.p......C |
| 43… | 11.6008… | G3-PC-that-works | Cisco_46:e0:cf | | -42 dBm | 83 | Action, SN=32, FN=0, Flags=.p......C |
| 43… | 11.6105… | Cisco_46:e0:cf | G3-PC-that-wor… | | -48 dBm | 173 | Action, SN=1616, FN=0, Flags=.p......C |

```
> Frame 2188: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Action, Flags: .p......C
v Data (17 bytes)
    Data: d9d8fad45f2c854364e599e233e4064172
    [Length: 17]
```

# Root cause : exhibit B



```
wlan.fc.type_subtype == 13

No.     Time      Source           Destination      MCS index  Signal stre  Lengtr  Info
  86…   6.010169  Cisco_46:e0:cf   G6-PC                       -47 dBm       89  Action, SN=3982, FN=0, Flags=.p......C
  86…   6.010705  G6-PC            Cisco_46:e0:cf              -37 dBm       73  Action, SN=47, FN=0, Flags=........C, Dialog Token=43
  92…   6.483293  Cisco_46:e0:cf   G6-PC                       -47 dBm       89  Action, SN=4013, FN=0, Flags=.p......C
  92…   6.483862  G6-PC            Cisco_46:e0:cf              -37 dBm       73  Action, SN=48, FN=0, Flags=........C, Dialog Token=140
  13…   7.488904  Cisco_46:e0:cf   G6-PC                       -47 dBm       89  Action, SN=0, FN=0, Flags=.p......C
  13…   7.489399  G6-PC            Cisco_46:e0:cf              -37 dBm       73  Action, SN=49, FN=0, Flags=........C, Dialog Token=188
  17…   8.494916  Cisco_46:e0:cf   G6-PC                       -47 dBm       89  Action, SN=80, FN=0, Flags=.p......C
  17…   8.495444  G6-PC            Cisco_46:e0:cf              -37 dBm       73  Action, SN=50, FN=0, Flags=........C, Dialog Token=27
  20…   9.215867  Cisco_46:e0:cf   G6-PC                       -47 dBm       89  Action, SN=131, FN=0, Flags=.p......C

> Frame 8632: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: Block Ack (3)
      Action code: Add Block Ack Response (0x01)
      Dialog token: 0x2b
      Status code: Successful (0x0000)
    > Block Ack Parameters: 0x1003, A-MSDUs, Block Ack Policy
      Block Ack Timeout: 0x1388
```

# Root cause !

New Intel bug : when PMF is enabled, the client sends the ADDBA action frame as unencrypted while it should be encrypted.

Depending on how the AP likes it, it can cause throughput issues or other undesirable behaviors.

# IPTV streaming of your favourite TV shows

# The context

I have laptops watching multicast video streams and the quality is horrible over wireless

Wait wait, what kind of stream ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# The context

IPTV streams. They are MPEG-2 streams coming from a satelite IPTV appliance

What kind of bad quality are you seeing ? Is wired working fine ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# The context

That’s the funny bit. Some TV channels work perfectly but others not. Wired laptops have no issues

??!?!?!?!??

# Video proofs …

- File “4a-wireless client.mpeg” : Stream saved on the wireless client. Notice how differently it plays depending on the app you use to play it (VLC/Quicktime/etc …)
- File “4b- customer filmed.mov” . The customer filmed their screen playing the bad stream with their phone. This allows to visualize the actual customer experience !

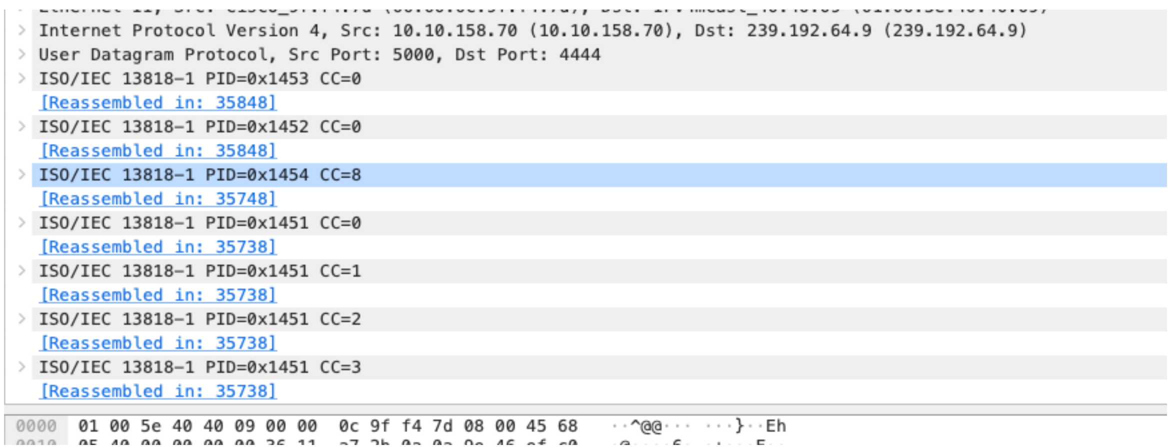
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# How does a good MPEG-2 stream looks like ?

- Each MPEG2 packet can contain 7 different (possibly unrelated) video segments
- Each ”segment” has a frame identifier and a sequence number
- Sequence numbers are only from 0x0 to 0xF before rolling over to 0x0 again
- You won’t notice 2 dropped packets as the sequence number roll over within 2 packets!

# How does a good MPEG-2 stream looks like ?

- Example of a MPEG packet containing sequence 0,1,2,3 for frame 1451 but also sequence 8 for frame 1454, sequence 0 for frame 1452

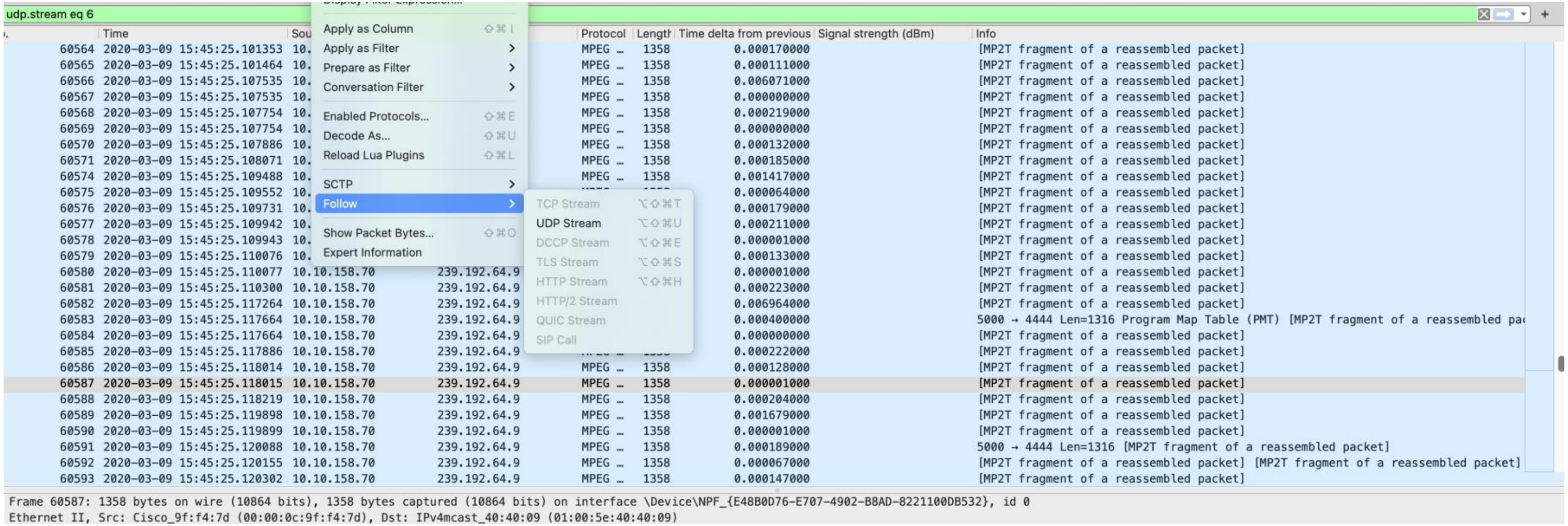


```
> Internet Protocol Version 4, Src: 10.10.158.70 (10.10.158.70), Dst: 239.192.64.9 (239.192.64.9)
> User Datagram Protocol, Src Port: 5000, Dst Port: 4444
> ISO/IEC 13818-1 PID=0x1453 CC=0
  [Reassembled in: 35848]
> ISO/IEC 13818-1 PID=0x1452 CC=0
  [Reassembled in: 35848]
> ISO/IEC 13818-1 PID=0x1454 CC=8
  [Reassembled in: 35748]
> ISO/IEC 13818-1 PID=0x1451 CC=0
  [Reassembled in: 35738]
> ISO/IEC 13818-1 PID=0x1451 CC=1
  [Reassembled in: 35738]
> ISO/IEC 13818-1 PID=0x1451 CC=2
  [Reassembled in: 35738]
> ISO/IEC 13818-1 PID=0x1451 CC=3
  [Reassembled in: 35738]

0000  01 00 5e 40 40 09 00 00  0c 9f f4 7d 08 00 45 68   ··^@@···  ···}··Eh
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Reconstructing MPEG video from PCAP

- By doing Follow->UDP stream on the mpeg flow, you can export the payload as “RAW” and get a video file as it was streamed over the network. You save the MPEG and watch the quality



```
udp.stream eq 6

.      Time                        Sou                           Protocol Length Time delta from previous Signal strength (dBm) Info
 60564 2020-03-09 15:45:25.101353  10.                           MPEG …   1358   0.000170000             [MP2T fragment of a reassembled packet]
 60565 2020-03-09 15:45:25.101464  10.                           MPEG …   1358   0.000111000             [MP2T fragment of a reassembled packet]
 60566 2020-03-09 15:45:25.107535  10.                           MPEG …   1358   0.006071000             [MP2T fragment of a reassembled packet]
 60567 2020-03-09 15:45:25.107535  10.                           MPEG …   1358   0.000000000             [MP2T fragment of a reassembled packet]
 60568 2020-03-09 15:45:25.107754  10.                           MPEG …   1358   0.000219000             [MP2T fragment of a reassembled packet]
 60569 2020-03-09 15:45:25.107754  10.                           MPEG …   1358   0.000000000             [MP2T fragment of a reassembled packet]
 60570 2020-03-09 15:45:25.107886  10.                           MPEG …   1358   0.000132000             [MP2T fragment of a reassembled packet]
 60571 2020-03-09 15:45:25.108071  10.                           MPEG …   1358   0.000185000             [MP2T fragment of a reassembled packet]
 60574 2020-03-09 15:45:25.109488  10.                           MPEG …   1358   0.001417000             [MP2T fragment of a reassembled packet]
 60575 2020-03-09 15:45:25.109552  10.                                           0.000064000             [MP2T fragment of a reassembled packet]
 60576 2020-03-09 15:45:25.109731  10.                                           0.000179000             [MP2T fragment of a reassembled packet]
 60577 2020-03-09 15:45:25.109942  10.                                           0.000211000             [MP2T fragment of a reassembled packet]
 60578 2020-03-09 15:45:25.109943  10.                                           0.000001000             [MP2T fragment of a reassembled packet]
 60579 2020-03-09 15:45:25.110076  10.                                           0.000133000             [MP2T fragment of a reassembled packet]
 60580 2020-03-09 15:45:25.110077  10.10.158.70  239.192.64.9                    0.000001000             [MP2T fragment of a reassembled packet]
 60581 2020-03-09 15:45:25.110300  10.10.158.70  239.192.64.9                    0.000223000             [MP2T fragment of a reassembled packet]
 60582 2020-03-09 15:45:25.117264  10.10.158.70  239.192.64.9                    0.006964000             [MP2T fragment of a reassembled packet]
 60583 2020-03-09 15:45:25.117664  10.10.158.70  239.192.64.9                    0.000400000             5000 → 4444 Len=1316 Program Map Table (PMT) [MP2T fragment of a reassembled pa
 60584 2020-03-09 15:45:25.117664  10.10.158.70  239.192.64.9                    0.000000000             [MP2T fragment of a reassembled packet]
 60585 2020-03-09 15:45:25.117886  10.10.158.70  239.192.64.9                    0.000222000             [MP2T fragment of a reassembled packet]
 60586 2020-03-09 15:45:25.118014  10.10.158.70  239.192.64.9    MPEG …   1358   0.000128000             [MP2T fragment of a reassembled packet]
 60587 2020-03-09 15:45:25.118015  10.10.158.70  239.192.64.9    MPEG …   1358   0.000001000             [MP2T fragment of a reassembled packet]
 60588 2020-03-09 15:45:25.118219  10.10.158.70  239.192.64.9    MPEG …   1358   0.000204000             [MP2T fragment of a reassembled packet]
 60589 2020-03-09 15:45:25.119898  10.10.158.70  239.192.64.9    MPEG …   1358   0.001679000             [MP2T fragment of a reassembled packet]
 60590 2020-03-09 15:45:25.119899  10.10.158.70  239.192.64.9    MPEG …   1358   0.000001000             [MP2T fragment of a reassembled packet]
 60591 2020-03-09 15:45:25.120088  10.10.158.70  239.192.64.9    MPEG …   1358   0.000189000             5000 → 4444 Len=1316 [MP2T fragment of a reassembled packet]
 60592 2020-03-09 15:45:25.120155  10.10.158.70  239.192.64.9    MPEG …   1358   0.000067000             [MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
 60593 2020-03-09 15:45:25.120302  10.10.158.70  239.192.64.9    MPEG …   1358   0.000147000             [MP2T fragment of a reassembled packet]

Frame 60587: 1358 bytes on wire (10864 bits), 1358 bytes captured (10864 bits) on interface \Device\NPF_{E48B0D76-E707-4902-B8AD-8221100DB532}, id 0
Ethernet II, Src: Cisco_9f:f4:7d (00:00:0c:9f:f4:7d), Dst: IPv4mcast_40:40:09 (01:00:5e:40:40:09)
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Can wireshark detect MPEG packet drop ?

- File 4d- SPAN.mpeg
- Comparing the exported stream from a PCAP collected on a wired PC allows to see that the wired network does not impact the MPEG quality at all, whatever problem happens over wireless.

# Can wireshark detect MPEG packet drop ?

- Filter “mp2t.analysis.skips >= 1”
- Filter “mp2t.cc.drop”

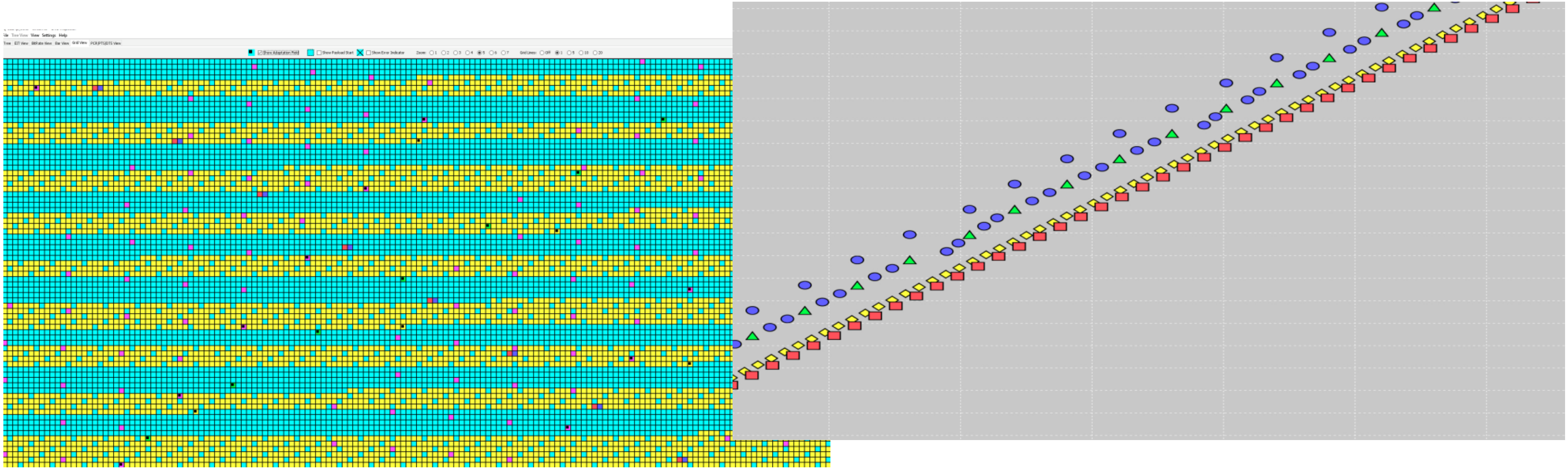
# But why would one TV channel work and not another ?

- Time to pull out the big gun : DVB inspector

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# But why would one TV channel work and not another ?

- Good stream

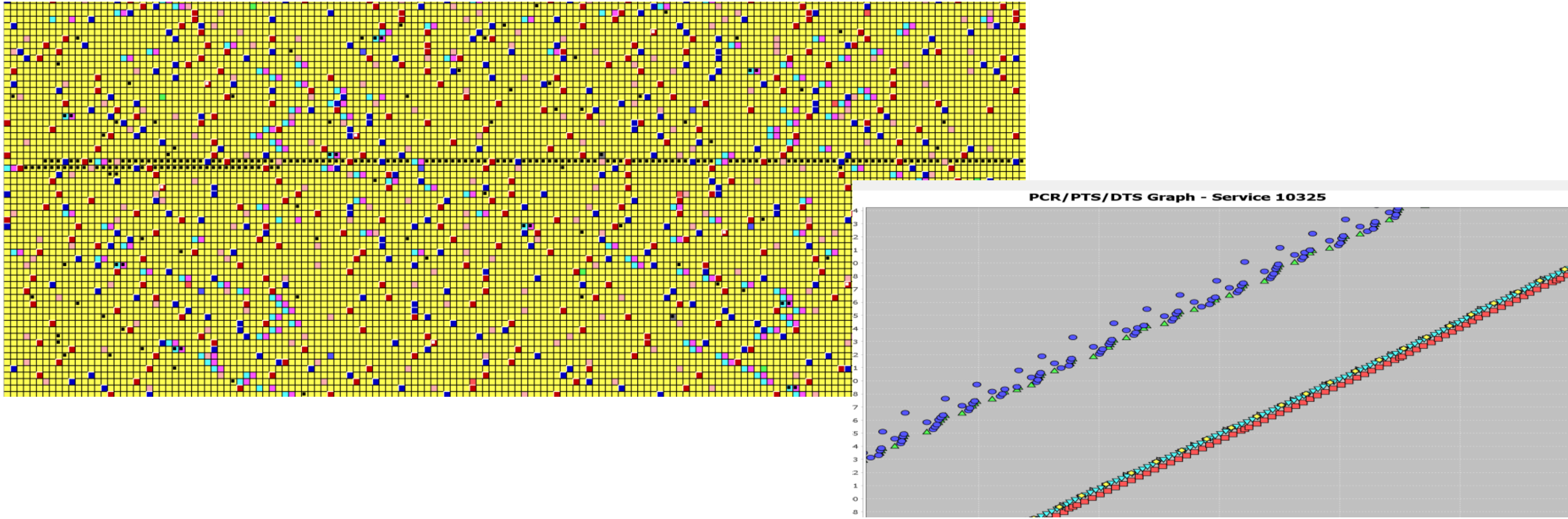


ile Tree View View Settings Help
Tree EIT View BitRate View Bar View Grid View PCR|PTS|DTS View

☑ Show Adaptation Field ☐ Show Payload Start ☐ Show Error Indicator Zoom: ○1 ○2 ○3 ○4 ●5 ○6 ○7 Grid Lines: ○Off ●1 ○5 ○10 ○20

# But why would one TV channel work and not another ?

- Bad stream



# Story conclusions

# IPTV: Key takeaways

- Human network is critical : you cannot be an expert at everything (i.e. MPEG)
- Compare the working with the non-working, always
- It is key to understand the type of traffic you have, regardless of what it is:
  - Does it do buffering or is it super real-time ?
  - Is the stream itself multicast ? Or was it a multicast discovery only ?
  - What’s the tolerance to packet loss and/or reorder ?

# IPTV: What happened ?

- We took all the possible measures to reduce the amount of packet loss, but it was definitely in the 1% expected range
- If some streams worked and not others, it was a clear pointer that some TV channel streams were poorly encoded. Suggested looking into finding some way to transcode the streams or change IPTV provider.

**Achievement Unlocked!**
Video codec CCIE

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Agenda

14.15 : start and intro

14.30 : Some stories from Nico

16.15 : coffee break

16.45 : Even More stories from Javier

18.45 : End !

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Agenda

14.15 : start and intro

14.30 : Some stories from Nico

16.15 : coffee break

16.45 : Even More stories from Javier

18.45 : End !

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# If it walks like a duck… Could be an orange

# The Story starts…

- Large customer, multiple offices across the world
- Social Media (so IT/Tech)
- Fancy buildings, high density environment
- Mixed Client types

- Problem: Clients can't connect, on some places, some times…

# Sometimes Problems are not what it seems

- Client can't connect
- EAP authentication error
  - No EAP ID response

```
2022/05/11 19:17:55.137668 {wncd_x_R0-0}{1}: [eap]
[16660]: (debug): 'Authenticator ReqId Retransmit'
timer expired for EAP sesion handle 0x.

2022/05/11 19:18:00.138002 {wncd_x_R0-0}{1}: [eap]
[16660]: (debug): 'Authenticator ReqId Retransmit'
timer expired for EAP sesion handle 0x.

2022/05/11 19:18:00.138624 {wncd_x_R0-0}{1}:
[ewlc-infra-evq] [16660]: (ERR):
SANET_AUTHC_FAILURE - No Response from Client,
audit session id xx
```

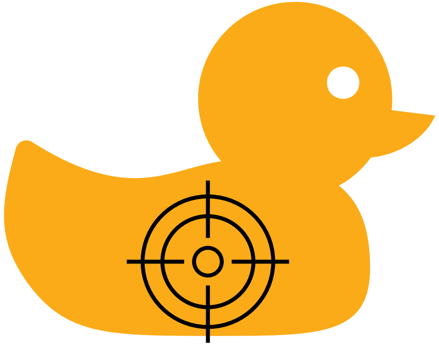
# Questions arise

- Happens for all client types?
    - Yes
- Multiple sites? Single location?
    - Mostly seen in some sites
    - Never seen in site X/Y
- Permanent failure?
    - Sometimes yes, but occasionally recovers
    - If you move client, it works

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Jumping into early guess

- EAP ID Failure: Common client issue (wireless profile config)
- Quickly discarded:
  - Issue is intermittent at client
  - Issue happens across different client types
  - Issue is tied to physical/AP location
  - Restarting AP recovers the problem



# Initial data collection

- Log traces:
  - Shows Controller sending EAP ID request, no response on specific Aps
- AP traces:
  - EAP ID transmitted, no response seen:

```
Jul 25 12:25:04 kernel: [*07/25/2022 12:25:04.7993] [1658751904:799273] [LHR105.09.04] [1e:83:f4:2f:1e:53]
<apr1v2> [D:W] EAP_PACKET.Request : Id 0x01 type 1 Identity

Jul 25 12:25:09 kernel: [*07/25/2022 12:25:09.7999] [1658751909:799825] [LHR105.09.04] [1e:83:f4:2f:1e:53]
<apr1v2> [D:W] EAP_PACKET.Request : Id 0x01 type 1 Identity

Jul 25 12:25:14 kernel: [*07/25/2022 12:25:14.7998] [1658751914:799692] [LHR105.09.04] [1e:83:f4:2f:1e:53]
<apr1v2> [D:W] EAP_PACKET.Request : Id 0x01 type 1 Identity
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

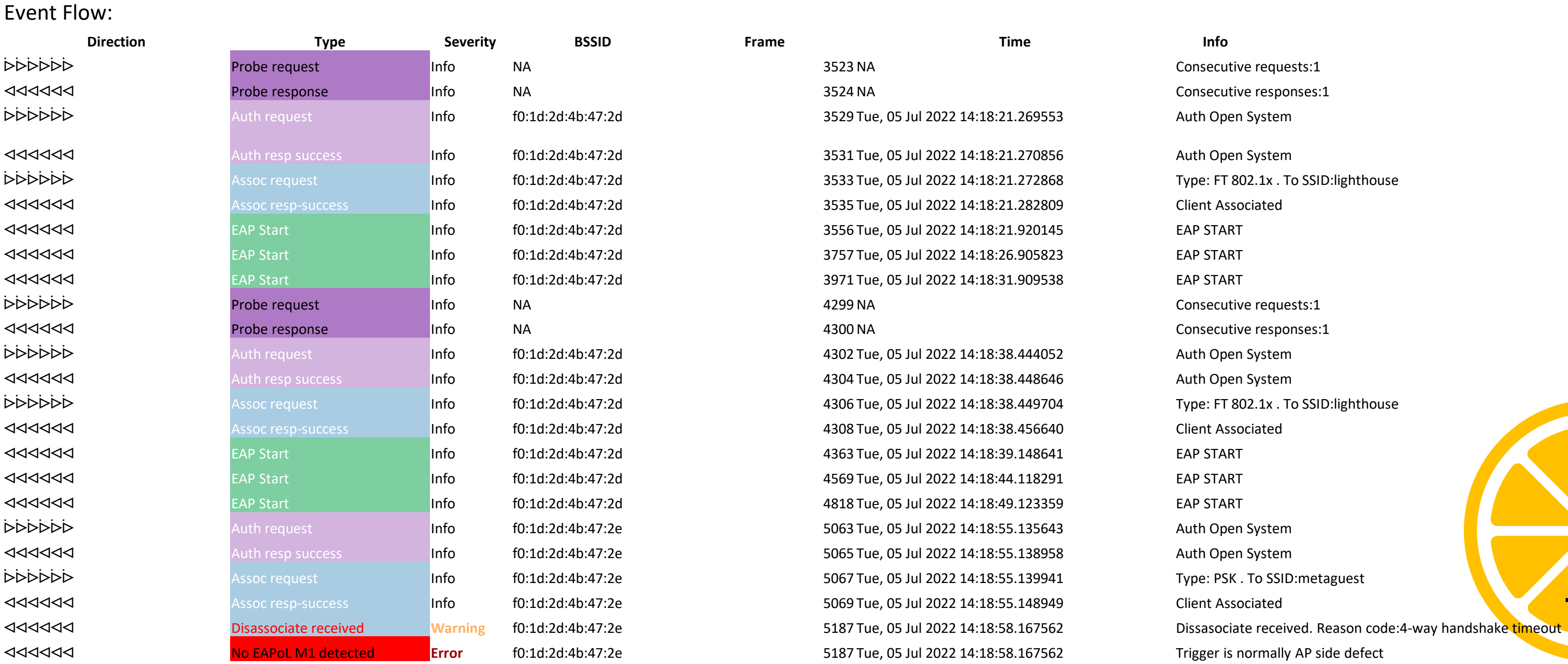
# Isolation flow

- Full picture required:
  - RA trace + Internal
  - AP logs
  - Wireless Sniffer trace

- Several iterations of capture needed to get the problem properly

# Sniffer trace shows “where” it happens

- WiFI-Hawk paints a different picture

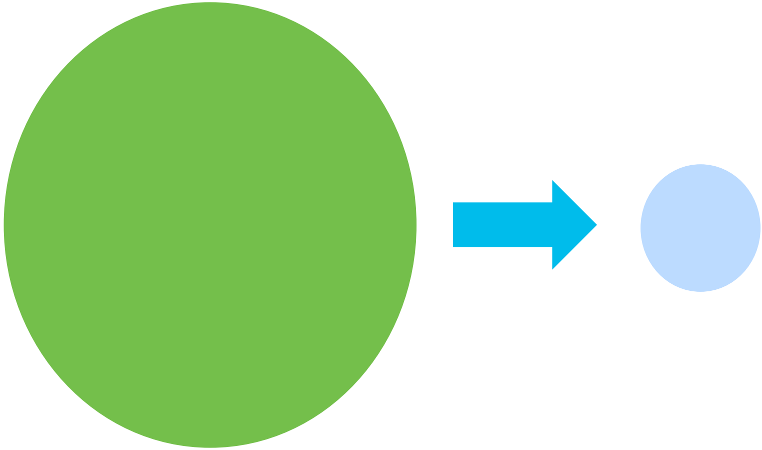


Event Flow:

| Direction | Type | Severity | BSSID | Frame | Time | Info |
|---|---|---|---|---|---|---|
| ▷▷▷▷▷▷ | Probe request | Info | NA | 3523 | NA | Consecutive requests:1 |
| ◁◁◁◁◁◁ | Probe response | Info | NA | 3524 | NA | Consecutive responses:1 |
| ▷▷▷▷▷▷ | Auth request | Info | f0:1d:2d:4b:47:2d | 3529 | Tue, 05 Jul 2022 14:18:21.269553 | Auth Open System |
| ◁◁◁◁◁◁ | Auth resp success | Info | f0:1d:2d:4b:47:2d | 3531 | Tue, 05 Jul 2022 14:18:21.270856 | Auth Open System |
| ▷▷▷▷▷▷ | Assoc request | Info | f0:1d:2d:4b:47:2d | 3533 | Tue, 05 Jul 2022 14:18:21.272868 | Type: FT 802.1x . To SSID:lighthouse |
| ◁◁◁◁◁◁ | Assoc resp-success | Info | f0:1d:2d:4b:47:2d | 3535 | Tue, 05 Jul 2022 14:18:21.282809 | Client Associated |
| ◁◁◁◁◁◁ | EAP Start | Info | f0:1d:2d:4b:47:2d | 3556 | Tue, 05 Jul 2022 14:18:21.920145 | EAP START |
| ◁◁◁◁◁◁ | EAP Start | Info | f0:1d:2d:4b:47:2d | 3757 | Tue, 05 Jul 2022 14:18:26.905823 | EAP START |
| ◁◁◁◁◁◁ | EAP Start | Info | f0:1d:2d:4b:47:2d | 3971 | Tue, 05 Jul 2022 14:18:31.909538 | EAP START |
| ▷▷▷▷▷▷ | Probe request | Info | NA | 4299 | NA | Consecutive requests:1 |
| ◁◁◁◁◁◁ | Probe response | Info | NA | 4300 | NA | Consecutive responses:1 |
| ▷▷▷▷▷▷ | Auth request | Info | f0:1d:2d:4b:47:2d | 4302 | Tue, 05 Jul 2022 14:18:38.444052 | Auth Open System |
| ◁◁◁◁◁◁ | Auth resp success | Info | f0:1d:2d:4b:47:2d | 4304 | Tue, 05 Jul 2022 14:18:38.448646 | Auth Open System |
| ▷▷▷▷▷▷ | Assoc request | Info | f0:1d:2d:4b:47:2d | 4306 | Tue, 05 Jul 2022 14:18:38.449704 | Type: FT 802.1x . To SSID:lighthouse |
| ◁◁◁◁◁◁ | Assoc resp-success | Info | f0:1d:2d:4b:47:2d | 4308 | Tue, 05 Jul 2022 14:18:38.456640 | Client Associated |
| ◁◁◁◁◁◁ | EAP Start | Info | f0:1d:2d:4b:47:2d | 4363 | Tue, 05 Jul 2022 14:18:39.148641 | EAP START |
| ◁◁◁◁◁◁ | EAP Start | Info | f0:1d:2d:4b:47:2d | 4569 | Tue, 05 Jul 2022 14:18:44.118291 | EAP START |
| ◁◁◁◁◁◁ | EAP Start | Info | f0:1d:2d:4b:47:2d | 4818 | Tue, 05 Jul 2022 14:18:49.123359 | EAP START |
| ▷▷▷▷▷▷ | Auth request | Info | f0:1d:2d:4b:47:2e | 5063 | Tue, 05 Jul 2022 14:18:55.135643 | Auth Open System |
| ◁◁◁◁◁◁ | Auth resp success | Info | f0:1d:2d:4b:47:2e | 5065 | Tue, 05 Jul 2022 14:18:55.138958 | Auth Open System |
| ▷▷▷▷▷▷ | Assoc request | Info | f0:1d:2d:4b:47:2e | 5067 | Tue, 05 Jul 2022 14:18:55.139941 | Type: PSK . To SSID:metaguest |
| ◁◁◁◁◁◁ | Assoc resp-success | Info | f0:1d:2d:4b:47:2e | 5069 | Tue, 05 Jul 2022 14:18:55.148949 | Client Associated |
| ◁◁◁◁◁◁ | Disassociate received | Warning | f0:1d:2d:4b:47:2e | 5187 | Tue, 05 Jul 2022 14:18:58.167562 | Dissassociate received. Reason code:4-way handshake timeout |
| ◁◁◁◁◁◁ | No EAPoL M1 detected | Error | f0:1d:2d:4b:47:2e | 5187 | Tue, 05 Jul 2022 14:18:58.167562 | Trigger is normally AP side defect |

# Problem Isolated to AP

- AP is not TX/RX EAP frames
- AP is sending Association/Beacon/Auth
- Where in AP is this being dropped?



# Now it gets ugly

- No related details seen on logs/AP debugs
- Debugging is difficult due to other “noise” triggered by IPv6 HSRP
- High Impact, frequency is high
- AP debug images needed
- Customer asks for workaround

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

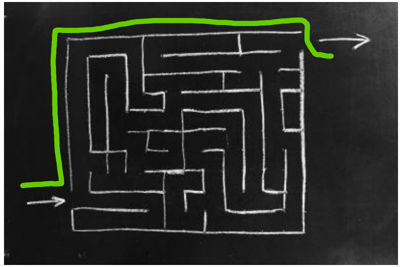
# Long nights later

- DFS event correlated to start of problem
- AP sees radar, no channel change, TX stops
- Message drop between Firmware - Driver – Kernel
- Trigger known but no full fix

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

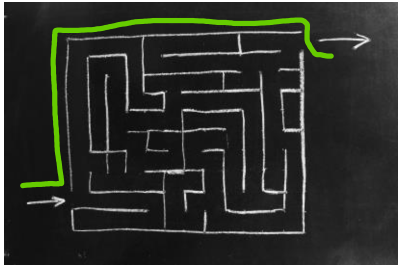
# Workaround on the Rocks

- Customer needs workaround
  - AP side detection failed
  - Not possible to add any server to run scripts/python
- EEM to the rescue
  - Goes over AP list, pulls 9130 models, and runs remote command
  - Controller monitors syslog for command output, with flag set
  - When flag detected, AP gets CAPWAP restart



# Workaround on the Rocks

```
event manager applet dfs-collect
event timer watchdog time 1800 maxrun 120
action 101 cli command "en"
action 110 cli command "term len 0"
action 120 cli command "sh ap summary | ex AP Name|Number of APs:|-----------------------------"
action 130 foreach line "$_cli_result" "\n"
action 140  regexp "(9130)" "$line"
action 150  if $_regexp_result eq "1"
action 160    regexp "^([^ ]+).*\r$" "$line" _match _AP_NAME
action 170    if $_regexp_result eq "1"
action 180     cli command "ap name $_AP_NAME remote command $q sh dot11 generic iwpriv wifi1 g_dfs_pending $q"
action 190    end
action 200   end
action 210  end

event manager applet dfs_detect
event syslog pattern "g_dfs_pending:1" maxrun 120
action 101 cli command "en"
action 102 cli command "term len 0"
action 110 foreach line "$_syslog_msg" "\n"
action 120   regexp "AP_LOG-6-([\_A-Za-z0-9\-\.]+)" "$line" match _AP_NAME
action 130   if $_regexp_result eq "1"
action 140     syslog msg "** DFS lock detected for AP: $_AP_NAME, resetting CAPWAP"
action 180     cli command "ap name $_AP_NAME reset capwap"
action 190    end
action 250  end
```



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Fixed - CSCwc78435

- Invalid Channel extension sent to driver
- Controller never gets notification, so DFS is not completed, radio in “invalid” state
- Day one issue
- Why not seen before:
  - RF design
  - HD density
  - 40 MHz
  - Client types

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Story conclusions

# Several learnings

- Not jumping into conclusions: Symptom had nothing to do with real issue
- Using EEM as Workaround Automation
- RF environment and configuration can play a huge role

# The Tale of the Three Defects

# Emergency: Authentications Failing

- Multiple customers reporting authentication failures
- Some happening per site, some globally
- Reload recovers

```
RADIUS: id 1, priority 1, host    <IP addr>    , auth-port 1812, acct-port 1813, hostname ZCC-Cloud-SRV-1
     State: current UP, duration 167530s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 167529s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
     Platform State from WNCD (1) : current DEAD
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
```

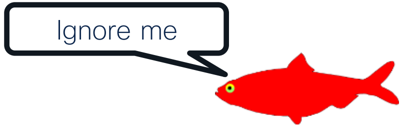
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Questions start

- Is server failing?
  - No errors on AAA side.

```
%SESSION_MGR-5-FAIL: Chassis 1 R0/0: wncd: Authorization failed or unapplied for client (X.X.X) on Interface
capwap_900001cc AuditSessionID YYY. Failure reason: Authc fail. Authc failure reason: AAA Server Down.
```

- Recovery by controller reload
  - So probable device side issue
- Any recent changes?
  - “Not that I recall” (for some cases)
  - Upgraded to 17.3.4/17.6.1 few days ago



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Data collection

- ACL/FW: Not present
- Client RA trace:

```
{wncd_x_R0-3}{1}: [dot1x] [20560]: (info): [X.X.X:capwap_90c0091a] Received EAPOL packet - Version : 1,EAPOL Type : EAP, 
Payload Length : 10, EAP-Type = Identitycc
{wncd_x_R0-3}{1}: [radius] [20560]: (ERR): RSPE- Delete Idle sockets in a Socket Pool : Input Validation Failed
{wncd_x_R0-3}{1}: [radius] [20560]: (ERR): RSPE- Create New Socket Data : Dynamic socket pool limit is still at Maximum 96 
after clean up
{wncd_x_R0-3}{1}: [radius] [20560]: (ERR): $$$$ RSPE- Crete New Socket Data : Worst case scenario Reached $$$$
{wncd_x_R0-3}{1}: [radius] [20560]: (ERR): RSPE- Get Socket_Fd and Free Identifier : Failed to get Free socket and Free 
Identifier
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS: Send Access-Request to Z.Z.Z.Z:1812 id 0/125, len 426
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:  authenticator
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:  User-Name           [1]     7  ”user"
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:   Cisco AVpair       [1]    21  "service-type=Framed"
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:  Framed-MTU          [12]    6  1485
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:  EAP-Message         [79]   12  ...
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:  Message-Authenticator[80]   18  ...
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:  EAP-Key-Name        [102]   2  *
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:   Cisco AVpair       [1]    43  "audit-session-
id=06FD11AC0002844AF892D07C"
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:   Cisco AVpair       [1]    14  "method=dot1x"
{wncd_x_R0-3}{1}: [radius] [20560]: (info): RADIUS:  Nas-Identifier      [32]   36  "nas"
{wncd_x_R0-3}{1}: [radius] [20560]: (ERR): could not set the l3_packet info in the socket
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Data collection

- RA trace process:

```
wlc#debug platform condition feature wireless mac X.X.X

wlc#debug platform condition start
```

Repro problem

```
wlc#debug platform condition stop

wlc# show logging profile wireless level debug filter mac X.X.X
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Data collection – 17.9.2 +

New!

- Client Debug Bundle

```
wlc#debug wireless bundle client <client_mac1 ...client_mac5>
Repro problem
wlc#no debug wireless bundle client <client_mac1 ...client_mac5>
```

- Auto–stop at 30 min
- Copy tar file to server:

```
copy bootflash:wireless_bundle_x.x.x_UTC_Sep_20_2022.tar tftp://<TFTP IP>/<TFTP PATH>
```

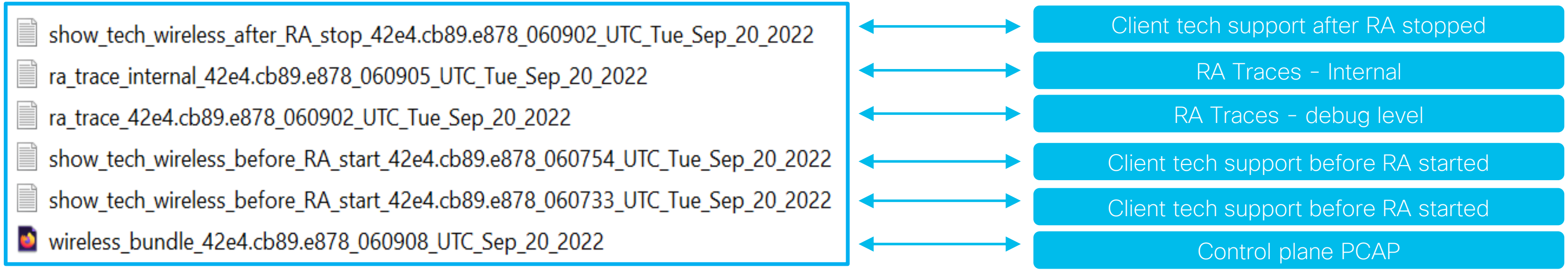
- Optional EPC capture:

```
debug wireless bundle include epc client
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Bundle Contents

- Two sets of RA traces for all the clients
- Two sets of clients tech support
- WLC control plane captures

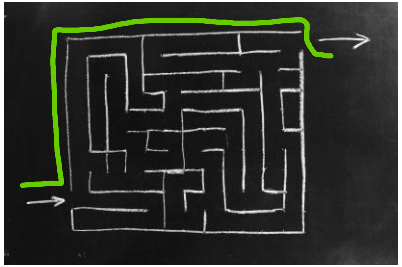


| | |
|---|---|
| show_tech_wireless_after_RA_stop_42e4.cb89.e878_060902_UTC_Tue_Sep_20_2022 | Client tech support after RA stopped |
| ra_trace_internal_42e4.cb89.e878_060905_UTC_Tue_Sep_20_2022 | RA Traces - Internal |
| ra_trace_42e4.cb89.e878_060902_UTC_Tue_Sep_20_2022 | RA Traces - debug level |
| show_tech_wireless_before_RA_start_42e4.cb89.e878_060754_UTC_Tue_Sep_20_2022 | Client tech support before RA started |
| show_tech_wireless_before_RA_start_42e4.cb89.e878_060733_UTC_Tue_Sep_20_2022 | Client tech support before RA started |
| wireless_bundle_42e4.cb89.e878_060908_UTC_Sep_20_2022 | Control plane PCAP |

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Workarounds?

- TAC had happy idea:
  - Disabling Accounting help
- Reload controller
- Workaround should have limited impact
- Isolated to 17.3.4/17.6.1: Downgrade helps



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Root Cause Analysis

- What is known:
  - Problem starts X time after upgrade to 17.3.4
  - Time delayed problem: Leak
- RA trace:
  - Radius socket error
- What has changed?
  - Related Commits in 17.3.4: CSCvx50397 Radius Source port extension Enhancement for support IPv4 and IPv6
- Trigger is on Accounting request retransmissions, causing a socket entry leak

# Damage Control

- Quick "fix": Removal of CSCvx50397 using CSCvz30708.
  17.3.4c
- Full fix: CSCvz55484 Wireless client authentications fail as the controller is unable to send RADIUS packets
  17.3.5 +
- Changes to feature sanity testing

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Story conclusions

# Data collection + testing failure

- RA client trace shows the problem
  - Extensive actions plans were not needed
- Leak delay masked the trigger
- Improvements needed on negative test case scenarios

# Flapping around

# Context

- University in U.S
- Migrated to C9800 WLCs
- Mix of Access Points – 2802s, 9120s with some 2700s and 1562s
- Symptom Reported: Intermittent network outage due to AP Flaps

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Defining the problem symptom

- Are APs crashing or flapping?
- show ap uptime

```
AP Name Ethernet MAC  Radio MAC    AP Up Time                              Association Up Time
------------------------------------------------------------------------------------------------------------
AP1      Eth1        Radmac1       1 day 21 hours 14 minutes 17 seconds    1 day 21 hours 12 minutes 3 seconds
AP2      Eth2        Radmac2       1 day 1 hour 49 minutes 7 seconds                      13 minutes 25 seconds
AP3      Eth3        Radmac3       1 day 21 hours 13 minutes 25 seconds                    9 minutes 37 seconds
AP4      Eth4        Radmac4       1 day 21 hours 13 minutes 25 seconds                   10 minutes 11 seconds
AP5      Eth5        Radmac5       1 day 21 hours 14 minutes 17 seconds    1 day 21 hours 11 minutes 58 seconds
AP6      Eth6        Radmac6       1 day 21 hours 13 minutes 26 seconds                    6 minutes 6 seconds
AP7      Eth7        Radmac7       1 day 21 hours 14 minutes 17 seconds    1 day 21 hours 11 minutes 55 seconds
```

- Dir bootflash:*.crash

```
Directory of bootflash:/*.crash

No such file
```

- Conclusion: APs are only flapping capwap tunnel, they’re not crashing

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# AP Flaps – First Steps

- Identify the capwap disconnect reason for APs
- Show wireless stats ap join summary

```
Number of APs: 600

Base MAC     Ethernet MAC    AP Name         IP Address    Status  Last Failure Phase   Last Disconnect Reason
---------------------------------------------------------------------------------------------------------------------
RadioMAC1    EthernetMAC1    E1-F2-AP1                   Joined      Run                Heart beat timer expiry
RadioMAC2    EthernetMAC2    C3-F1-AP3                   Joined      Run                DTLS close alert from peer
RadioMAC3    EthernetMAC3    C1-F4-AP2                   Joined      Join               DTLS close alert from peer
RadioMAC4    EthernetMAC4    C5-F2-AP4                   Joined      Run                DTLS close alert from peer
RadioMAC5    EthernetMAC5    M1-F19-AP1                  Joined      Run                DTLS close alert from peer
RadioMAC6    EthernetMAC6    P4-F10-AP1                  Joined      Run                DTLS close alert from peer
RadioMAC7    EthernetMAC7    C3-F1-AP6                   Joined      Run                DTLS close alert from peer
…
```

- DTLS Close alert from Peer is the highest hit count

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Did you know?

- DTLS failures usually indicate problems with the certificate used for DTLS/CAPWAP Join
- AP uses Manufacturing Installed Certificate (MIC) for DTLS
- C9800 appliances (C9800-40, C9800-80, C9800-L) uses SUDI for DTLS
- C9800-CL (private or public cloud) uses Self-Signed Certificate (SSC) mapped to Wireless management interface (WMI) for DTLS

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Typical Certificate Problems

- Clock on the WLC is not set making the WLC certificate invalid
  - show clock/show time
  - Fixed by setting up NTP
- Certificate on the AP has expired
  - show crypto (on AP)
  - show crypto pki
  - Workaround: Configure certify expiry ignore on the WLC
- Depending on AP Model and version, it might be using SHA1 certificate while the WLC is using SHA2 certificate by default

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# TAC's Engineer's Take away

- The common problems are constant and need user intervention to recover

Except…

- APs recover on their own
- APs flap intermittently is intermittent

Next Steps:

- Identify trend failure for one AP
- Identify event in network or on WLC/AP matching trend

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Identify trend of AP Flaps

- show wireless stats ap history mac-address <AP_Ethernet_MAC>

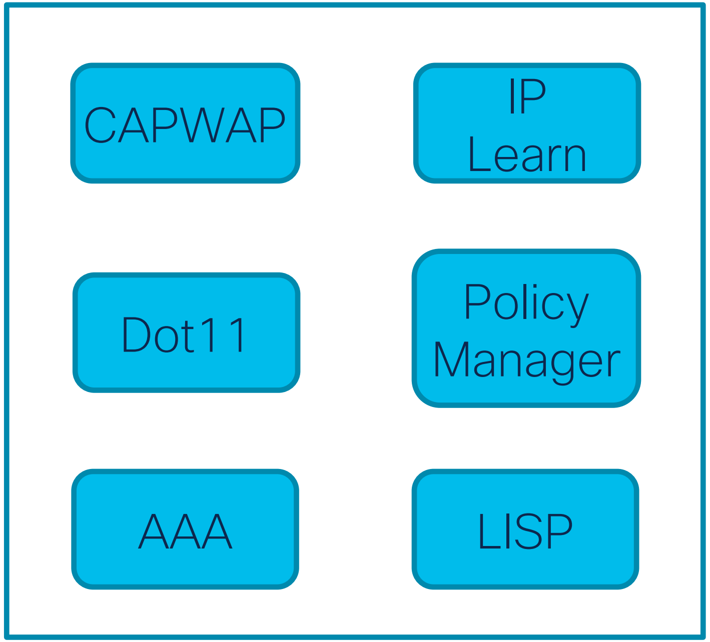
```
AP Name Radio MAC  Event      Time         Recent Disconnect Time    Disconnect Reason
--------------------------------------------------------------------------------------


APName  APRadioMAC Joined     05/27/22 10:08:36    NA
APName  APRadioMAC Disjoined  05/27/22 10:08:05    NA        DTLS close alert from peer
APName  APRadioMAC Joined     05/27/22 10:05:24    NA
APName  APRadioMAC Disjoined  05/27/22 10:04:53    NA        DTLS close alert from peer
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# TAC Engineer’s Conclusions

- Specific times at which AP is flapping is identified
- Unfiltered output shows total number of affected APs identified
- Multiple iterations of unfiltered output also shows if same APs are affected at each incident
- Co-located APs share RF space and on C9800 are recommended to be assigned to same site tag and therefore, same WNCd instance

# Wireless Network Control Daemon (WNCd)



WNCd : controller process managing AP and client session

- Capwap : AP discovery
- Dot11 : Client dot11
- SANET/AAA: Client authentication
- EPM : Client policies
- SISF : client IP learning
- Client Orchestrator : Client State Transitions
- LISP-agent : L2 Lisp handling for Fabric deployment

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# C9800 High CPU – Show commands

- CPU cores used by IOSd

```
show process cpu sorted
```

- CPU cores used by BinOS processes

```
show process cpu platform sorted
```

- Traffic Punted to CPU

```
show platform hardware chassis active qfp feature wireless punt
statistics (multiple iterations)
```

- CPU Queues and Policers

```
show platform software punt-policer
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# C9800 High CPU – CPU PCAP

- Steps to capture CPU only PCAP (CLI only)

```
monitor capture CPUCAP control-plane both
monitor capture CPUCAP match any
monitor capture CPUCAP buffer size 100
monitor capture CPUCAP start
```

- Collect captures during high CPU and export as a .pcap.

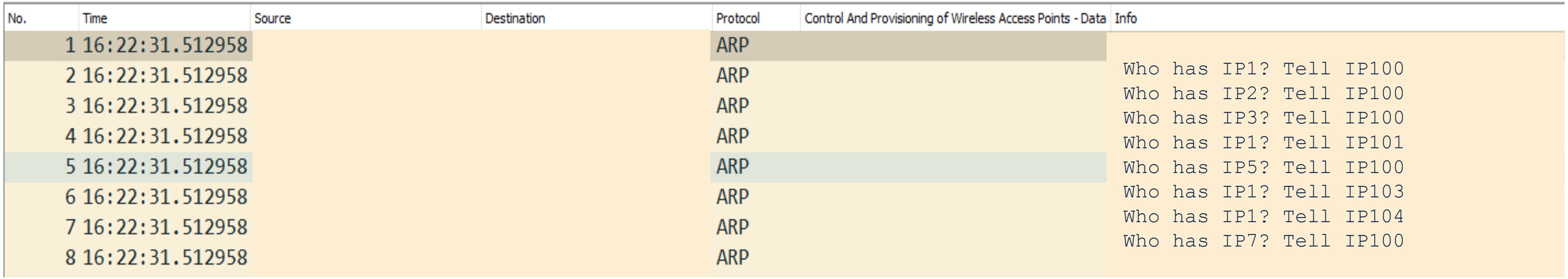
```
monitor capture CPUCAP stop
monitor capture CPUCAP export {bootflash:|tftp:…}/filename.pcap
```

- Once the file is obtained and verified to open in Wireshark, remember to clear the buffer and disable the capture

```
monitor capture CPUCAP clear
no monitor capture CPUCAP
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# EPC CPU Only Analysis



| No. | Time | Source | Destination | Protocol | Control And Provisioning of Wireless Access Points - Data | Info |
|---|---|---|---|---|---|---|
| 1 | 16:22:31.512958 | | | ARP | | Who has IP1? Tell IP100 |
| 2 | 16:22:31.512958 | | | ARP | | Who has IP2? Tell IP100 |
| 3 | 16:22:31.512958 | | | ARP | | Who has IP3? Tell IP100 |
| 4 | 16:22:31.512958 | | | ARP | | Who has IP1? Tell IP101 |
| 5 | 16:22:31.512958 | | | ARP | | Who has IP5? Tell IP100 |
| 6 | 16:22:31.512958 | | | ARP | | Who has IP1? Tell IP103 |
| 7 | 16:22:31.512958 | | | ARP | | Who has IP1? Tell IP104 |
| 8 | 16:22:31.512958 | | | ARP | | Who has IP7? Tell IP100 |

- ARP storm triggered by some clients

# Root Cause / Workaround

- Digging down on the problem clients (client card, OS, driver, supplicant) specific driver was identified as the common factor
- Engaged client card vendor
- Known issue on the driver
- Fixed via driver update

17.3.5+

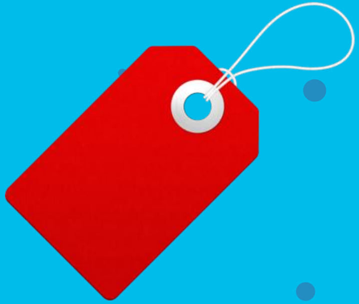
# Optimization on C9800

- Exclude clients triggering the storm based on configurable fields of packets per second and burst-interval.

```
ip arp limit rate <pps>
ip arp limit rate <burst-interval>
ip arp limit rate {pps | burst-interval | none}
```

- PPS = Maximum ARP packets allowed for client/sec (Default:100)
- Burst-interval = consecutive interval in seconds to see max PPS for ARP (Default: 5secs)
- Create explicit exclusion reason for excessive ARP activity

# Tagging Etiquette

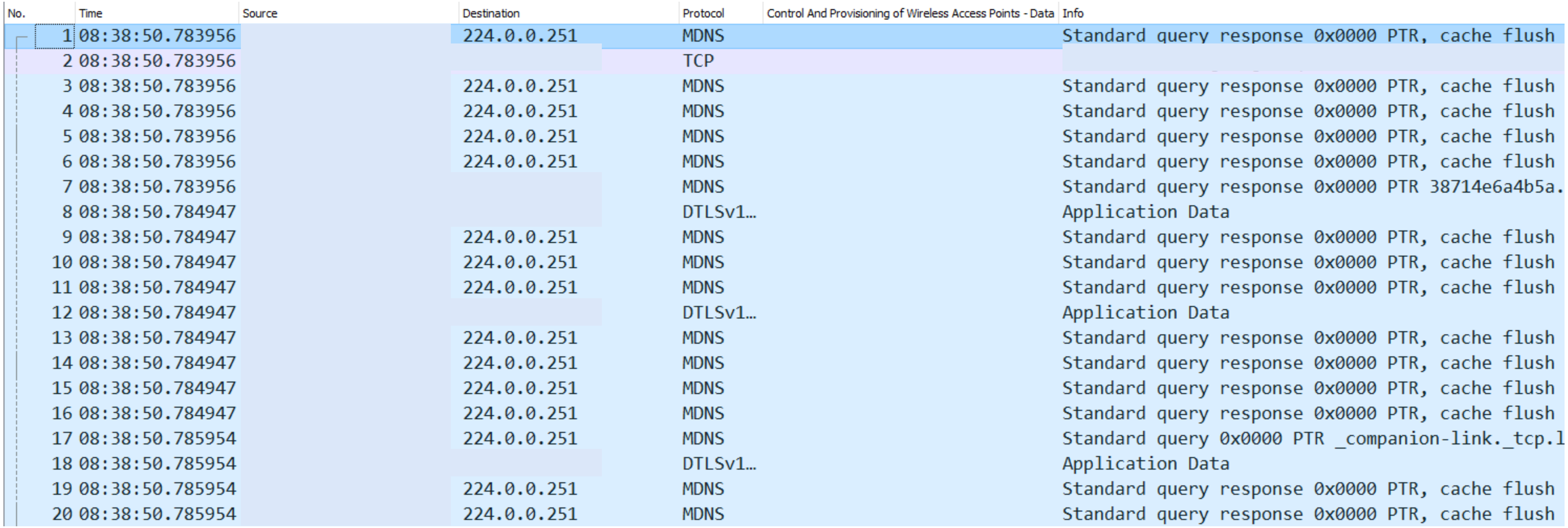


# Context

- U.S University
- C9800, 17.3.4c
- AP Models: 9130s, 2800s
- Problem Symptom: Intermittent network outage **in certain areas** due to AP Flaps

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

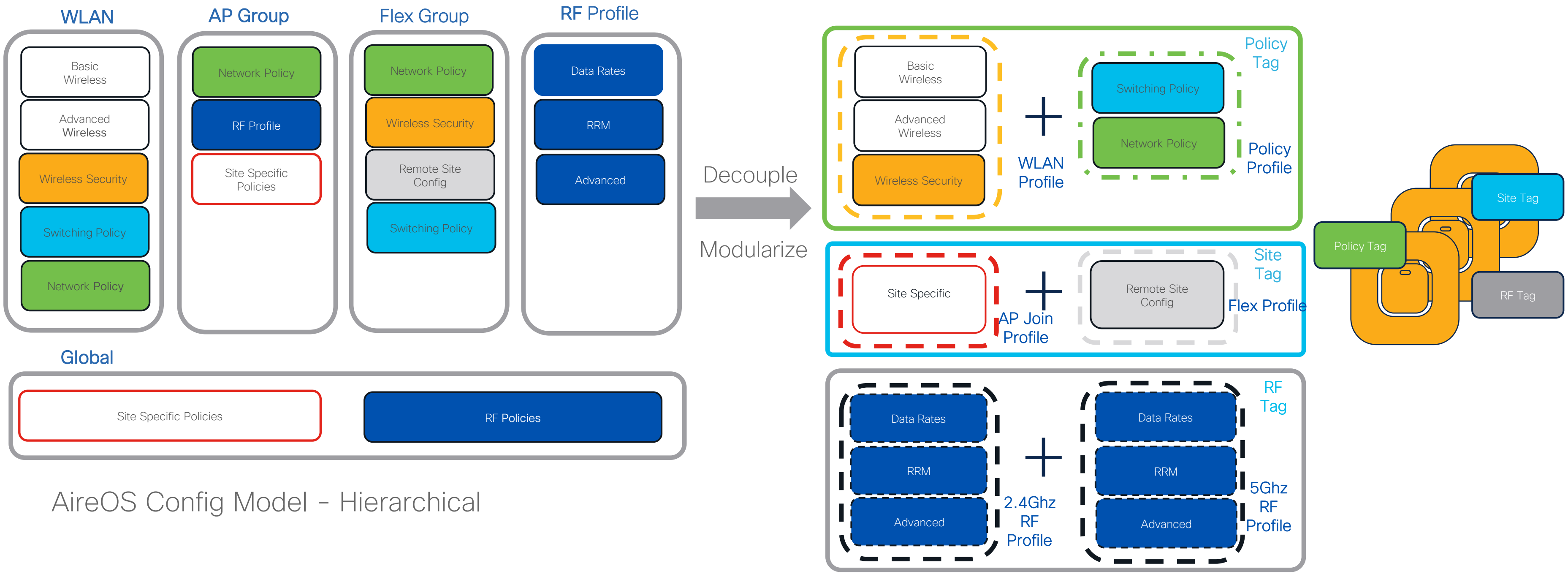
# EPC CPU Analysis



| No. | Time | Source | Destination | Protocol | Control And Provisioning of Wireless Access Points - Data | Info |
|---|---|---|---|---|---|---|
| 1 | 08:38:50.783956 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 2 | 08:38:50.783956 | | | TCP | | |
| 3 | 08:38:50.783956 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 4 | 08:38:50.783956 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 5 | 08:38:50.783956 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 6 | 08:38:50.783956 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 7 | 08:38:50.783956 | | | MDNS | | Standard query response 0x0000 PTR 38714e6a4b5a. |
| 8 | 08:38:50.784947 | | | DTLSv1… | | Application Data |
| 9 | 08:38:50.784947 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 10 | 08:38:50.784947 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 11 | 08:38:50.784947 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 12 | 08:38:50.784947 | | | DTLSv1… | | Application Data |
| 13 | 08:38:50.784947 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 14 | 08:38:50.784947 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 15 | 08:38:50.784947 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 16 | 08:38:50.784947 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 17 | 08:38:50.785954 | | 224.0.0.251 | MDNS | | Standard query 0x0000 PTR _companion-link._tcp.l |
| 18 | 08:38:50.785954 | | | DTLSv1… | | Application Data |
| 19 | 08:38:50.785954 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |
| 20 | 08:38:50.785954 | | 224.0.0.251 | MDNS | | Standard query response 0x0000 PTR, cache flush |

# AireOS vs. Catalyst 9800 Config Model

**Modularized and Reusable** model with **Logical decoupling** of configuration entities



AireOS Config Model – Hierarchical

C9800 Config Model – Non-Hierarchical

# Other References

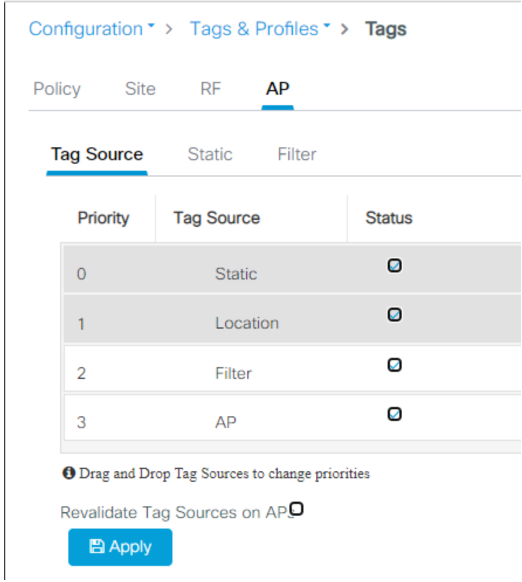
- BRKEWN-2338: Catalyst Wireless – How to Successfully Migrate to Catalyst 9800
- https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Tag Sources and Priority

- Tags are only active after they are applied to one or more APs.
- AP can have multiple tag sources
  - Static – user configured per AP mac
  - Location – Basic Setup Flow
  - Filter – regular expression matching on AP Name
  - AP – tags saved on AP
- These sources are in order of their priority

Statically applied tag is preferred over tags provided by basic setup which, in turn is preferred over filters



Configuration > Tags & Profiles > Tags

Policy Site RF AP

Tag Source Static Filter

| Priority | Tag Source | Status |
|---|---|---|
| 0 | Static | ☑ |
| 1 | Location | ☑ |
| 2 | Filter | ☑ |
| 3 | AP | ☑ |

Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on AP □

Apply

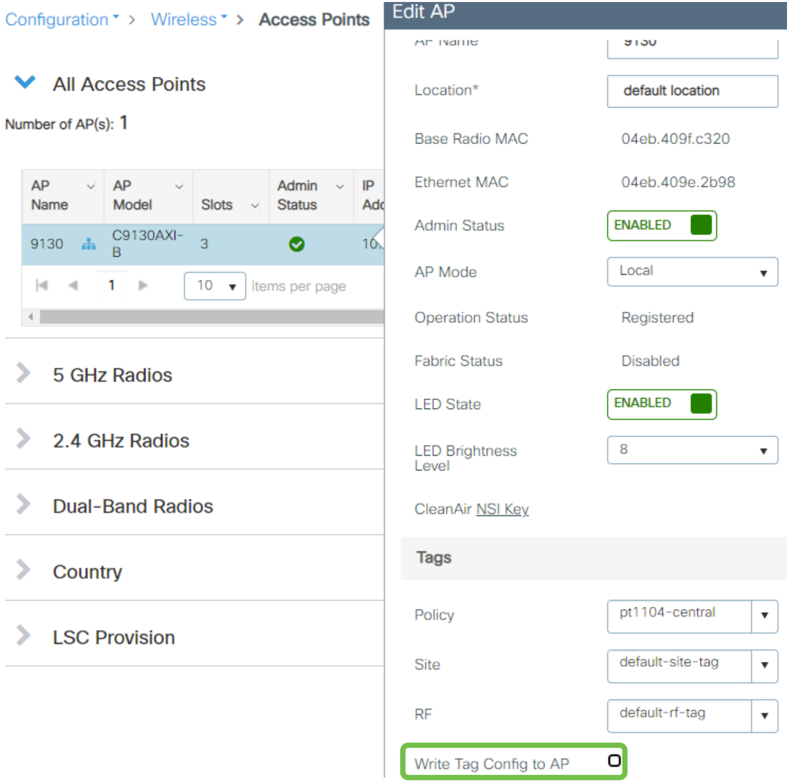
# Tag Persistency

- When an AP joins a C9800, it does not save the tags to its own memory by default.
- Result: When AP moves to another C9800(say WLC2), it will only inherit tags as per the configuration (static or location or filter) on WLC2 or end up with default tags When AP moves
- Explicit configuration is needed to save tags to AP’s flash.
- Before 17.6.1, tags had to be saved on individual APs

  (config)#ap name <APNAME> write tag-config
- Starting 17.6.1, global command was added on C9800

  (config)#ap tag persistency enable

# Tag Persistency



Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

| AP Name | AP Model | Slots | Admin Status | IP Add |
|---|---|---|---|---|
| 9130 | C9130AXI-B | 3 | ✓ | 10. |

1 — 10 items per page

- 5 GHz Radios
- 2.4 GHz Radios
- Dual-Band Radios
- Country
- LSC Provision

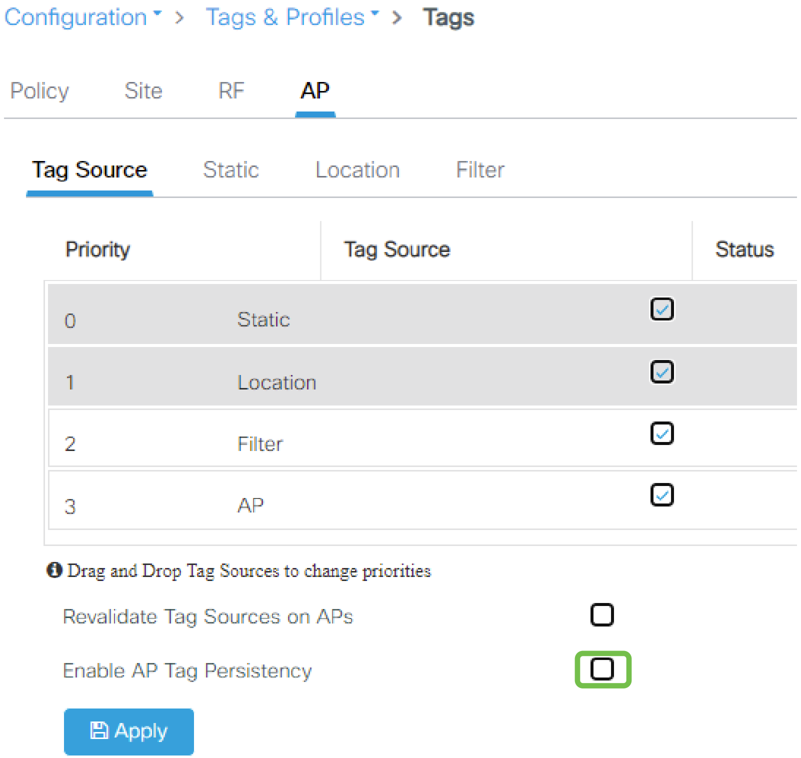
Edit AP

| | |
|---|---|
| AP Name | 9130 |
| Location* | default location |
| Base Radio MAC | 04eb.409f.c320 |
| Ethernet MAC | 04eb.409e.2b98 |
| Admin Status | ENABLED |
| AP Mode | Local |
| Operation Status | Registered |
| Fabric Status | Disabled |
| LED State | ENABLED |
| LED Brightness Level | 8 |
| CleanAir NSI Key | |

Tags

| | |
|---|---|
| Policy | pt1104-central |
| Site | default-site-tag |
| RF | default-rf-tag |

Write Tag Config to AP □



Configuration > Tags & Profiles > Tags

| Priority | Tag Source | Status |
|---|---|---|
| 0 | Static | ☑ |
| 1 | Location | ☑ |
| 2 | Filter | ☑ |
| 3 | AP | ☑ |

Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs □

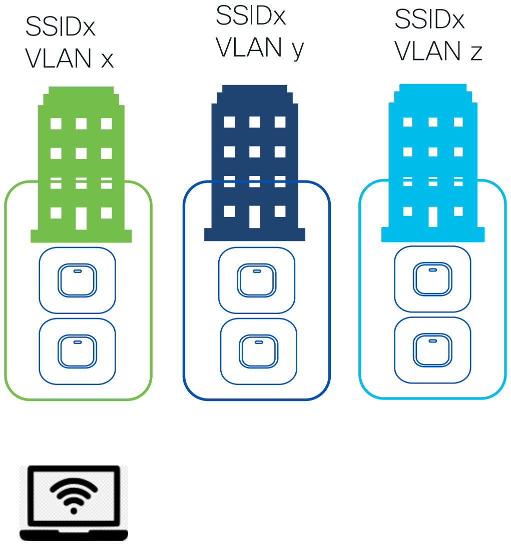
Enable AP Tag Persistency □

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Roaming across Policy Profiles

- Vlan to which wireless clients belong, for a given SSID is defined on the policy profile. Policy tag is then used to map SSID/wlan profile to policy profile.
- On a large campus, multiple policy profiles may be in use to map same SSID to different vlans.
- Until 17.3, roaming between APs tagged with different policy profiles was not supported.
- On 17.3, seamless roaming can be achieving by running global config command

```
wireless client-vlan persistent
```



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

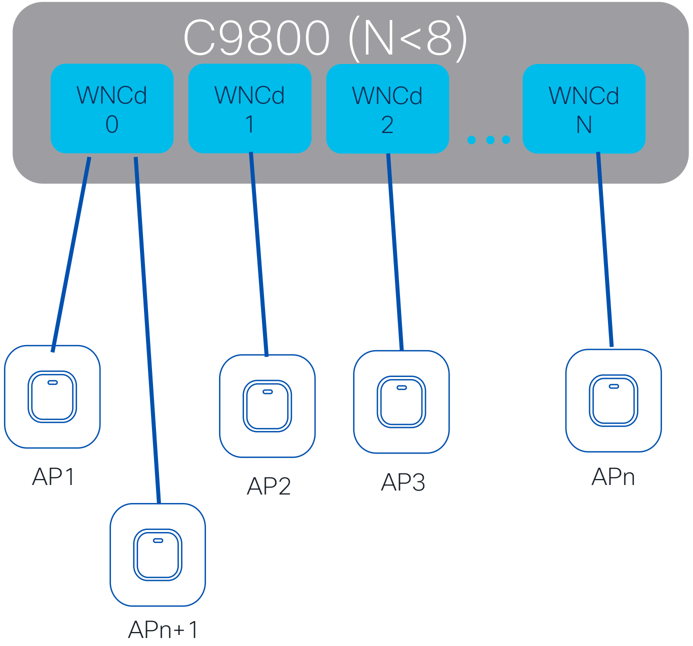
# Workaround / Design Update

- Area affected (or site tag X) is the busiest building – high client count and roaming expected
- WNCd mapping to the site tag X also has 3 other site tags mapped which are all fairly busy
- Other WNCds have site tags with AP count ranging from 1-20

Design Recommendation: Split site tag X

# New Config Model – Site Tag

- With no tag config on C9800, AP gets assigned default tags:
  - Default-policy-tag
  - Default-site-tag
  - Default-rf-tag
- APs get load balanced across WNCd instances round-robin
- Proximity based features like 11k,11v,CHD are managed within each WNCd and only starting will break if neighbors are on different WNCds until 17.7 where this limitation was removed

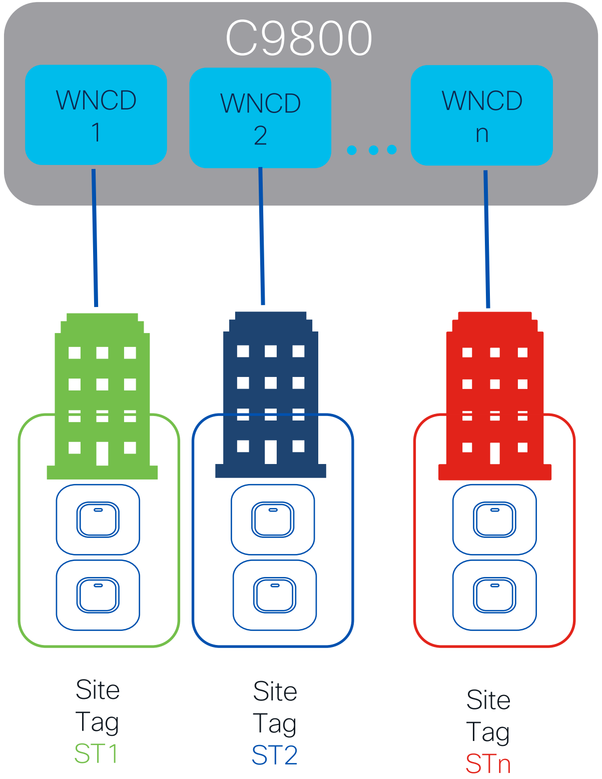


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# New Config Model – Recommendations

- Configure **custom site-tag**
- Assign site-tag based on roaming domain
- For flex, 100 APs per flex site tag (increased to 300 starting 17.8)
- For local mode AP

| | Max APs allowed per site tag | APs recommended per site tag |
|---|---|---|
| 9800-40 | 800 | 500 |
| 9800-80, 9800-CL (med/large) | 1600 | 500 |



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Mapping AP to a WNCd instance

- show wireless loadbalance tag affinity wncd <0-7>
- show wireless loadbalance ap affinity wncd <0-7>

```
AP Mac         Discovery Timestamp       Join Timestamp            Tag
--------------------------------------------------------------------------------
RadMac1      05/27/22 10:08:26         05/27/22 10:08:36         sitetag01
RadMAc2      05/27/22 10:06:53         05/27/22 10:06:59         sitetag01
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Tag balancing

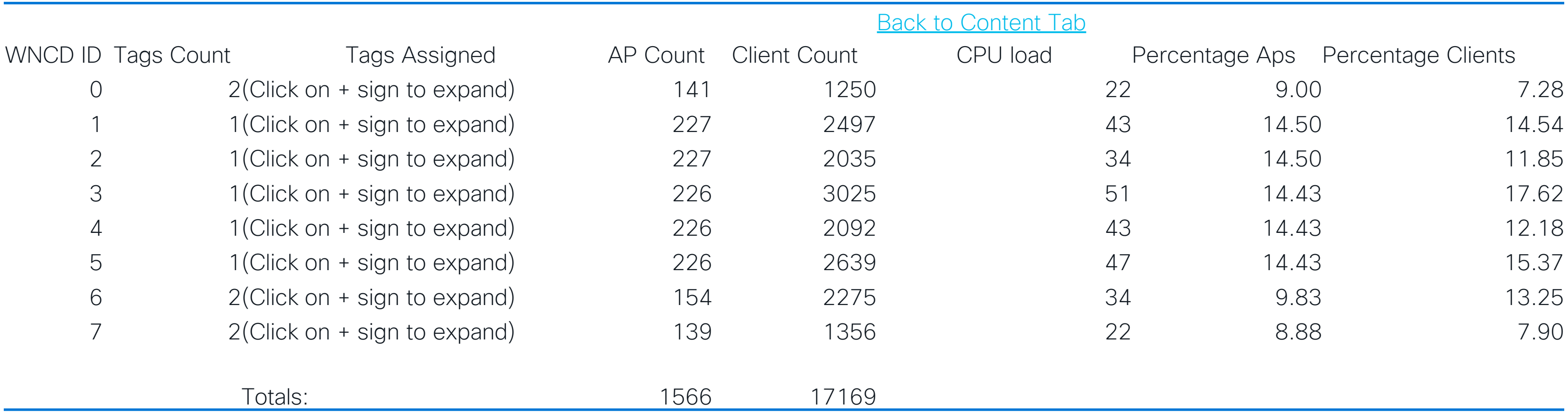
- Tags are allocated to WNCD/CPU as AP join
- Distribution can change
- Ideal scenario: AP/Client count per tag is balanced across WNCDs
- 17.10: Manual influence

```
dao2(config)#wireless tag site eft-test-tag
dao2(config-site-tag)#load ?
  <0-1000>  Estimate of the relative load contributed by the site. AP count can
            be used as an approximation
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Monitoring/Troubleshooting

- WCAE as summarization tool



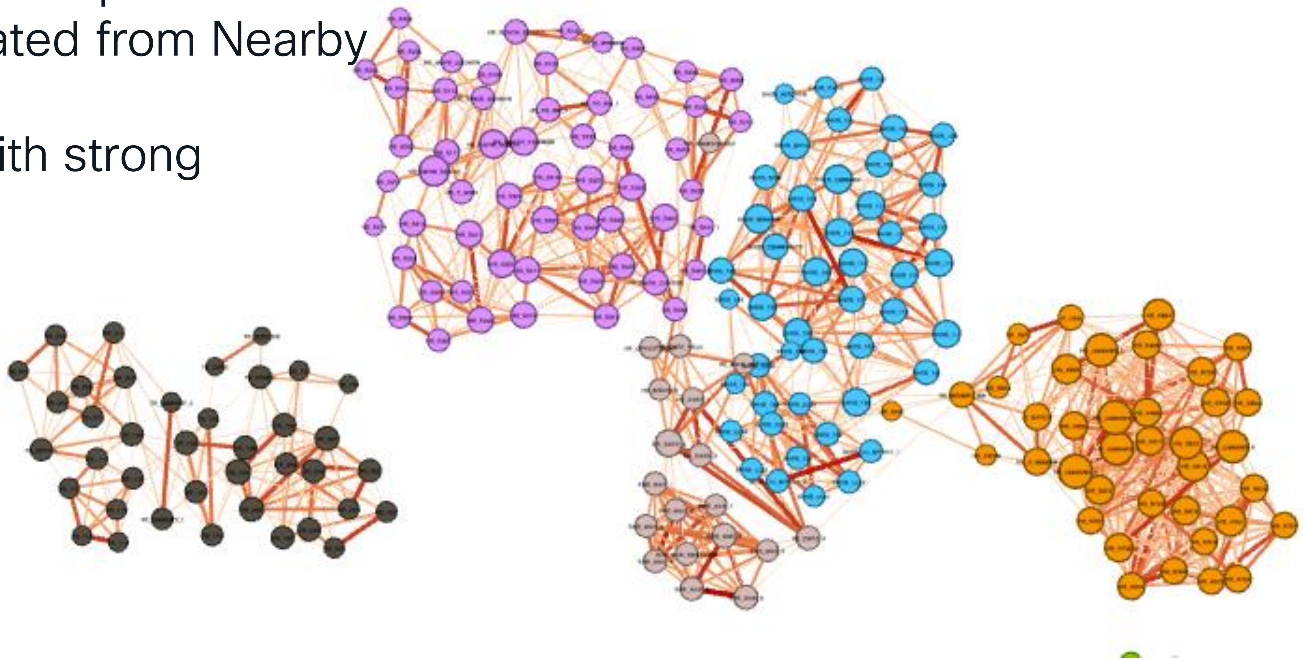
Back to Content Tab

| WNCD ID | Tags Count | Tags Assigned | AP Count | Client Count | CPU load | Percentage Aps | Percentage Clients |
|---|---|---|---|---|---|---|---|
| 0 | 2 | (Click on + sign to expand) | 141 | 1250 | 22 | 9.00 | 7.28 |
| 1 | 1 | (Click on + sign to expand) | 227 | 2497 | 43 | 14.50 | 14.54 |
| 2 | 1 | (Click on + sign to expand) | 227 | 2035 | 34 | 14.50 | 11.85 |
| 3 | 1 | (Click on + sign to expand) | 226 | 3025 | 51 | 14.43 | 17.62 |
| 4 | 1 | (Click on + sign to expand) | 226 | 2092 | 43 | 14.43 | 12.18 |
| 5 | 1 | (Click on + sign to expand) | 226 | 2639 | 47 | 14.43 | 15.37 |
| 6 | 2 | (Click on + sign to expand) | 154 | 2275 | 34 | 9.83 | 13.25 |
| 7 | 2 | (Click on + sign to expand) | 139 | 1356 | 22 | 8.88 | 7.90 |
| | | Totals: | 1566 | 17169 | | | |

# WCAE Tag Creation using AP RF relationships

For reference

- Ideal for large open spaces
- Adjacencies created from Nearby data
- Cluster of Aps with strong relationship

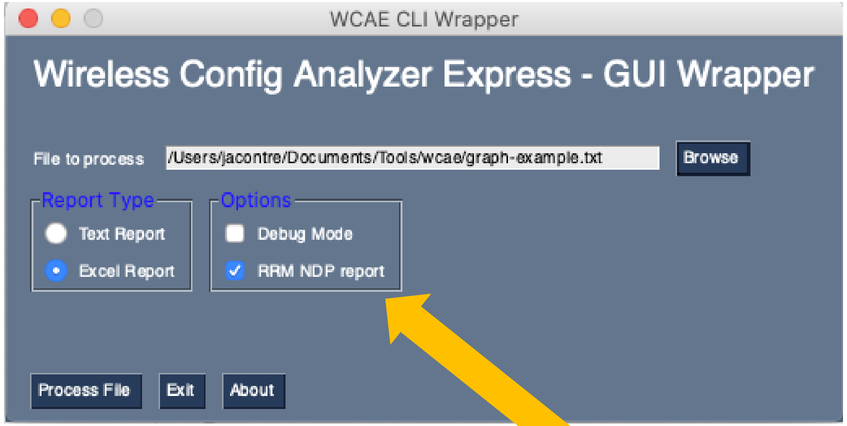


More in BRKEWN-3006

For reference

# RF Graph Analysis

- You need Desktop version
- Uses external tool for visualization and “preparation” (Gephi)
- Few steps required
- https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!rf-graph-analysis-using-wcae-desktop-and-gephi/initial-requirements



WCAE CLI Wrapper

Wireless Config Analyzer Express - GUI Wrapper

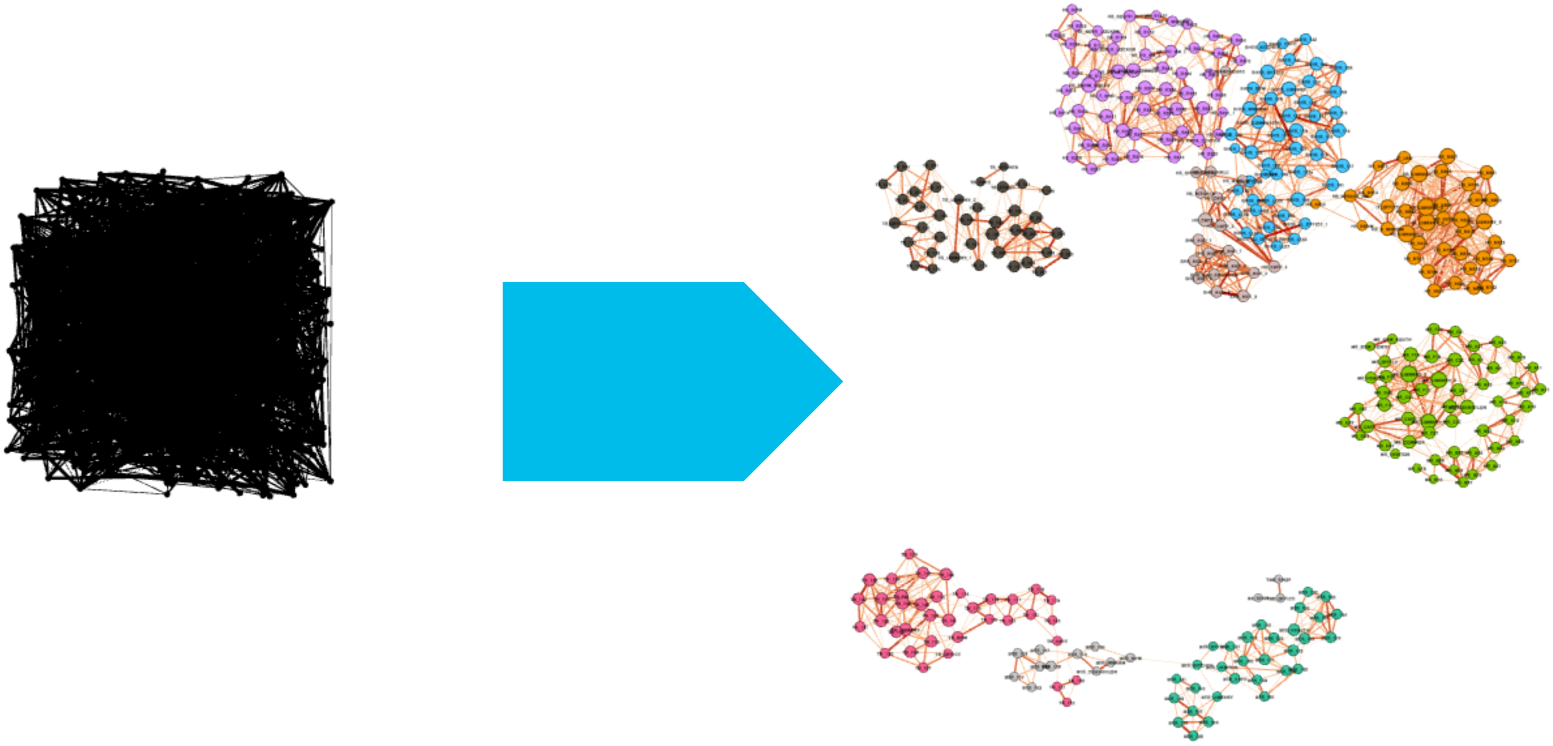
File to process /Users/jacontre/Documents/Tools/wcae/graph-example.txt

Report Type
○ Text Report
● Excel Report

Options
□ Debug Mode
☑ RRM NDP report

# RF Graph Analysis

For reference



# Key Takeaways

- Good design and configuration is the key to preventing network problems
- New Config Model has a learning curve for folks just getting into Catalyst 9800 WLC
- Many documents and tools (on-box and off-box) available to help with AireOS to C9800 migration
- Modularity and Reusability of New Config Model make config management easy for network admins

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# The Real Thing

## Short Extra

# VM Woes

- Wireless client running VM
  - NAT mode works
  - Bridge mode can't get IP address

- Customer provided clear problem description
  - Tested working/non-working scenario
  - Already confirmed capture shows drop done at controller
  - AP models in use
  - Controller version
- Why NAT: Security needs

Parallels®

vmware®

VirtualBox

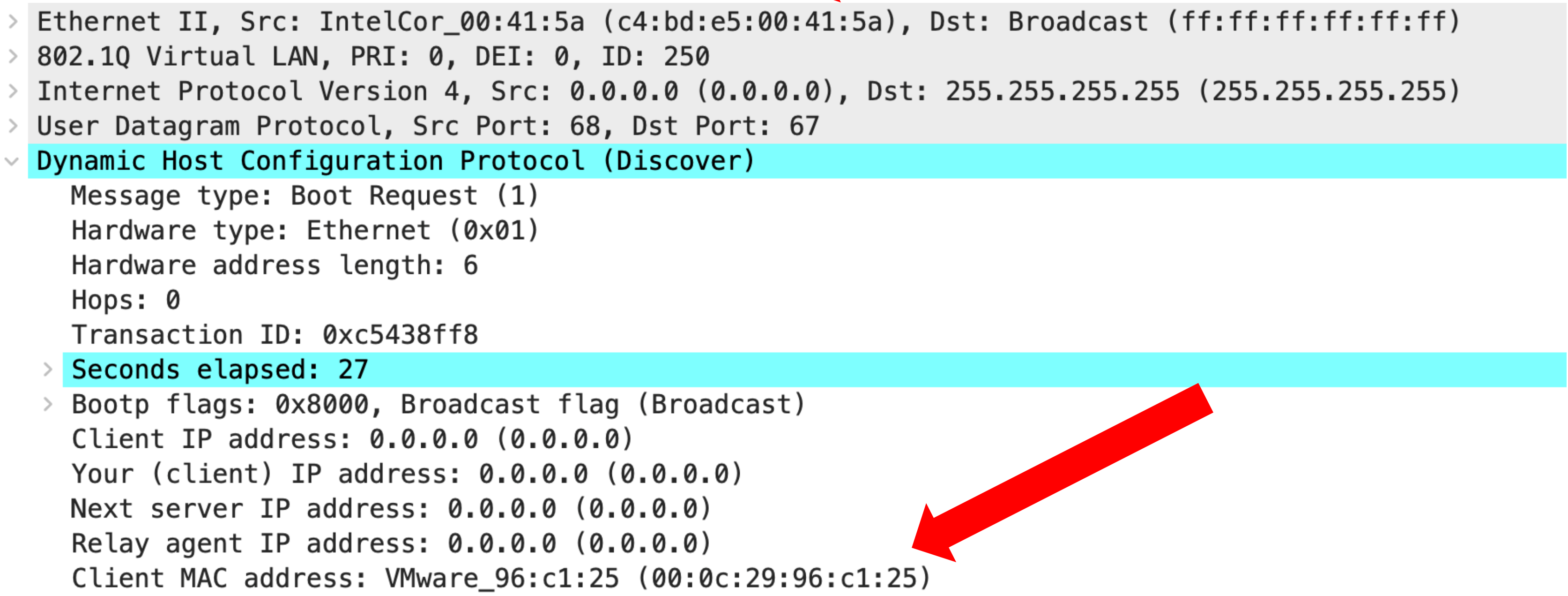
# How it goes

- TAC reproduces problem
  - Enough data to go to lab and try
  - First thought:  defect

- Internal Alias contacted for validation

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# What it is



```
> Ethernet II, Src: IntelCor_00:41:5a (c4:bd:e5:00:41:5a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 250
> Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xc5438ff8
  > Seconds elapsed: 27
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: VMware_96:c1:25 (00:0c:29:96:c1:25)
```

Thid party WGB

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Controller controls!

- Strict address validation for DHCP and ARP payloads
- Good for security
- ARP is not broadcasted
- Passive Client / ARP Broadcast
  - Adds unknown ARP flooding
- Address Binding (17.8)
  - Removes address tracking and enforcement

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Story conclusions

# Happy ending

- Clear problem helped to speed up understanding
- Once the problem was understood, it was matched to existing feature

```
wireless profile policy default-policy-profile
   shutdown
   ipv4 dhcp required
   no ip mac-binding
   passive-client
   no shutdown
```

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Networking

## Catalyst 9800 with Wi-Fi6/6E

Learn from experts on wireless topics such as WiFi6 an WiFi6E standards enhancements. You will understand what you need to know about designing for 6GHz, migrating from AireOS to Catalyst 9800, and what you need to know about 5G and WiFi6E

START

Feb 5 | 16:45
**LABEWN-1528**
9800 Embedded Wireless Controller on Wi-Fi 6 Access Points

Feb 5 | 19:00
**LABEWN-2202**
9800 Wireless Controller Upgrade with Zero Downtime

Feb 7 | 10:00
**BRKEWN-2846**
High Availability Design with Cisco Catalyst 9800 Wireless Controllers

Feb 7 | 11:30
**BRKEWN-2024**
Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points

Feb 7 | 14:45
**BRKEWN-1742**
7 Ways to Fail - on Wi-Fi 6(E)

Feb 7 | 16:45
**BRKEWN-2284**
Becoming a Wi-Fi Guest star: Better Practices for Guest Networks on Cisco Catalyst Wireless

Feb 8 | 08:30
**BRKEWN-3413**
Advanced RF Tuning for Wi-Fi6E with Catalyst Wireless: Become an Expert, while getting a little help from AI

Feb 8 | 10:45
**BRKEWN-2926**
Cisco Wi-Fi: how to tune your design and configurations for your most demanding clients and applications

Feb 8 | 14:00
**LTREWN-2034**
9100 Wi-Fi 6E APs Managed from Cloud or On Premises? We've got you Covered!

Feb 8 | 14:00
**LTREWN-2724**
Be My Guest: Designing and Troubleshooting Wireless Guest Networks with Catalyst 9800 Wireless Controller

If you are unable to attend a live session, you can watch it On Demand after the event

Feb 8 | 14:45
**BRKOPS-2402**
Automate the Deployment of a Wireless Network with the Help of Cisco DNA Center

Feb 9 | 08:30
**BRKEWN-2338**
Successful Migration and Deployment Best Practices for Catalyst 9800 Wireless Networks

Feb 9 | 10:30
**BRKEWN-2087**
High Density Wi-Fi Design, Deployment and Optimization

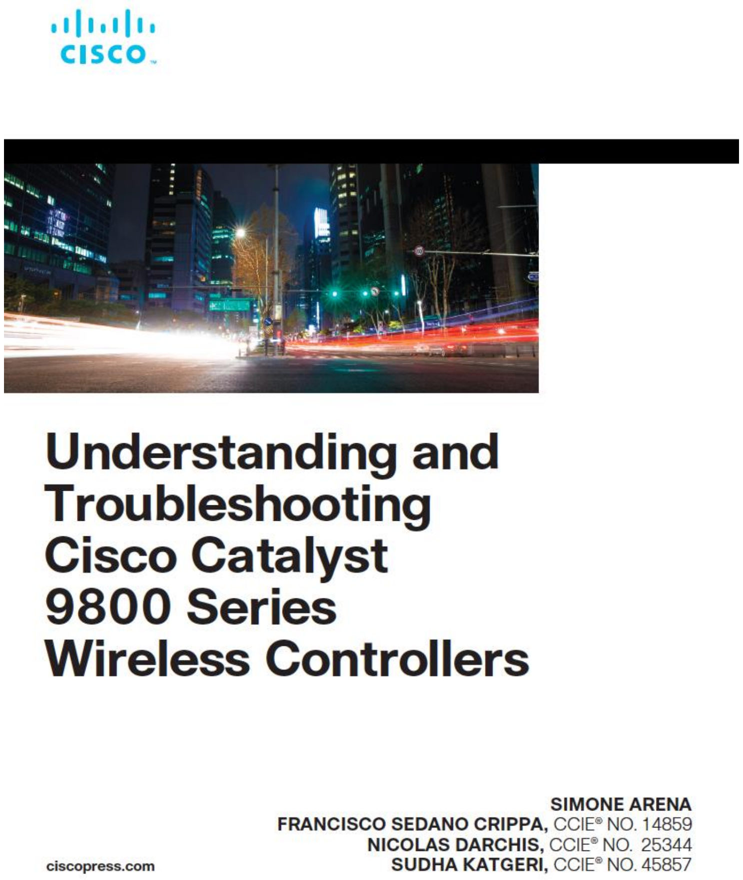
Feb 9 | 15:45
**BRKEWN-2030**
Wi-Fi6/6E and Private 5G for the Enterprise – a 'Better Together' Journey

Feb 9 | 16:00
FINISH **BRKEWN-2094**
Successfully Configuring Catalyst 9800 Wireless on Your First Shot

If you are unable to attend a live session, you can watch it On Demand after the event

# Conclusion

Save 40% on Cisco Press eBooks and 60% on video courses when you use discount code **CISCOLIVE** during checkout. Shop now at [www.ciscopress.com/store](http://www.ciscopress.com/store). Offer valid February 6-10, 2023



cisco

**Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers**

**SIMONE ARENA**
**FRANCISCO SEDANO CRIPPA,** CCIE® NO. 14859
**NICOLAS DARCHIS,** CCIE® NO. 25344
**SUDHA KATGERI,** CCIE® NO. 45857

ciscopress.com

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the " Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

# Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco The bridge to possible

# Thank you

cisco Live!