
cisco Live!
Let's go

The bridge to possible

Troubleshoot Catalyst 9800 Wireless Controllers

like a piece of cake

Nicolas Darchis, Sr Technical Leader, Customer eXperience (TAC)
@DarchisNicolas

About me

About me

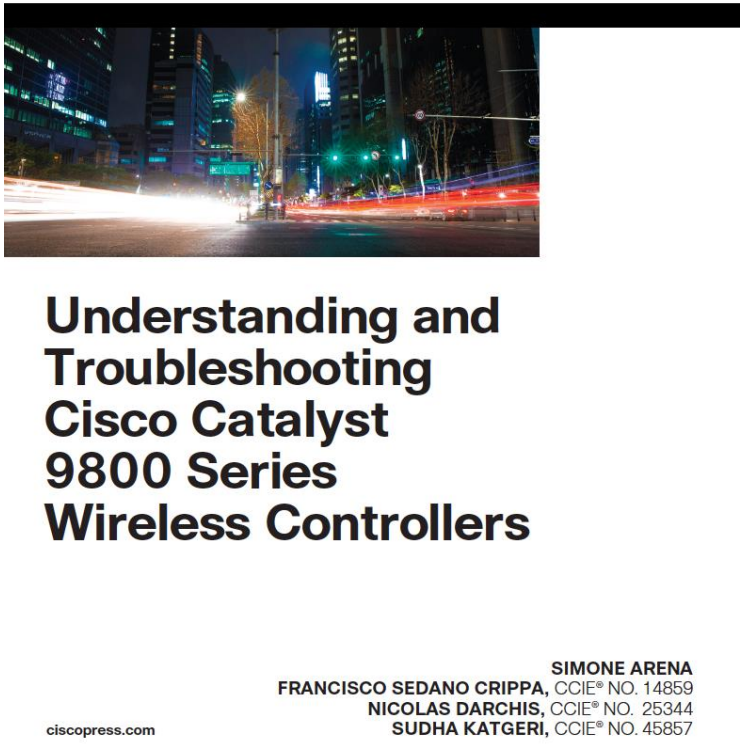
- 17 years (and counting) in Wireless (and AAA) TAC
- Love Cat9800, but love video games even more
- Very good at remembering small useless and weird facts
- Have a hard time remember important stuff
- When I speak, I know I’m right. It’s why I’m a silent person.
- Failed my CCNA first attempt
- 5 attempts to get my CCIE in 2009
- Did my master degree thesis with a Cisco Distinguished Engineer and failed it
- Banned to enter the USA

Agenda

- Introduction
- Cat9800 debugging (CP & DP)
- Access point debugging (CP & DP)
- WLC top issues
- Latest hot topics

Shamless plug

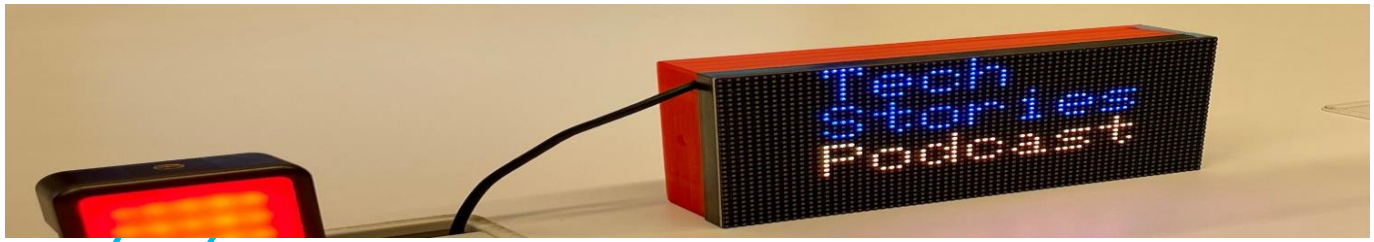
3 books (digital codes) to win today !



Introducing Cisco Tech Stories

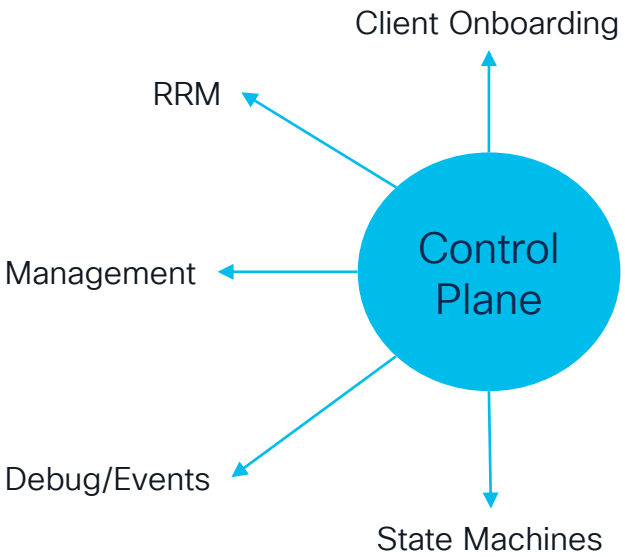
Nicolas is an outdtanding speaker. Entertaining combined with very deep knowledge. A pleasure listening. P.S.: is there a TAC stories podcast?

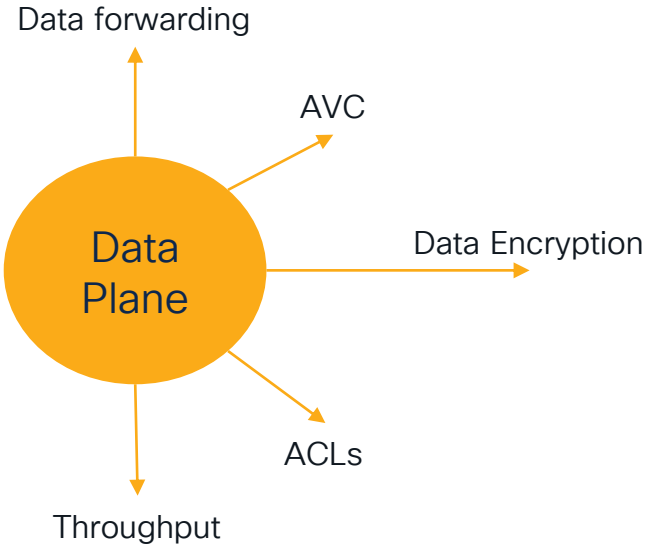
- “Cisco Tech Stories” on Apple podcast,Spotify, Audible, Google podcast.
- “Cisco podcast network” on Soundcloud.
- Put yourself in the shoes of TAC escalation. Come to learn new technologies, stay for hearing the crazy stories.



Introduction

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



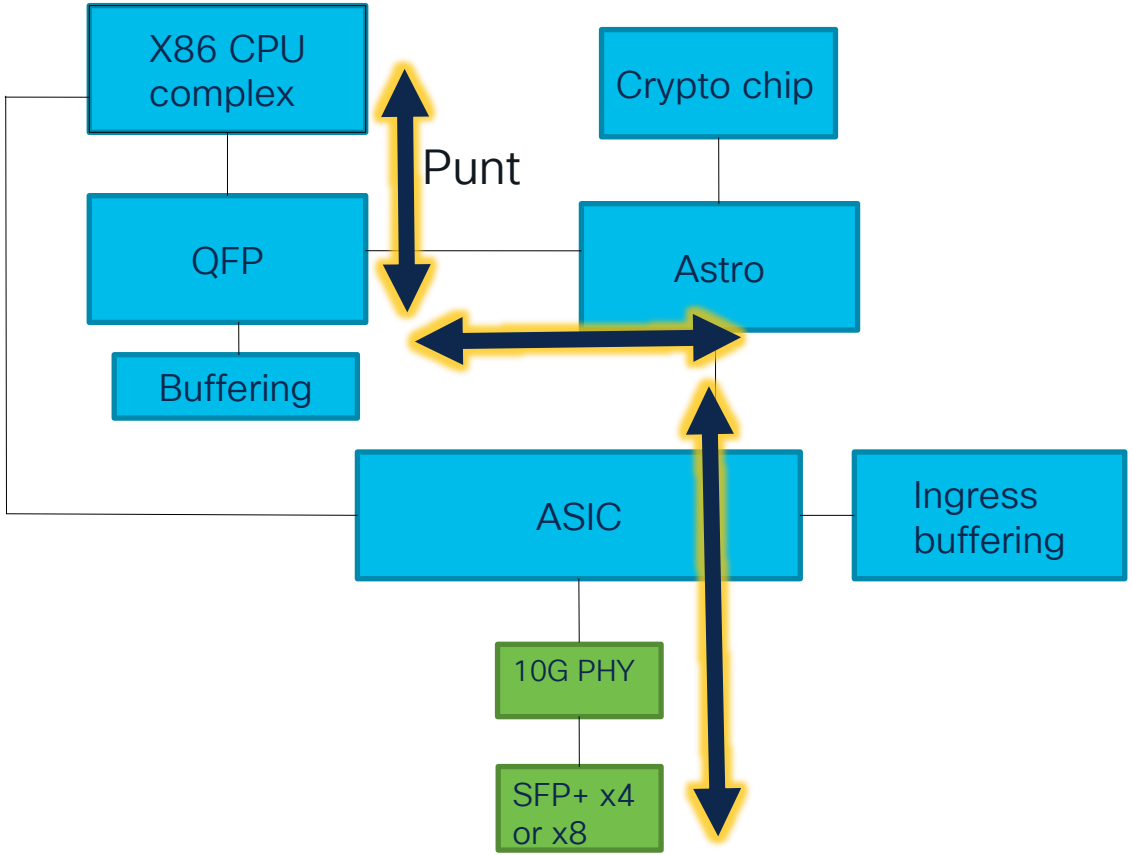


Introduction

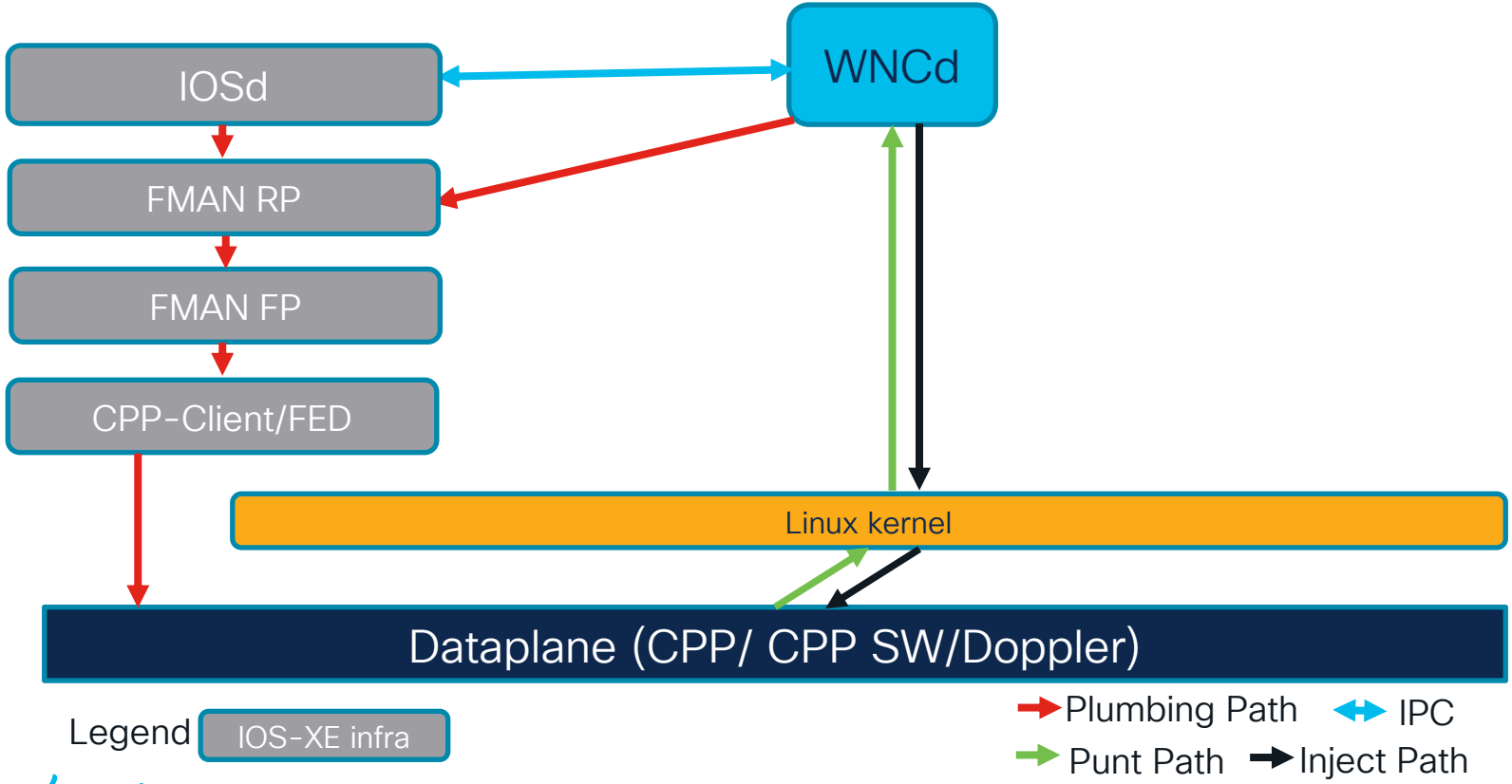
Just tell me fun stories !!!

- It’s hard to articulate this presentation around issues types (DHCP, web auth, etc …) as each can have a variety of logs to collect depending on the situation (Local switching ?)
- It’s articulated around traffic flow types and do contain your everyday stories for each

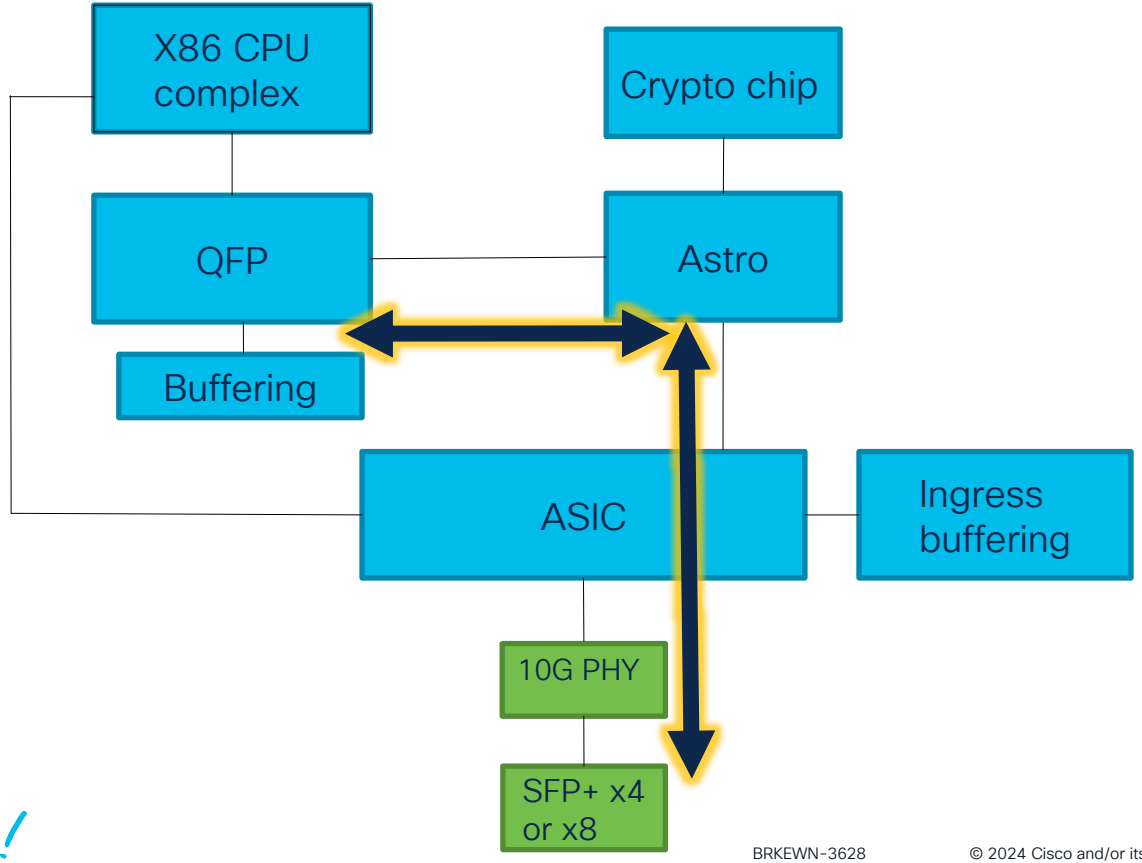
Life of a Packet : Control plane



Punt/Inject/Plumb path



Life of a Packet: wireless client traffic in dataplane



What did we learn ?

- Difference between control plane and data plane
- Why it matters
- Packets, where do they go ?

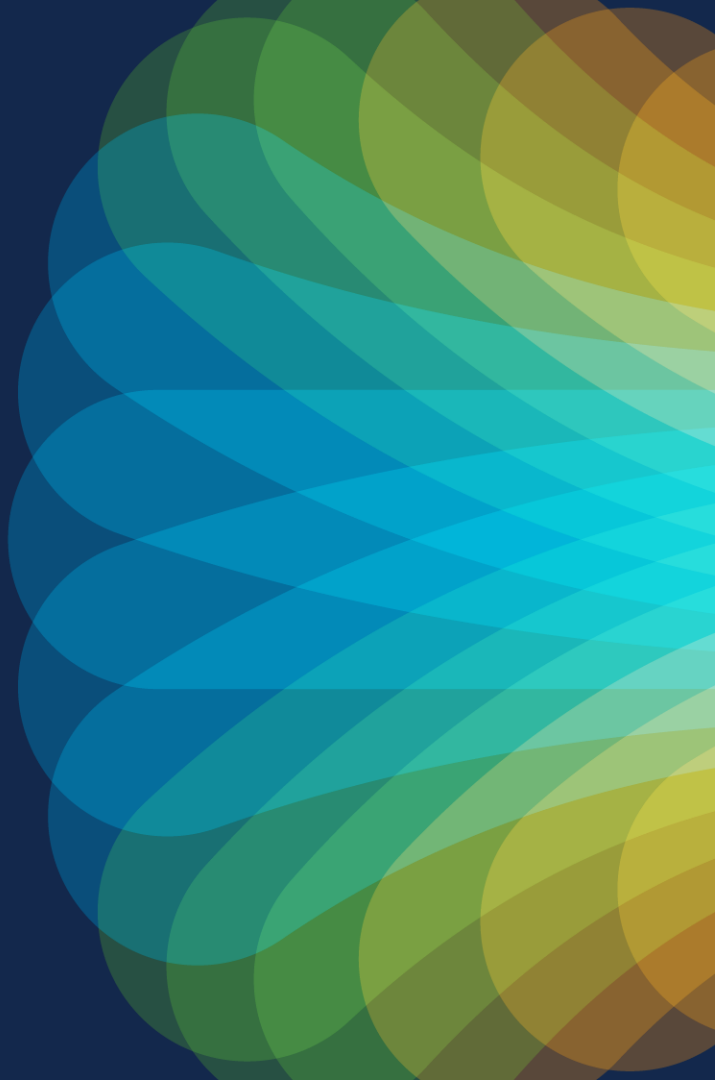
slido

Pick what is WLC control plane traffic

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

WLC Control Plane debugging

IOS-XE Tracing and Debugging



IOS-XE Tracing/Debugging

Concepts

IOSd Logging

- Your Traditional Syslog

Binary Tracing

- Fast infrastructure for real-time logging

Always On Tracing

- Real time data collection for all relevant events

Conditional Debugging/Radioactive Tracing

- Per IP/MAC address debugging

Non-Conditional Debugging/Per Process Tracing

- Your traditional debug

Archive bundle

IOSd Logging

IOSd Syslog is leveraged to present any system errors and can be viewed using #show logging

It is a good place to start troubleshooting process

AP Join:

```
May 22 2019 09:34:31.251 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Capwap2, changed state to up
May 22 2019 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 2019 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
```

The chef’s trick :

```
WLC-5#show log last 100
```

IOS-XE Tracing

Binary trace (Btrace)

- Binary, line rate tracing mechanism
- Each BinOS (non-IOSd) process has its own tracelog file
- File starts in memory
- At X size - > compressed and moved to disk
- Logs are written using syslog-like severity levels
- IOSd still uses IOS logger. Migration to btrace in progress.
- Base infrastructure for other features

IOS-XE Tracing

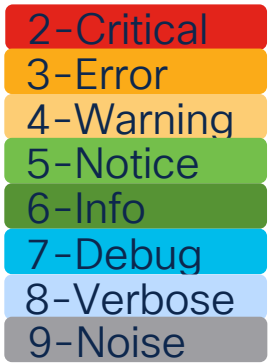
Binary trace in bootflash (VM) or harddisk (large appliances)

```
myc9800-CL#dir bootflash:tracelogs
Directory of bootflash:/tracelogs/
372968  -rw-         982  Nov 25 2022 13:28:59 +01:00  droputil_R0-0.3547_48683.20221125122619.bin.gz
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
- NOISE Not clear if any human can read this



Introducing Always On tracing

Contextual Logs WITHOUT enabling debugs

- Each process writes relevant events at Notice level
- No debug required
- 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

- Per Process (last 10 minutes only by default):

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

- Export to file:

```
# show logging process <process daemon> to-file <alwayson-processname.txt>
```

- Display in console:

```
# more bootflash:alwayson-processname.txt
```

- Export:

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

Always on Tracing

How to view

- 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>
```

Default time: last 10 minutes

- Specify the time you want !

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

Always on : successful client connection

 # 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

RAtracing 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
```

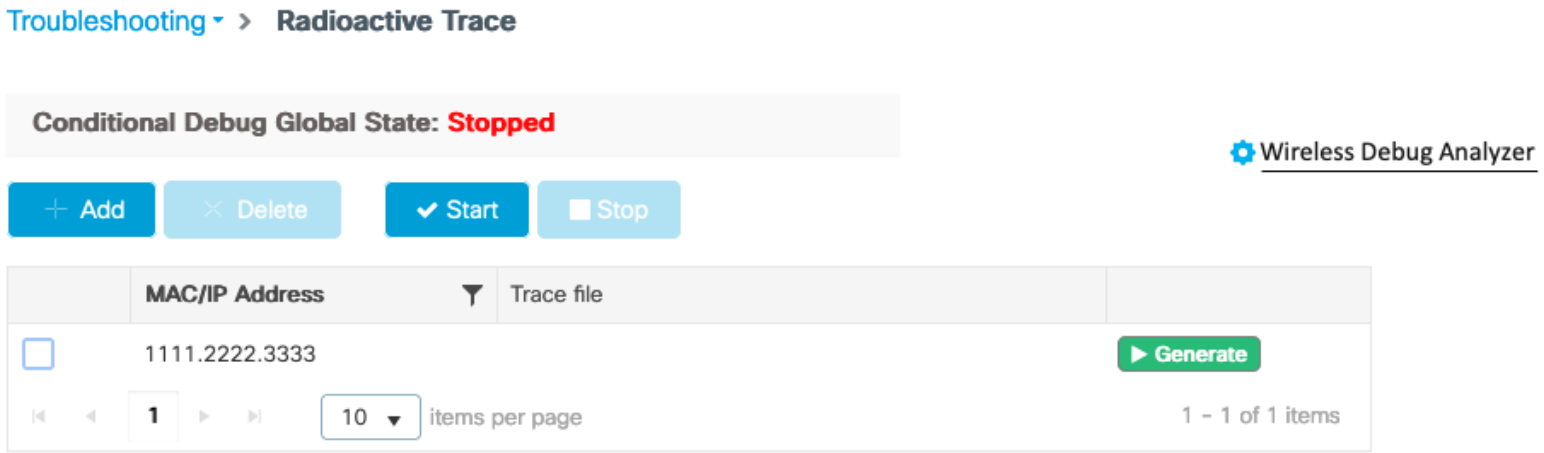
Customer problem example 1

-Always-on logs of selected clients. Were they failing to connect (stuck in IP LEARN?) ? Were they being intentionally disconnected ? RADIUS / authentication issue ?

-Of course Cisco Catalyst Center is key in such a triaging too

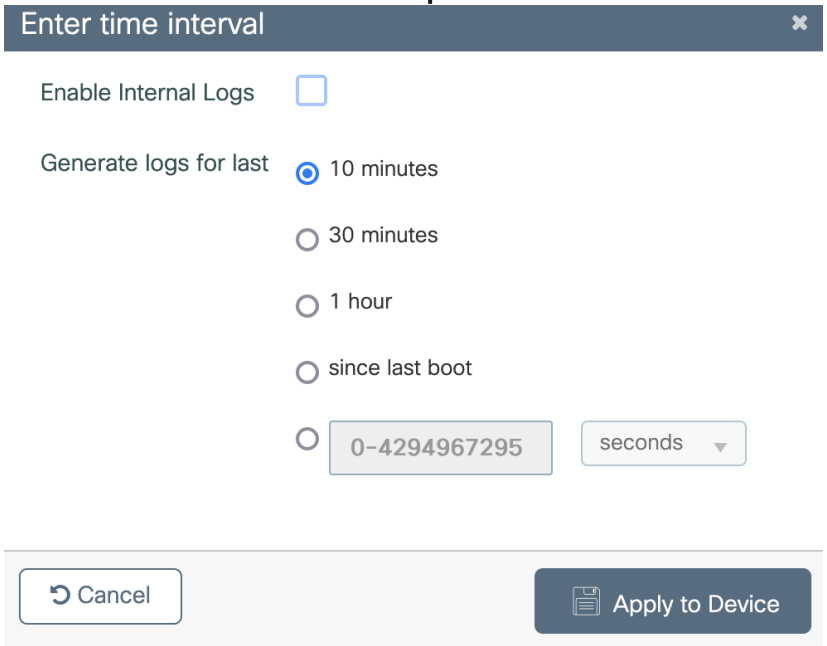
RadioActive Tracing

RAtracing automatically enables all debugs when a given MAC or IP is mentioned is seen



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

The debug wireless CLI command is a macro that starts RAtracing for a period of time and then 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>
```

Client debug bundle

The client debug bundle collects

- Show tech wireless
- Show tech wireless client mac <client mac>
- RAtraces
- Optional packet capture
- Show logging

Client debug bundle


```
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 <client_mac1
...client_mac5>
To disable
C9800# no debug wireless bundle include epc client <client_mac1
...client_mac5>
```

Client debug bundle

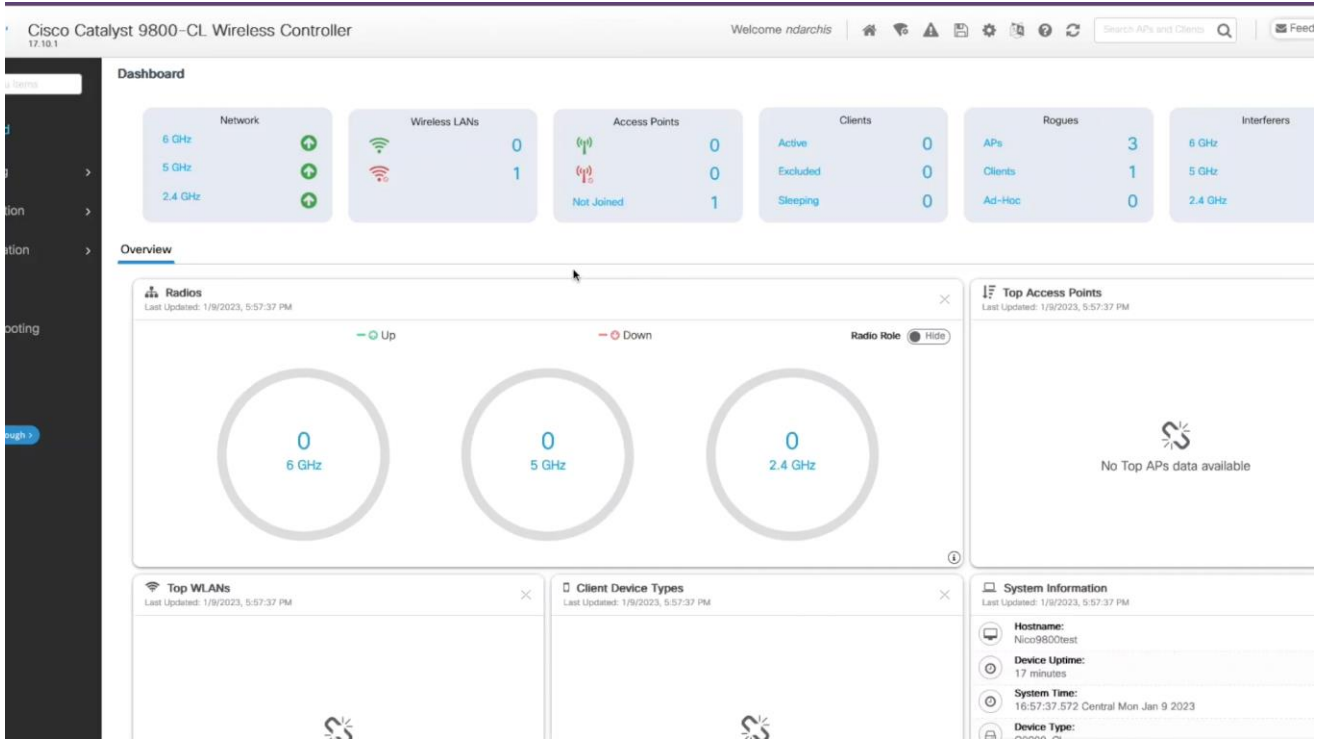

```
C9800#show bootflash: | inc 2022.tar
1047    1230336 Sep 19 2022 17:20:01.0000000000 +00:00
wireless_bundle_42e4.cb89.e878 _171958_UTC_Sep_19_2022.tar
1048     316416 Sep 19 2022 17:40:51.0000000000 +00:00
wireless_bundle_42e4.cb89.e878_174050_UTC_Sep_19_2022.tar
C9800#
```

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

RadioActive Tracing

RAtracing ON

- Example of an AP not joining



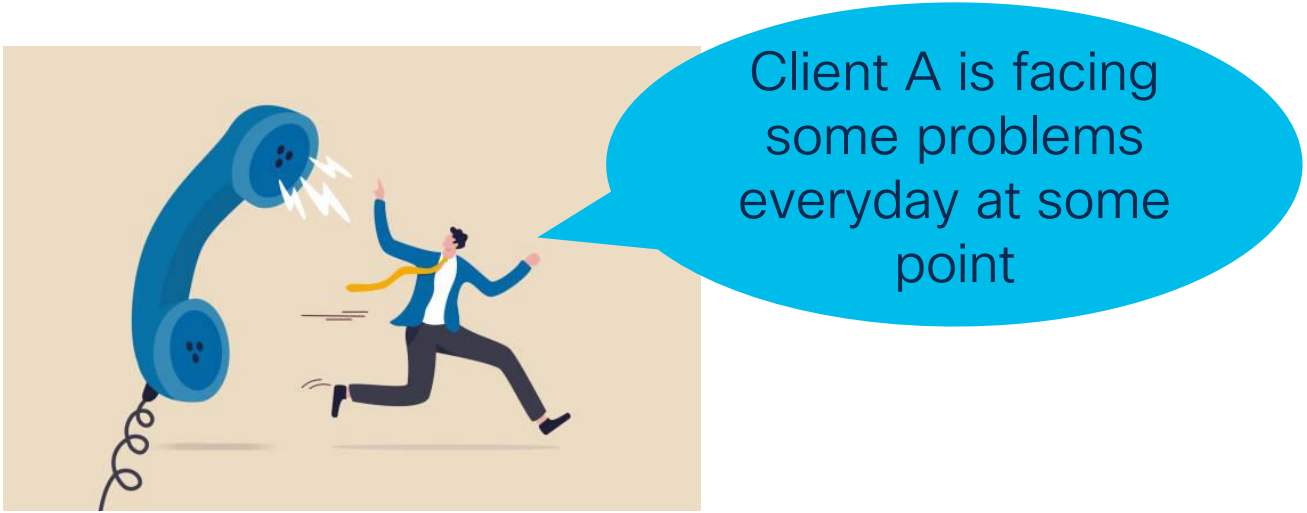
Customer problem example 2

-RAtrace of one AP MAC if it's still trying to join

-AP console (syslog) outputs to see if it indeed tries to join the right WLC

-PCAPs

Customer problem example 3



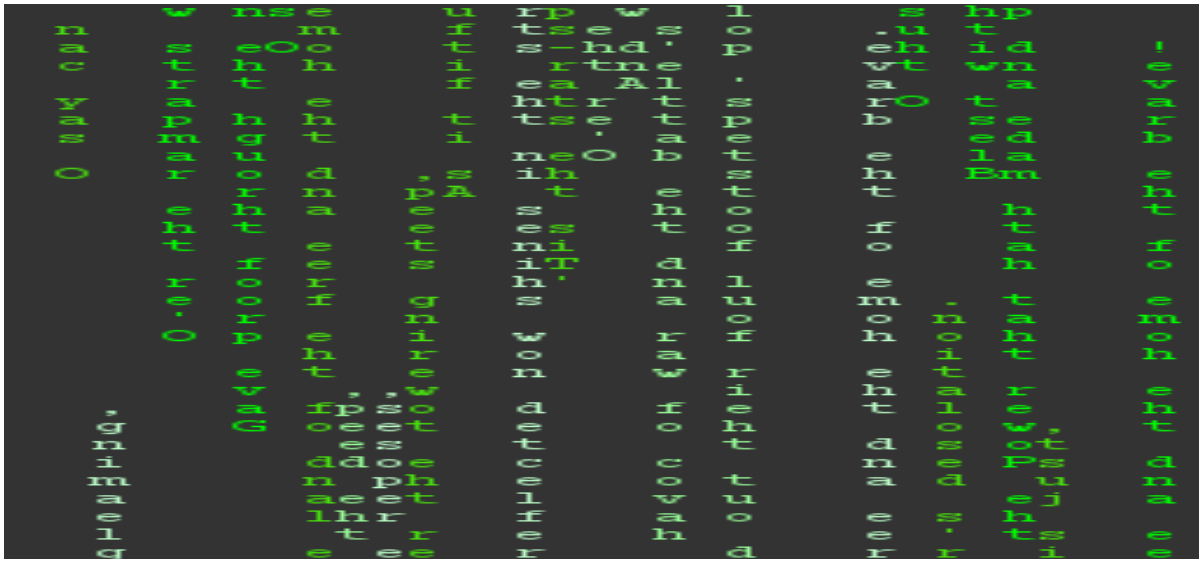
-RAtrace of the client running for the whole day

-Monitor easily up to 10 client MAC addresses. For more, keep an eye on the CPU utilization.

RadioActive Tracing

It is also possible to debug a client and see output real-time with

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



Unconditional debugging

1. Enable **set platform software trace <rrm-mgrd | nginx | nmspd> chassis active R0 {Modules | all-modules } {level}**
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**

Archive Bundle

- Generates a tar file
- Combines all available logs for each process

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

- File can be several Gb and is a collection of binary files, not readable until decoded.
- Useful for investigation when the whole box is affected.

What did we learn ?

- Collecting logs for one or more clients : RATrace
- Collectings more logs for one or more clients : Client bundle
- Collecting logs from processes, changing log levels
- Collecting all logs from the box
- AP join statistics/logging and debugging

slido

How can I check the logs for channel changes globally on the WLC?

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

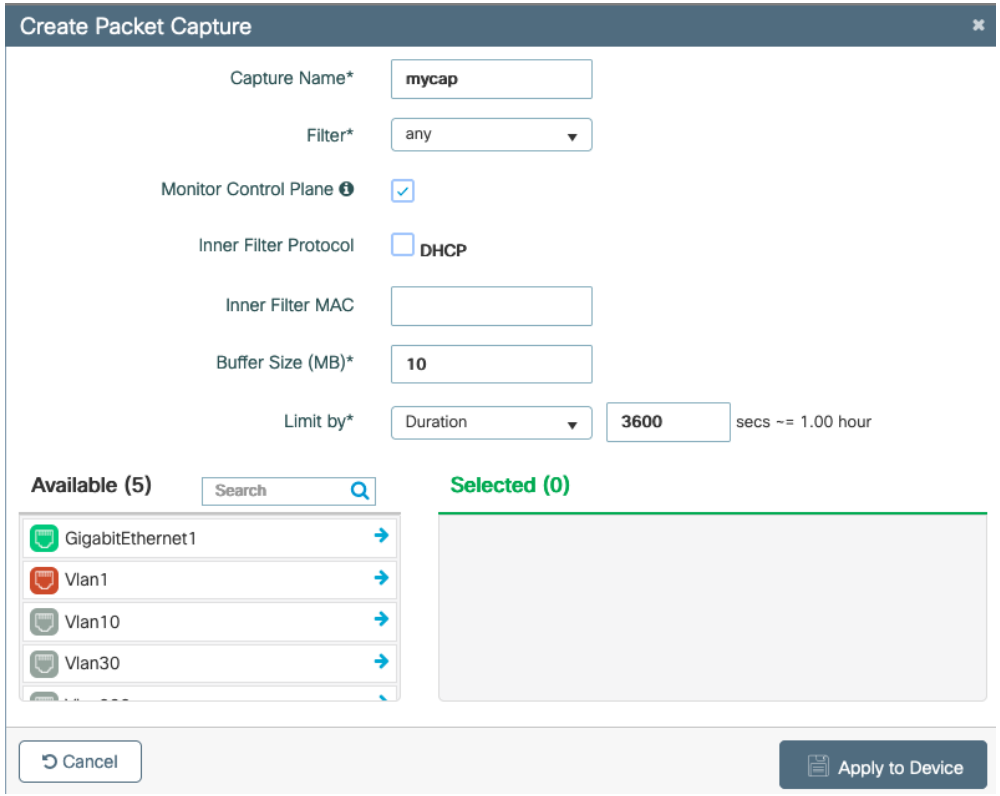
Dataplane debugging

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

- 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

-Catalyst Center Health center (Assurance)

-PCAP on the WLC, filtered on the AP IP

Customer problem example 4

P3 The 5 GHz radio 1 on AP "H01L0-IL-HI1298" is experiencing high utilization.

Status: Open

Issue Profile: global Edit Issue Settings

Description	The 5 GHz radio "1" on the AP "H01L0-IL-HI1298" has exceeded the 70% threshold and is currently experiencing 91% utilization.
Time	Feb 3, 2024 9:50 AM
Location	Global/CLEUR 2024/Hal-1-WOS/Hal-1_L0

IMPACT SUMMARY

19 Client(s) Affected

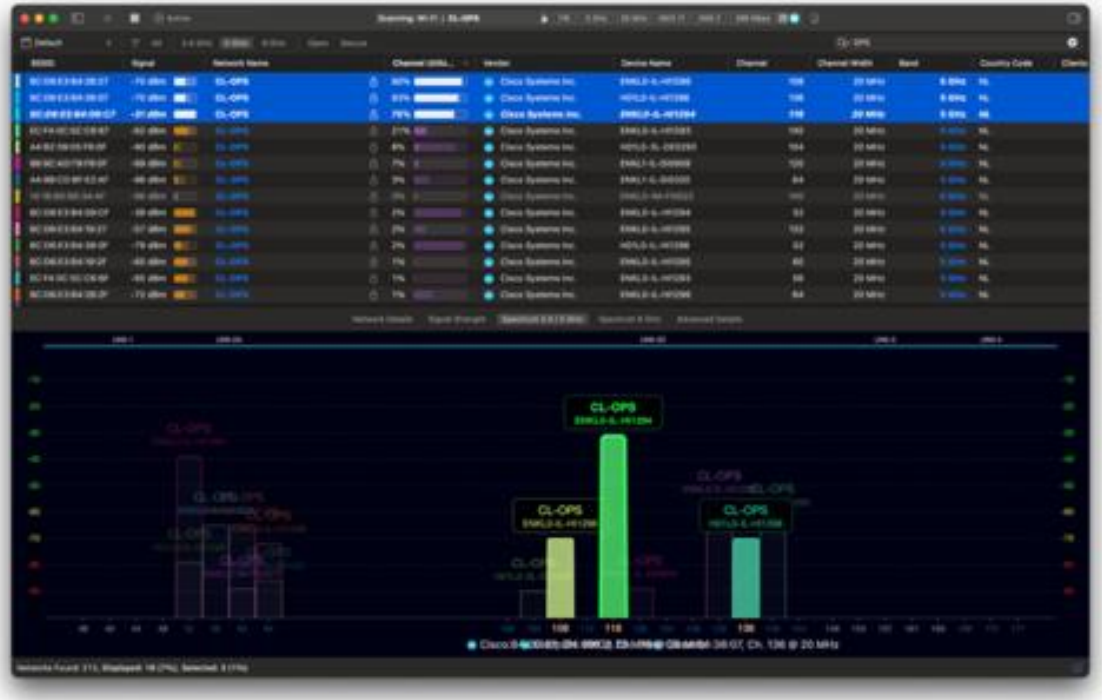
- Problem Details
- Impact Details
- Troubleshooting
- Suggested Actions

Problem Details

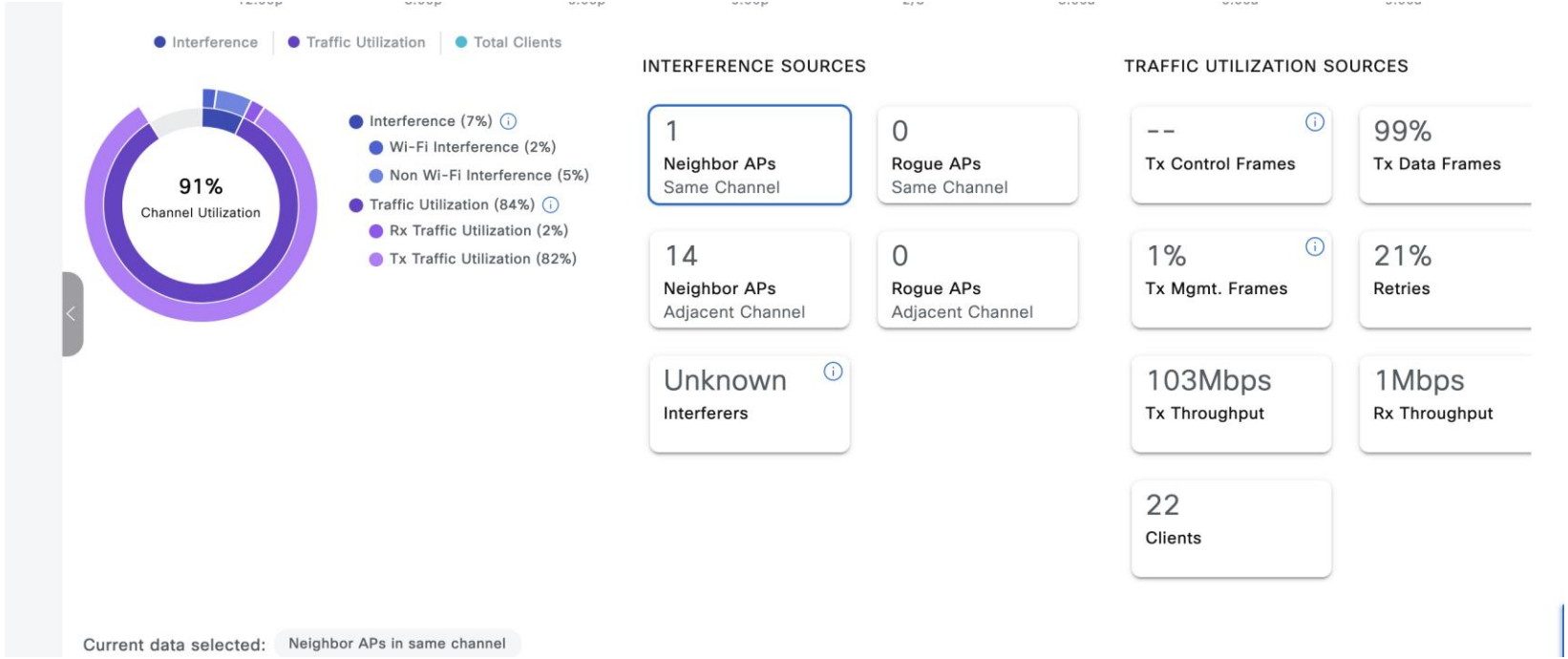
The 5 GHz radio "1" on the AP "H01L0-IL-HI1298" has exceeded the 70% threshold and is currently experiencing 91% utilization. H01L0-IL-HI1298

Customer problem example 4

Customer problem example 4



Customer problem example 4



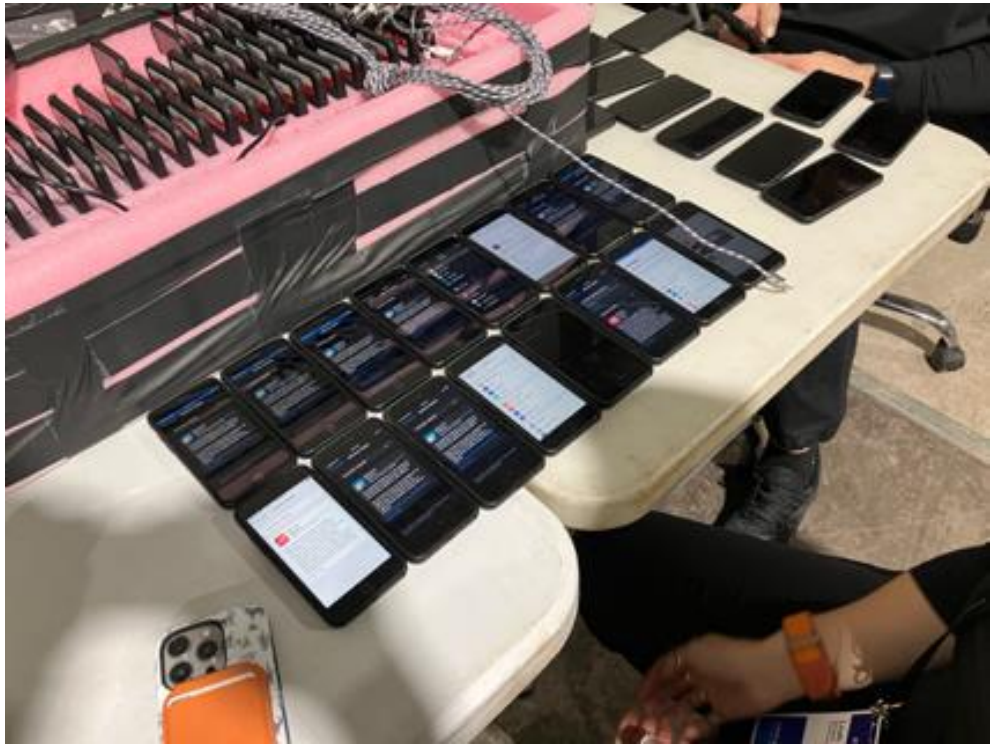
Customer problem example 4

155	2024-02-03 09:46:21.230975	2a01:b740:a02:f000::1	2a11:d940:2:83ff:c909:7247:7f2:488a	1368	STA will stay up	Continuation Data
156	2024-02-03 09:46:21.230975	2a01:b740:a02:f000::5	2a11:d940:2:83ff:3cf2:c434:8fd5:cacf	1368	STA will stay up	Continuation Data
157	2024-02-03 09:46:21.230975	2a01:b740:a02:f000::5	2a11:d940:2:83ff:3cf2:c434:8fd5:cacf	1368	STA will stay up	Continuation Data
158	2024-02-03 09:46:21.230975	2a04:4e42:600::776	2a11:d940:2:83ff:b4ed:4243:9dfd:628c	1398	STA will stay up	Continuation Data
159	2024-02-03 09:46:21.230975	2a04:4e42:600::776	2a11:d940:2:83ff:b4ed:4243:9dfd:628c	1398	STA will stay up	Continuation Data
160	2024-02-03 09:46:21.230975	2a04:4e42:600::776	2a11:d940:2:83ff:b4ed:4243:9dfd:628c	1398	STA will stay up	Continuation Data
161	2024-02-03 09:46:21.230975	2a01:b740:a02:f000::5	2a11:d940:2:83ff:29bd:e631:d3bc:f14b	1368	STA will stay up	Continuation Data
162	2024-02-03 09:46:21.230975	2a01:b740:a02:f100::8	2a11:d940:2:83ff:98e1:287d:aeee:d56c	1368	STA will stay up	Ignored Unknown Record
163	2024-02-03 09:46:21.230975	2a01:b740:a02:f000::5	2a11:d940:2:83ff:29bd:e631:d3bc:f14b	1368	STA will stay up	Continuation Data
164	2024-02-03 09:46:21.230975	2a01:b740:a02:f100::8	2a11:d940:2:83ff:98e1:287d:aeee:d56c	1368	STA will stay up	Ignored Unknown Record
165	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::3	2a11:d940:2:83ff:cdad:aced:5d65:ca5d	1368	STA will stay up	Continuation Data
166	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::3	2a11:d940:2:83ff:cdad:aced:5d65:ca5d	1368	STA will stay up	Continuation Data
167	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::7	2a11:d940:2:83ff:7028:3925:2991:5e8a	1368	STA will stay up	Continuation Data
168	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::7	2a11:d940:2:83ff:7028:3925:2991:5e8a	1368	STA will stay up	Continuation Data
169	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::5	2a11:d940:2:83ff:5460:351f:d805:43ea	1368	STA will stay up	Continuation Data
170	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::5	2a11:d940:2:83ff:5460:351f:d805:43ea	1368	STA will stay up	Continuation Data
171	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::5	2a11:d940:2:83ff:29bd:e631:d3bc:f14b	1368	STA will stay up	Continuation Data
172	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::5	2a11:d940:2:83ff:29bd:e631:d3bc:f14b	1368	STA will stay up	Continuation Data
173	2024-02-03 09:46:21.231982	2a04:4e42:600::776	2a11:d940:2:83ff:b4ed:4243:9dfd:628c	1398	STA will stay up	Continuation Data
174	2024-02-03 09:46:21.231982	2a04:4e42:600::776	2a11:d940:2:83ff:b4ed:4243:9dfd:628c	1398	STA will stay up	Continuation Data
175	2024-02-03 09:46:21.231982	2a04:4e42:600::776	2a11:d940:2:83ff:b4ed:4243:9dfd:628c	1398	STA will stay up	Continuation Data
176	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::5	2a11:d940:2:83ff:3cf2:c434:8fd5:cacf	1368	STA will stay up	Continuation Data
177	2024-02-03 09:46:21.231982	2a01:b740:a02:f000::5	2a11:d940:2:83ff:3cf2:c434:8fd5:cacf	1368	STA will stay up	Continuation Data
178	2024-02-03 09:46:21.231982	2a01:b740:a02:f100::8	2a11:d940:2:83ff:98e1:287d:aeee:d56c	1368	STA will stay up	Ignored Unknown Record
179	2024-02-03 09:46:21.231982	2a01:b740:a02:f100::8	2a11:d940:2:83ff:98e1:287d:aeee:d56c	1368	STA will stay up	Ignored Unknown Record

```
> Frame 127: 1368 bytes on wire (10944 bits), 1368 bytes captured (10944 bits)
> Ethernet II, Src: Cisco_e7:f8:8b (cc:b6:c8:e7:f8:8b), Dst: Cisco_9f:f0:01 (00:00:0c:9f:f0:01)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 130
> Internet Protocol Version 4, Src: wlc3-main.ciscolive.network (10.130.240.13), Dst: 10.7.79.146 (10.7.79.146)
> User Datagram Protocol, Src Port: capwap-data (5247), Dst Port: pk (5272)
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: ......F.
> Logical-Link Control
> Internet Protocol Version 6, Src: 2a01:b740:a02:f000::7 (2a01:b740:a02:f000::7), Dst: 2a11:d940:2:83ff:7028:3925:2991:5e8a (2a11:d940:2:83ff:7028:3925:2991:5e8a)
> Transmission Control Protocol, Src Port: https (443), Dst Port: 56775 (56775), Seq: 21745, Ack: 1, Len: 1208
  Transport Layer Security
```

Customer problem example 4

- 50 iphones upgrading IoS



What did we learn ?

- EPC capture : how does it work

slido

What happens if you enable “Monitor Control Plane” in an EPC ?

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

Access point debugging- Control plane

Troubleshooting 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_ACTION : (.)
[*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 : (.)
```

Troubleshooting on the AP side

For Wave 2 and Wifi 6 APs

AP console output/ Syslogs are stored in the flash even after reboot

Debug client <mac> is a macro that will trigger a control-plane sniffer capture. Various options exist to save as .pcap or export in hex

Since 17.3, you can export an AP support bundle to the WLC

Since 17.12, you can see hit counters on flex ACLs

Much more in “**Troubleshoot COS APs**” on cisco.com

Can I run commands on the AP from the WLC

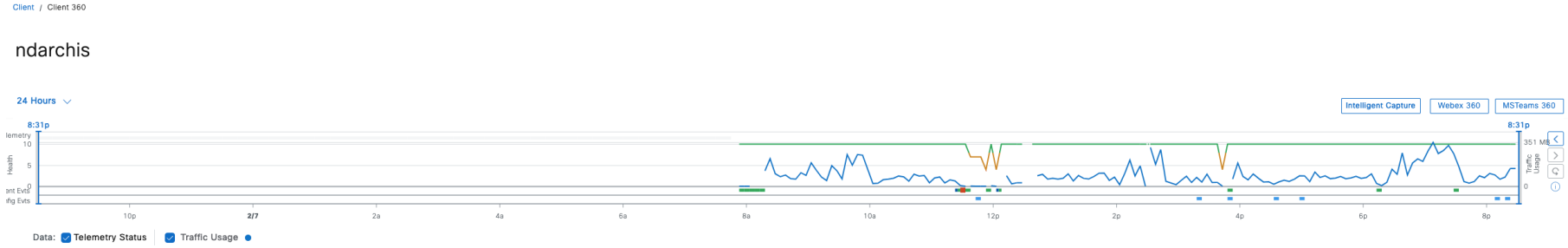
For when you lost the AP SSH credentials …

```
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#
```

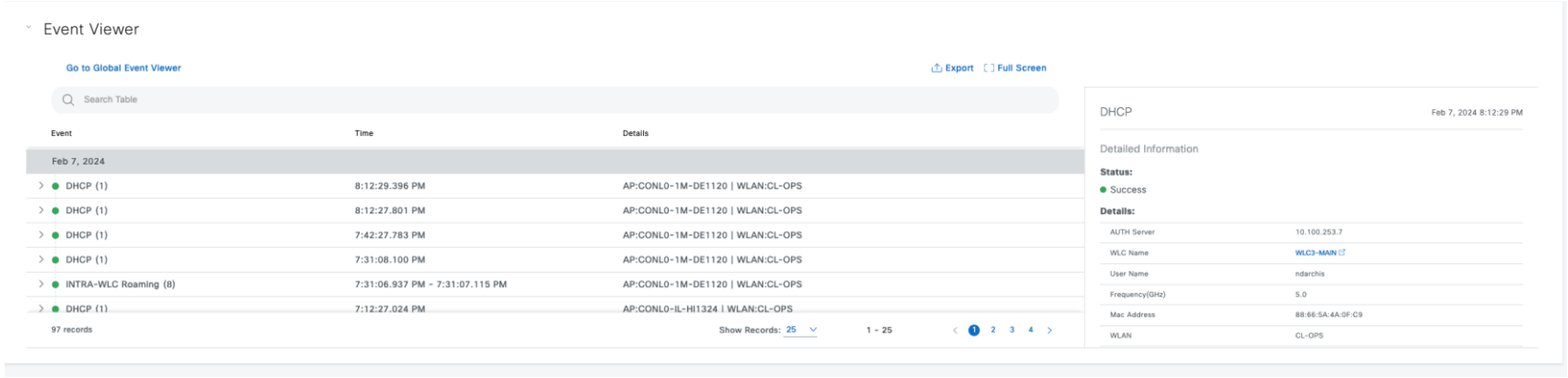
AP client debug bundle

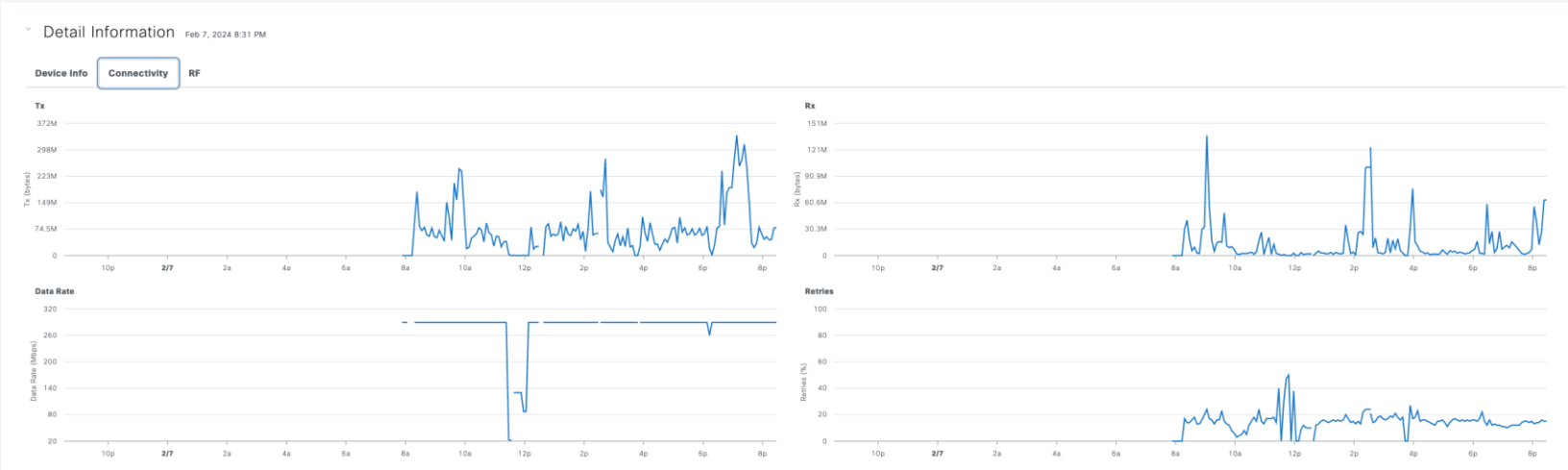

```
AP0CD0-F894-4D64#debug client-bundle start debug 22:0F:23:B1:82:EC
AP0CD0-F894-4D64#show client-bundle
  status  Show client bundle status
AP0CD0-F894-4D64#show client-bundle status
Client Bundle Status              : Started
Client Bundle Starting Addresses  : 22:0F:23:B1:82:EC
Client Bundle Upload 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



Client 360 view

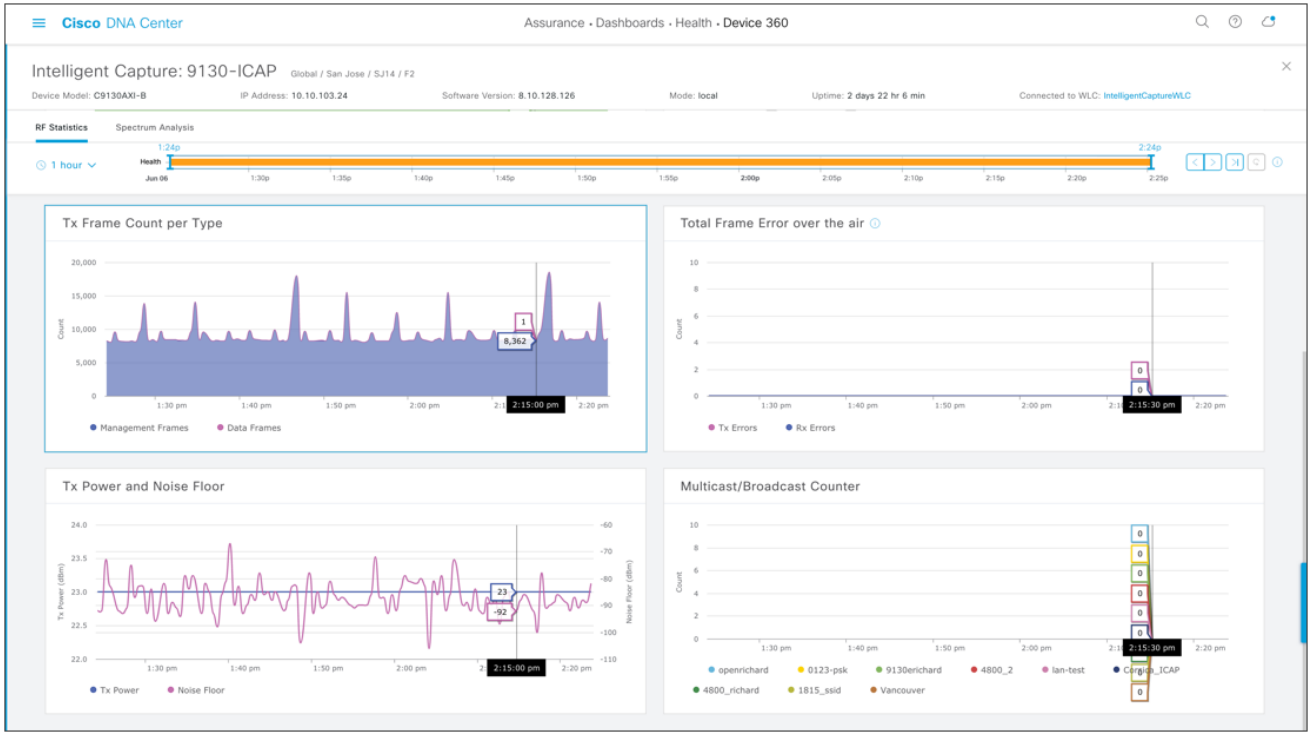




Intelligent capture

Cisco Catalyst Center RF stats

RF stats can be enabled globally or on specific APs



Customer problem example 5

-Cisco Catalyst Center Intelligent capture (Channel utilization, drops, ...)

-Show commands on the APs themselves

slido

Which one of these does not exist / is not useful ?

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

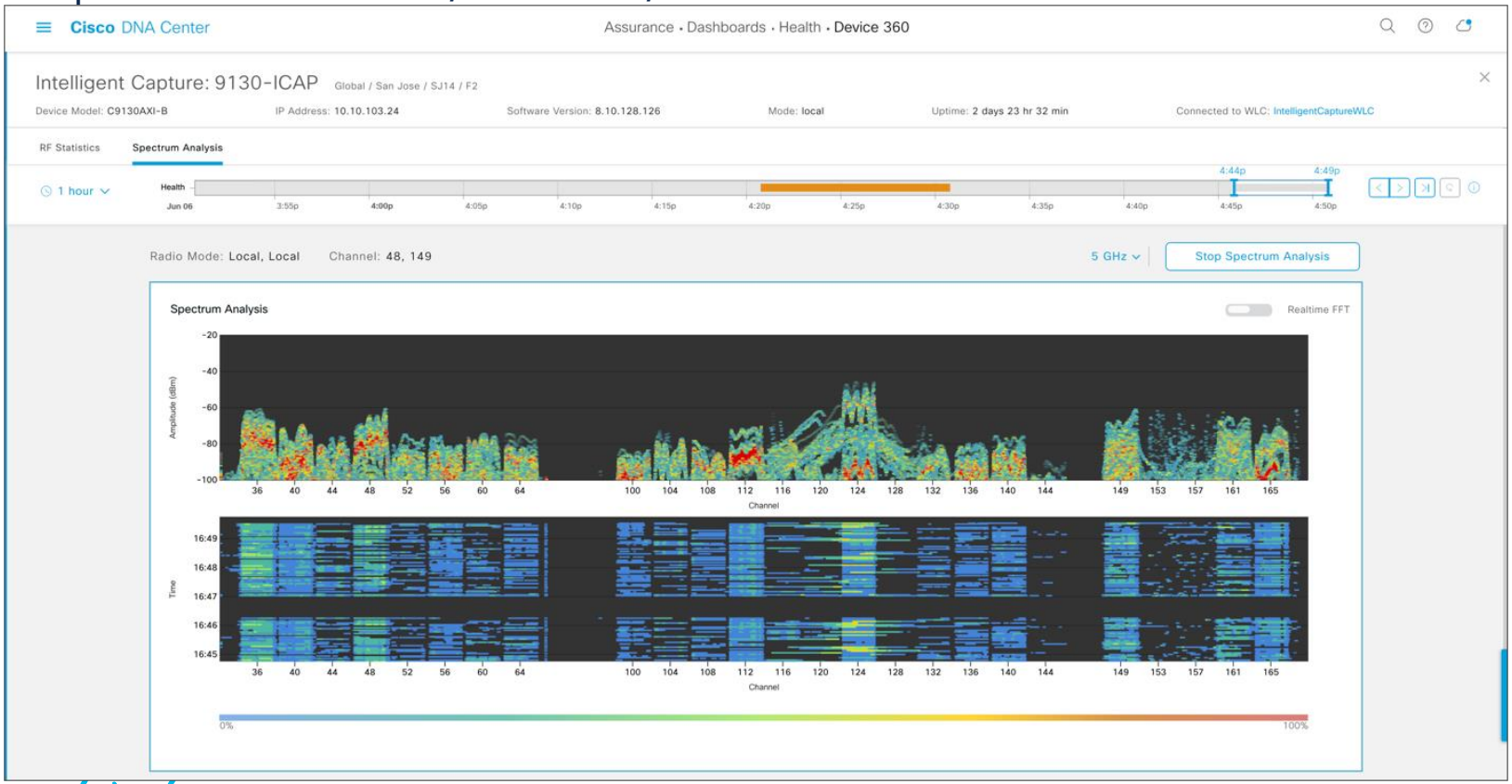
What did we learn ?

- Access point tech support bundle
- Access point client debug bundle
- Access points debugs

Access point debugging-dataplane

Intelligent capture

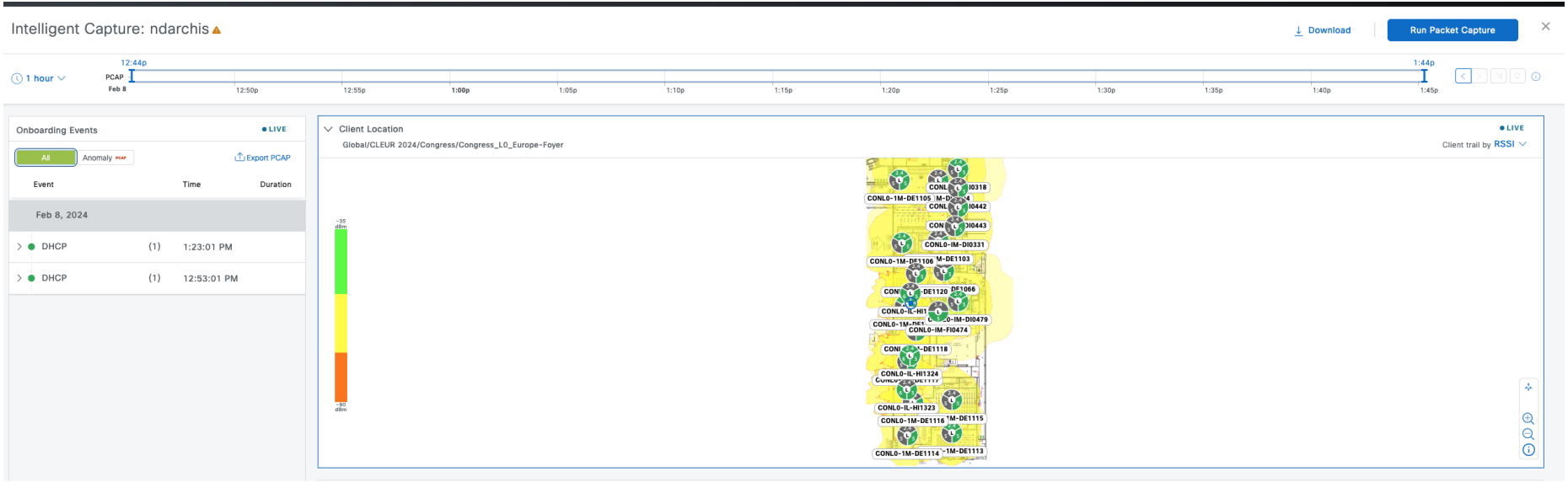
The power of Cleanair / RF Asic / Cleanair Pro



Intelligent capture

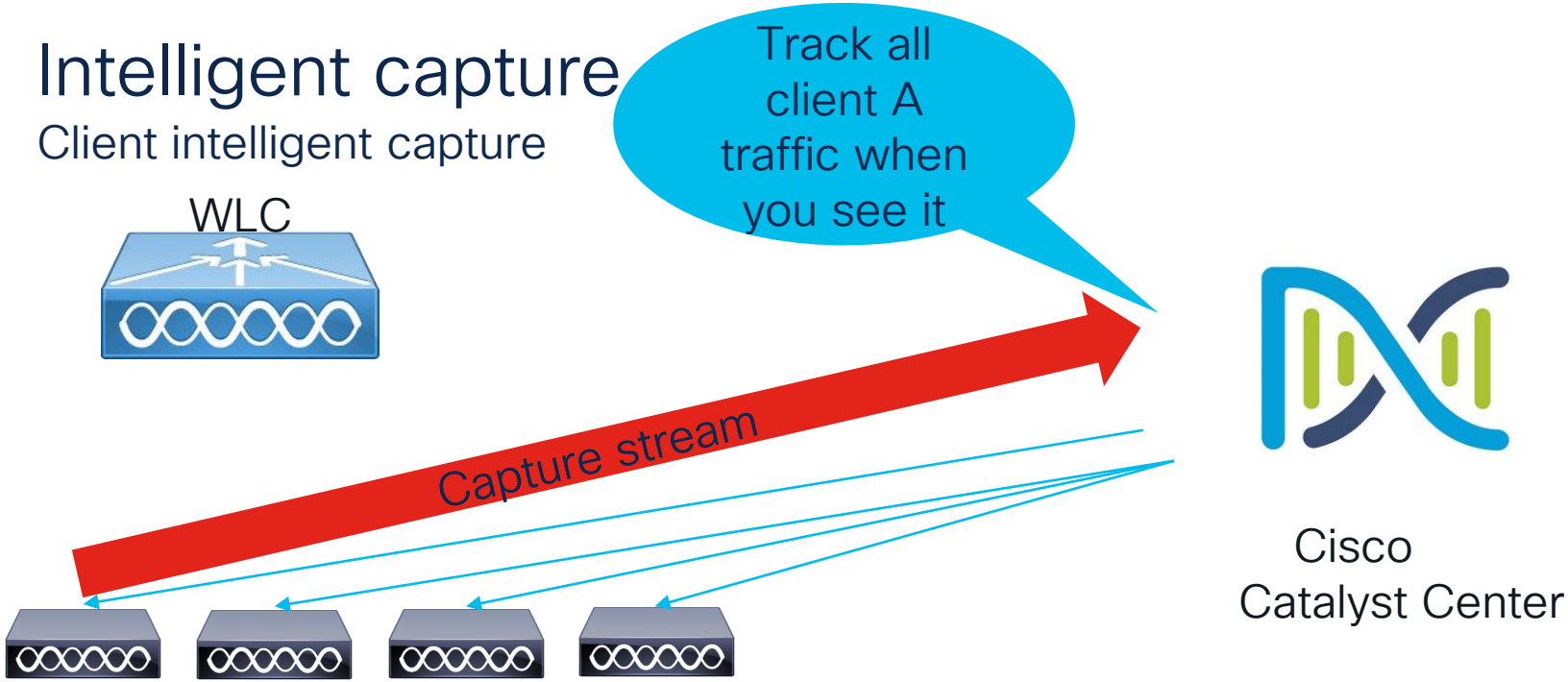
Client intelligent capture

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



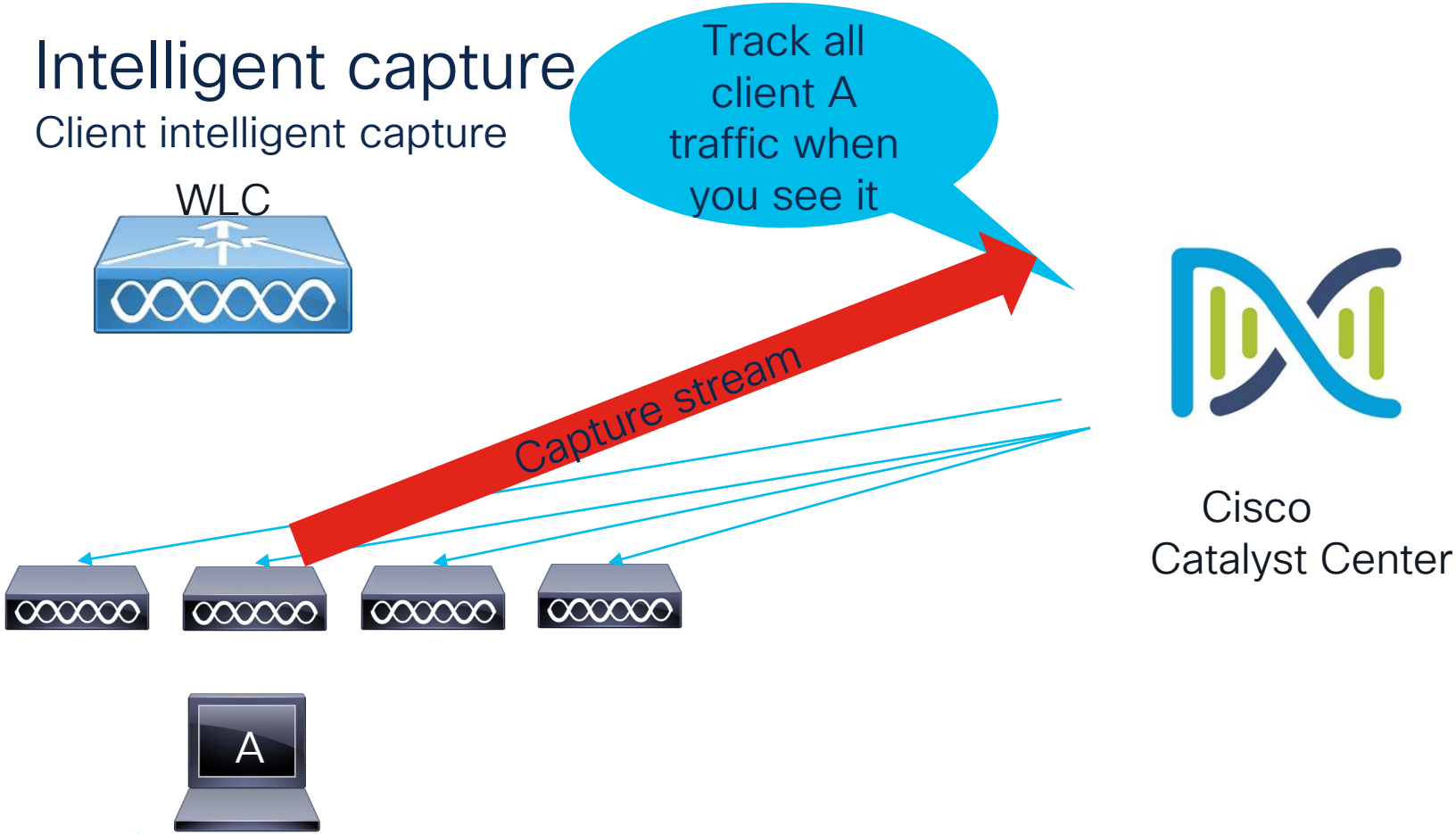
Intelligent capture

Client intelligent capture



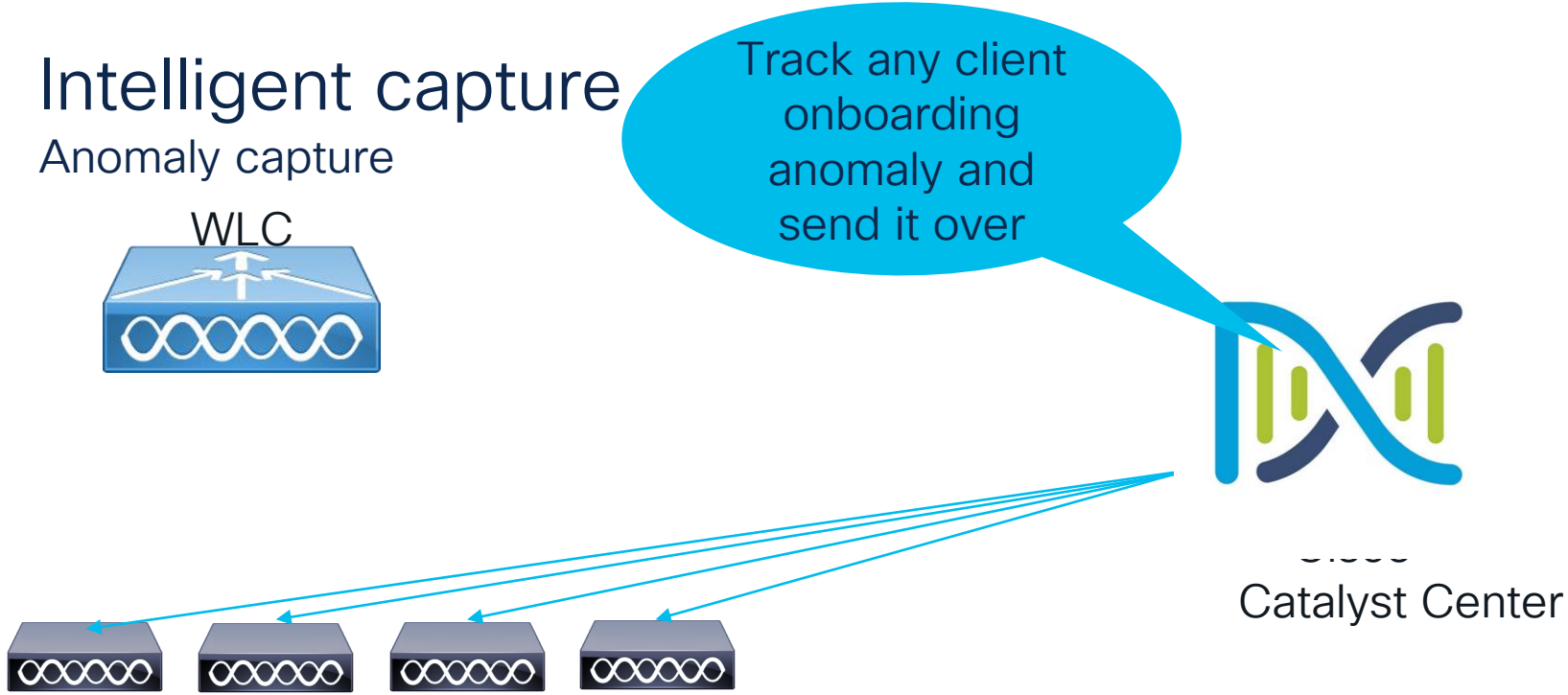
Intelligent capture

Client intelligent capture



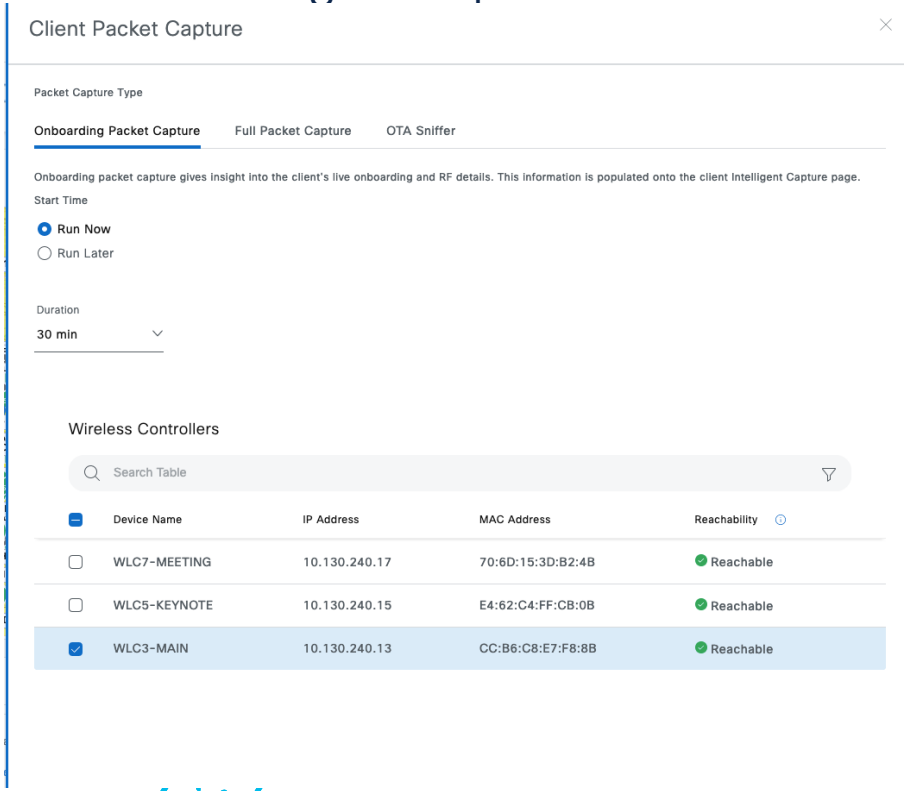
Intelligent capture

Anomaly capture



Intelligent capture

Client intelligent capture

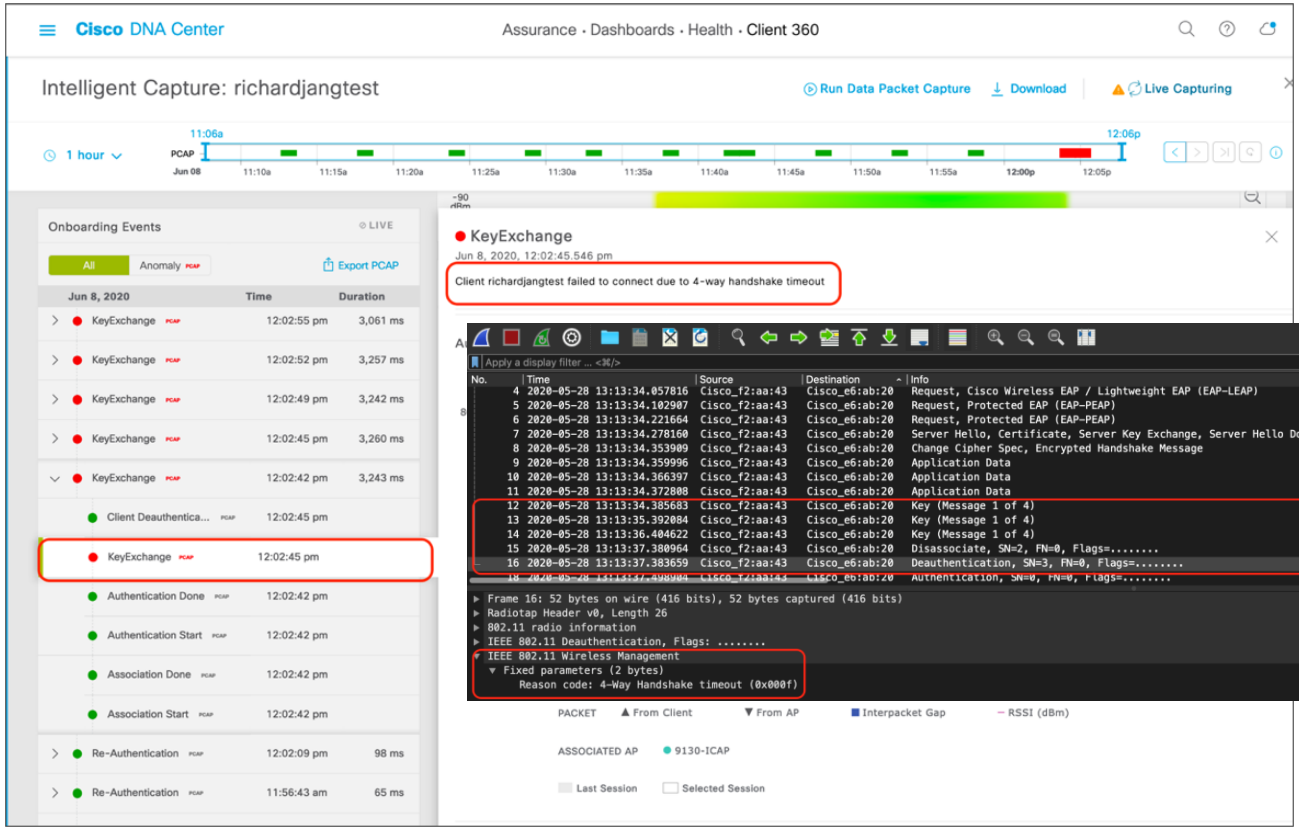


Data packet capture supported on 4800 , 9130, 9166

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

Intelligent capture

Anomaly capture



Customer problem example 6

-Debugs on the AP (debug client/client trace/client debug bundle)

-PCAP on the AP switchport

Customer problem example 7

-Debugs on the AP (debug client/client trace/client debug bundle)

-PCAP on the AP switchport

-Intelligent Capture

slido

Which statement is FALSE regarding Intelligent Capture ?

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

What did we learn ?

- Intelligent capture
- RF stats
- OTA capture

WLC top issues

WLC High CPU issues

WLC High CPU

What does the CPU handle?

- Client onboarding and authentication
- RRM
- Web authentication interception
- Rogue detection
- mDNS

What does the dataplane handle?

- 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.
- This command only shows you the 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

- This is the “real” CPU usage command

```
WLC3-MAIN#show proc cpu platform sorted
CPU utilization for five seconds: 15%, one minute: 17%, five minutes: 18%
Core 0: CPU utilization for five seconds: 11%, one minute: 17%, five minutes: 16%
Core 1: CPU utilization for five seconds: 14%, one minute: 13%, five minutes: 16%
Core 2: CPU utilization for five seconds: 18%, one minute: 17%, five minutes: 18%
Core 3: CPU utilization for five seconds:  8%, one minute: 15%, five minutes: 18%
Core 4: CPU utilization for five seconds:  9%, one minute: 15%, five minutes: 16%
Core 5: CPU utilization for five seconds:  9%, one minute: 15%, five minutes: 16%
(...)
 Pid    PPid    5Sec    1Min    5Min  Status      Size  Name
------------------------------------------------------------------------------
 20509  20501   54%     58%     54%   S         892872  wncd_4
 23713  23705   49%     53%     53%   S         858348  odm_0
 20390  20382   27%     27%     26%   S         637644  wncd_3
 20624  20616   24%     23%     22%   S         622304  wncd_5
 20045  20037   22%     23%     23%   S         597228  wncd_0
 26791  26784   19%     22%     21%   S         900532  pubd
```

WLC High CPU

- 2 Exceptions: 9800-CL and 9800-L use dedicated CPU cores for dataplane forwarding

```
#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:  99%, one minute: 99%, five minutes: 99%
   Pid    PPid    5Sec    1Min    5Min  Status       Size  Name
-----------------------------------------------------------------------------------
 22225   21691     99%     99%     99%  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

- Is my WLC reaching its maximum forwarding capacity ?

```
#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

- Is my WLC reaching its maximum capacity ?

WLCs are documented to support a maximum amount of throughput, APs and clients.

Those are maximums.

Extremely busy environments cause higher stress (CPU) and data forwarding capacity goes down with some features (AVC,ACLs, ...) and depends on packets sizes.

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

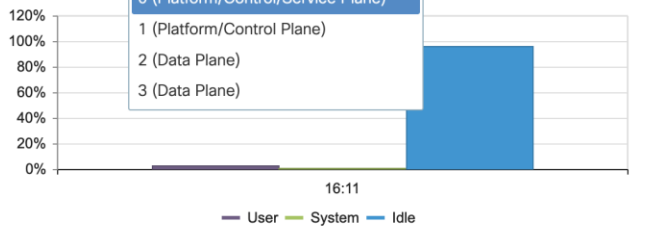
Datapath Utilization Dump

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

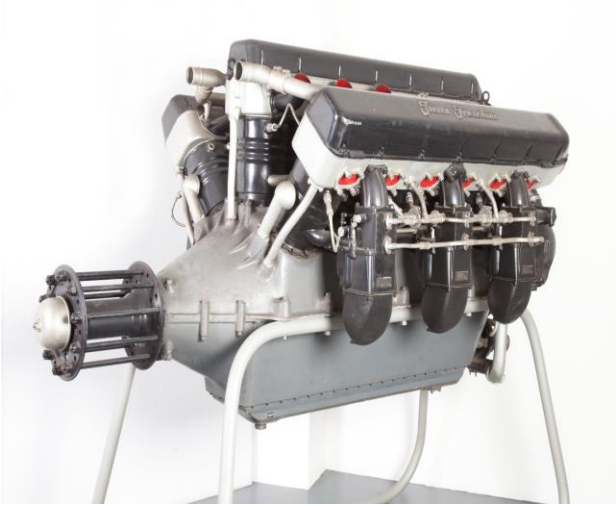


WLC High CPU

What to do in case a specific process like WNCD is on high CPU ?
You want to run on all cylinders of your engine

You don’t want to drive a Lambo like a Twingo

Or swap a Rollex for a Casio



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
```

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

Drop Cause	Packets	Octets
Wls Client V6 Max Address Error	2327420	308222027
Wls Client IPGlean Counter Index Error	0	0
Wls Client IPGlean Counter Unchanged Error	18830926	2232780511
Wls Client IPGlean alloc no memory Error	0	0
Wls Client iplearn l2 punt data packet skip	25	21952
Wls Client iplearn v4 punt data packet skip	351216	94564584
Wls Client iplearn v6 punt data packet skip	266367	60601909
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
Wls vlan bridging src wlclient i/p SB miss error	0	0
Wls Client input config missing	0	0
Wls Client global mac address fetch error	0	0

Data Plane Statistics – Traffic sent to CPU

show platform hardware chassis active qfp feature wireless punt statistics

App Tag	Packet Count
CAPWAP_PKT_TYPE_DOT11_PROBE_REQ	59322162
CAPWAP_PKT_TYPE_DOT11_MGMT	37260139
CAPWAP_PKT_TYPE_DOT11_IAPP	95348878
CAPWAP_PKT_TYPE_DOT11_RFID	0
CAPWAP_PKT_TYPE_DOT11_RRM	0
CAPWAP_PKT_TYPE_DOT11_DOT1X	4769507
CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE	18744317
CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE	132120
CAPWAP_PKT_TYPE_CAPWAP_CNTRL	125349464
CAPWAP_PKT_TYPE_CAPWAP_DATA	0
CAPWAP_PKT_TYPE_CAPWAP_DATA_PAT	3077
CAPWAP_PKT_TYPE_MOBILITY_CNTRL	526128
WLS_SMD_WEBAUTH	0
SISF_PKT_TYPE_ARP	47462412
SISF_PKT_TYPE_DHCP	2396389
SISF_PKT_TYPE_DHCP6	1137774
SISF_PKT_TYPE_IPV6_ND	61149032
SISF_PKT_TYPE_DATA_GLEAN	40916
SISF_PKT_TYPE_DATA_GLEAN_V6	1685513
SISF_PKT_TYPE_DHCP_RELAY	0
WLCLIENT_PKT_TYPE_MDNS	0
CAPWAP_PKT_TYPE_CAPWAP_RESERVED	0

WLC High CPU

Other possible causes for high WNCD CPU usage :

-Very high probing activity

-ARP storms

-Huge amount of cleanair interferers

-Heavy mDNS usage

-Extremely high client density

What did we learn ?

- Specifics about data plane (hardware and software)
- Specifics about troubleshooting the dataplane and high CPU
- This is all explained in **“Understand High CPU Usage Reported for the Dataplane on Catalyst 9800”** on cisco.com

HA hot issues

WLC HA related concerns

```
------------------- show redundancy switchover history ------------------
Index   Previous Current   Switchover                    Switchover
        active   active    reason                        time
 -----  -------- -------   ----------                    ----------
1       1        2         active unit removed           03:26:22 central Mon Aug 29 2022
```

WLC HA related concerns

Are you experiencing unexpected failovers ?

- Verify the WLC reload reason and possible system reports and crash files. It could be as simple as a power failure
- If using 9800-CL, verify interactions with VMWare features : they could be freezing the VM and causing a failover
- You could be having too aggressive failover timers

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

```
test wireless redundancy capture start
test wireless redundancy capture stop

test wireless redundancy rpingp
```

WLC HA ISSU upgrade 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
```

AAA top issues

My RADIUS server is often 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.
```

=>RAtrace + PCAP

My RADIUS server is often not responding?

Getting an RAtrace of a client failing when the RADIUS is already marked dead will not show much.

The best is to get the trace of the specific client that made the 9800 declare the RADIUS as dead.

Not easy. You often need to set the WNCD logs to debug and collect WNCD logs over a period of time.

My RADIUS server is often 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
```

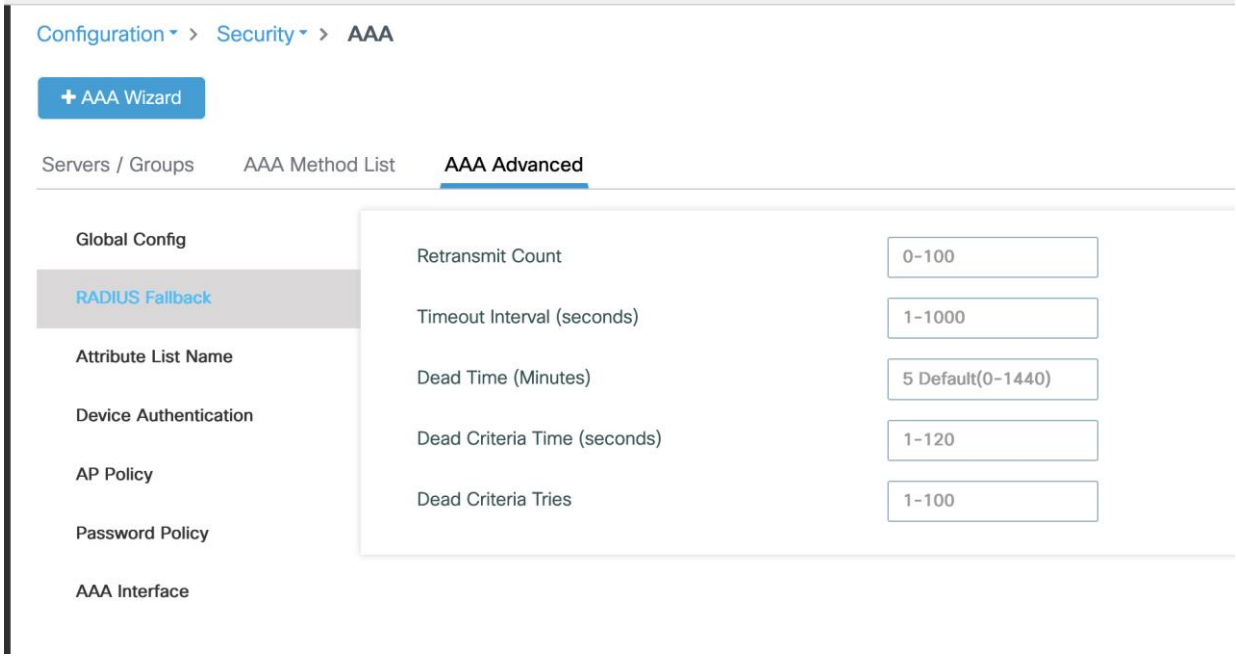
Typical causes

- ISE or other RADIUS servers may decide to ignore RADIUS requests in certain conditions

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 :	

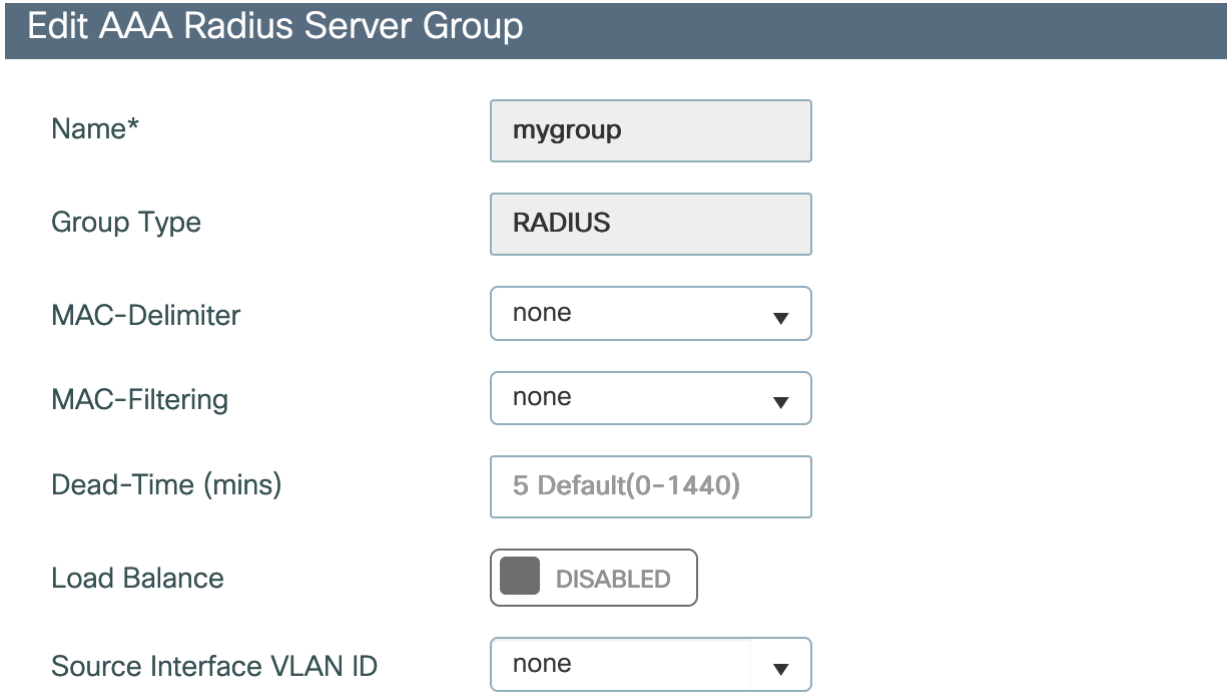
Typical causes

- 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”

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 Wi-Fi 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

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

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

Flash space issues

Can my WLC face free space problems ?

On appliances, it’s unlikely

Tracelogs are free to grow up to a certain size and rotate when reaching that maximum.

IOS images, crash files and system reports are free to fill the rest of the free space.

C9800-CL are typically limited on flash space

The latest stuff

17.12 : Catalyst APs going 115200 bauds

Meraki persona APs always had a console of 115200

To accelerate boot time, Catalyst personas also use 115200 bauds on 17.12

BUT

Not automatically upon upgrade. Only upon factory reset.

You could still order a brand new 9166 with 17.9.1 in the flash and 9600 bauds.

CSCvx32806 : Bootloop of death

CAPWAP image download is, by default, slow and somewhat unreliable (UDP).

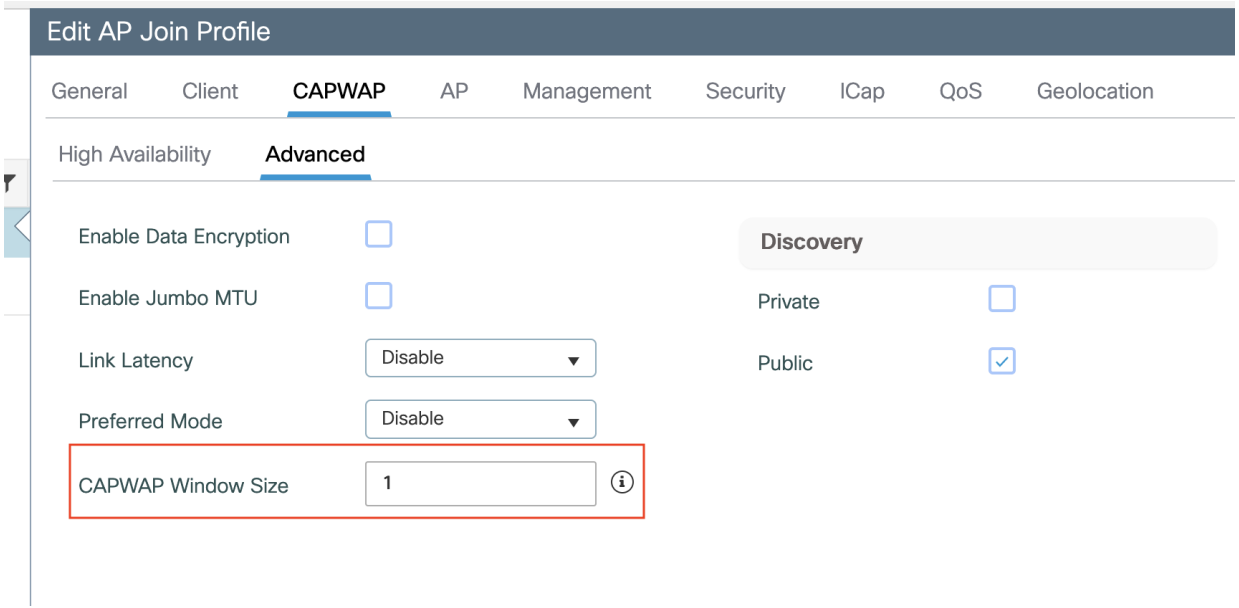
Risk of bootloop in versions before 17.9.3, especially when image is downloaded over WAN : https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html

Fix : Now image is properly verified during download.

17.13 has a complete corruption verification and prevention system

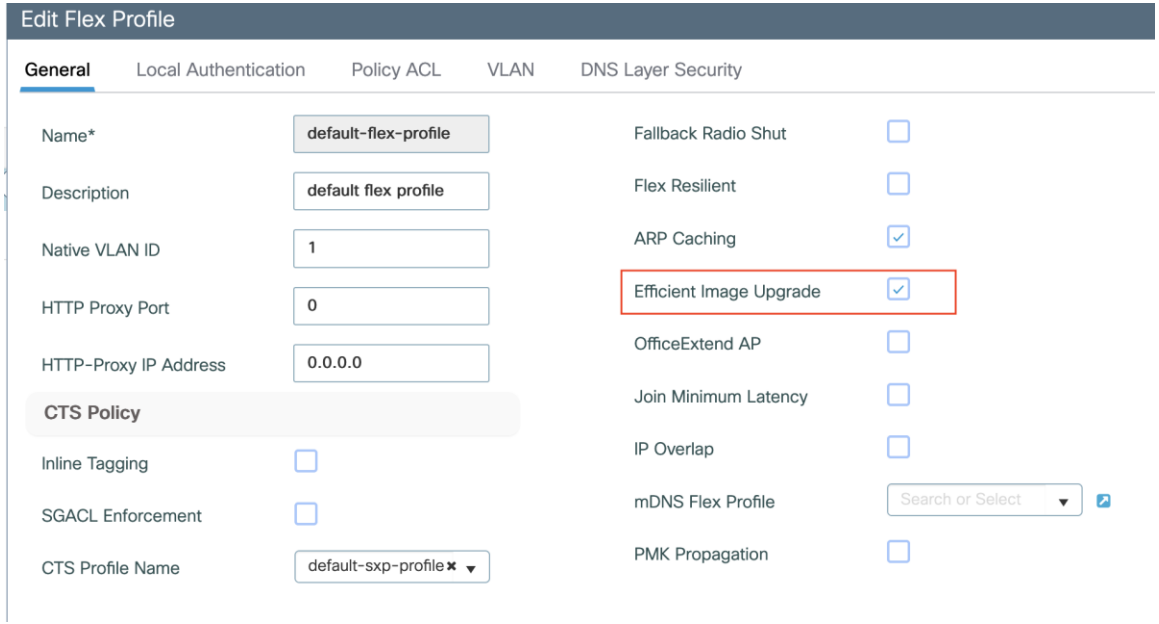
A short side-track about AP image download

You can accelerate AP image download via CAPWAP with the CAPWAP window (up to 15):



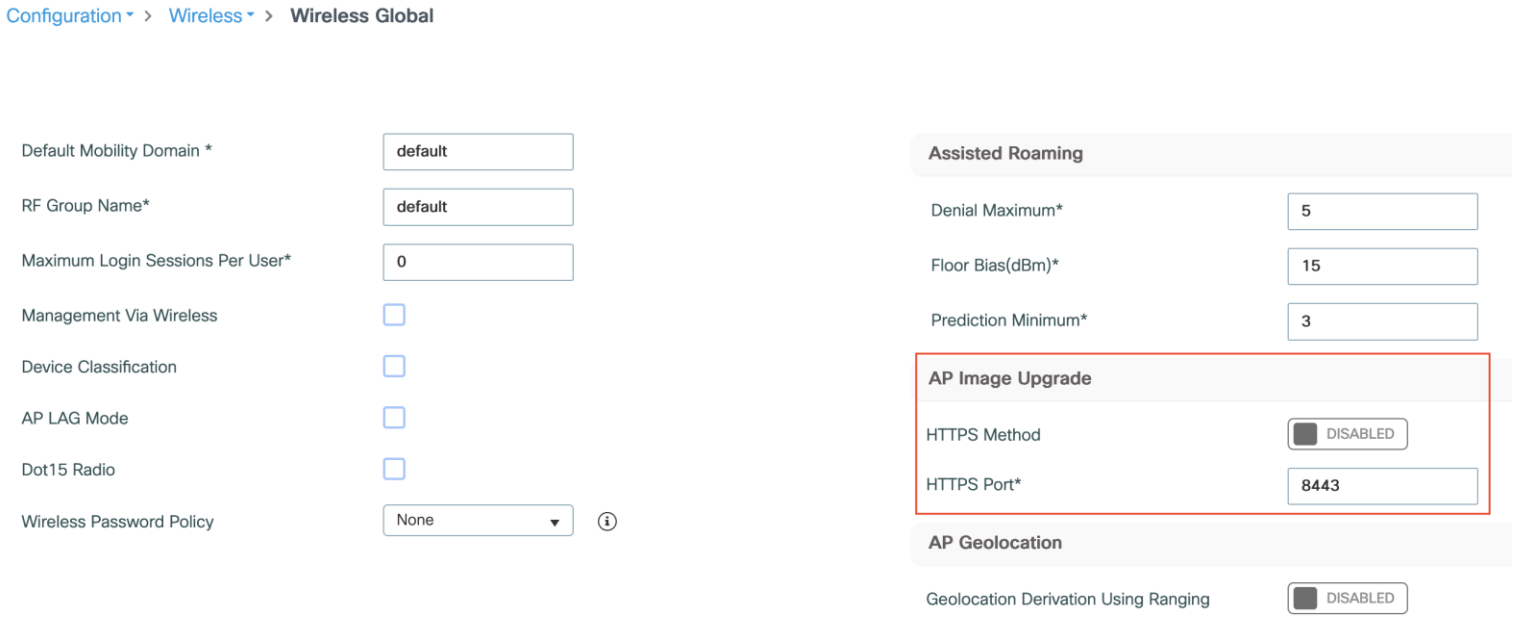
No, really let's keep it short

You can enable efficient upgrade for Flex APs to share images with each other:



Let’s not side track this too much, shall we

Since 17.11, APs can do TCP image download via HTTPS !



CVE-2023-20198 Web UI vuln.: Nico's summary

Affects public IP WLCs mostly. Does not affect guest portal.

Upgrade to fixed software 17.6.6a,17.9.4a, 17.12.2 (or SMUs)

Workarounds : Disable HTTP(s) server

Configure an ACL on the web server

"ip http secure-active-session-modules none"
(disables http management access)

FN-72578 Licensing high CPU: Nico's summary

Devices might report high CPU or memory usage. In some scenarios, devices might report both high CPU and memory usage.

Affecting 17.3.6,17.6.4

CSCvv72609 : High CPU usage triggered by RUM reports

CSCwa85525 : Memory leak due to Smart Agent Memory utilization

CSCwa85199 : Unackowledged reports can cause high CPU

FN72510- weak crypto not allowed

Starting 17.11, weak crypto are not tolerated in IPSEC anymore

-Only concerns IPSEC

-Keep an eye on release notes for upcoming weak crypto drops

IOS APs : They’re won’t be back(17.9.6/17.12.4)

Upgrade path watch out

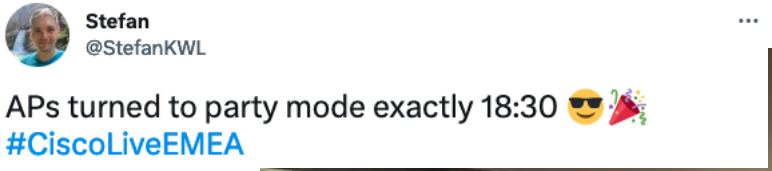
17.3.5 works as upgrade hop towards 17.9 especially for 9130

17.2.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.9.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.9.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.9.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.9.x.

Problem : APs that you kept in stock or got through RMA might not join a 17.9 WLC anymore. Migration from AireOS can be complicated

Solution: Manual upgrade or interim hop WLC

Bonus : Party mode



Stefan
@StefanKWL

APs turned to party mode exactly 18:30 😎🎉
#CiscoLiveEMEA

Bonus : Party mode

```
event manager applet EEM_PARTY_MODE_START
 event timer cron name FEB_8_2024_17_30_UTC cron-entry "30 17 8 2 2024" maxrun 600
 action 101 cli command "enable"
 action 102 cli command "terminal length 0"
 action 103 cli command "show ap summary | i Registered"
 action 104 foreach line "$_cli_result" "\n"
 action 105  regexp "^([^\s]+)" "$line" _match _AP_NAME
 action 106  if $_regexp_result eq "1"
 action 107   cli command "ap name $_AP_NAME led flash start duration 0"
 action 108  end
 action 109 end
```

Bonus : EEM scripts

```
event manager applet AP_AUTO_CH_TX
 event none maxrun 7200
 action 101 cli command "enable"
 action 102 cli command "terminal length 0"
 action 103 cli command "show ap summary | i Registered"
 action 104 foreach line "$_cli_result" "\n"
 action 105  regexp "^([^\s]+)" "$line" _match _AP_NAME
 action 106  if $_regexp_result eq "1"
 action 107   cli command "ap name $_AP_NAME dot11 5ghz channel auto"
 action 108   cli command "ap name $_AP_NAME dot11 5ghz txpower auto"
 action 109   cli command "ap name $_AP_NAME dot11 dual-band channel auto"
 action 110   cli command "ap name $_AP_NAME dot11 dual-band txpower auto"
 action 111  end
 action 112 end
 action 113 cli command "terminal length 30"
```

Bonus : EEM scripts

```
alias exec mv event manager run PRIMARY_SECONDARY_TERTIARY_MAIN
event manager applet PRIMARY_SECONDARY_TERTIARY_MAIN
 event none maxrun 600
 action 101 cli command "en"
 action 102 cli command "term len 0"
 action 104 cli command "sh ap summary | i $_none_arg1"
 action 105 puts "sh ap summary | i $_none_arg1"
 action 106 foreach line "$_cli_result" "\n"
 action 107  regexp "^([^ ]+).*\r$" "$line" _match _AP_NAME
 action 108  if $_regexp_result eq "1"
 action 110   cli command "ap name $_AP_NAME no controller primary WLC1"
 action 111   cli command "ap name $_AP_NAME no controller secondary WLC2"
 action 112   cli command "ap name $_AP_NAME no controller tertiary WLC3"
 action 123   cli command "ap name $_AP_NAME controller primary WLC3-MAIN 10.130.240.13"
 action 124   cli command "ap name $_AP_NAME controller secondary WLC5-KEYNOTE 10.130.240.15"
 action 135  end
 action 136 end
```

Tools and References

Monitor 9800 KPIs

What commands to collect to monitor 9800 operations?

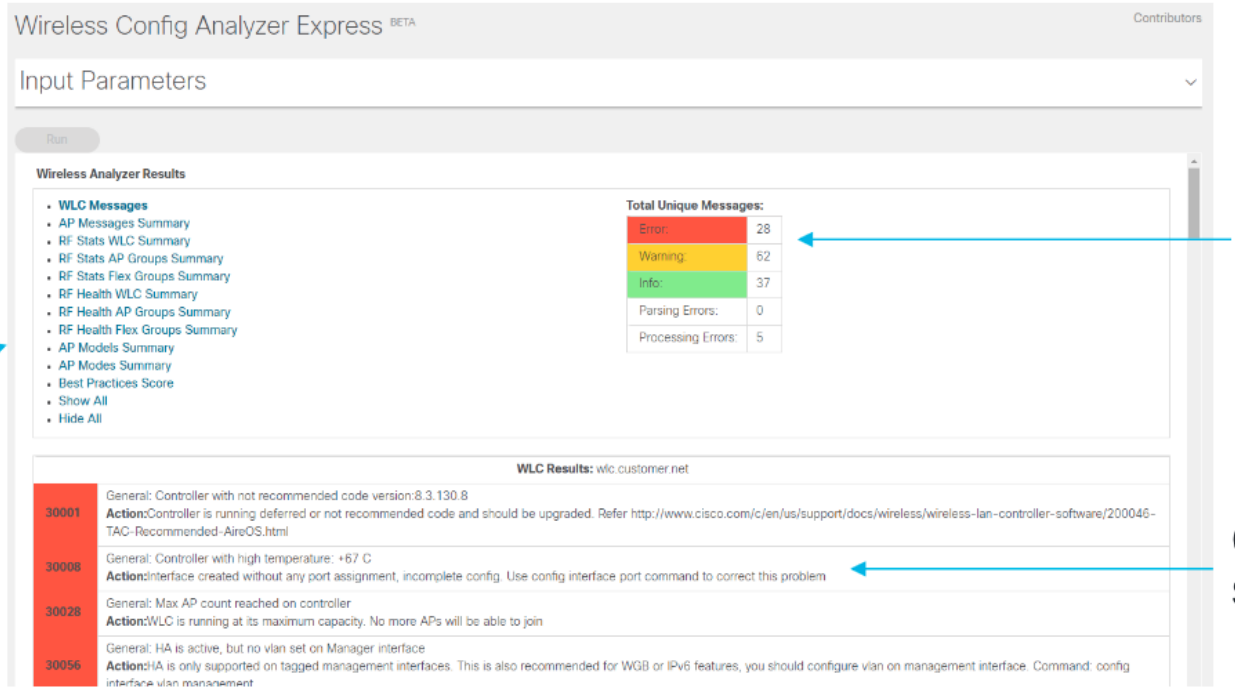
https://blogs.cisco.com/networking/wireless-catalyst-9800-wlc-kpis-part-1

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

Compatibility

IOS-XE	DNACenter	Identity Services Engine	Prime Infrastructure	CMX, DNA Spaces	AireOS
17.3.8	2.1.2.4->2.3.3.5	3.1	3.8->3.10.1	10.6.2-89->10.6.3-146	8.5.164.216->8.5.182.104 8.10.130->8.10.181
17.6.6	2.2.2.4->2.3.3.5	2.4->3.0	3.10	10.6.3-70->10.6.3-146	8.5.164->8.5.182.104 8.10.130->8.10.181
17.9.4	2.3.3.5	2.4->3.2	3.10.2	10.6.3-70->10.6.3-146	8.5.176.2->8.5.182.104 8.10.130->8.10.181
17.12.2	2.3.5.5/2.3.7.3	2.7->3.2	3.10.3	10.6.3	8.5.176.2->8.5.182.104 8.10.130->8.10.190

WCAE

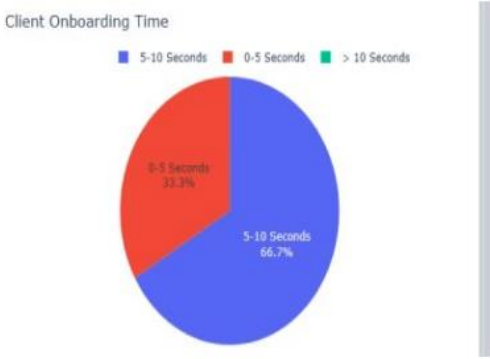


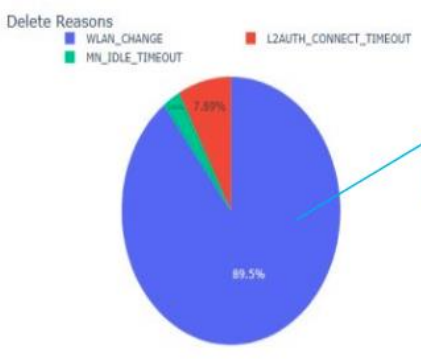
Menu Area

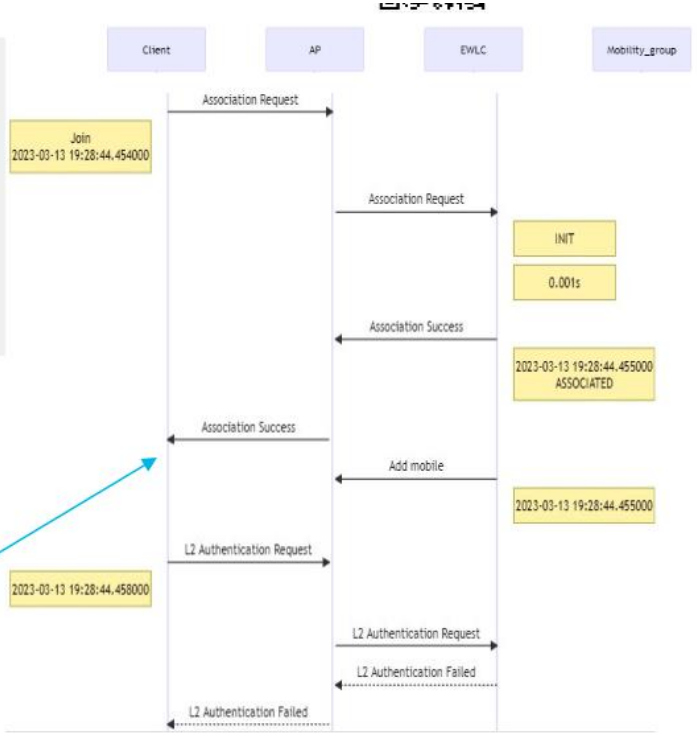
Message Counts

Open summary

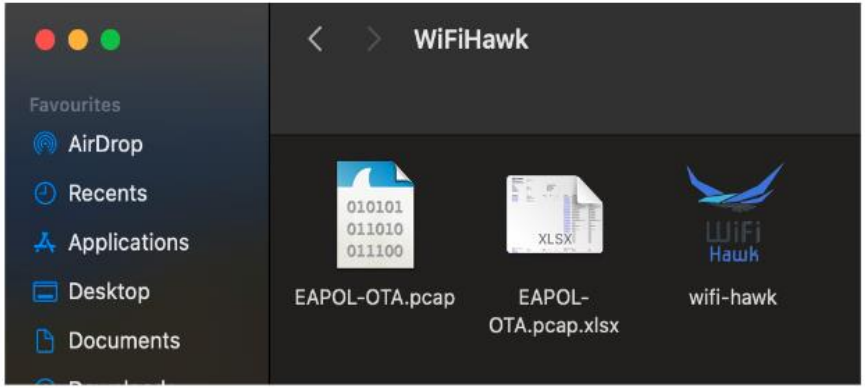
Debug Analyzer







Wifi Hawk

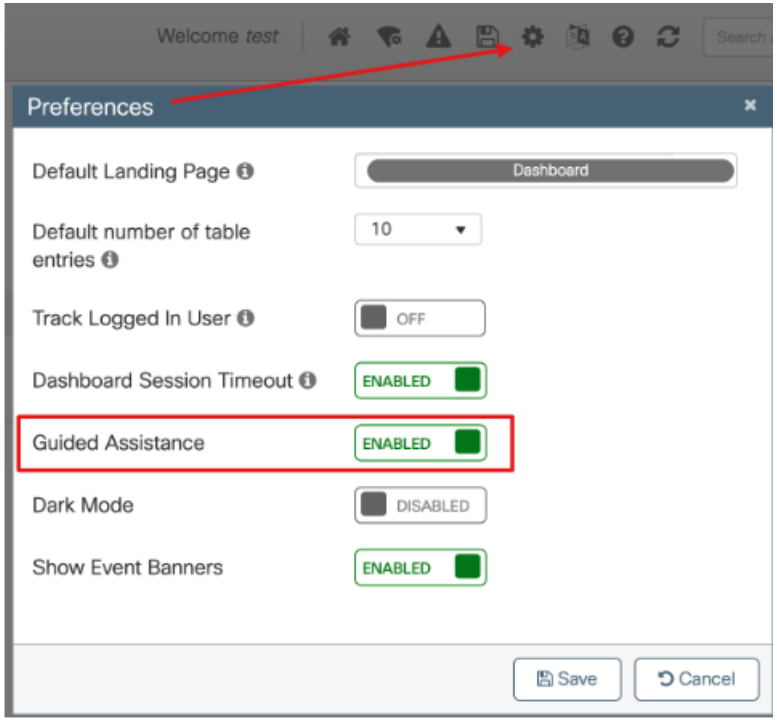


	TX	RX
Dot11 Auth Requests	2	2
Association Requests:	2	2
Reassociation Requests:	0	0
Data frames:	5	273
Retries:	1	17
Multi-retry events:	1	

Event Flow:

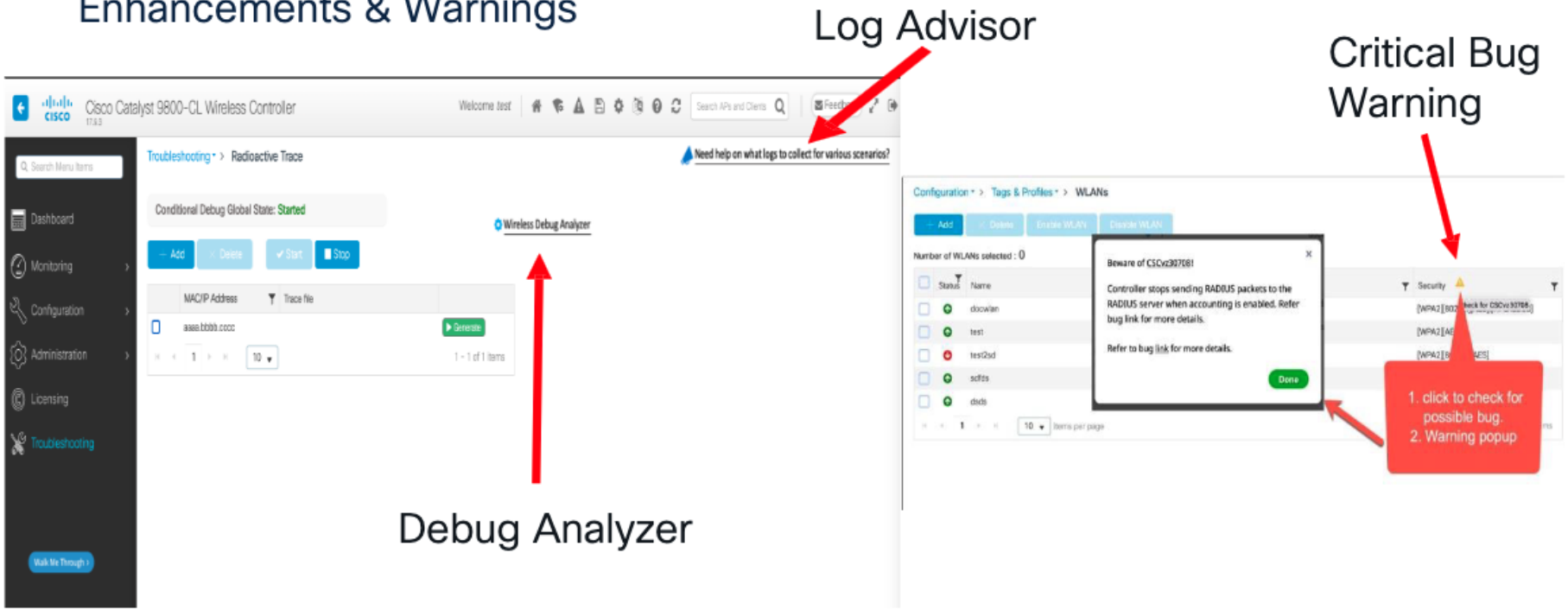
Direction	Type	Severity	BSSID	Frame	Time	Info
▷▷▷▷▷▷	Auth request	Info	aa:aa:bb:bb:cc:cc	13724	Tue, 10 Oct 2023 14:10:04.537097	Auth Open System
◁◁◁◁◁◁	Auth resp success	Info	aa:aa:bb:bb:cc:cc	13731	Tue, 10 Oct 2023 14:10:04.539519	Auth Open System
▷▷▷▷▷▷	Assoc request	Info	aa:aa:bb:bb:cc:cc	13733	Tue, 10 Oct 2023 14:10:04.539525	Type: PSK . To SSID:Test_SSID
◁◁◁◁◁◁	Assoc resp success	Info	aa:aa:bb:bb:cc:cc	13745	Tue, 10 Oct 2023 14:10:04.544746	Client Associated
◁◁◁◁◁◁	EAP KEY RX	Info	aa:aa:bb:bb:cc:cc	13753	Tue, 10 Oct 2023 14:10:04.549212	EAPoL M1
▷▷▷▷▷▷	EAP KEY TX	Info	aa:aa:bb:bb:cc:cc	13755	Tue, 10 Oct 2023 14:10:04.549217	EAPoL M2
◁◁◁◁◁◁	EAP KEY RX	Info	aa:aa:bb:bb:cc:cc	13757	Tue, 10 Oct 2023 14:10:04.550940	EAPoL M3
▷▷▷▷▷▷	EAP KEY TX	Info	aa:aa:bb:bb:cc:cc	13759	Tue, 10 Oct 2023 14:10:04.550949	EAPoL M4
------	EAPoL 4-way Complete	Info	aa:aa:bb:bb:cc:cc	13759	Tue, 10 Oct 2023 14:10:04.550949	Completed PSK auth (EAPoL 4-way)
▷▷▷▷▷▷	RM Neighbor Report Request	Info	aa:aa:bb:bb:cc:cc	13766	Tue, 10 Oct 2023 14:10:04.552536	Client requested Radio Measurament report
▷▷▷▷▷▷	Action frame from client	Info	aa:aa:bb:bb:cc:cc	13881	Tue, 10 Oct 2023 14:10:04.577609	Action frame from client. Continuous frames:1
◁◁◁◁◁◁	Action frame to client	Info	aa:aa:bb:bb:cc:cc	13889	Tue, 10 Oct 2023 14:10:04.578780	Action frame to client. Continuous frames:3

WalkMe- Guided Conceptual Assistance



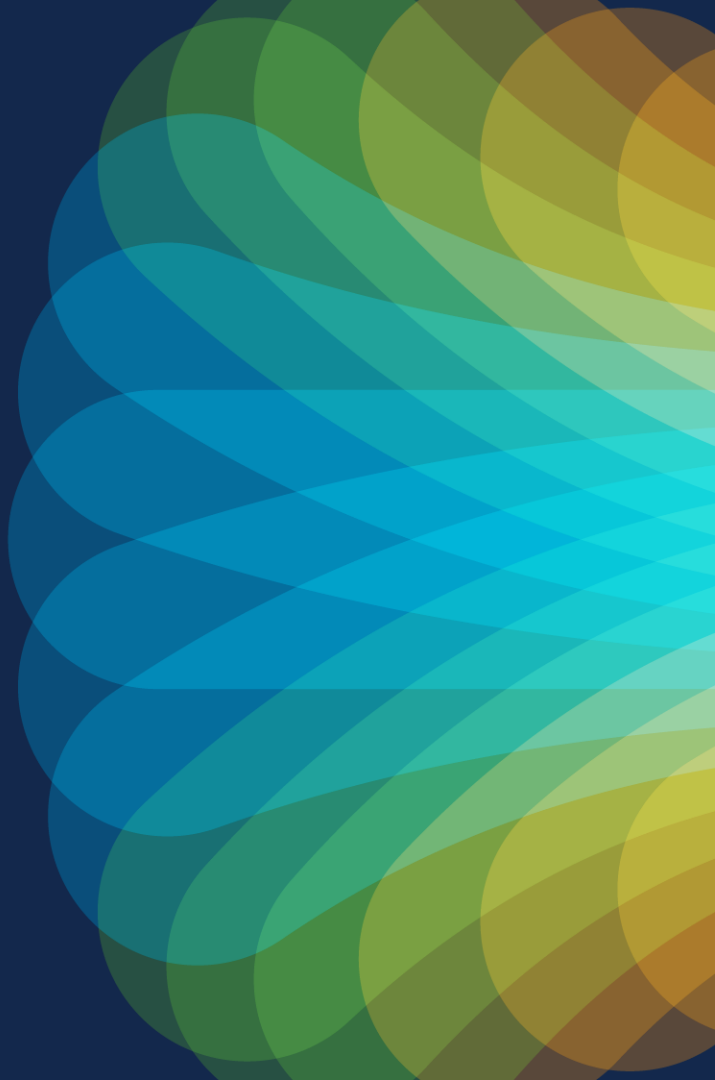
WalkMe- Guided Conceptual Assistance

Enhancements & Warnings



The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go