The bridge to possible

Troubleshoot Catalyst 9800 Wireless Controllers

Javier Contreras Albesa
Principal Engineer
BRKEWN-3628

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-3628

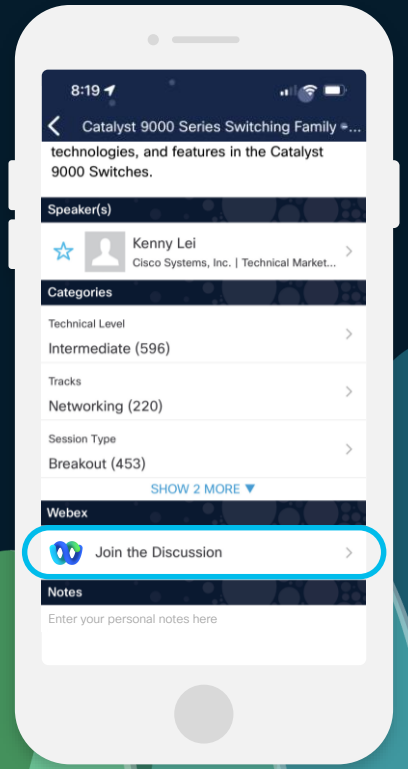
Questions?

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 by the speaker until June 7, 2024.



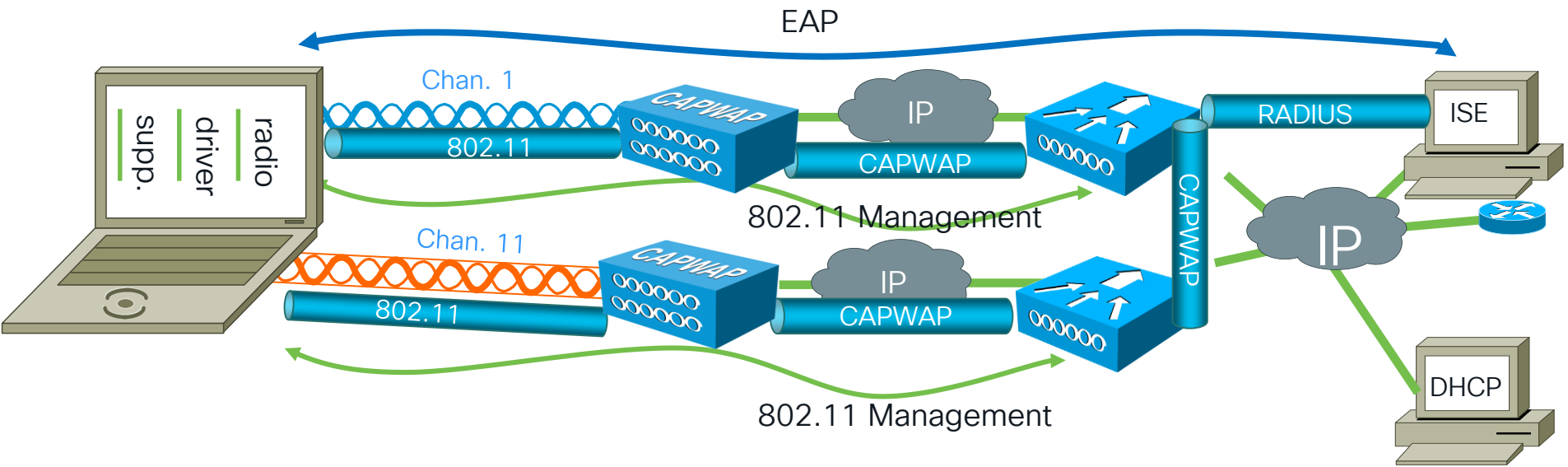
About Javier

Agenda

- Troubleshooting 101
- Architecture Basics
- Cat9800 Control Plane debugging
- Cat9800 Data Plane debugging
- Access point Control Plane debugging
- Access point Data Plane debugging
- WLC top issues
- Conclusion

Troubleshooting 101

Where do we start?

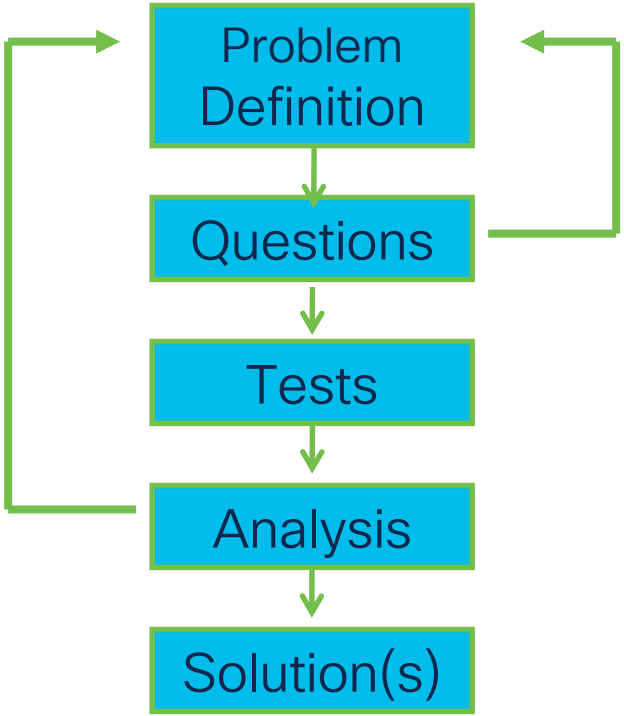


Wireless Link = Complex multi-variable equation

✓ Isolate and remove the variables

Troubleshooting Basics

- Troubleshooting 101
  - Clearly define the problem
  - Understand any possible triggers
  - Know the expected behavior
  - Reproducibility
  - Do not jump to conclusions



Troubleshooting Basics

- Logical and procedural mindset
- Step 1: Define the problem
  - Bad: “Client slow to connect”
  - Good: “Client associations are rejected with Status17 several times before they associate successfully.”
  - Reduce Scope!
  - Isolate multiple possible problems

Troubleshooting Basics

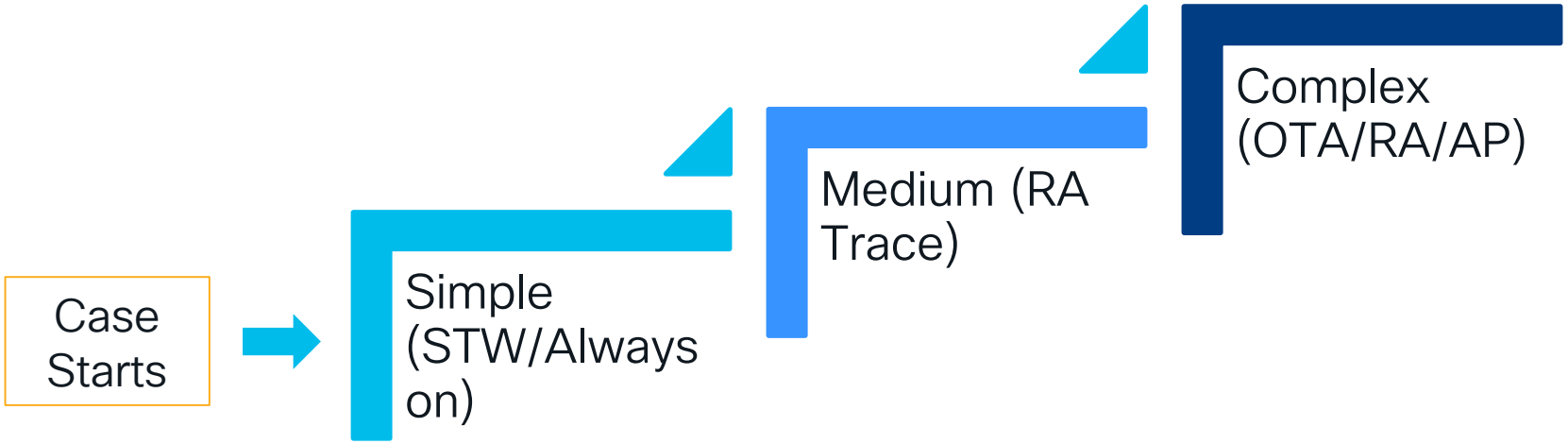
- Step 2: Understand triggers
  - Did it work before?
  - Changes
  - Finding a pattern
- Step 3: Know the expected behavior
  - Example: “One way audio between Phone A and B, because Phone A does not get an ARP Response for Phone B”

Troubleshooting Basics

- Step 4: Reproducibility
  - Reproducible = Easier

- Step 5: Fix
  - Validate Root Cause Analysis
  - Develop Fix
  - Test for solution, intersection

Complexity Control



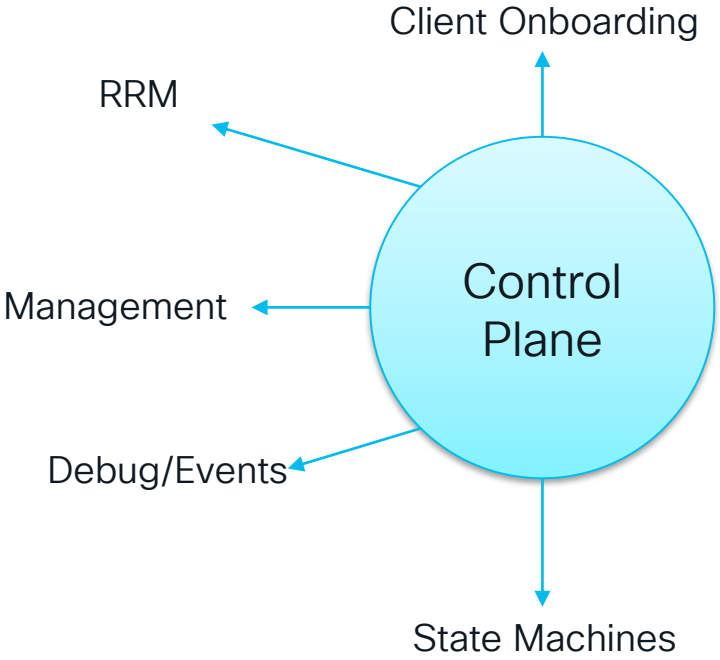
Support Case Starting Suggestions

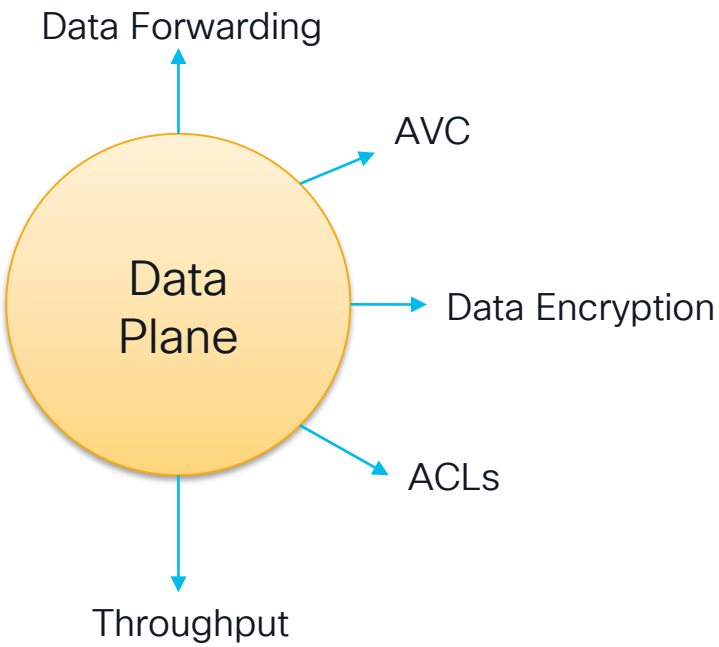
- Client issue:
  - Show tech wireless
  - RA Trace or Always on tracing
- Device Reload
  - Any support bundle/core/crash report
  - Show tech wireless
- Any feature/config question
  - Show tech wireless
- Run WCAE

Architecture Basics

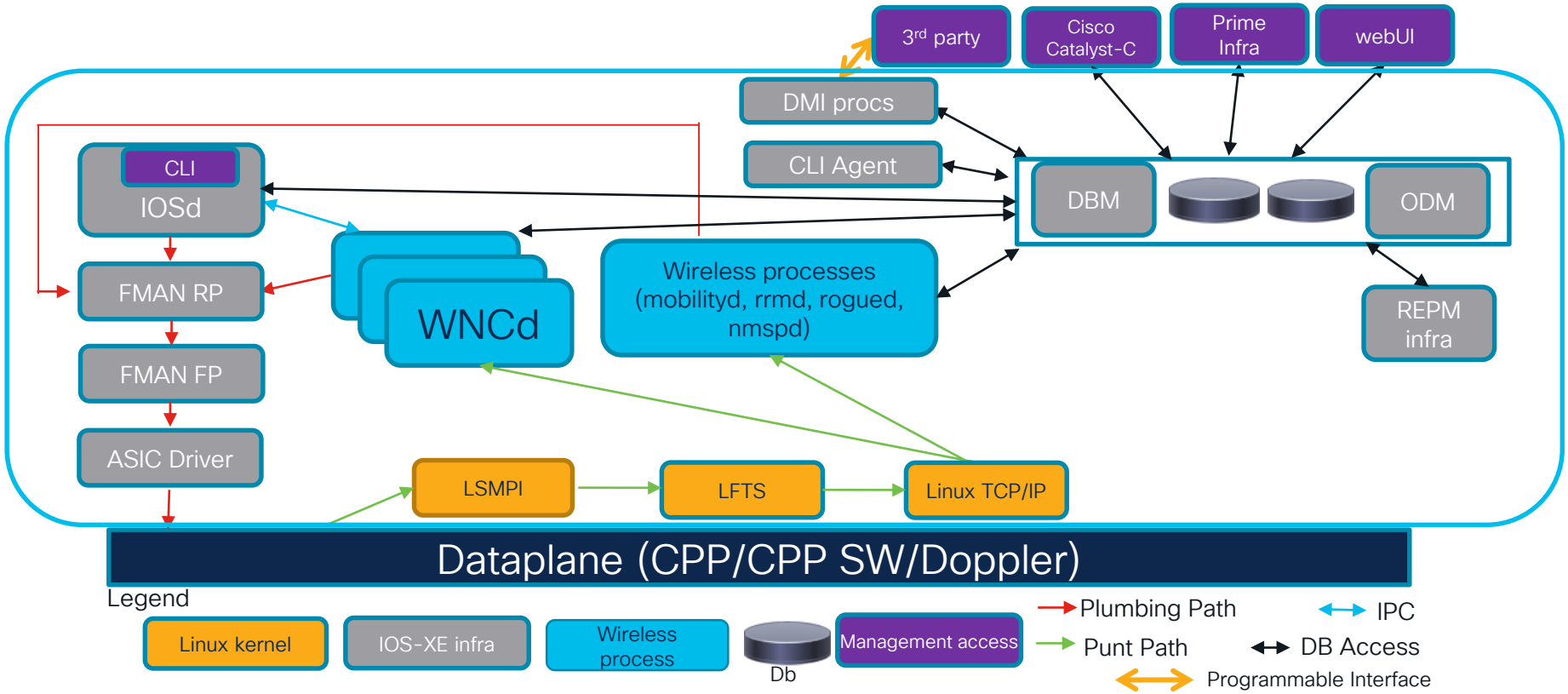
Introduction

Why do I need to care about those control plane and data plane details ?

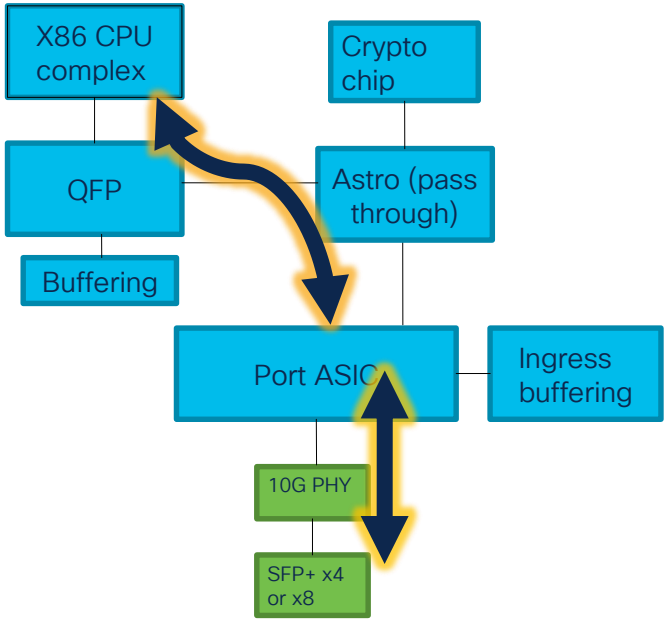




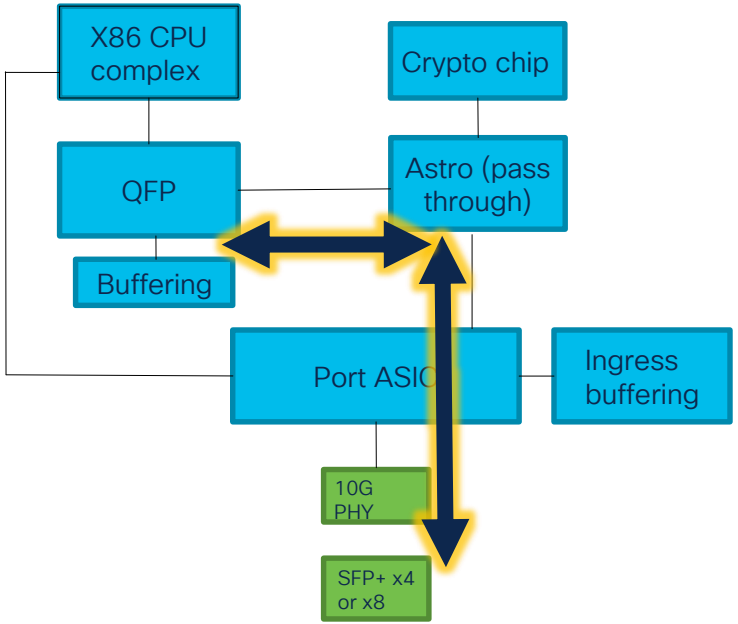
C9800 Software Process Architecture



Life of Packet – Control and Data Plane



Control Plane Packet (Punt/Inject)



Data Plane Packet

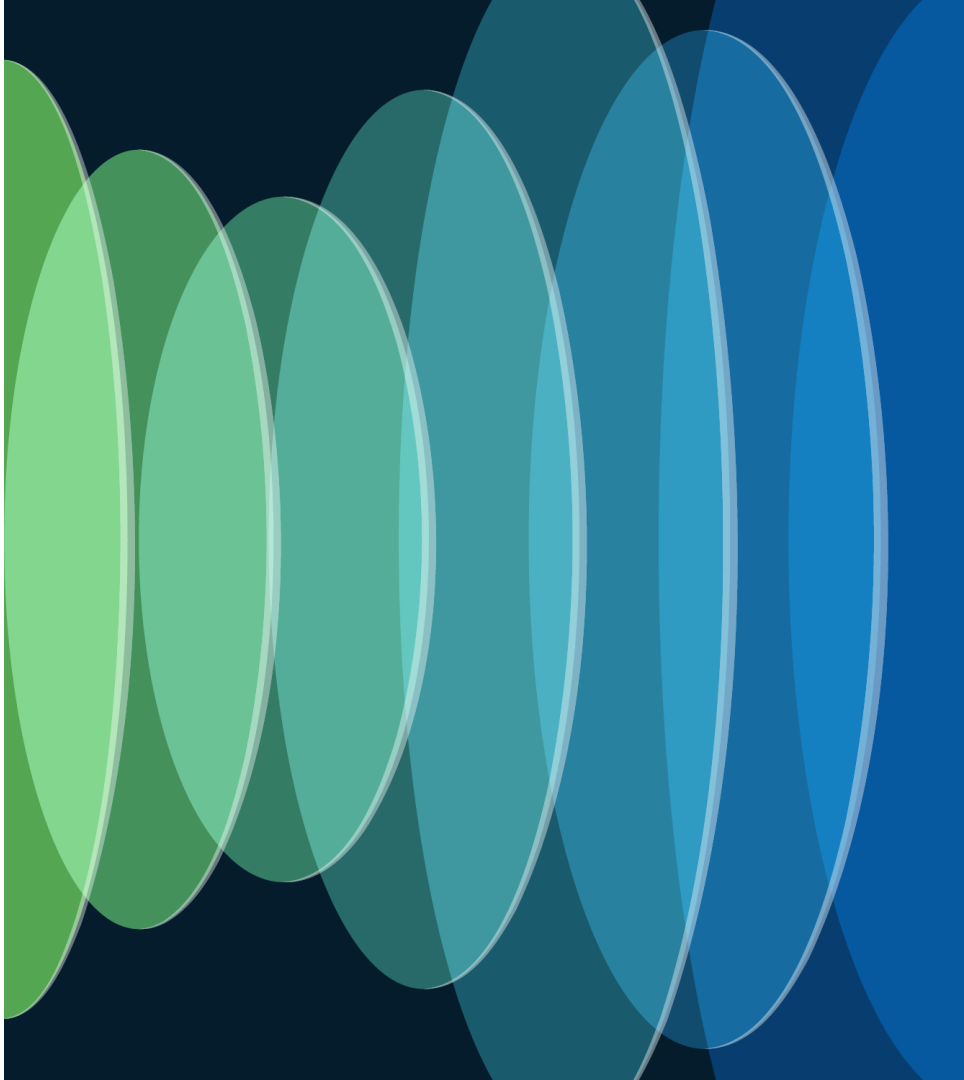
slido

What belongs to Control Plane

ⓘ Start presenting to display the poll results on this slide.

WLC Control Plane

Tracing and Debugging



IOS-XE Tracing/Debugging

IOS Logging

IOSd Syslog:

- System
- Good starting point
- Get it with: `#show logging`

AP Join:

```
May 22 2023 09:34:31.251 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Capwap2, changed state
to up
May 22 2023 09:34:31.249 UTC: %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1 R0/0: wncd:
AP Event: AP Name: ap3800i-r2-sw1-te0-1, MAC: 0042.68a0.ee78 Joined
May 22 2023 09:36:19.548 UTC: %CAPWAPAC_SMGR_TRACE_MESSAGE-3-EWLC_GEN_ERR: Chassis 1 R0/0: wncd:
Error in Session-IP: 192.168.25.101[5264] Mac: 00a3.8ec2.da00 Heartbeat timer expiry for AP. Close
CAPWAP DTLS session
```

IOSd Logging

Admin GUI connection:

```
May 29 2019 08:43:37.238 UTC: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login
Successful from host 192.168.0.110 by user 'admin' using crypto cipher 'ECDHE-RSA-AES128-GCM-
SHA256’
```

Wrong PSK:

```
May 29 2019 08:48:25.388 UTC: %CLIENT_EXCLUSION_SERVER-5-ADD_TO_BLACKLIST_REASON: Chassis 1
R0/0: wncmgrd: Client MAC: 001e.e5e2.35cf was added to exclusion list, reason: Wrong PSK
```

IOS-XE Tracing

- Binary, line rate tracing mechanism
- No CPU impact
- Each BinOS (non-IOSd) process has its own tracelog file (before 17.7)
- Unified tracing in 17.7+
- File starts in memory
- Rotation: At X size - > compressed and moved to disk
- Syslog-like severity levels
- Base infrastructure for other features

IOS-XE Tracing

- Binary trace (Btrace)

```
myc9800-CL#dir bootflash:tracelogs
Directory of bootflash:/tracelogs/
372820  -rw-            5270  Nov 25 2022 13:28:43 +01:00  plogd_R0-0.22150_44788.20221125122727.bin.gz
372746  -rw-            5265  Nov 25 2022 13:27:27 +01:00  plogd_R0-0.22150_44787.20221125122611.bin.gz
372495  -rw-         2263043   Aug 1 2022 23:42:49 +02:00  wncd_x_R0-0.17829_27.20220731171658.bin.gz
372508  -rw-         2290676  Jul 31 2022 19:17:48 +02:00  wncd_x_R0-0.17829_26.20220730103553.bin.gz
372767  -rw-         2284388  Jul 30 2022 12:36:12 +02:00  wncd_x_R0-0.17829_25.20220729001047.bin.gz
372545  -rw-         2276683  Jul 29 2022 02:11:42 +02:00  wncd_x_R0-0.17829_24.20220727124941.bin.gz
372493  -rw-           88311  Jul 28 2022 20:58:02 +02:00  cpp_ha_F0-0.22679_2.20220718170801.bin.gz
```

IOS-XE Tracing

Binary trace levels

- **ERROR** level represent abnormal situations. We want to raise the user attention to these
- **WARNING** represent an incident that could potentially lead to an error (or not…)
- **NOTICE** is the default logging level for binos daemons. It captures significant events if they are normal working conditions. (client connect, failover)
- **INFO** contains details about state machines and the communication flow
- **DEBUG** contains traces needed to root cause failure conditions
- **VERBOSE** voluminous traces more tuned to help developers with bugs

2-Critical
3-Error
4-Warning
5-Notice
6-Info
7-Debug
8-Verbose

Always On tracing

- Contextual Logs WITHOUT debugging
- Each process writes relevant events at Notice level
- General Problem isolation assistance
  - Is client facing authentication issues or DHCP issue or something else
- Helps establish trends
  - Isolate if reported client connectivity problem is specific to certain APs or certain client mac addresses
- Box can store 48h approx. at max HW capacity, weeks typically

Always on Tracing CLI

- Useful commands

```
# show logging process <process daemon>
```

This is last 10 minutes by default

```
# show logging process <process daemon> to-file <alwayson-process.txt>
# more bootflash:alwayson-process.txt
```

```
# copy bootflash:alwayson-process.txt tftp://<serverip>/path OR ftp://user:pass@serverip/path
```

Always on Tracing

This is Most Used

- Aggregated view across processes:

```
# show logging profile wireless filter {mac | ip} {client-mac | mobility-peer-ip}
to-file <alwayson-clientmac>.txt
```

- Focus on time window, export to file

```
# show logging profile wireless start timestamp “MM/DD/YYYY HH:MM:SS” filter mac
<mac addr> to-file <filename>
```

- Changing time displayed

```
# show logging profile wireless start last 30 minutes
```

Always on : successful client connection

RA tracing OFF

```
# show log profile wireless filter mac 0040.96b9.b5c4 to-file output.txt

[client-orch-sm] [24632]: (note): MAC: 0040.96b9.b5c4  Association received. BSSID 0038.df25.f12f, old BSSID 0000.0000.0000, WLAN
1, Slot 1 AP 0038.df25.f120, AP0038.DF24.62A8
[client-orch-state] [24632]: (note): MAC: 0040.96b9.b5c4  Client state transition: S_CO_INIT ->S_CO_ASSOCIATING
[dot11] [24632]: (note): MAC: 0040.96b9.b5c4  Association success. AID 1, Roaming = 0, WGB = 0, 11r = 0, 11w = 0
[client-orch-state] [24632]: (note): MAC: 0040.96b9.b5c4  Client state transition: S_CO_ASSOCIATING ->S_CO_L2_AUTH_IN_PROGRESS
[client-auth] [24632]: (note): MAC: 0040.96b9.b5c4  ADD MOBILE sent. Client state flags: 0x71  BSSID: MAC: 0038.df25.f12f  capwap
IFID: 0xf90400004
[client-auth] [24632]: (note): MAC: 0040.96b9.b5c4  L2 Authentication initiated. method DOT1X, Policy VLAN 1,AAA override = 0
[ewlc-infra-evq] [24632]: (note): Authentication Success. Resolved Policy bitmap:11 for client 0040.96b9.b5c4
[client-auth] [24632]: (note): MAC: 0040.96b9.b5c4  L2 Authentication Key Exchange Start. EAP type: PEAP, Resolved VLAN: 16, Audit
Session id: 22100A090000000E89D69B30
[client-keymgmt] [24632]: (note): MAC: 0040.96b9.b5c4  EAP Key management successful. AKM:DOT1X Cipher:CCMP WPA2
[client-orch-sm] [24632]: (note): MAC: 0040.96b9.b5c4  Mobility discovery triggered. Client mode: Local
[client-orch-state] [24632]: (note): MAC: 0040.96b9.b5c4  Client state transition: S_CO_L2_AUTH_IN_PROGRESS -
>S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
[client-auth] [24632]: (note): MAC: 0040.96b9.b5c4  ADD MOBILE sent. Client state flags: 0x72  BSSID: MAC: 0038.df25.f12f  capwap
IFID: 0xf90400004
[client-orch-state] [24632]: (note): MAC: 0040.96b9.b5c4  Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -
>S_CO_DPATH_PLUMB_IN_PROGRESS
[dot11] [24632]: (note): MAC: 0040.96b9.b5c4  Client datapath entry params - ssid:dot1x_j,slot_id:1 bssid ifid: 0x0, radio_ifid:
0xf90400002
[dpath_svc] [24632]: (note): MAC: 0040.96b9.b5c4  Client datapath entry created for ifid 0xfa0000001
[client-orch-state] [24632]: (note): MAC: 0040.96b9.b5c4  Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -
>S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [24632]: (note): MAC: 0040.96b9.b5c4  Client IP learn successful. Method: DHCP IP: 9.10.16.121
[client-orch-state] [24632]: (note): MAC: 0040.96b9.b5c4  Client state transition: S_CO_IP_LEARN_IN_PROGRESS ->S_CO_RUN
```

Always on : successful client connection

RA trace ON

```
2022/02/25 09:30:14.179966 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     19  "dc-protocol-map=9"
2022/02/25 09:30:14.179972 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     30  "dhcp-option=                "
2022/02/25 09:30:14.179977 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     57  "dhcp-option=                                        "
2022/02/25 09:30:14.179983 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     25  "dhcp-option=            "
2022/02/25 09:30:14.180003 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Framed-IP-Address   [8]      6  10.6.119.13
2022/02/25 09:30:14.180006 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Framed-IPv6-Address [168]   18  ...
2022/02/25 09:30:14.180026 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  User-Name           [1]     14  "Nico"
2022/02/25 09:30:14.180032 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     43  "audit-session-id=91208A0A001379C630372E5F"
2022/02/25 09:30:14.180037 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     13  "vlan-id=691"
2022/02/25 09:30:14.180043 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     14  "method=dot1x"
2022/02/25 09:30:14.180046 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Called-Station-Id   [30]    19  "00-1e-49-2a-8c-ff"
2022/02/25 09:30:14.180050 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Calling-Station-Id  [31]    19  "00-22-58-2b-1c-30"
2022/02/25 09:30:14.180054 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  NAS-IP-Address      [4]      6  10.138.32.145
2022/02/25 09:30:14.180057 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  NAS-Port-Id         [87]    17  "capwap_90400156"
2022/02/25 09:30:14.180061 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  NAS-Port-Type       [61]     6  802.11 wireless          [19]
2022/02/25 09:30:14.180070 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     23  "cisco-wlan-ssid=ssw"
2022/02/25 09:30:14.180076 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Cisco AVpair       [1]     29  "wlan-profile-name=300-ssw"
2022/02/25 09:30:14.180082 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:   Airespace-WLAN-ID  [1]      6  300
2022/02/25 09:30:14.180085 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Nas-Identifier      [32]    15  "sdegdc99n3001"
2022/02/25 09:30:14.180088 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Session-Id     [44]    10  "00017cdc"
2022/02/25 09:30:14.180092 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Input-Octets   [42]     6  0
2022/02/25 09:30:14.180095 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Input-Giga-Words[52]     6  0
2022/02/25 09:30:14.180098 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Output-Octets  [43]     6  0
2022/02/25 09:30:14.180101 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Output-Giga-Words[53]     6  0
2022/02/25 09:30:14.180104 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Input-Packets  [47]     6  0
2022/02/25 09:30:14.180108 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Output-Packets [48]     6  0
2022/02/25 09:30:14.180111 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Authentic      [45]     6  Remote                   [3]
2022/02/25 09:30:14.180115 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Status-Type    [40]     6  Watchdog                 [3]
2022/02/25 09:30:14.180118 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Event-Timestamp     [55]     6  1645781414
2022/02/25 09:30:14.180121 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  Acct-Delay-Time     [41]     6  0
2022/02/25 09:30:14.180175 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS: Started 2 sec timeout
2022/02/25 09:30:14.180192 {wncd_x_R0-1}{1}: [auth-mgr] [22336]: (info): [0022.582b.1c30:capwap_90400156] Device type for the session is detected as Un-Classified Device and old Un-Classified Device &Device name for the sess
2022/02/25 09:30:14.186568 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS: Received from id 1813/188 10.138.16.74:0, Accounting-response, len 20
2022/02/25 09:30:14.186576 {wncd_x_R0-1}{1}: [radius] [22336]: (info): RADIUS:  authenticator 0b af 5e 94 b8 e7 72 0a - d7 1d c8 a2 a8 d7 02 42
2022/02/25 09:30:14.193967 {wncd_x_R0-1}{1}: [sisf-packet] [22336]: (info): RX: DHCPv4 from interface capwap_90400156 on vlan 691 Src MAC: 0008.e3ff.fc04  Dst MAC: 0022.582b.1c30  src_ip: 10.4.215.21, dst_ip: 255.255.255.255
2022/02/25 09:30:16.880012 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'ping'(app-id: 0xd0001df), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:30:17.879130 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'dhcp'(app-id: 0xd00000d), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:30:19.880687 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'unknown'(app-id: 0xd000001), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided
2022/02/25 09:30:28.494692 {wncd_x_R0-1}{1}: [client-orch-sm] [22336]: (info): MAC: 0022.582b.1c30  Failed to get ewlc dot11 packet handler. Dot11 action processing error. Dropping request
2022/02/25 09:30:56.947807 {wncd_x_R0-1}{1}: [client-orch-sm] [22336]: (info): MAC: 0022.582b.1c30  Failed to get ewlc dot11 packet handler. Dot11 action processing error. Dropping request
2022/02/25 09:31:15.229113 {wncd_x_R0-1}{1}: [client-orch-sm] [22336]: (info): MAC: 0022.582b.1c30  Failed to get ewlc dot11 packet handler. Dot11 action processing error. Dropping request
2022/02/25 09:31:33.150633 {wncd_x_R0-1}{1}: [client-orch-sm] [22336]: (info): MAC: 0022.582b.1c30  Failed to get ewlc dot11 packet handler. Dot11 action processing error. Dropping request
2022/02/25 09:31:46.295867 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'ping'(app-id: 0xd0001df), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:31:46.296145 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'protocol-0xd000000'(app-id: 0xd000000), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <r
2022/02/25 09:31:46.296176 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'icmp'(app-id: 0x1000001), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:31:46.296205 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'protocol-0xd000000'(app-id: 0xd000000), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <r
2022/02/25 09:31:46.296228 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'snmp'(app-id: 0x30000a1), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:31:46.296351 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'icmp'(app-id: 0x1000001), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided>,
2022/02/25 09:31:46.296380 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'ping'(app-id: 0xd0001df), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided>,
2022/02/25 09:31:46.296407 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'snmp'(app-id: 0x30000a1), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:31:46.296420 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'snmp'(app-id: 0x30000a1), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided>,
2022/02/25 09:31:46.296436 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'snmp'(app-id: 0x30000a1), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided>,
2022/02/25 09:31:46.296472 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'dhcp'(app-id: 0xd00000d), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided>,
2022/02/25 09:31:46.296490 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'dhcp'(app-id: 0xd00000d), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:31:46.298170 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'snmp'(app-id: 0x30000a1), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction egress (1), WLAN ID <not provided>, #
2022/02/25 09:31:46.298192 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'snmp'(app-id: 0x30000a1), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided>,
2022/02/25 09:31:46.298224 {wstatsd_R0-0}{1}: [avc-stats] [21340]: (debug): Received stats record for app 'snmp'(app-id: 0x30000a1), client MAC: 0022.582b.1c30  , SSID 'sswa2', direction ingress (0), WLAN ID <not provided>,
2022/02/25 09:31:46.715441 {wncd_x_R0-1}{1}: [client-orch-sm] [22336]: (info): MAC: 0022.582b.1c30  Failed to get ewlc dot11 packet handler. Dot11 action processing error. Dropping request
```

Wireless Debug Analyzer

Cisco TAC Tool - Wireless Debug Analyzer

Javier Contreras

Show Advanced Debug Insights NEW!!

Select a client MAC Address and connection to see logs.

Download CSV

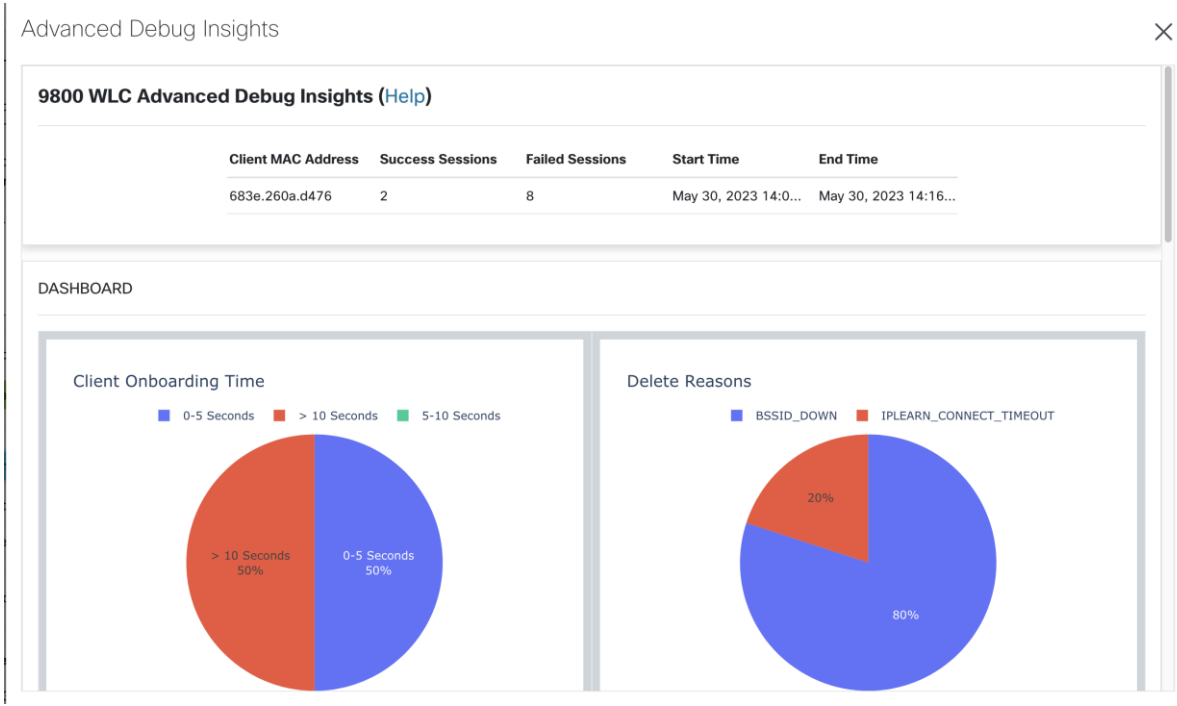
683e.260a.d476

Connection 2 of 11 1 2 3 4 5 ... 11

Show Time Show Task Show Translated Show Original Show Prior First Connection Show All

Time	Task	Translated
2023/05/30 14:08:27.671	client-orch-sm	Client roamed to a new AP/BSSID: BSSID f01[illegible]6e, WLAN test, Slot 1 AP f01[illegible], Floor6-AP4
2023/05/30 14:08:27.671	dot11	Association success for client, assigned AID is: 1. Client performed fast roam.
2023/05/30 14:08:27.671	client-orch-sm	Client started layer 2 authentication (either dot1X or PSK)
2023/05/30 14:08:27.699	client-auth	Entering 802.1X authentication process
2023/05/30 14:08:27.699	client-auth	Entering 802.1X authentication process
2023/05/30 14:08:27.700	dot1x	Controller/AP sent EAPOL Identity Request to client

Wireless Debug Analyzer



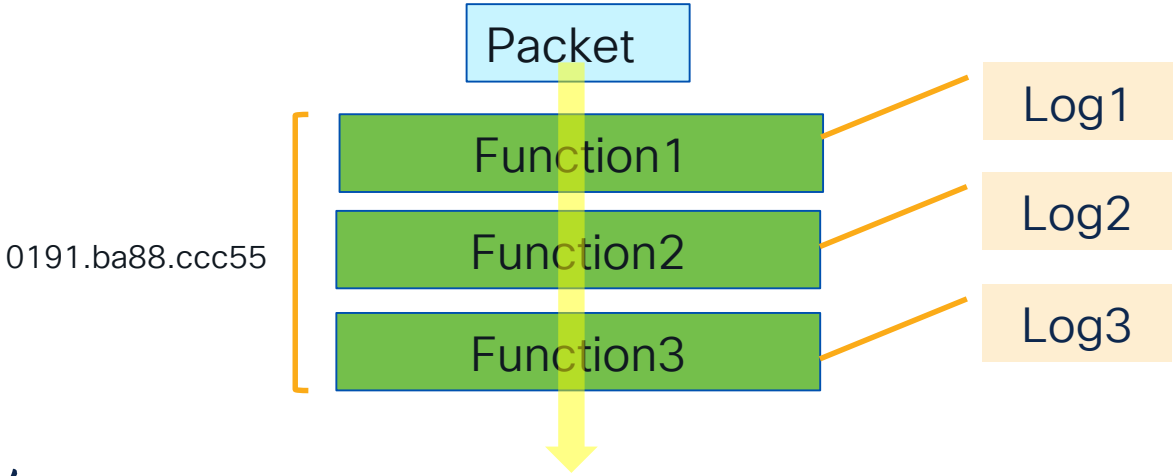
Problem example 1

Yesterday we had many users complaining about wifi in a given area

- Always on logs of selected clients.
  - Connection last state (stuck in IP LEARN?) ?
  - Were they being intentionally disconnected ?
  - RADIUS / authentication issue ?
- Cisco Catalyst Center can be key

What is Radioactive Tracing

- Track “trace of execution” for a given application context
- Application defines what is interesting
- Only context has increased verbosity



Radioactive Tracing

RA trace automatically enables all debugs when a given MAC or IP is processed

Troubleshooting > Radioactive Trace

Conditional Debug Global State: Stopped

Wireless Debug Analyzer

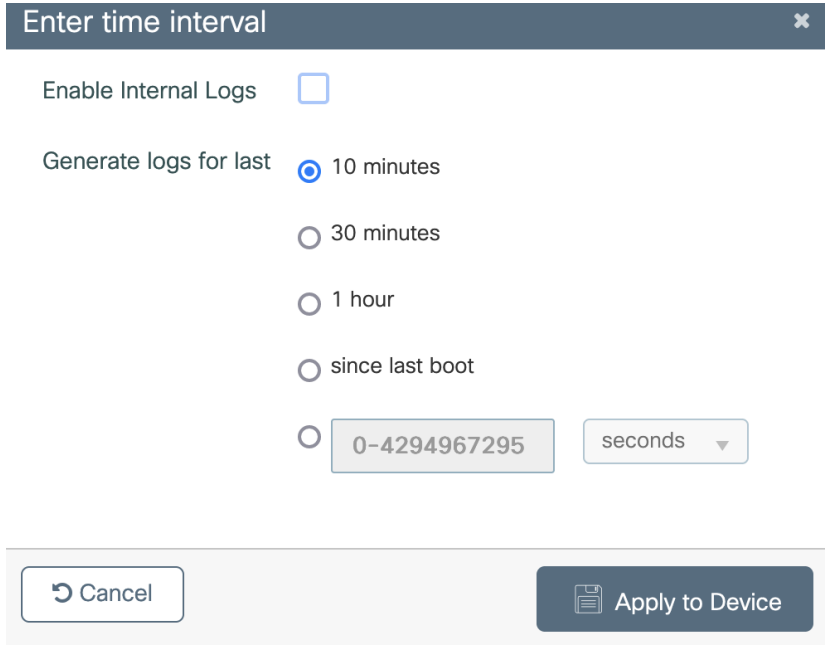
Add | Delete | Start | Stop

	MAC/IP Address	Trace file	
☐	1111.2222.3333		Generate

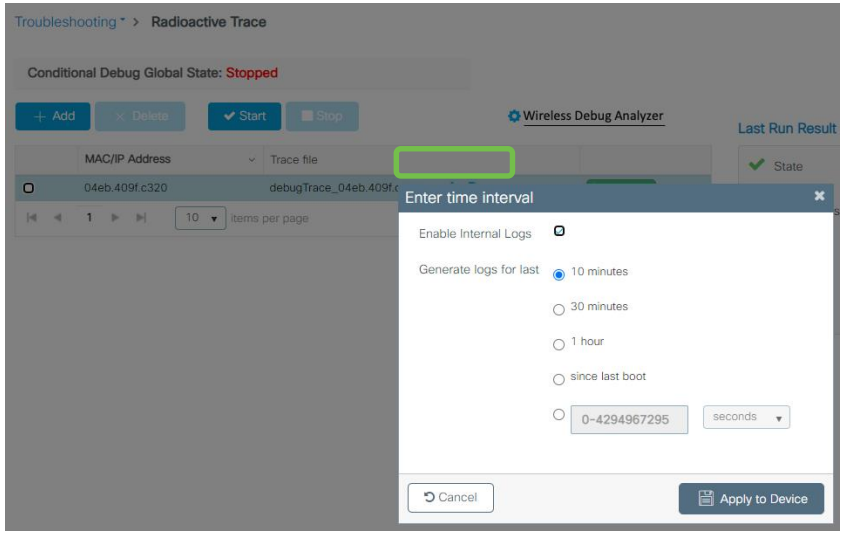
1 | 10 items per page | 1 - 1 of 1 items

Radioactive Tracing

Clicking “Generate” will decode the on-flash binary logs and collate a readable text file filtered on the mac/IP requested.



Radioactive Tracing with Internal Flag



- Logs extremely verbose
- Only need to collect TAC and BU is involved
- Always On: 14 lines
- RA Trace: 400 lines
- RA Trace + Internal: 3000 lines

Radioactive Tracing

- Debug wireless CLI is a macro
- RA tracing for a period of time
- Collates the result

```
#debug wireless mac 1111.2222.3333 ?
 ftp-server    Move log file to FTP server, temporary storage: "flash:/"
 internal      Collect all logs.(Default: only customer curated logs)
 level         Select logs above specific level (Default: debug)
 monitor-time  Max time to trace the condition (Default: 30min)
 to-file       File path in internal storage, default storage: "flash:/"
<cr>          <cr>
```

Radioactive Tracing

Basic client/AP data collection:

- Data is there, just pull it…
- Collect data with `show logging profile wireless filter {mac | ip}`

Advanced client/AP:

- Use Radioactive Tracing
- `debug wireless mac mac.of.client ftp-server ser.ver.ip.add /directory`

Basic Box logs

- Traditional show logs/syslog

Live Debugging

- Optional: Output on real time
- Similar to AireOS “debug client”
- Console is reserved

```
monitor logging profile wireless filter mac <mac>
```

Radioactive Trace – Association Failures

- Client sends disassociate

```
[client-orch-sm] [20370]: (info): MAC: <CLIENT_MAC>  Deleting the client, reason: 2,
CO_CLIENT_DELETE_REASON_DEAUTH_OR_DISASSOC_REQ, Client state S_CO_RUN
[client-orch-sm] [20370]: (note): MAC: <CLIENT_MAC>  Client delete initiated. Reason:
CO_CLIENT_DELETE_REASON_DEAUTH_OR_DISASSOC_REQ, fsm-state transition
00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|01|07|13|17|18|28|33|42|44|46|48|4d|5c|5e|7f|a4|
```

- Data Rate Mismatch in Client Association Request

```
[dot11-validate] [23406]: (ERR): MAC: <CLIENT_MAC>  Dot11 validate radio rates. Missing Supported Rate for
index = 5, encode value: 12, radio type: DOT11_RADIO_TYPE_BG
```

- AP has max clients connected

```
[ewlc-infra-evq] [17707]: (ERR): <CLIENT_MAC> CLIENT_ASSOC_FAIL Failure = IE_POST_VALIDATION_FAILURE
Validation Failure Type = 17, WLAN profile = WLAN1, Policy profile = POLICY1
[dot11] [17707]: (ERR): MAC: <CLIENT_MAC> Dot11 update co assoc fail. Sent assoc failure to CO. delete
reason: 41, CO_CLIENT_DELETE_REASON_DOT11_MAX_STA
[client-orch-sm] [17707]: (note): MAC: <CLIENT_MAC>  Client delete initiated. Reason:
CO_CLIENT_DELETE_REASON_DOT11_MAX_STA, fsm-state transition
00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|01|08|10|
```

RadioActive Trace – Failed Authentication

- Group Key Update Failed

```
[client-keymgmt] [23562]: (ERR): MAC: CLIENT_MAC  Keymgmt: Failed to eapol key m5
retransmit failure. Max retries for M5 over
[client-orch-sm] [23562]: (ERR): MAC: CLIENT_MAC  L2 Authentication of station failed.
[client-orch-sm] [23562]: (note): MAC: CLIENT_MAC  Client delete initiated. Reason:
CO_CLIENT_DELETE_REASON_GROUP_KEY_UPDATE_TIMEOUT, fsm-state transition
```

- AAA Server Down

```
[errmsg] [17837]: (note): %DOT1X-5-FAIL: Authentication failed for client CLIENT_MAC)
with reason (AAA Server Down) on Interface capwap_9000000c AuditSessionID
0B7CFB2C000002145E61348E
[ewlc-infra-evq] [17837]: (ERR): SANET_AUTHC_FAILURE - AAA Server Down username , audit
session id 0B7CFB2C000002145E61348E
[errmsg] [17837]: (note): %SESSION_MGR-5-FAIL: Authorization failed or unapplied for
client (CLIENT_MAC) on Interface capwap_9000000c AuditSessionID
0B7CFB2C000002145E61348E. Failure reason: Authc fail. Authc failure reason: AAA Server
Down.
[client-orch-sm] [17837]: (note): MAC: a86d.aa32.5271  Client delete initiated. Reason:
CO_CLIENT_DELETE_REASON_AAA_SERVER_UNAVAILABLE, fsm-state transition
00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|01|07|
13|1a|23|
```

Customer problem example 2

Client A is facing some problems everyday at some point

- RA trace of the client running for the whole day

Radioactive Tracing bundle

New in 17.10/ 17.9.2

Client debug bundle:

- Show tech wireless
- Show tech wireless client mac <client mac>
- RA traces
- Optional packet capture
- Show logging
- In 17.11+: AP logs are also included

Radioactive Tracing bundle

New in 17.10/ 17.9.2

```
To Enable RA traces and client details
C9800# debug wireless bundle client <client_mac1 ...client_mac5>
To disable
C9800# no debug wireless bundle client <client_mac1 ...client_mac5>
```

```
To Enable Packet capture
C9800# debug wireless bundle include epc client <mac>
To disable
C9800# no debug wireless bundle include epc client <mac>
```

Radioactive Tracing bundle

New in 17.10/ 17.9.2

```
C9800#show bootflash: | inc 2022.tar
1047    1230336 Sep 19 2022 17:20:01.0000000000 +00:00
wireless_bundle_42e4.cb89.e878 _171958_UTC_Sep_19_2022.tar
1048     316416 Sep 19 2022 17:40:51.0000000000 +00:00
wireless_bundle_42e4.cb89.e878_174050_UTC_Sep_19_2022.tar
C9800#
```

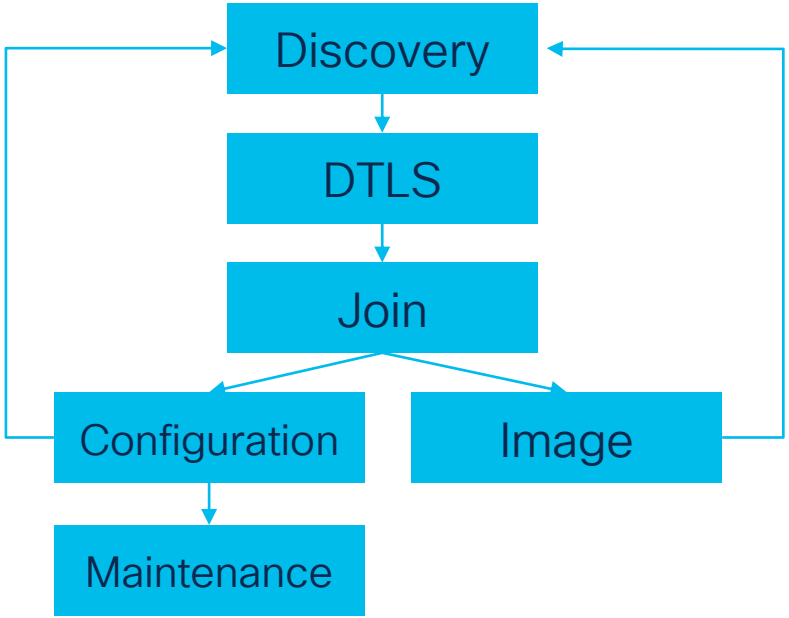
```
C9800#copy
bootflash:wireless_bundle_42e4.cb89.e878_060908_UTC_Sep_20_2022.tar
tftp://<TFTP IP>/<TFTP PATH>
C9800#
```

Customer problem example 3

My new APs are not joining the WLC

- Controller known information about AP
- RA trace of one AP MAC
- AP console (syslog) outputs
- PCAPs

AP Join Process



AP Discover/Join

- Known
- Configured
- Broadcast
  - Reaches WLCs with MGMT Interface in local subnet of AP
  - Use “ip helper-address <ip>” with “ip forward-protocol udp 5246”
- Dynamic
  - DNS: cisco-capwap-controller
  - DHCP: Option 43
- PnP
  - Only with no config

Debugging AP Join Issues

- Basics First

```
9800cl-1#sh ap uptime
Number of APs: 3


AP Name                Ethernet MAC    Radio MAC       AP Up Time       Association Up Time
-----------------------------------------------------------------------------------------------
ap9136-1               687d.b45c.14bc  687d.b45e.f7b0  175 days 1 hour  21 days 8 hours 17 min
ap9136-4               687d.b45c.1398  687d.b45e.ea00  153 days 1 hour  21 days 6 hours 52 min
9130I-r3-sw2-1_0_40    04eb.409e.1dc4  04eb.409f.5480  0  days 1 hour   0 days 0 hours 52 min
```

slido

AP joins after a disconnect. What is the first command you collect ?

ⓘ Start presenting to display the poll results on this slide.

Debugging AP Issues

```
9800cl-1#sh wireless stats ap join summary

Number of APs: 7


Base MAC        Ethernet MAC    AP Name                    IP Address       Status      Last Failure Phase    Last Disconnect Reason

-----------------------------------------------------------------------------------------------------------------------------------------

0042.68c6.4870  0042.68a0.d248  ap3800i-r3sw2-te-1-0-39-dev 192.168.41.49    Joined      NA                    NA

04eb.409f.5480  04eb.409e.1dc4  9130I-r3-sw2-1_0_40         192.168.41.43    Joined      NA                    NA

0c75.bdb5.7e80  0c75.bdb6.28c0  9130E-r3-sw2-g1012          192.168.41.48    Joined      NA                    NA

0042.68c6.4870  687d.b45c.1398  ap9136-4                    192.168.41.44    Joined      Run                   Heart beat timer expiry

687d.b45e.f240  687d.b45c.1448  ap9136-2                    192.168.41.47    Joined      Run                   Max Retransmission to AP

687d.b45e.f7b0  687d.b45c.14bc  ap9136-1                    192.168.41.46    Joined      NA                    NA

687d.b45f.1160  687d.b45c.16e0  ap9136-3                    192.168.41.45    Joined      Run                   Wtp reset config cmd sent
```

Debugging AP Issues

```
9800cl-1#show wireless stats ap mac-address 0042.68c6.4870   join detailed

Discovery phase statistics

..

Last AP message decryption failure details

  Reason for last message decryption failure              : NA

AP reported disconnect detail

  Disconnect reason from AP                               : Max retransmission reached

AP reported reboot detail

  Reboot reason from AP                                   : Reboot cmd from AP console

Last AP disconnect details

  Last Disconnect Phase                                    : NA

  Last Disconnect Reason                                   : NA

  Last Disconnect Time                                    : NA

  Current Join Status                                     : Joined
```

Debugging AP Issues

- Collect logs
  - Radio mac: general
  - Ethernet mac: discovery/dtls

```
show logging profile wireless filter mac 687d.b45c.16e0

2023/06/07 19:27:53.753618033 {wncmgrd_R0-0}{1}: [capwapac-discovery] [15193]: (note): MAC:
687d.b45f.1160  Public IP learnt is FALSE, public IP discovery is FALSE, private IP discovery is TRUE.

2023/06/07 19:27:53.753751387 {wncmgrd_R0-0}{1}: [capwapac-discovery] [15193]: (note): MAC:
687d.b45f.1160  IP:192.168.41.246[5256], Discovery Response sent

2023/06/07 19:27:53.937692128 {wncmgrd_R0-0}{1}: [capwapac-discovery] [15193]: (note): MAC:
687d.b45f.1160  Public IP learnt is FALSE, public IP discovery is FALSE, private IP discovery is TRUE.

2023/06/07 19:27:53.937843498 {wncmgrd_R0-0}{1}: [capwapac-discovery] [15193]: (note): MAC:
687d.b45f.1160  IP:192.168.41.246[5256], Discovery Response sent
```

Debugging AP Side

- Check Logs first!

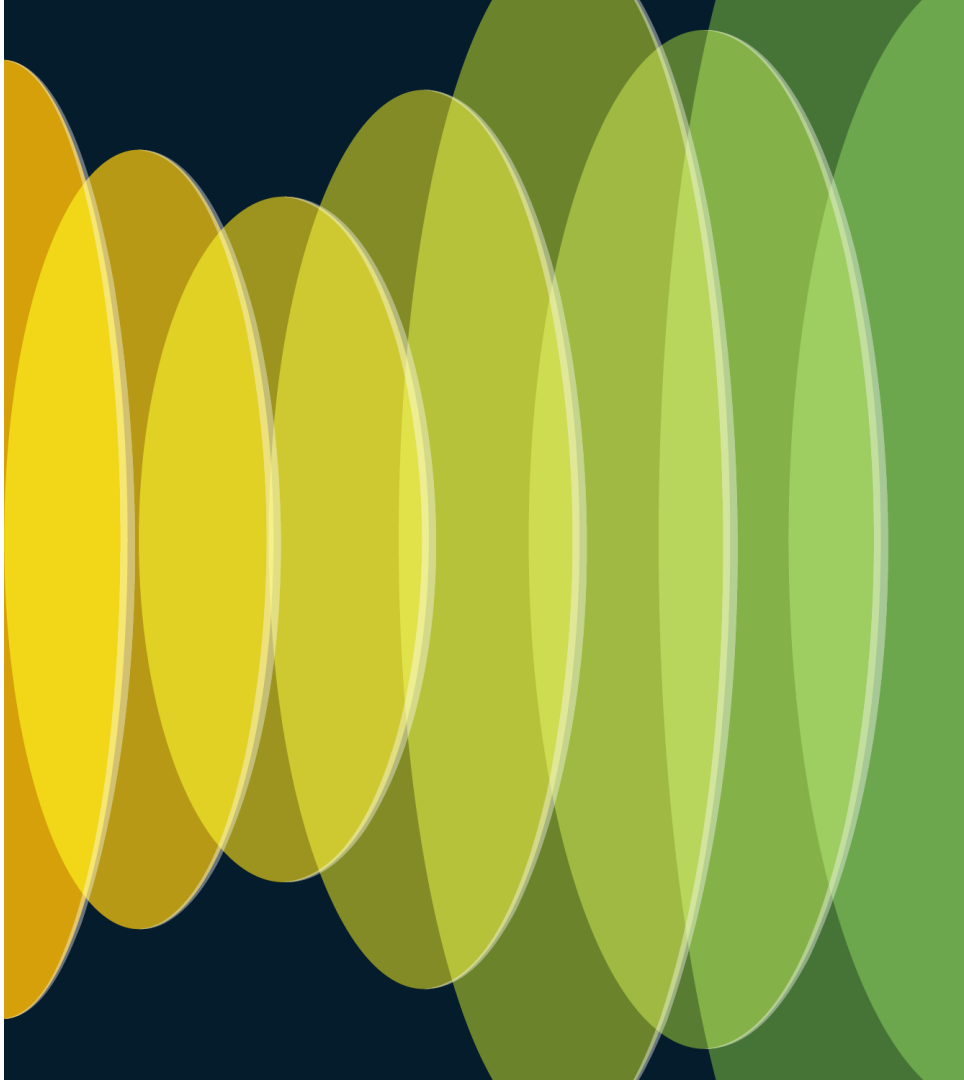
```
ap9136-3#sho log

Console logging : Level - notification, Status - enabled

Syslog logging  : Level - information, Status - active, IP - 255.255.255.255

Syncing syslogs to flash every 600 seconds.

System logging :

May 27 04:01:48 kernel: [*05/27/2023 04:01:48.5450] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=238,
NumofPendingMsgs=2

May 27 04:01:48 kernel: [*05/27/2023 04:01:48.5450]

May 27 11:59:54 kernel: [*05/27/2023 11:59:54.6813] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=243,
NumofPendingMsgs=2
```

Debugging AP Side

- CAPWAP Client debug as next step

```
ap9136-3#deb cap client error

ap9136-3#deb cap client events

[*06/07/2023 17:41:39.7436] CAPWAP State: Run

[*06/07/2023 17:41:39.7460] CAPWAP moved to RUN state stopping post join timer

[*06/07/2023 17:41:39.7472] CAPWAP IP nexthopmac F872.EAB7.3A40

[*06/07/2023 17:41:39.7668] CAPWAP data tunnel ADD to forwarding SUCCEEDED

[*06/07/2023 17:41:39.8051] AP has joined controller 9800cl-1

[*06/07/2023 17:41:39.8056] AP in local mode config starting timer

[*06/07/2023 17:41:39.8066] Change State Event Response from 192.168.40.10

[*06/07/2023 17:41:39.8070] IOT device ttyiot0 not found

[*06/07/2023 17:41:39.8286] Change State Event Response from 192.168.40.10
```

Other debugging points



Unconditional debugging

1. Enable **set platform software trace <rrm-mgrd | nginx | nmspd> chassis active R0 all debug**
2. Reproduce the issue
3. Collect **show logging process <rrm-mgrd | nginx | nmspd> to-file <FILENAME.txt>**
4. View with **more bootflash:FILENAME.txt**
5. Export with **copy bootflash:FILENAME.txt {tftp| ftp|https|scp }**
6. Disable traces with **undebug all** OR **set platform software trace <> chassis active R0 all notice**

Client Delete Reasons

- Tracking “all” client removal events, good and bad
- Around 320 delete points, both form controller and AP
- Covers:
  - Normal (session timeout/idle timeout)
  - Errors/Defects (i.e. wrong bits in M2)
  - “It depends” (i.e. Key timeout)

```
9800-cl#sh wireless stats client delete reasons

Total client delete reasons

---------------------------

Controller deletes

---------------------------

Datapath plumb                                          : 0

WPA key exchange timeout                                : 107

802.11w MAX SA queries reached                          : 0
```

Client Delete Reasons

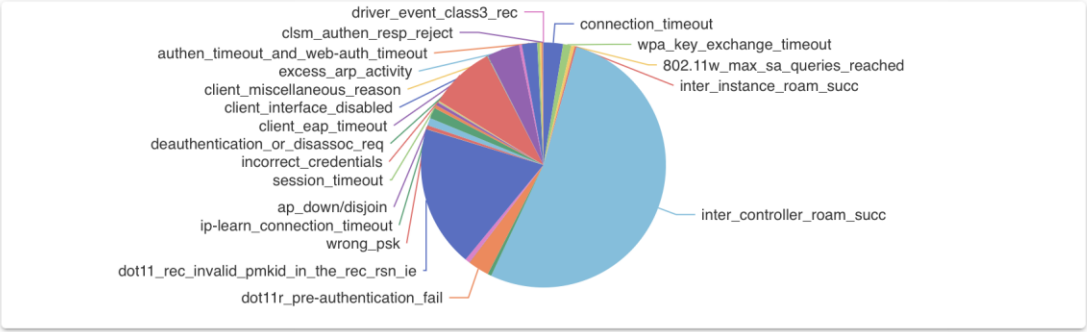
Wireless Config Analyzer Express

WCAE
GUI: 0.7, Engine:0.31

Welcome to WCAE | File: WLC7 MeetingV(10.130.240.17)--20-46-25.log | Feedback

- Summary
- Checks
- Access Points
- Controller
- Site Tags
- WLANs Summary
- AP RF View
- RF Profiles
- Channel View
- RF Stats
- RF Health
- Rogue Report
- Clients
  - Types
  - Delete Reasons
- Export
- WCAE Logs

Client Delete Reasons



Delete Reason	Count	Log Signature	Level
Connection Timeout	246	CO_CLIENT_DELETE_REASON_CONNECT_TIMEOUT	May need validation
Wpa Key Exchange Timeout	103	CO_CLIENT_DELETE_REASON_KEY_XCHNG_TIMEOUT	May happen during Normal Or
802.11w Max Sa Queries Reached	45	CO_CLIENT_DELETE_REASON_MAX_SAQUERIES	May happen during Normal Or
Inter Instance Roam Success	23	CO_CLIENT_DELETE_REASON_INTER_WNCD_ROAM_SUCCESS	May happen during Normal Or
Inter Controller Roam Success	5034	CO_CLIENT_DELETE_REASON_INTER_CTRL_ROAM_SUCCESS	May happen during Normal Or
Due To Mobility Fail(ed/ures)	47	CO_CLIENT_DELETE_REASON_MOBILITY_FAILURE	May happen during Normal Or
Dot11r Pre-authentication Fail(ed/ures)	269	CO_CLIENT_DELETE_REASON_FT_AUTH_RESPONSE	May happen during Normal Or
Sae Authentication Fail(ed/ures)	6	CO_CLIENT_DELETE_REASON_SAE_AUTH_FAILURE	May need validation

Wireless Detector

- Pull individual failures with:

```
show logging profile wireless start last X min filter mac 1111.2222.333
```

- Use Wireless Detector tool for general assessment

Wireless Detector v0.1

General Information

Total Clients:	15
Clients deleted by errors:	1
Clients deleted by warnings:	5
Clients deleted by info/normal:	3
Clients deleted by unknown reason:	5
Timestamp:	2023_Apr_18_14_58
Period collected:	1 day
Maximum Clients to display	10

Client delete events per type:

Error Delete reasons Found:

Reason code	Count
CO_CLIENT_DELETE_REASON_DOT11_DENIED_RATES	1

Warning Delete reasons Found:

Reason code	Count
CO_CLIENT_DELETE_REASON_KEY_XCHNG_TIMEOUT	1
CO_CLIENT_DELETE_REASON_MN_AP_DRIVER_EVENT_CLASS3_RECV	4

Archive Bundle

17.12
per day

- Generates a tar file
  Combines all available logs for each process
- File can be several GB
- Binary files, must be decoded by Cisco
- Post mortem Analysis

```
C9800#request platform software trace archive last <days> to-file bootflash:<archive file>
```

Summary

- Something happened yesterday:
  - Always on logging: show logging mac XXX last XX
- AP/Client debugging
  - RA trace: debug wireless mac XXX or GUI
- How AP joins/stats
- Full controller log collection

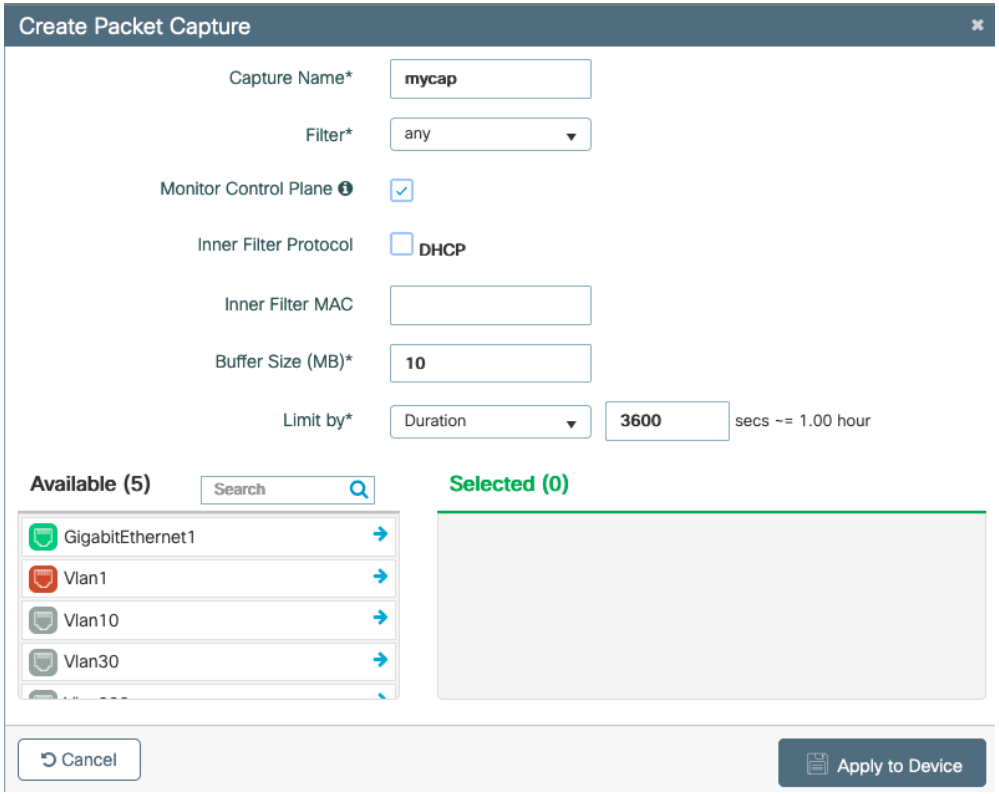
Dataplane Debugging

Embedded Packet Capture

- Get packets sent from or to and through the controller
- Export to Wireshark
- No need for switch capture
- Accessible either from GUI or CLI

Embedded Packet Capture

- Web interface to the existing EPC CLI “monitor capture …”
- One click start/stop/download
- Physical and VLAN interfaces can be selected



Embedded Packet Capture (EPC) CLI

```
monitor capture <CAPTURE_NAME> interface <> both
monitor capture <CAPTURE_NAME> control-plane both (optional)
monitor capture <CAPTURE_NAME> match any
monitor capture <CAPTURE_NAME> inner mac <CLIENT_MAC> | access-list <ACL>
monitor capture <CAPTURE_NAME> buffer size 100 circular
monitor capture <CAPTURE_NAME> limit pps 1000000
monitor capture <CAPTURE_NAME> start
monitor capture <CAPTURE_NAME> stop
monitor capture <CAPTURE_NAME> export bootflash:<CAPTURE_NAME>.pcap
```

Embedded Packet Capture

New in 17.12

- In 17.12, EPC allows to capture on a circular buffer

```
C9800#monitor capture <name> buffer file <2-5> <fsize 1-500Mb>
[circular]
```

Data Plane Statistics – Global Wireless Drops

show platform hardware chassis active qfp statistics drop all | inc Global|Wls

```
Global Drop Stats                    Packets                 Octets
PuntGlobalPolicerDrops                     0                      0
SdwanGlobalDrop                            0                      0
WlsCapwapError                       1471733              327309563
WlsCapwapFragmentationErr                  0                      0
WlsCapwapNoUidb                            0                      0
WlsCapwapReassAllocErr                     0                      0
WlsCapwapReassFragConsume          242814618            37954342616
WlsCapwapReassFragDrop                     0                      0
WlsClientError                     212513426            62965772923
WlsClientFNFV9Err                          0                      0
WlsClientFNFV9Report                       0                      0
WlsDtlsProcessingError                     0                      0
```

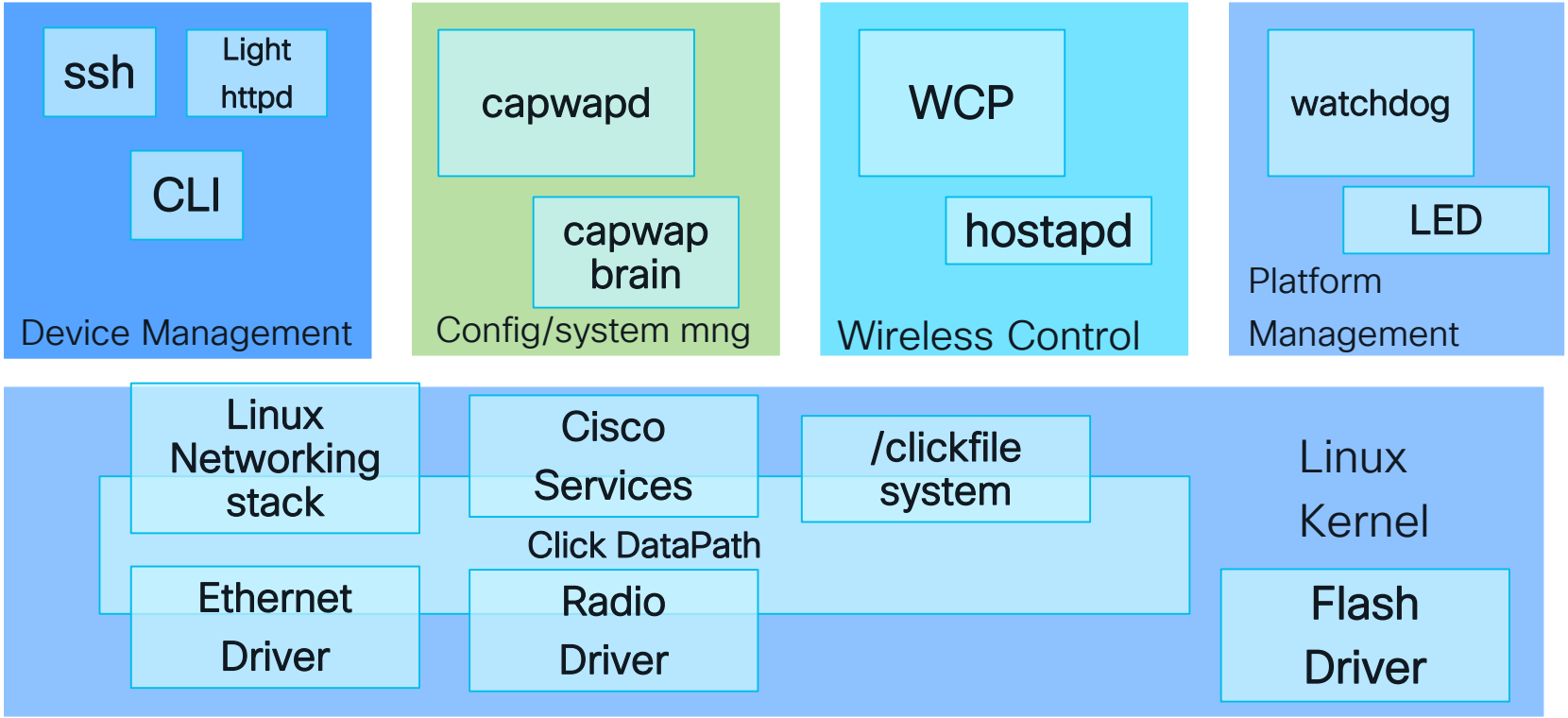
Customer problem example 4

- RA trace of the client
- PCAP on the WLC, filtered on the client MAC

Access Point Control Plane

Catalyst APs

- Simplified View



Troubleshooting on the AP side

For Wave 2 and Wifi 6/6e APs

- AP console output/ Syslogs are stored in the flash even after reboot
- **Debug client <mac>** : macro for control-plane capture. Can be exported to .pcap or export in hex
- 17.3+: you can export an AP support bundle to the WLC
- ACL and counters: **show client access-lists**
- Much more in "**Troubleshoot COS APs**"

AP Serviceability

APs have various Flash Directories to view syslog, crash and core dumps

```
ap9136-3#show flash syslogs
Directory of /storage/syslogs/
total 1848K
-rw-r--r--    1 root     root         36722 Nov 29  2022 19
-rw-r--r--    1 root     root         40916 Nov 29  2022 19.0
ap9136-3#show flash cores
Directory of /storage/cores/
total 13128K
-rw-rw-rw-    1 root     root       1974149 Jan 12 15:02 ap9136-3__27149-core-wcpd.17.9.2.52.2023-01-12.tgz
ap9136-3#show flash crash
No AP crashfile found
```

Troubleshooting Clients on the AP side

AP client trace

```
AP0CD0.F894.46E4#show ap client-trace events mac CLIENT_MAC
[*04/06/2022 10:11:54.287675] [AP] [CLIENT_MAC] <apr1v1> [U:W] DOT11_AUTHENTICATION : (.)
[*04/06/2022 10:11:54.288144] [AP] [CLIENT_MAC] <apr1v0> [D:W] DOT11_AUTHENTICATION : (.)
[*04/06/2022 10:11:54.289870] [AP] [CLIENT_MAC] <apr1v0> [U:W] DOT11_ASSOC_REQUEST : (.)
[*04/06/2022 10:11:54.317341] [AP] [CLIENT_MAC] <apr1v0> [D:W] DOT11_ASSOC_RESPONSE : (.)
[*04/06/2022 10:11:54.341370] [AP] [CLIENT_MAC] <apr1v0> [D:W] EAPOL_KEY.M1 : DescType 0x02 KeyInfo 0x008b
[*04/06/2022 10:11:54.374500] [AP] [CLIENT_MAC] <apr1v0> [U:W] EAPOL_KEY.M2 : DescType 0x02 KeyInfo 0x010b
[*04/06/2022 10:11:54.377237] [AP] [CLIENT_MAC] <apr1v0> [D:W] EAPOL_KEY.M3 : DescType 0x02 KeyInfo 0x13cb
[*04/06/2022 10:11:54.390255] [AP] [CLIENT_MAC] <apr1v0> [U:W] EAPOL_KEY.M4 : DescType 0x02 KeyInfo 0x030b
[*04/06/2022 10:11:54.396855] [AP] [CLIENT_MAC] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2022 10:11:54.416650] [AP] [CLIENT_MAC] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2022 10:11:54.469089] [AP] [CLIENT_MAC] <apr1v0> [U:W] DOT11_AC[illegible] : (.)
[*04/06/2022 10:11:54.469157] [AP] [CLIENT_MAC] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2022 10:11:57.921877] [AP] [CLIENT_MAC] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2022 10:11:57.921942] [AP] [CLIENT_MAC] <apr1v0> [D:W] DOT11_ACTION : (.)
```

U = upstream (from client)
D = downstream (to client)
W - Wireless driver
E - Ethernet driver
C - Click driver

AP commands from Controller

When SSH is not possible…

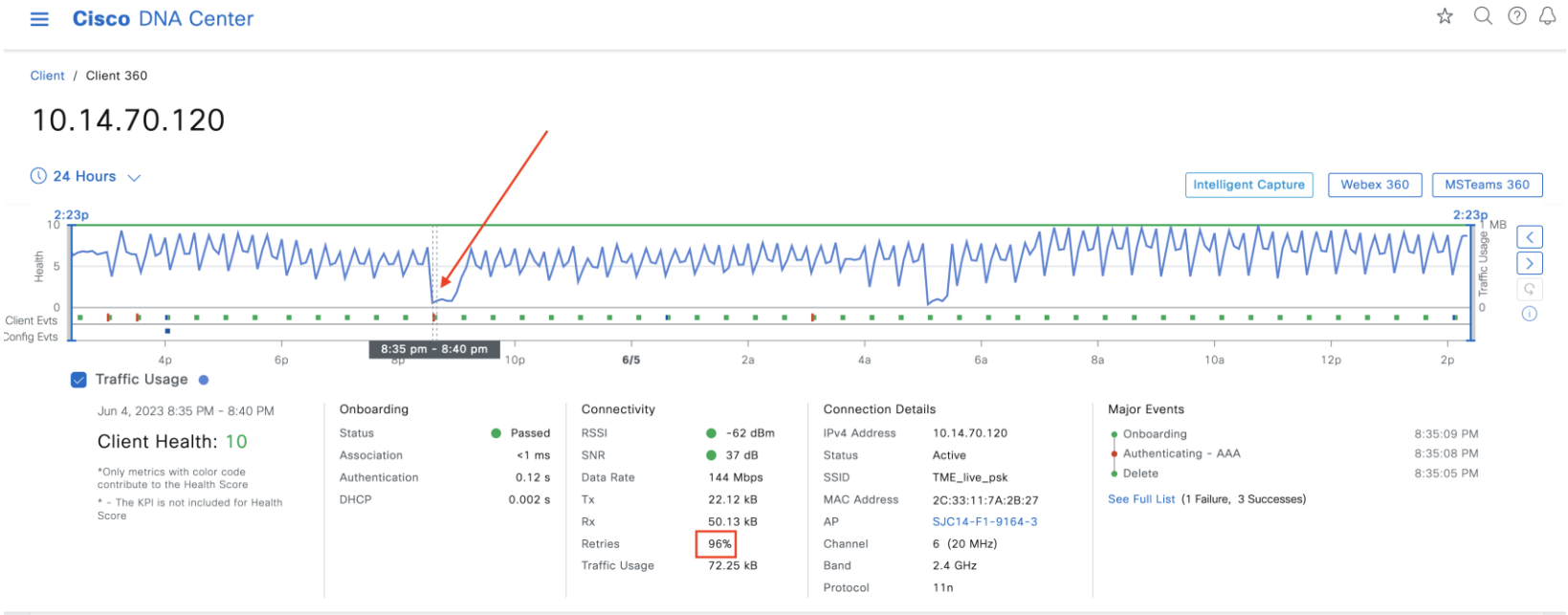
```
myc9800-CL#ap name 9120-etage remote enable
myc9800-CL#ap name 9120-etage remote command "show clock"
myc9800-CL#term mon
myc9800-CL#ap name 9120-etage remote command "show clock"
myc9800-CL#
Jan  4 18:59:25 CET: %AP_LOG-6-9120-etage : Chassis 1 *17:59:25 UTC Wed Jan  4 2023
myc9800-CL#
```

AP client debug bundle

New in 17.12

```
AP0CD0-F894-4D64#debug client-bundle start debug
22:0F:23:B1:82:EC AP0CD0-F894-4D64#show client-bundle
status Show client bundle status AP0CD0-F894-4D64#show client-
bundle status Client Bundle Status : Started
Client Bundle Starting Addresses : 22:0F:23:B1:82:EC Client
Bundle Upload Status : None
Client Bundle Upload File : None
AP0CD0-F894-4D64#debug client-bundle stop debug
22:0F:23:B1:82:EC AP0CD0-F894-4D64#debug client-bundle upload
scp admin@192.168.1.133:/bootflash 22:0F:23:B1:82:EC
```

Client 360 View

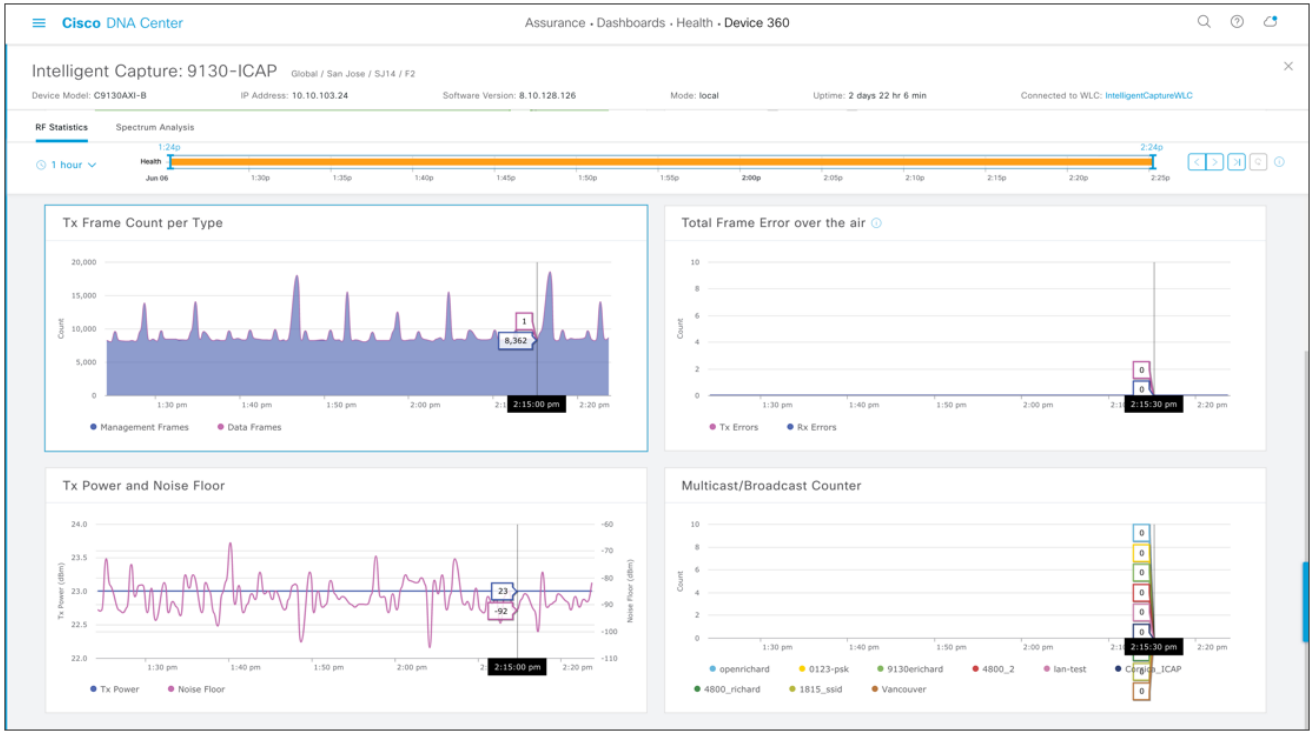


Intelligent capture

You can enable intelligent capture for a given client in the Client Health 360 dashboard

Intelligent capture

RF stats can be enabled globally or on specific APs



Customer problem example 5

Specific APs lead to bad user experience

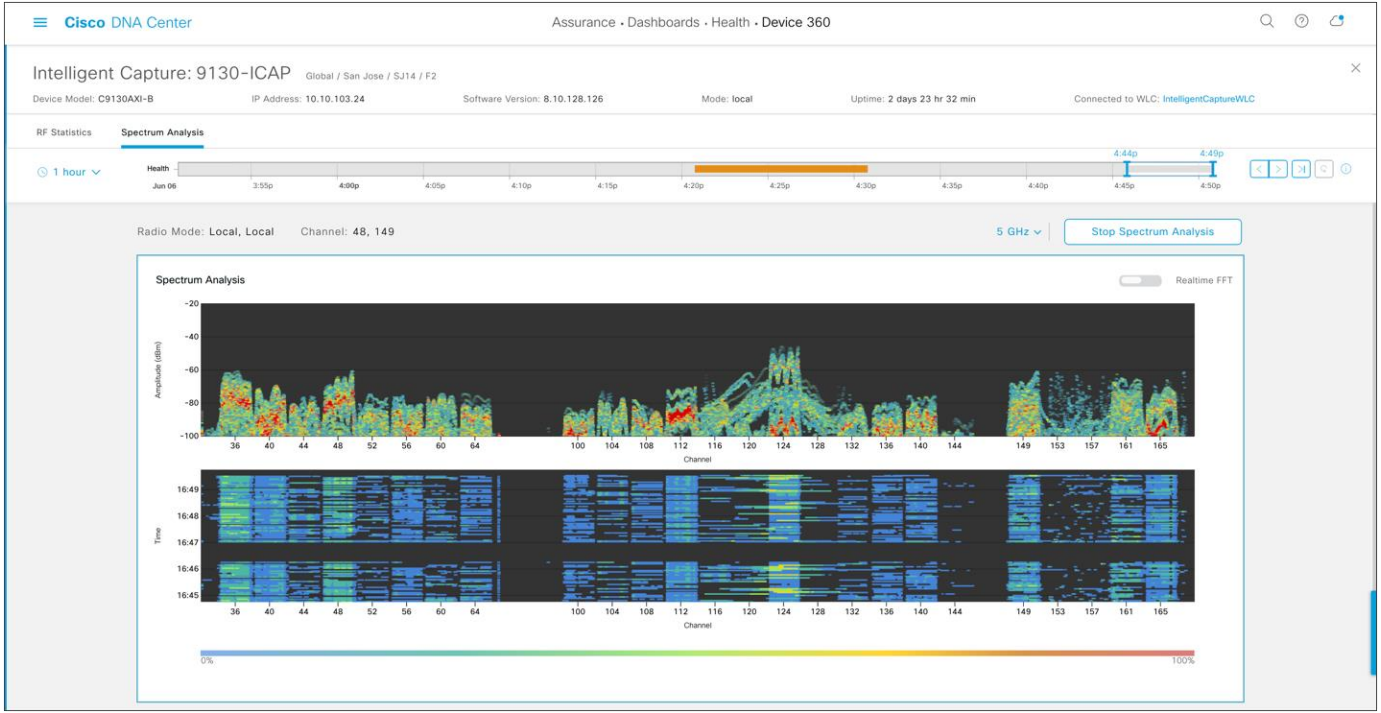
- Cisco Catalyst-C Intelligent capture (Channel utilization, drops, …)
- show commands on the APs themselves

Access Points

Dataplane Debugging

Intelligent capture

- The power of Cleanair / RF Asic / Cleanair Pro

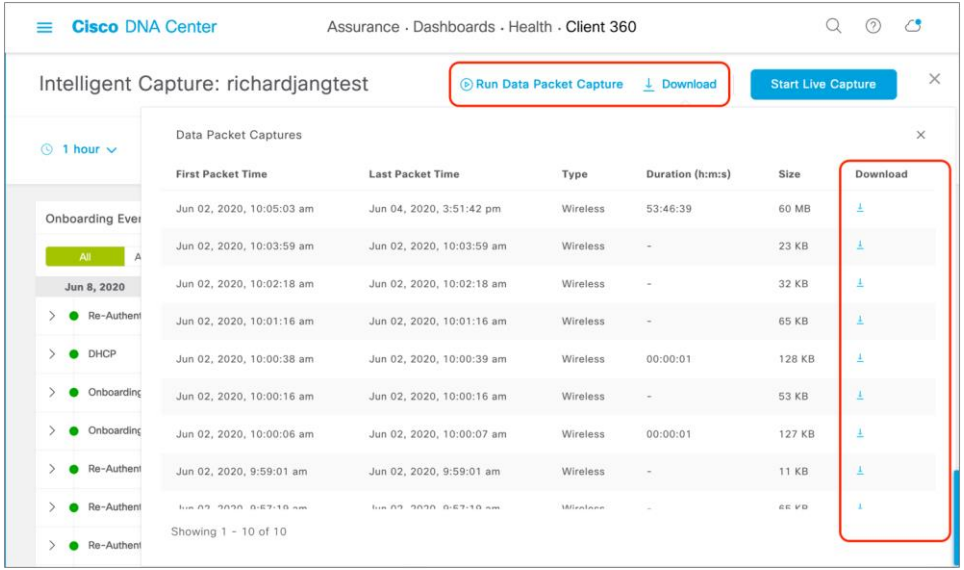


Intelligent capture

Intelligent capture page gives you an overview of events related to the client

Intelligent capture

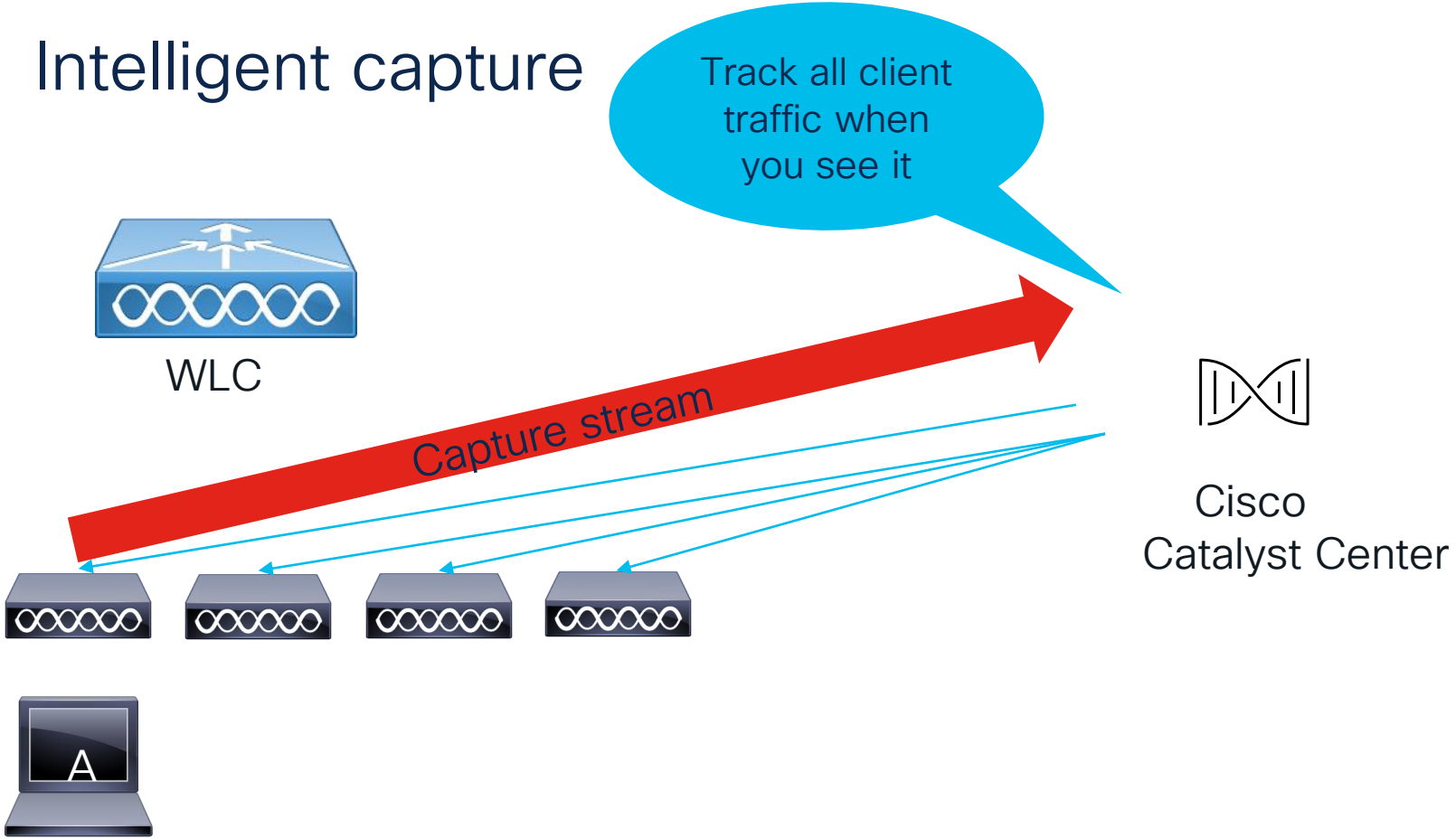
- Client intelligent capture



Data packet capture supported on 4800 , 9130, 9166

Live Capture (onboarding) on all other AP models including 9160s

Intelligent capture



Intelligent capture

Anomaly capture

Cisco DNA Center — Assurance · Dashboards · Health · Client 360

Intelligent Capture: richardjangtest — Run Data Packet Capture | Download | Live Capturing

1 hour — PCAP — Jun 08 — 11:06a – 12:06p

Onboarding Events — LIVE

All | Anomaly | Export PCAP

Jun 8, 2020	Time	Duration
KeyExchange	12:02:55 pm	3,061 ms
KeyExchange	12:02:52 pm	3,257 ms
KeyExchange	12:02:49 pm	3,242 ms
KeyExchange	12:02:45 pm	3,260 ms
KeyExchange	12:02:42 pm	3,243 ms
Client Deauthentica...	12:02:45 pm	
KeyExchange	12:02:45 pm	
Authentication Done	12:02:42 pm	
Authentication Start	12:02:42 pm	
Association Done	12:02:42 pm	
Association Start	12:02:42 pm	
Re-Authentication	12:02:09 pm	98 ms
Re-Authentication	11:56:43 am	65 ms

KeyExchange
Jun 8, 2020, 12:02:45.546 pm

Client richardjangtest failed to connect due to 4-way handshake timeout

Auto Packet Analyzer — Show: IPv4 and IPv6 — Download Packets

802.11 Open Auth, Association, 802.1x/EAP, DHCP, Data, 802.11k/11v, Associated AP

Interpacket Gap (µs): 100,000,000 / 100,000 / 100 / 0.1

RSSI (dBm): 50 / 0 / -50 / -100

Packets

PACKET — From Client — From AP — Interpacket Gap — RSSI (dBm)

ASSOCIATED AP — 9130-ICAP

Last Session — Selected Session

WLC top issues

WLC High CPU

Control Plane:

- Client onboarding and authentication
- RRM
- Web authentication interception
- Rogue detection
- mDNS
- AP CAPWAP state
- 802.11k/v

Data Plane:

- AP and client data traffic
- ACLs
- AVC
- QoS

WLC High CPU

- “High CPU” can happen on any single CPU core if a single process is causing it.
- CPU utilization within IOSd :

```
#show process cpu sorted
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 698      288459     7731847         37  0.07%  0.01%  0.00%   0 NTP
 309      437356     7723454         56  0.07%  0.00%  0.00%   0 nbar-graph-sende
 236     1150250   240761597          4  0.07%  0.02%  0.00%   0 IP ARP Retry Age
 682      854081    38604249         22  0.07%  0.01%  0.00%   0 ONEP Network Ele
 495      123974     7981160         15  0.07%  0.00%  0.00%   0 Crypto IKEv2
```

WLC High CPU

- The real command

```
9800-l#sh processes cpu platform sorted

CPU utilization for five seconds: 17%, one minute: 16%, five minutes: 17%
Core 0: CPU utilization for five seconds: 12%, one minute: 11%, five minutes: 17%
Core 1: CPU utilization for five seconds: 14%, one minute: 13%, five minutes: 16%
Core 2: CPU utilization for five seconds: 16%, one minute: 10%, five minutes: 28%
Core 3: CPU utilization for five seconds: 10%, one minute: 11%, five minutes: 23%
Core 4: CPU utilization for five seconds: 15%, one minute: 14%, five minutes: 17%
Core 5: CPU utilization for five seconds: 13%, one minute: 27%, five minutes: 21%
Core 6: CPU utilization for five seconds:  5%, one minute: 74%, five minutes: 39%
..
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
-------------------------------------------------------------------------------
  4046    3974     89%     60%     57%  S          2435268  linux_iosd-imag
 27483   27476     36%     36%     36%  S         10557400  pubd
 19435   19422     36%     94%     95%  S           130092  smand
 20672   20656      5%      6%      6%  S           564508  odm_0
 17955   17947      5%      4%      4%  S           895584  wncd_1
```

WLC High CPU

- Exception for 9800-CL and 9800-L: dedicated CPU cores DP

```
#show process cpu platform sorted
CPU utilization for five seconds:  8%, one minute:  5%, five minutes:  5%
Core 0: CPU utilization for five seconds:  1%, one minute:  1%, five minutes:  1%
Core 1: CPU utilization for five seconds:  2%, one minute:  2%, five minutes:  2%
Core 2: CPU utilization for five seconds:  1%, one minute:  1%, five minutes:  2%
Core 3: CPU utilization for five seconds:  6%, one minute: 17%, five minutes: 17%
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
-------------------------------------------------------------------------------
 22225   21691     29%     29%     29%  S           248940  ucode_pkt_PPE0
 29758    8871      1%      1%      1%  S          1140752  linux_iosd-imag
 21672   21163      1%      1%      1%  S           255992  fman_fp_image
 29725   29544      0%      0%      0%  S             9672  pttcd
 29653   29388      0%      0%      0%  S           206924  pubd
```

WLC High CPU

- Checking DP load

```
#show platform  hardware chassis active qfp datapath utilization summ
  CPP 0:                    5 secs        1 min        5 min       60 min
Input:     Total (pps)           7            5            5            5
                 (bps)        4224        12584        11216        10872
Output:    Total (pps)           5            4            3            3
                 (bps)       20712        11056        10976        10856
Processing: Load (pct)           0            0            0            0
```

WLC High CPU

CPU Utilization | Wireless Interface | Management Summary | Redundancy

IOS Daemon CPU Usage(Top 5 Process)

IOSD CPU Dump

Process	5Sec	1Min	5Min
HTTP CORE	0.00%	1.82%	0.83%
SEP_webui_wsma_h	0.00%	0.45%	0.18%
Check heaps	0.00%	0.03%	0.05%
SASRcvWQWrk2	0.00%	0.08%	0.04%
Crimson config p	0.07%	0.03%	0.02%

Datapath Utilization

Datapath Utilization Dump

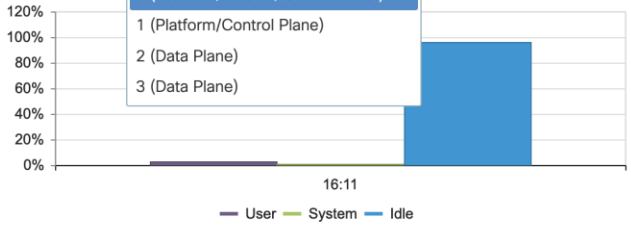
Data Plane	Core 2	Core 3
PP (%)	0.43	0.00
RX (%)	0.00	0.03
TM (%)	0.00	1.40
IDLE (%)	99.57	98.57

CPU trend
(CPU (%) vs Device Time)

Slot: Active CPU: 0 (Platform/Control/Service Plane)

Control Plane Data

- 0 (Platform/Control/Service Plane)
- 1 (Platform/Control Plane)
- 2 (Data Plane)
- 3 (Data Plane)



WLC High CPU

What to do in case a specific process like WNCD is on high CPU ?

Check the balancing of APs across WNCD processes

```
#show wireless loadbalance tag affinity wncd 0
Tag                          Tag type                  No of AP's Joined
-------------------------------------------------------
Site1                   SITE TAG                          200
Site2                   SITE TAG                          200
```

WLC High CPU

Leverage WCAE for WNCD analysis

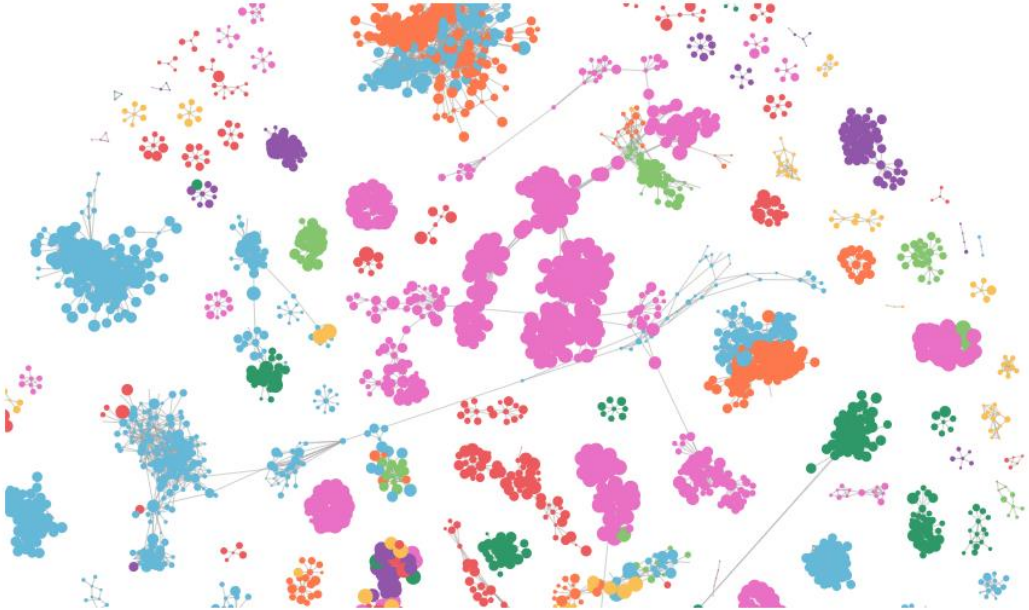
Back to Content Tab

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			

WLC High CPU

RF View - Band: 5 GHz

AP Classified per : WNCD. NDP RSSI: -85



Radio Count: 3498
Link Count: 14740

WNCD	AP Count	Client Count
wncd0	278	1262
wncd1	700	1843
wncd2	119	1800
wncd3	194	2210
wncd4	682	11152
wncd5	241	461
wncd6	270	1132
wncd7	481	1576

☐ Show Legend | View Type: WNCD | Link RSSI Filter: -85

Control Plane Drops

sh platform software punt-policer {drops}

Punt Cause	Description	Config Rate(pps) Normal	Config Rate(pps) High	Conform Packets Normal	Conform Packets High	Dropped Packets Normal	Dropped Packets High	Config Burst(pkts) Normal	Config Burst(pkts) High
2	IPv4 Options	874	655	0	0	0	0	874	655
3	Layer2 control and legacy	8738	2185	947389	0	0	0	8738	2185
4	PPP Control	437	1000	0	0	0	0	437	1000
5	CLNS IS-IS Control	8738	2185	0	0	0	0	8738	2185
6	HDLC keepalives	437	1000	0	0	0	0	437	1000
7	ARP request or response	437	1000	0	1702688	0	0	437	1000
8	Reverse ARP request or repso	437	1000	0	0	0	0	437	1000
9	Frame-relay LMI Control	437	1000	0	0	0	0	437	1000

Data Plane Statistics – Traffic sent to CPU

show platform hardware chassis active qfp feature wireless capwap datapath statistics drop all

```
Drop Cause                                    Packets                Octets
==============================================================================
Wls Capwap unsupported link type Error              0                     0
Wls Capwap invalid tunnel Error                     0                     0
Wls Capwap input config missing Error               0                     0
Wls Capwap invalid TPID Error                       0                     0
Wls Capwap ingress parsing Error                    0                     0
Wls Capwap invalid FC subtype Error                 0                     0
Wls Capwap SNAP Invalid HLEN Error                  0                     0
Wls Capwap Invalid SNAP Error                 1461925             323436123
Wls Capwap ipv4 tunnel not found Error          10943               4017497
```

Data Plane Statistics – Traffic sent to CPU

show platform hardware chassis active qfp feature wireless wlclient datapath statistics drop all

```
9800-cl#show platform hardware chassis active qfp feature wireless wlclient datapath statistics drop all

Drop Cause                                                                  Packets               Octets
============================================================ ===================== =====================
Wls Client V6 Max Address drop                                                    0                    0
Wls Client IPGlean Counter Index Error                                            0                    0
Wls Client IPGlean Counter Unchanged Error                                        0                    0
Wls Client IPGlean alloc no memory Error                                          0                    0
Wls Client IPGlean bucket max limit drop                                          0                    0
Wls Client iplearn l2 punt data packet skip                                       0                    0
Wls Client iplearn v4 punt data packet skip                                       5                 1373
Wls Client iplearn v6 punt data packet skip                                       5                  950
Wls Client input subblock missing error                                           0                    0
Wls vlan bridging mcast/bcast DMAC i/p SB miss error                              0                    0
Wls vlan bridging src SVI i/p SB miss error                                       0                    0
```

WLC High CPU

Other possible causes for high WNCD CPU usage :

- Very high probing activity
- ARP storms (controlled now with auto-exclusion)
- Huge amount of cleanair interferers
- Heavy mDNS usage

HA hot issues

WLC HA related concerns

```
Katar2#show redundancy switchover history
Index  Previous  Current  Switchover              Switchover
       active    active   reason                  time
-----  --------  -------  ----------              ----------
   8       2        1     active unit removed     14:06:05 CEST Wed Mar 29 2023
   9       1        2     active unit removed     14:25:29 CEST Wed Mar 29 2023
   10      2        1     Active RMI port down    11:00:22 CEST Thu Mar 30 2023
   11      1        2     active unit removed     11:08:53 CEST Thu Mar 30 2023
   12      2        1     active unit removed     11:18:47 CEST Thu Mar 30 2023
   13      1        2     active unit removed     11:34:32 CEST Thu Mar 30 2023
   14      2        1     active unit removed     11:51:34 CEST Thu Mar 30 2023
   15      1        2     user forced             12:01:51 CEST Thu Mar 30 2023
   16      2        1     active unit removed     12:08:46 CEST Thu Mar 30 2023
   17      1        2     user forced             09:40:40 CEST Tue May 9 2023
```

WLC HA related concerns

Unexpected failovers:

- Check WLC reload reason, system reports and crash files
- For 9800-CL: VMWare features
- Aggressive failover timers

ISSU HA Failures

First step is to check the ISSU compatibility matrix

```
#show redundancy config-sync failures historic mcl
 Mismatched Command List
------------------------
-snmp-server enable traps hsrp
```

```
#show install log
```

WLC HA useful troubleshooting commands

```
Show tech wireless redundancy
Show chassis detail
show platform software stack-mgr chassis active R0 sdp-counters
show platform software stack-mgr chassis standby R0 sdp-counters
show platform software stack-mgr chassis standby R0 peer-timeout
show logging process stack_mgr start last 30 minutes to-file
bootflash:stack_mgr_logs.txt
show logging process rif_mgr start last 30 minutes to-file
bootflash:rif_mgr_logs.txt
```

WLC HA useful testing commands

- Useful to troubleshoot RP
- Capture all traffic in port

```
test wireless redundancy packetdump start
test wireless redundancy packetdump stop
Katar2#dir
Directory of bootflash:/

25      -rw-          237568  May 10 2023 11:51:30 +02:00  haIntCaptureLo.pcap
1087409  drwx           90112  May 10 2023 11:50:59 +02:00  tracelogs

test wireless redundancy rpingp
```

AAA top issues

Intermittent RADIUS server not responding

Is it because the 9800 is not even sending RADIUS requests ?

Because it marked the RADIUS as dead ?

```
%RADIUS-4-RADIUS_DEAD: RADIUS server <ip-address>:1812,1813 is not responding.
```

- RA trace + EPC

Intermittent RADIUS server not responding

- RA trace after server is dead: not useful
- Best: RA trace for client triggering dead state
- Not easy. May need WNCD logs to debug and collect over a period of time.

Intermittent RADIUS server not responding

```
#Show aaa servers
RADIUS: id 18, priority 1, host 1.1.1.1, auth-port 1812, acct-port 1813, hostname r1
State: current UP, duration 304s, previous duration 0s Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 304s, previous duration 0s SMD
 Platform Dead: total time 0s, count 0
Platform State from WNCD (1) : current UP
Platform State from WNCD (2) : current UP
Platform State from WNCD (3) : current UP
Platform State from WNCD (4) : current UP
Platform State from WNCD (5) : current UP
Platform State from WNCD (6) : current UP
Platform State from WNCD (7) : current UP
Platform State from WNCD (8) : current UP, duration 2559s, previous duration 0s Platform Dead: total time 0s,
count 0
```

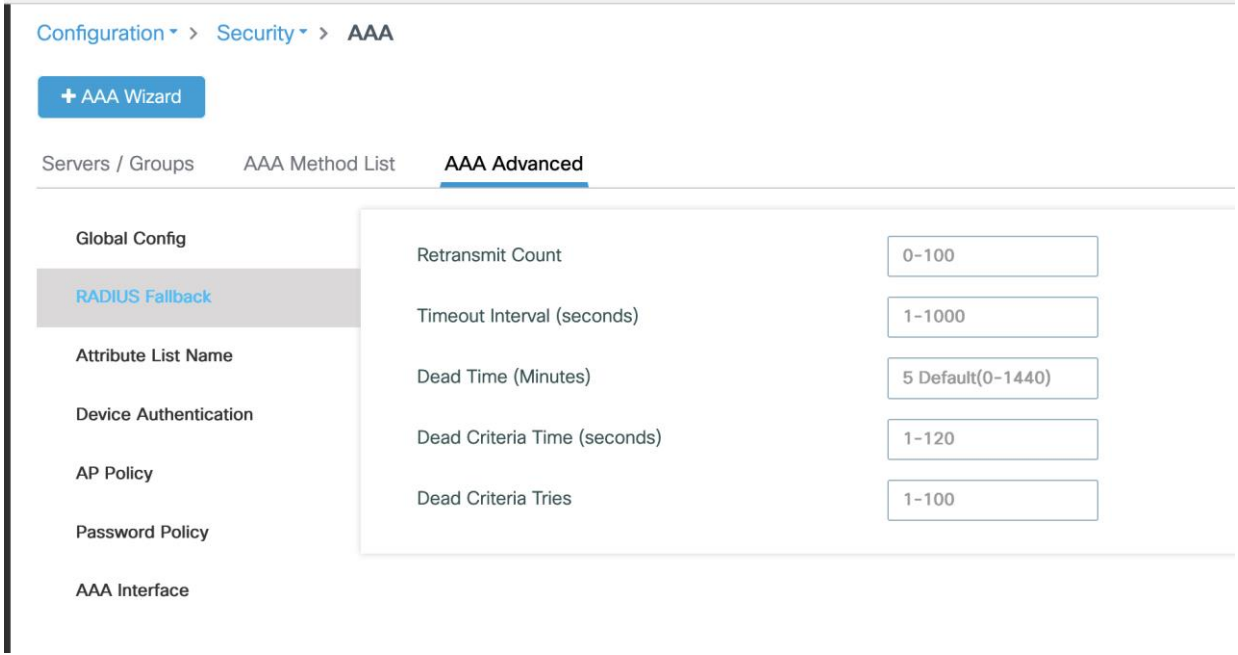
Typical causes

- RADIUS servers may ignore RADIUS requests

Authentication Summary	
Logged At:	October 18,2012 12:00:14.499 PM
RADIUS Status:	RADIUS Request dropped:
NAS Failure:	
Username:	
MAC/IP Address:	00:21:97:6C:68:E1
Network Device:	SWTHO6002279:192.168.10.66:FastEthernet0/36
Allowed Protocol:	
Identity Store:	
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	

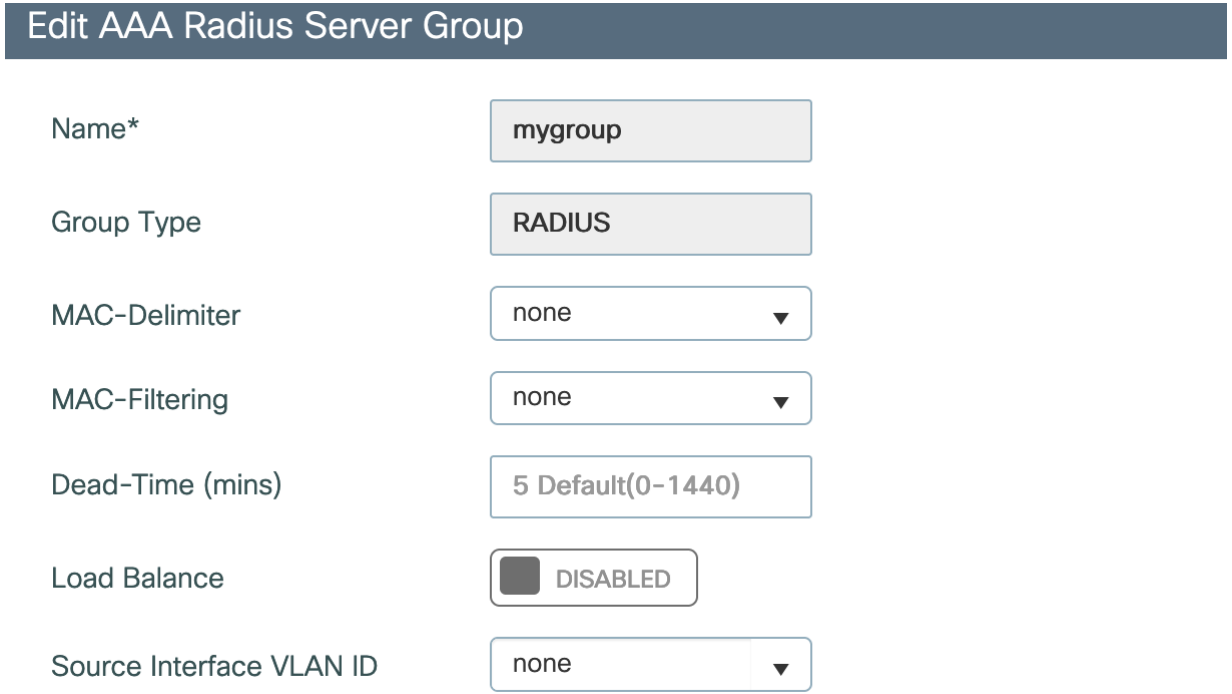
Typical causes

- Dead time not set means dead RADIUS is immediately marked back alive



Typical causes

- Dead timer can be set within AAA server groups



Throughput Issues

What is slow ?

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

Important: Delimited problem description

- 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 ?

- General “wifi is slow” versus one app (Citrix)
- Per application behavior. FTP vs iPerf, TCP vs UDP
- Fragmentation impact (adjust MSS) or latency
- Isolate client types
- Isolate locations, Aps
- Get RF data
- Is client roaming?

What is slow ?

Very slow: Over the Air capture

- Frame retries vs Total
- Gaps: no AP or client TX
- Reconnections ?
- MCS data rates used
- Beacon loss

What is slow ?

“Could be better”:

- Open/WPA2-AES or better
- WMM
- Frame aggregation. Block ACKing 64 vs acking 3-4 frames
- MCS Data rate
- Spatial streams

Flash space issues

Can my WLC face free space problems ?

- Low frequency on appliances
- Tracelogs have limit in size and file count
- Automatic rotation
- IOS images, crash files, system reports can use rest of space
- C9800-CL are typically limited on flash space
- Common: Old CL on 8 GB disk (16 mandatory now)

Public Service Announcements!

Legacy Crypto Deprecation

- 17.15 kills DES, MD5, RSA<1024
- SNMPv3 may stop working if using them
- Any public key (SSH/Certs) using 1024 will get deleted
- IOS-XE has been warning since 17.9.2
- 17.12.4/17.9.6: `crypto engine compliance shield disable`

17.12 AP console now in 115.200

- Default speed is now 115.200
- Only for clear config
- Upgrades or manufacturing new will stay at 9600
- Alignment with Meraki persona
- Faster boot

AP Image Corruption

- CAPWAP download over WAN (fragmentation)
- Image may get corrupted, AP ends on boot loop

```
Verify signature failed for /bootpart/part2/ramfs_data_cisco.squashfs (File system corruption detected)

SQUASHFS error: xz decompression failed, data probably corrupt

|

Fatal error: failed to start the image. Please fall back to alternate partition... (Recovery Logic)
```

AP Recovery..

- What is Alternate-Boot enhancement?
- 17.3.8, 17.6.6, 17.9.4 & above..

Without Alt-boot

- No recovery
- Indefinite attempts to boot
- Console Recovery

With Alt-boot

- AP remote recovery
- Attempt to boot 5 times
- Boot backup image

CVE-2023-20198 Web UI Vulnerability

- Install Fixed Image
  - Now....!
- It does not impact Guest feature
- Possible Workarounds:
  - Disable HTTPs/HTTP
  - Disable all http session modules (no UI)
  - Use ACL

IOS-Aps… Gone, not Gone, here we go

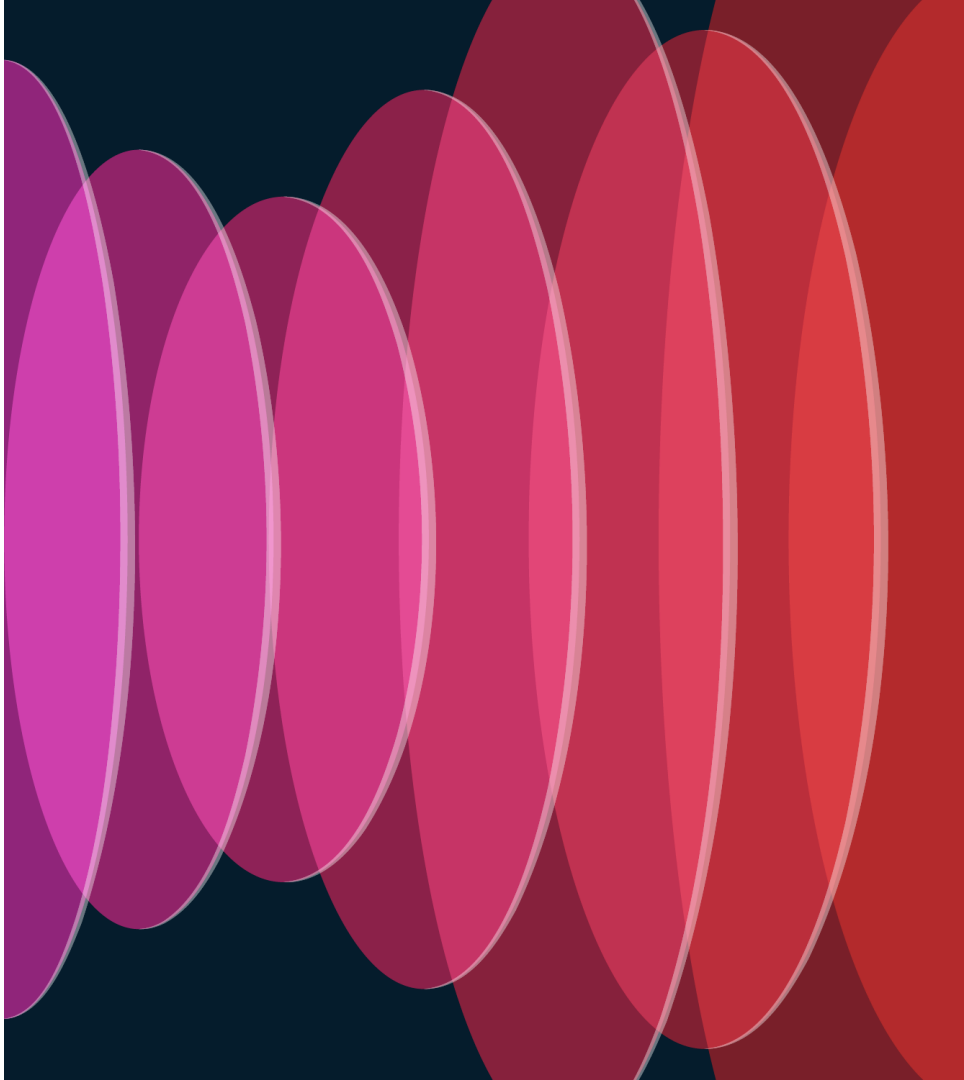
- 17.9.6, 17.12.4+: AP will be allowed to join
  - No support whatsoever
  - No further testing
- 17.13, 17.14
  - Not tested
- 17.15
  - Join rejected

Upgrading to IOS-XE 17.9 and higher

- Aps running Old code (8.10MR5 or lower)
- RMA stock
- Distributor stock

- Get interim through 8.10MR latest, or 17.3.5

Tools and References



Wireless Troubleshooting Tools

https://developer.cisco.com/docs/wireless-troubleshooting-tools/

- WCAE
- WiFi-Hawk
- WLAN Poller
- Wireless Debug Analyzer
- Guestshell scripts
- Cisco Support Assistant Extensions

Monitor 9800 KPIs

What commands to collect to monitor 9800 operations ?

https://blogs.cisco.com/networking/wireless-catalyst-9800-wlc-kpis-part-1

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217738-monitor-catalyst-9800-kpis-key-performa.html

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you