
cisco Live!
ALL IN

The bridge to possible

Troubleshoot Catalyst 9800 Wireless Controller

Sudha Katgeri, Technical Leader, CX- Wireless
@sudhakatgeri
BRKEWN-3628

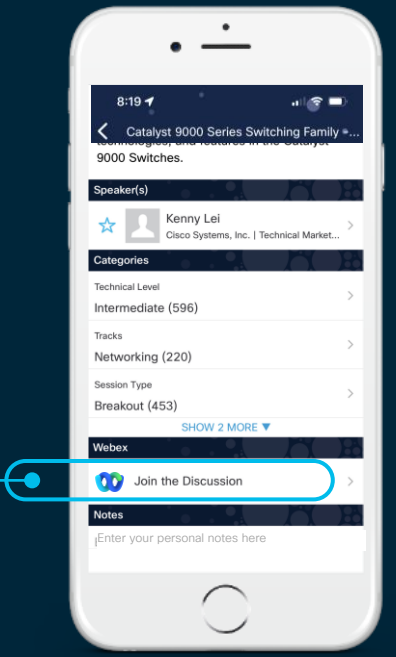
Cisco Webex App

Questions?

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

How

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



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

Webex spaces will be moderated by the speaker until June 17, 2022.

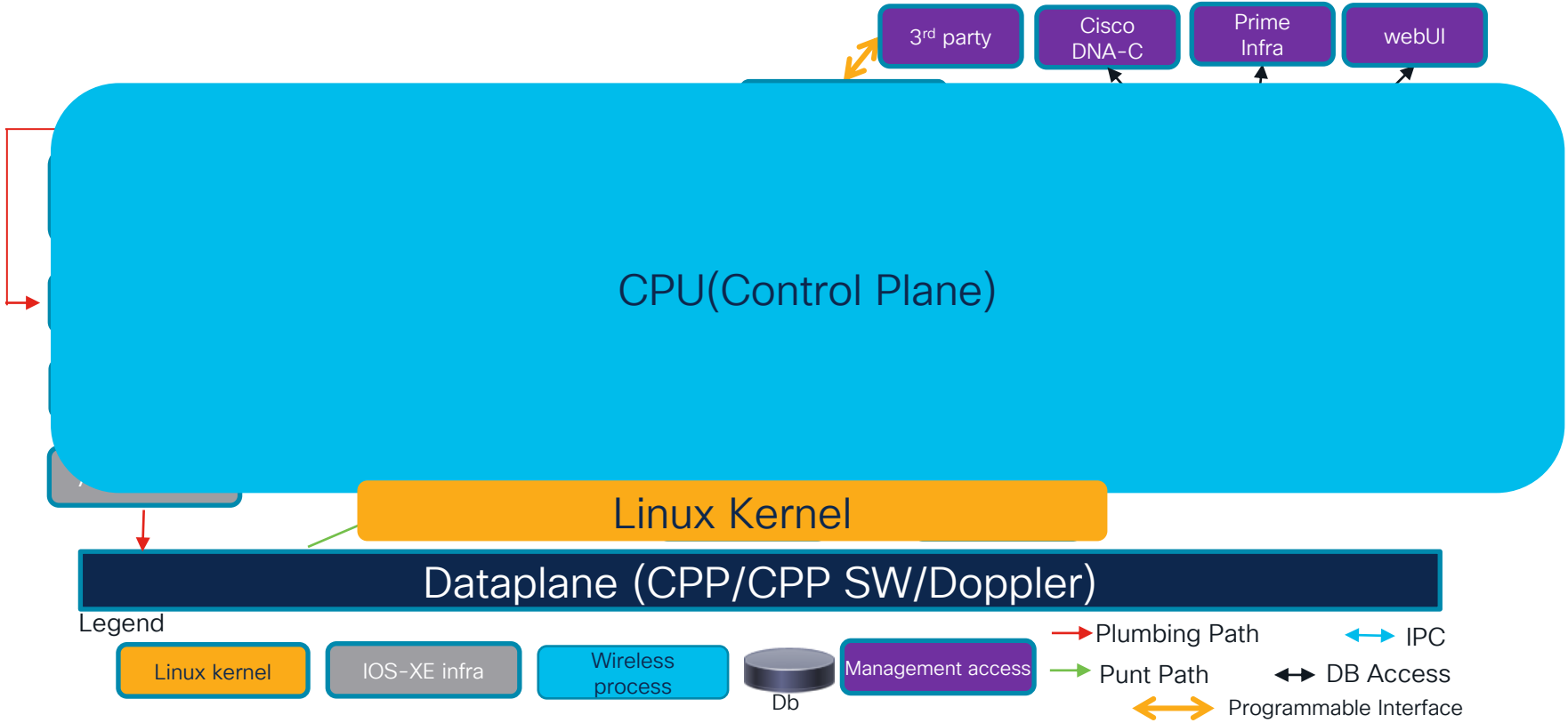
Agenda

- C9800 Software Architecture and On-box Troubleshooting Tools
- Client Troubleshooting – WLC, AP and Cisco DNA Center view
- AP Troubleshooting – WLC, AP and Cisco DNA Center view
- Conclusion
- Appendix
  - Data Plane Troubleshooting
  - High CPU
  - Memory Leak

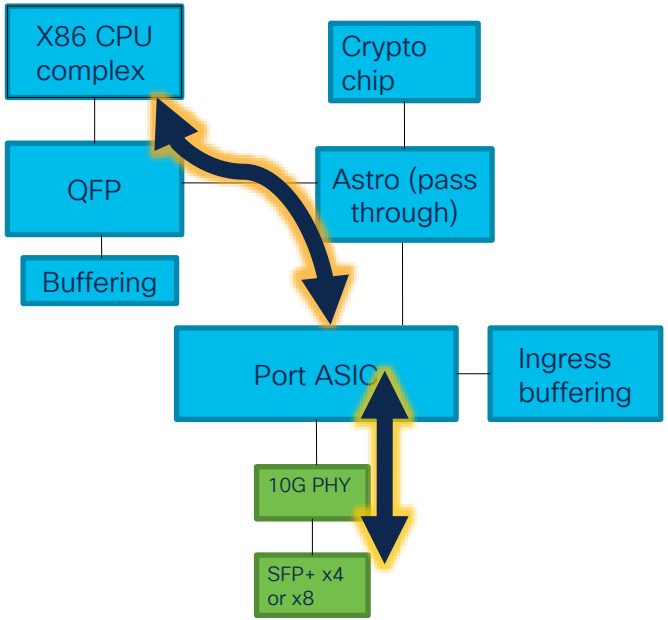
About me – Sudha Katgeri

Wireless CCIE (#45857)

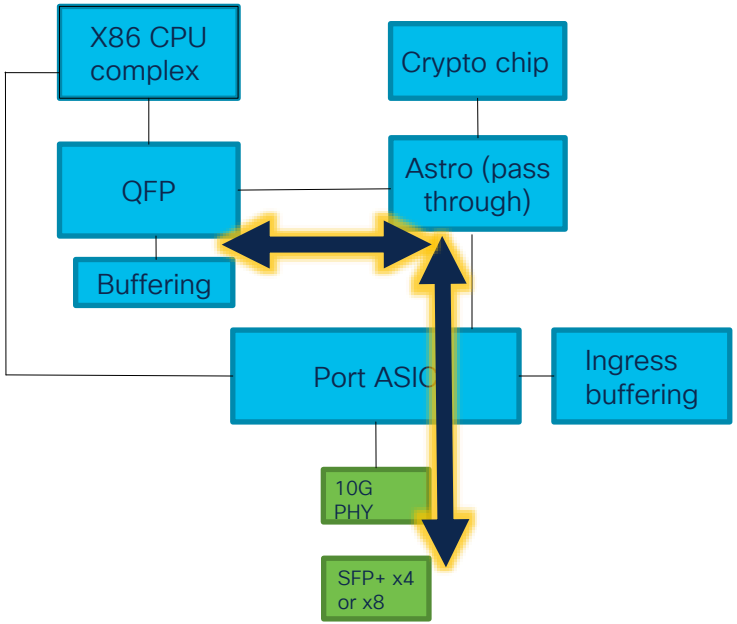
C9800 Software Process Architecture



Life of Packet – Control and Data Plane



Control Plane Packet (Punt/Inject)

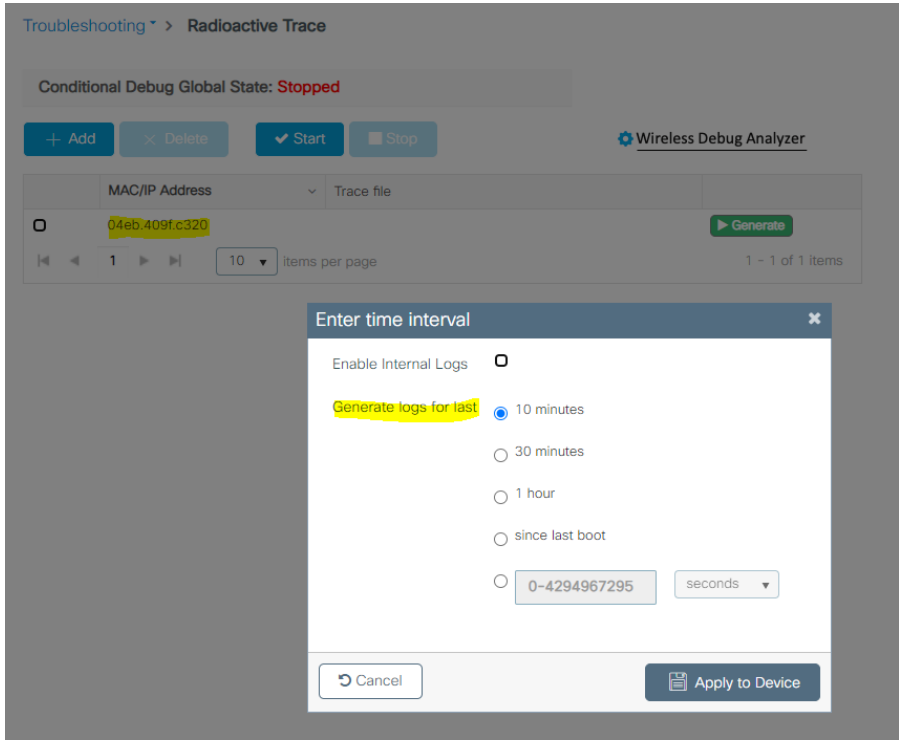


Data Plane Packet

Tracing on C9800

- Traces are written on the C9800 by software processes all the time at NOTICE level. These are the always-on traces
- RadioActive (RA) tracing is the intentional turning up of logging to DEBUG level specific to a condition or context.
- When no condition is available, processes and modules can be configured for debugging.

Always-on Tracing



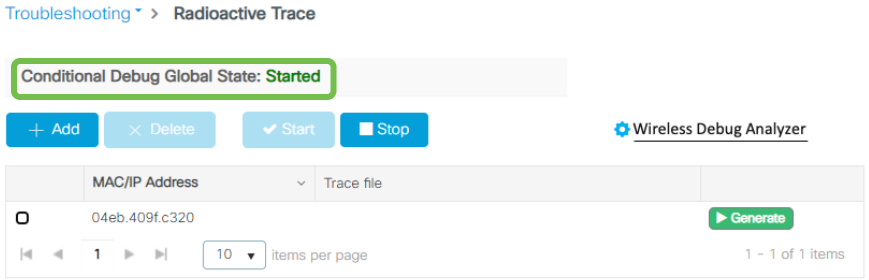
- Always-on traces and show help identify misconfigurations, errors and such
- GUI allows only conditional always-on traces
- CLI more robust

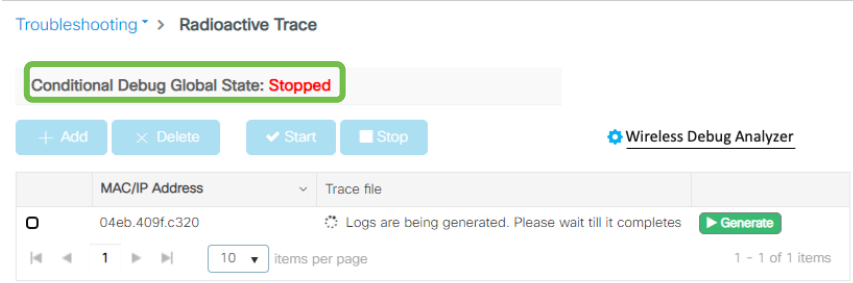
  show logging profile wireless to-file <>

  OR

  show logging process wncd
- By default, always-on traces from last 10 minutes are collected.
- You can choose duration over which to generate

RadioActive (RA) Tracing

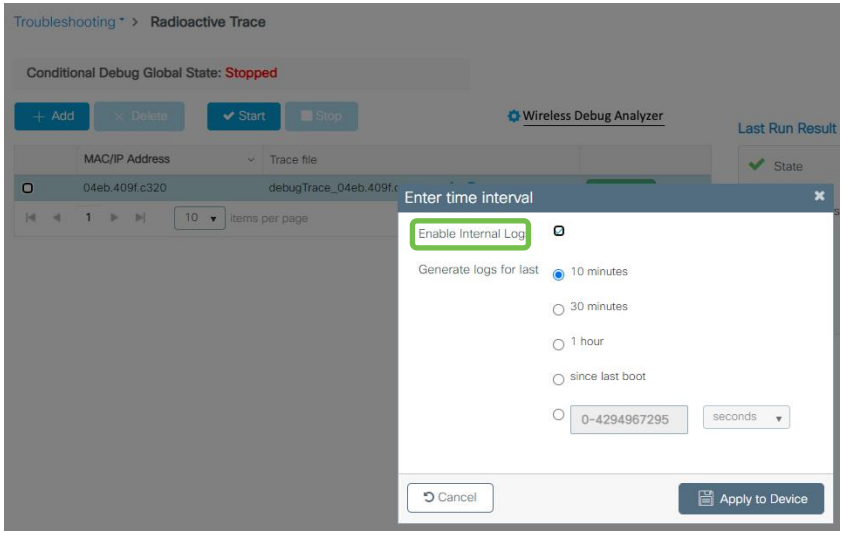




- More detailed logs than always-on
- User has to intentionally enable debug level logs.
- Also called condition debugging as debug is enabled per context
- CLI equivalent

debug wireless {mac | ip}
Reproduce problem
no debug wireless {mac | ip}

RadioActive (RA) Tracing with Internal Flag



- Logs extremely verbose
- Only need to collect TAC and BU is involved
- When collected in conjunction with RA trace
  - Start/Stop of debugs is not necessary
  - Problem need to be reproduced again

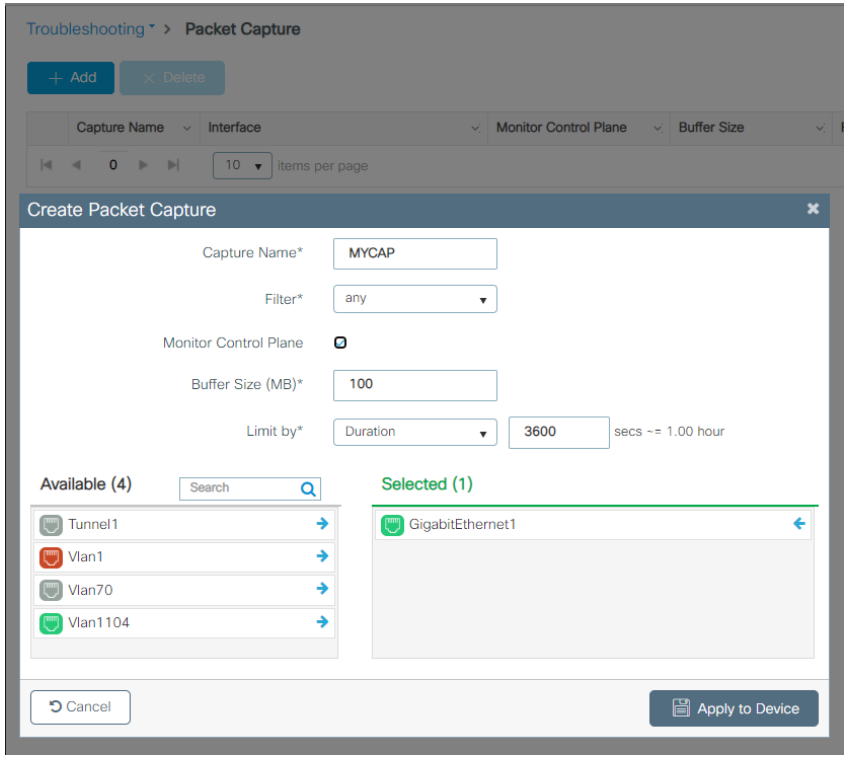
Unconditional Per-Process debugging

- Enable set platform software trace <rrm-mgrd | nginx | nmspd> chassis active R0 all debug

(reproduce issue)

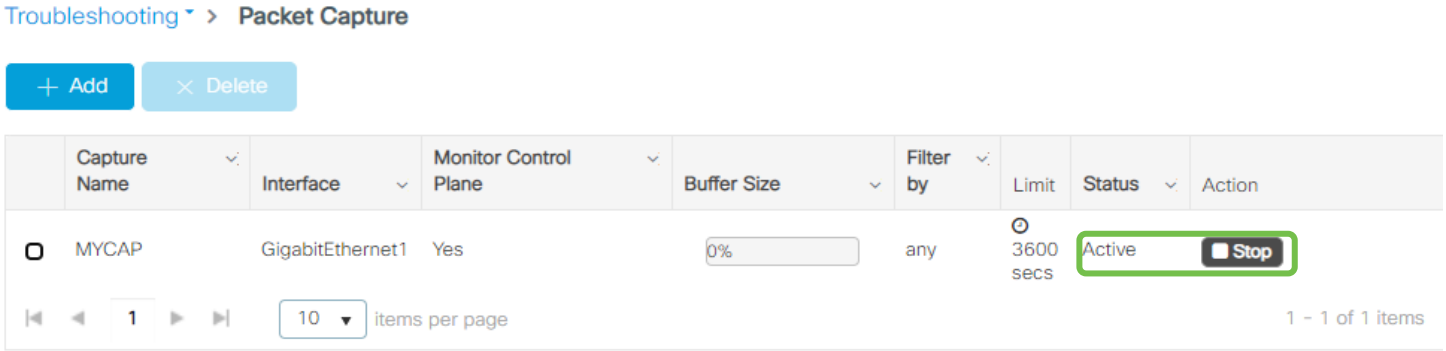
- Collect show logging process <rrm-mgrd | nginx | nmspd> to-file <FILENAME.txt>
- View more bootflash:FILENAME.txt
- Export copy bootflash:FILENAME.txt {tftp:, ftp:, http:, https:, scp:}
- Disable traces undebug all OR set platform software trace <> chassis active R0 all notice

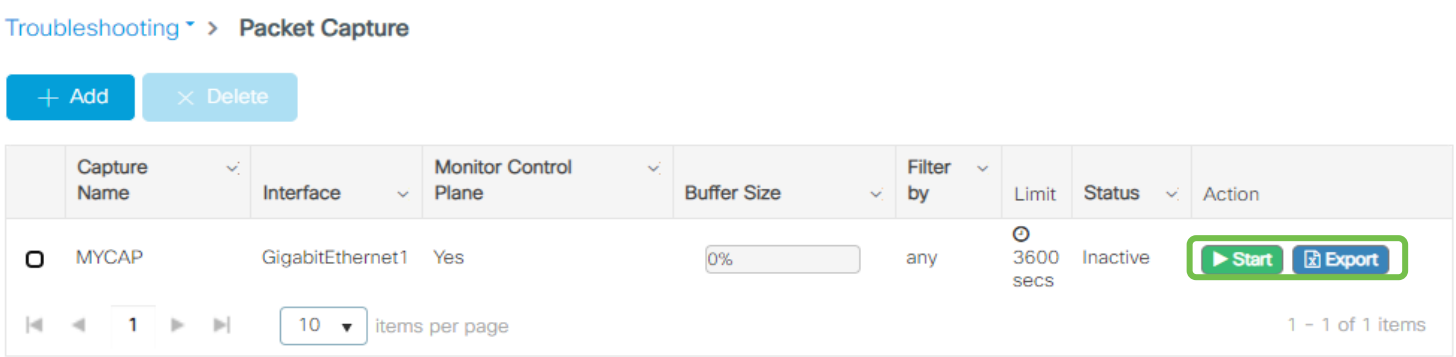
Embedded Packet Capture (EPC)



- Capture traffic from and to the C9800.
- Can be used to capture data traffic or control traffic or both
- Limited buffer = 100 MB (max)
- GUI incrementing adding filters already available in CLI

Embedded Packet Capture (EPC)

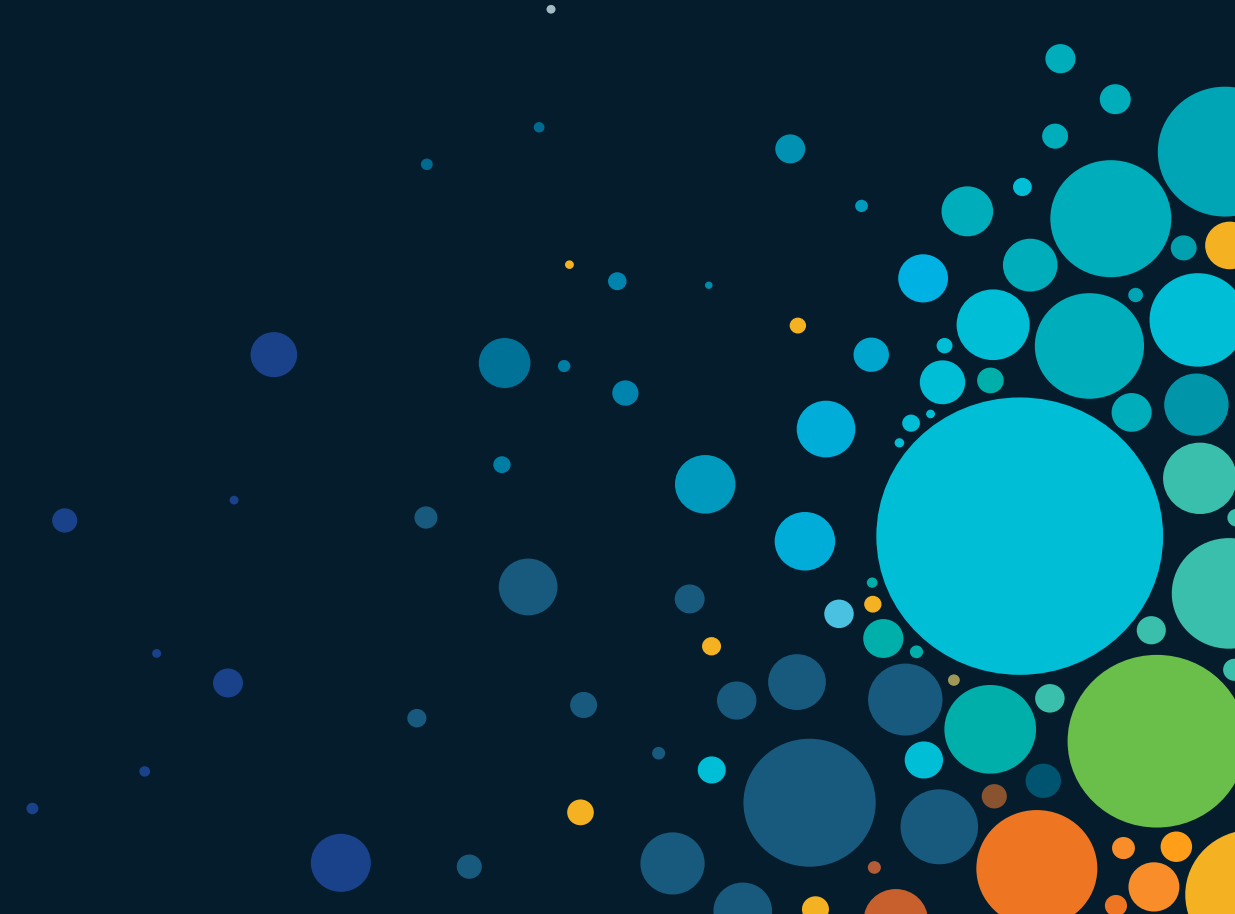




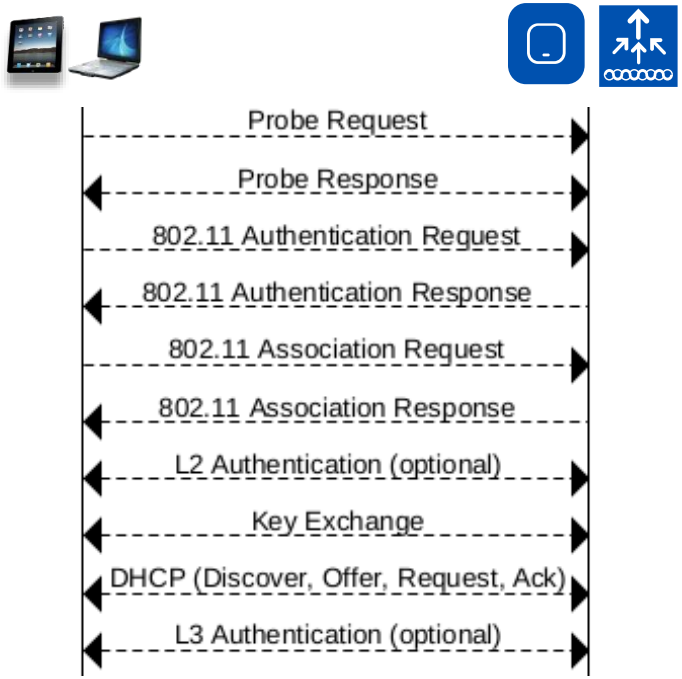
Embedded Packet Capture (EPC) CLI

```
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
```

Client Onboarding



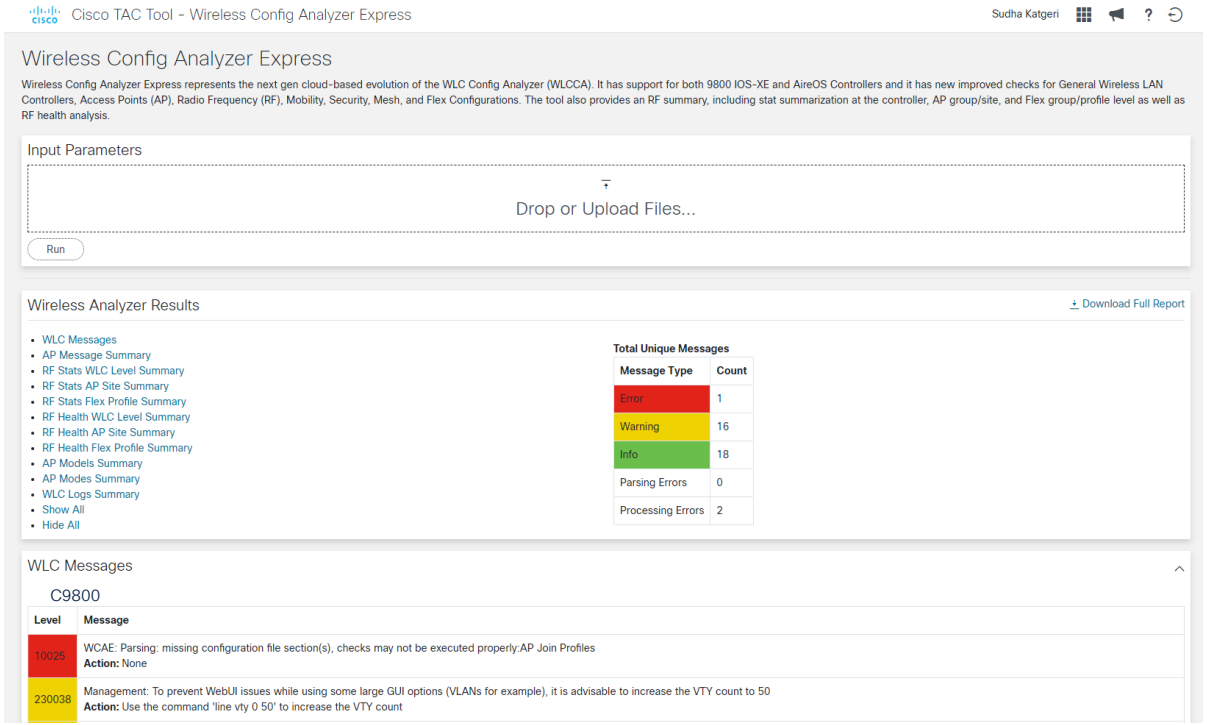
Client Onboarding



Wireless client cannot connect

- Client with mac address <MAC1> is not able to join the wireless network
- Clients dropped from the wireless network earlier today at 10AM and recovered
- Some clients fail to connect after a failover

Understand the environment




```
#show tech-support

#show tech-support
wireless
```

Off-box Tool:

[Wireless Config Analyzer Express]

On-box Tool:

```
#wireless config validate

#show log
```

Client State Verification

show wireless client mac-address <CLIENT_MAC> detailed

```
Client MAC Address : <CLIENT_MAC>
Client MAC Type : Locally Administered Address
Client DUID: NA
Client IPv4 Address : <CLIENT_IPv4>
Client IPv6 Addresses : <CLIENT_IPV6>
Client Username: N/A
AP MAC Address : <AP_RADIO_MAC>
AP Name: 9120
AP slot : 1
Client State : Associated
Policy Profile : ppcentral150
Flex Profile : N/A
Wireless LAN Id: 11
WLAN Profile Name: 9800psk
Wireless LAN Network Name (SSID): 9800psk
BSSID : <AP_BSSID>
Connected For : 71 seconds
Protocol : 802.11ax - 5 GHz
Channel : 100
Client IIF-ID : 0xa0000001
Association Id : 1
…
```

```
Mobility:
  Move Count                    : 0
  Mobility Role                 : Local
  Mobility Roam Type            : None
  Mobility Complete Timestamp   : 06/06/2022 08:59:36
Central
Client Join Time:
  Join Time Of Client : 06/06/2022 08:59:36 Central
…
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 71 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : FT-PSK
…
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : 150
Multicast VLAN : 0
…
```

Client State Verification

show wireless client mac-address <CLIENT_MAC> detailed

```
Session Manager:
…
  Resultant Policies:
          VLAN Name        : VLAN0150
          VLAN             : 150
          Absolute-Timer   : 1800

…
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
Client Statistics:
  Number of Bytes Received from Client : 0
  Number of Bytes Sent to Client : 0
  Number of Packets Received from Client : 0
  Number of Packets Sent to Client : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -61 dBm
  Signal to Noise Ratio : 35 dB
```

Always On: Successful Client Connection

show log profile wireless start last 10 minutes filter mac <CLIENT_MAC> to-file <FILENAME>.txt

```
[client-orch-sm] [23510]: (note): MAC: c23f.ba14.984a  Association received. BSSID c064.e423.c64d, WLAN 9800psk, Slot 1 AP
c064.e423.c640, 9120
[client-orch-state] [23510]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
[dot11] [23510]: (note): MAC: f0c1.f10b.8ac1  Association success. AID 1, Roaming = False, WGB = False, 11r = True, 11w = False
Fast roam = False
[client-orch-state] [23510]: (note): MAC: c23f.ba14.984a Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
[client-auth] [23510]: (note): MAC: c23f.ba14.984a  L2 Authentication initiated. method PSK, Policy VLAN 150, AAA override = 0,
NAC = 0
[ewlc-infra-evq] [23510]: (note): Authentication Success. Resolved Policy bitmap:11 for client c23f.ba14.984a
[client-auth] [23510]: (note): MAC: c23f.ba14.984a ADD MOBILE sent. Client state flags: 0x71  BSSID: MAC: c064.e423.c64d capwap
IFID: 0x90000004, Add mobiles sent: 1
[client-keymgmt] [23510]: (note): MAC: c23f.ba14.984a EAP Key management successful. AKM:FT-PSK Cipher:CCMP WPA Version:WPA2
[client-auth] [23510]: (note): MAC: c23f.ba14.984a  L2 PSK Authentication Success. EAP type: NA, Resolved VLAN: 150, Audit
Session id: 000000000000000B383DB2FF
[client-orch-sm] [23510]: (note): MAC: c23f.ba14.984a  Mobility discovery triggered. Client mode: Local
[client-orch-state] [23510]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_L2_AUTH_IN_PROGRESS ->
S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
[mm-client] [23510]: (note): MAC: c23f.ba14.984a Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client
IFID: 0xa0000001, Client Role: Local PoA: 0x90000004 PoP: 0x0
[client-auth] [23510]: (note): MAC: c23f.ba14.984a  ADD MOBILE sent. Client state flags: 0x72  BSSID: MAC: c064.e423.c64d capwap
IFID: 0x90000004, Add mobiles sent: 1
[client-orch-state] [23510]: (note): MAC: c23f.ba14.984a Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS ->
S_CO_DPATH_PLUMB_IN_PROGRESS
[dot11] [23510]: (note): MAC: c23f.ba14.984a  Client datapath entry params - ssid:9800psk,slot_id:1 bssid ifid: 0x0, radio_ifid:
0x90000002, wlan_ifid: 0xf040000b
[dpath_svc] [23510]: (note): MAC: c23f.ba14.984a Client datapath entry created for ifid 0xa0000001
[client-orch-state] [23510]: (note): MAC: c23f.ba14.984a Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS ->
S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [23510]: (note): MAC: c23f.ba14.984a Client IP learn successful. Method: DHCP IP: 10.150.1.11
[client-orch-state] [23510]: (note): MAC: c23f.ba14.984a Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

Always On: Failed Client Connection

show log profile wireless start last 10 minutes filter mac <CLIENT_MAC> to-file <FILENAME>.txt

```
[client-orch-sm] [23554]: (note): MAC: c23f.ba14.984a  Association received. BSSID c064.e423.c64d, WLAN 9800psk, Slot 1 AP
c064.e423.c640, 9120
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
[dot11] [23554]: (note): MAC: c23f.ba14.984a  Association success. AID 1, Roaming = False, WGB = False, 11r = True, 11w = False Fast
roam = False
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
[client-auth] [23554]: (note): MAC: c23f.ba14.984a  L2 Authentication initiated. method PSK, Policy VLAN 150, AAA override = 0, NAC =
0
[ewlc-infra-evq] [23554]: (note): Authentication Success. Resolved Policy bitmap:11 for client c23f.ba14.984a
[client-auth] [23554]: (note): MAC: c23f.ba14.984a  ADD MOBILE sent. Client state flags: 0x71  BSSID: MAC: c064.e423.c64d capwap
IFID: 0x90000004, Add mobiles sent: 1
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol key m2. 11r MIC validation failed
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol key m2. 11r MIC validation failed
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol key m2. 11r MIC validation failed
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to eapol key m1 retransmit failure. Max retries for M1 over
[client-orch-sm] [23554]: (note): MAC: c23f.ba14.984a  Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_EXCLUDE_WRONG_PSK,
details: , 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|15|1e|27|
[client-orch-sm] [23554]: (note): MAC: c23f.ba14.984a  Delete mobile payload sent for BSSID: c064.e423.c64d WTP mac: c064.e423.c640
slot id: 1
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_L2_AUTH_IN_PROGRESS ->
S_CO_DELETE_IN_PROGRESS
[errmsg] [23060]: (note): %CLIENT_EXCLUSION_SERVER-5-ADD_TO_EXCLUSIONLIST_REASON_DYNAMIC: R0/0: wncmgrd: Client MAC: c23f.ba14.984a
was added to exclusion list associated with AP Name:9120, BSSID:MAC: c064.e423.c64d, reason:Wrong PSK
[sanet-shim-translate] [23554]: (note): MAC: c23f.ba14.984a  Session manager disconnect event called, session label: 0x2b000002
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_DELETE_IN_PROGRESS -> S_CO_DELETED
```

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|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|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|01|07|
13|1a|23|
```

Wireless client cannot connect

- Client with mac address <MAC1> is not able to join the wireless network
- Clients dropped from the wireless network earlier today at 10AM and recovered
- Some clients fail to connect after a failover

Archive Trace and Live Core

- show logging profile wireless start last <> to-file bootflash:
  - request platform software trace archive target {harddisk: | bootflash:} <FILENAME>

- Live Core requires service internal to be enabled
  - Request platform software process <PROCESS_NAME>

Archive Trace Analysis – Onboarding Overview

Using Cisco internal Tools and Scripts

Events	Total	wncd_0	wncd_1	wncd_2	wncd_3	wncd_4	wncd_5	wncd_6	wncd_7
INCOMING_CLIENTS	268759	810	0	0	0	148965	82879	0	36105
OUTGOING_CLIENTS	13646	6	0	0	0	7239	4162	0	2239
ASSOCS_FRESH	18798	231	0	0	0	8288	8069	0	2210
INTRA_WNCD	131937	558	0	0	0	59559	45717	0	26103
INTER_WNCD	12268	5	0	0	0	6493	3930	0	1840
INTER_WLC	0	0	0	0	0	0	0	0	0
ASSOCS_FASTROAM	0	0	0	0	0	0	0	0	0
ASSOCS_ROAM	101117	434	0	0	0	45350	36990	0	18343
ASSOCS_DEL	88396	252	0	0	0	65441	17835	0	4868
AP_JOIN	62	0	0	0	0	36	26	0	0
AP_DISJOIN	6	0	0	0	0	6	0	0	0
APS_DISTRI	967	7	0	0	0	432	334	0	194

Archive Trace Analysis– Client Association Failures

Using Cisco internal Tools and Scripts

- During the problem incident, several clients fail to associate
- Need to identify client delete reasons

ASSOCS_DEL

	Total	0_min	1	2	3	4	5	6
0:00	26433	522	86	226	258	128	329	679
1:00	28186	1248	1224	4607	1931	2504	1940	904
2:00	16740	317	285	547	452	170	78	63
3:00	12804	185	18	74	80	689	684	758
4:00	4233	791	599	360	97	145	590	425

Archive Trace Analysis by Cisco - Client Delete Reasons

Using Cisco Internal Tools and Captures

- MN_REASSOC_TIMEOUT
  - Clients are unable to (re)associate
  - This is sometimes referred to, as thrashing behavior => clients keeps trying to associate to same AP over and over again
- DOT11_MAX_STA
  - Indicates AP is already servicing maximum allowed on the radio slot

wncd0	wncd1	wncd2	wncd3	wncd4	wncd5	wncd6	wncd7
				1871	2559		177

wncd_4	Count
CAPWAP_DOWN,	108
DOT11_MAX_STA,	129
EXCLUDE_ACL_FAIL,	2
FT_AUTH_RESPONSE,	9
INTER_WNCD_ROAM_SUCCESS,	385
MN_IDLE_TIMEOUT,	9
MN_REASSOC_TIMEOUT,	1119
MOBILITY_FAILURE,	64
REMOTE_MOBILITY_DELETE,	3
SANET,	4
WLAN_CHANGE,	37
wncd_5	**Count**
CAPWAP_DOWN,	116
DOT11_MAX_STA,	748
DPATH_FAILURE,	9
INTER_WNCD_ROAM_SUCCESS,	285
MN_IDLE_TIMEOUT,	4
MN_REASSOC_TIMEOUT,	1314
MOBILITY_FAILURE,	56
REMOTE_MOBILITY_DELETE,	2
SANET,	6
WLAN_CHANGE,	16

Client Delete Reasons

- show wireless stats client detail

or

- show wireless stats client delete reasons
- Delete reasons categorized by whether WLC, AP or client initiated delete.
- Also, informational deletes that can be ignored are explicitly listed

Client Statistics – Control Plane

For Your Reference

show wireless stats client detail

```
Total Number of Clients : 4
Protocol Statistics
---------------------------------------------
Protocol                      Client Count
802.11b                          0
802.11g                          0
802.11a                          0
802.11n-2.4 GHz                  0
802.11n-5 GHz                    0
802.11ac                         4
802.11ax-5 GHz                   0
802.11ax-2.4 GHz                 0
802.11ax-6 GHz                   0

Current client state statistics:
---------------------------------------------
  Authenticating          : 0
  Mobility                : 0
  IP Learn                : 0
  Webauth Pending         : 0
  Run                     : 0
  Delete-in-Progress      : 0
```

```
Client Summary
---------------------------------------
Current Clients   : 4
Excluded Clients  : 1
Disabled Clients  : 0
Foreign Clients   : 0
Anchor Clients    : 0
Local Clients     : 4
Idle Clients     : 0
Locally Administered MAC Clients: 0
```

- Total clients connected
- Per Protocol distribution
- State Distribution

Easy to spot network wide problems

Client Statistics – Control Plane

For Your Reference

show wireless stats client detail

```
client global statistics:
-------------------------------------------------------------
Total association requests received                : 22280
Total association attempts                         : 21381
Total FT/LocalAuth requests                        : 0
Total association failures                         : 1
…
Total AID allocation failures                      : 0
Total AID free failures                            : 0
Total roam attempts                                : 13435
  Total CCKM roam attempts                         : 0
  Total 11r roam attempts                          : 5454
…
Total add mobiles sent                             : 33024
Total delete mobiles sent                          : 16664
…
Total key exchange attempts                        : 7414
Total broadcast key exchange attempts              : 14298
Total broadcast key exchange failures              : 0
Total eapol key sent                               : 35720
Total eapol key received                           : 27565
…
```

- 98 different stats counters
- Easy to spot
  - Frequent Bcast rotation issues
  - Frequent L2/L3 auth failures
  - Frequent IP address learning failures
- Roaming types

Client Statistics – Control Plane

show wireless stats client detail

For Your Reference

```
client state statistics:
------------------------------------------------------------
Average Time in Each State (ms)
  Associated State    : 0
  L2 State       : 85
  Mobility State : 2
  IP Learn State : 2117
  L3 Auth State   : 0

Average Run State Latency (ms) : 1102

Average Run State Latency without user delay (ms) : 1061

Latency Distribution (ms)
  1 - 100     : 278025
  100 - 200   : 11511
  200 - 300   : 5590
  300 - 600   : 3519
  600 - 1000 : 6546
  1000+       : 41184
```

- Average time per state
- Spotting performance problems
- Variations over time

Client Statistics – Control Plane

For Your Reference

show wireless stats client detail

```
Webauth HTTP Statistics
-----------------------
  Intercepted HTTP requests    : 0
  IO Read events               : 0
  Received HTTP messages       : 0
…
Time spent in each httpd states (in msecs)
                              Total       Max         Min         Samples
-------------------------------------------------------------------------
IO Reading state                 0          0           0           0
IO Writing state                 0          0           0           0
IO AAA state                     0          0           0           0
Method after reading             0          0           0           0
…
Webauth HTTP status counts
--------------------------
 HTTP 200 OK                    : 0
 HTTP 201 Created               : 0
 HTTP 202 Accepted              : 0
 HTTP 203 Provisional Info      : 0
```

- Webauth HTTP statistics
- Webauth HTTP Response Codes

Client Statistics – Control Plane

For Your Reference

show wireless stats client detail

```
Webauth backpressure queue counters
-----------------------------------
Pending SSL handshakes             : 0
Pending HTTPS new requests         : 0
Pending AAA replies                : 0

Dot1x Global Statistics
-----------------------
RxStart = 97 RxLogoff = 0  RxResp = 1095 RxRespID = 282
RxReq = 0 RxInvalid = 0  RxLenErr = 0
RxTotal = 1486
TxStart = 0 TxLogoff = 0  TxResp = 0
TxReq = 1679 ReTxReq = 362  ReTxReqFail = 64
TxReqID = 643 ReTxReqID = 228  ReTxReqIDFail = 3
TxTotal = 2322
```

- WebAuth Queue full issues
- SSL session Exhaustion
- Dot1x Statistics

Client Statistics – Control Plane

show wireless stats client detail

```
Total client delete reasons
---------------------------
Controller deletes
---------------------------
No Operation                              : 0
Unknown                                   : 0
Session Manager                           : 0
Connection timeout                        : 0
Datapath plumb                            : 0
….
----------------------------
Informational Delete Reason
----------------------------
Mobility WLAN down                        : 0
AP upgrade                                : 0
L3 authentication failure                 : 0
AP down/disjoin                           : 0
MAC authentication failure                : 0
.....
```

- Client Delete Reasons categorized by
  - Controller initiated deletes
  - Information deletes

Client Statistics – Control Plane

For Your Reference

```
-----------------------------
Client initiate delete
-----------------------------
Deauthentication or disassociation request                    : 0
Client DHCP                                                        : 0
Client EAP timeout                                                 : 0
Client 8021x failure                                               : 0
Client device idle                                                 : 0
Client captive portal security failure                             : 0
…
-----------------------------
AP Deletes
-----------------------------
AP initiated delete when client is sending disassociation      : 0
AP initiated delete for idle timeout                           : 0
AP initiated delete for client ACL mismatch                    : 0
AP initiated delete for AP auth stop                           : 0
AP initiated delete for association expired at AP              : 0
AP initiated delete for 4-way handshake failed                 : 0
```

- Client Initiated Deletes
- AP Deletes

Wireless client cannot connect

- Client with mac address <MAC1> is not able to join the wireless network
- Clients dropped from the wireless network earlier today at 10AM and recovered
- Some clients fail to connect after a failover

Client State Across Components

show tech-support wireless client mac <CLIENT_MAC>

- WNCd View
  - show wireless client summary

```
Number of Clients: 12091

MAC Address    AP Name          Type  ID   State        Protocol    Method     Role
-------------------------------------------------------------------------------------
4ab9.6dfc.bb83 AP-NAME-AP1           WLAN   2    Run           11ac       None      Local
```

- FMAN-RP View
  - show platform software wireless-client chassis active/standby R0

```
 ID  MAC Address      WLAN  Client State
-------------------------------------------------
0xa0002a95  4ab9.6dfc.bb83      2  Run
```

Client State Across Components

show tech-support wireless client mac <CLIENT_MAC>

- FMAN-FP View
  - show platform software wireless-client chassis active/standby F0

```
 ID  MAC Address      WLAN  Client State           AOM ID  Status
------------------------------------------------------------------------
0xa0002a95  4ab9.6dfc.bb83      2  Run                    377818  Done
```

- CPP-Client View
  - show platform hardware chassis active/standby R0 feature wireless wlclient cpp-client summary

```
CPP IF_H     DPIDX      MAC Address    VLAN  CT  MCVL  AS  MS  E          WLAN          POA
-------------------------------------------------------------------------------------------
 0X4474    0XA0002A95   4ab9.6dfc.bb83  20   RG    0   RN  LC  N        SSID-1       0x90c00430
```

Client State Across Components

show tech-support wireless client mac <CLIENT_MAC>

- Dataplane View
  - show platform hardware chassis active/standby qfp feature wireless wlclient datapath summary

```
Vlan   pal_if_hdl   mac            Input Uidb Output Uidb
------ ------------ -------------- ---------- -----------
20     0xa0002a95   4ab9.6dfc.bb83   244629     244620
```

Client Onboarding – AP View

Troubleshooting on the AP side

Debugs on wave 2 / wifi6 APs

- Syslogs are stored in the flash even after reboot
- It is possible to export debugs to a syslog server
- **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
- **show client access-lists** allows to verify ACL and counters
- Much more at : https://www.cisco.com/c/en/us/support/docs/wireless/aironet-2800-series-access-points/214560-troubleshoot-wave-2-aps.html

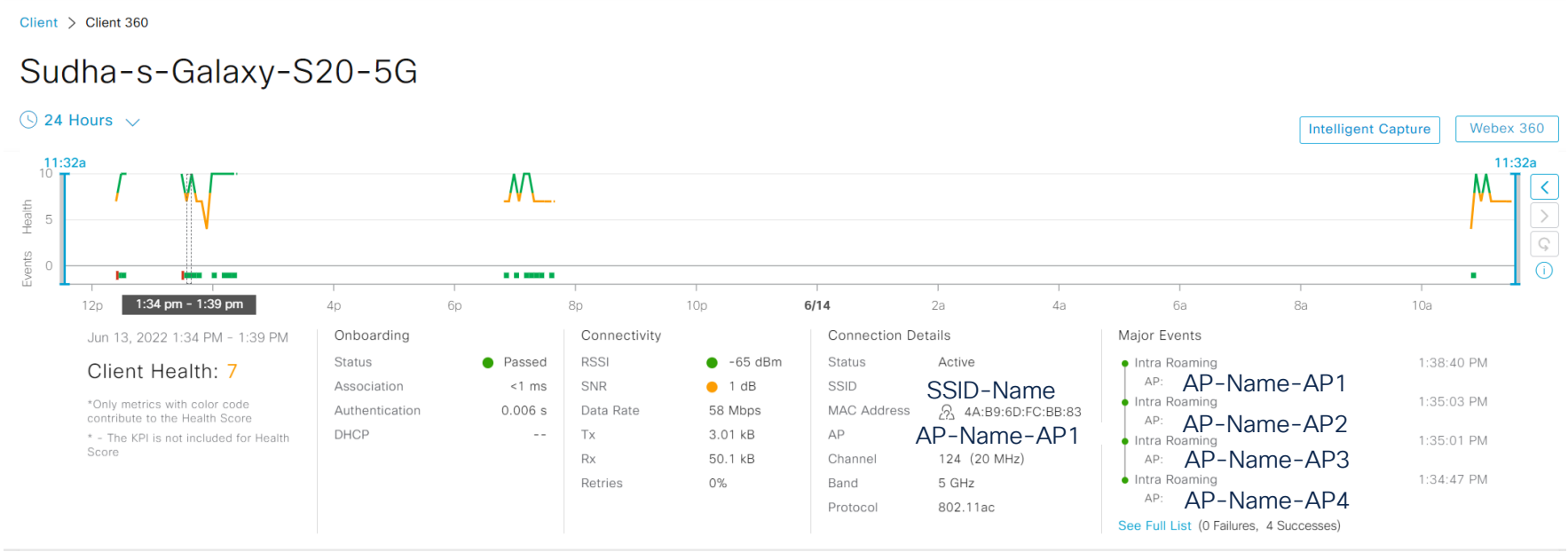
COS AP Client Trace – Successful Client Connection

```
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:                                <apr1v0> [D:W] DOT11_AUTHENTICATION : (.)
[*04/06/2022 10:                                <apr1v0> [U:W] DOT11_ASSOC_REQUEST : (.)
[*04/06/2022 10:                                <apr1v0> [D:W] DOT11_ASSOC_RESPONSE : (.)
[*04/06/2022 10:                                <apr1v0> [D:W] EAPOL_KEY.M1 : DescType 0x02 KeyInfo
0x008b
[*04/06/2022 10:                                <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 : (.)
```

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

Client Connectivity – Cisco DNA Center view

Client 360 View



Intelligent capture

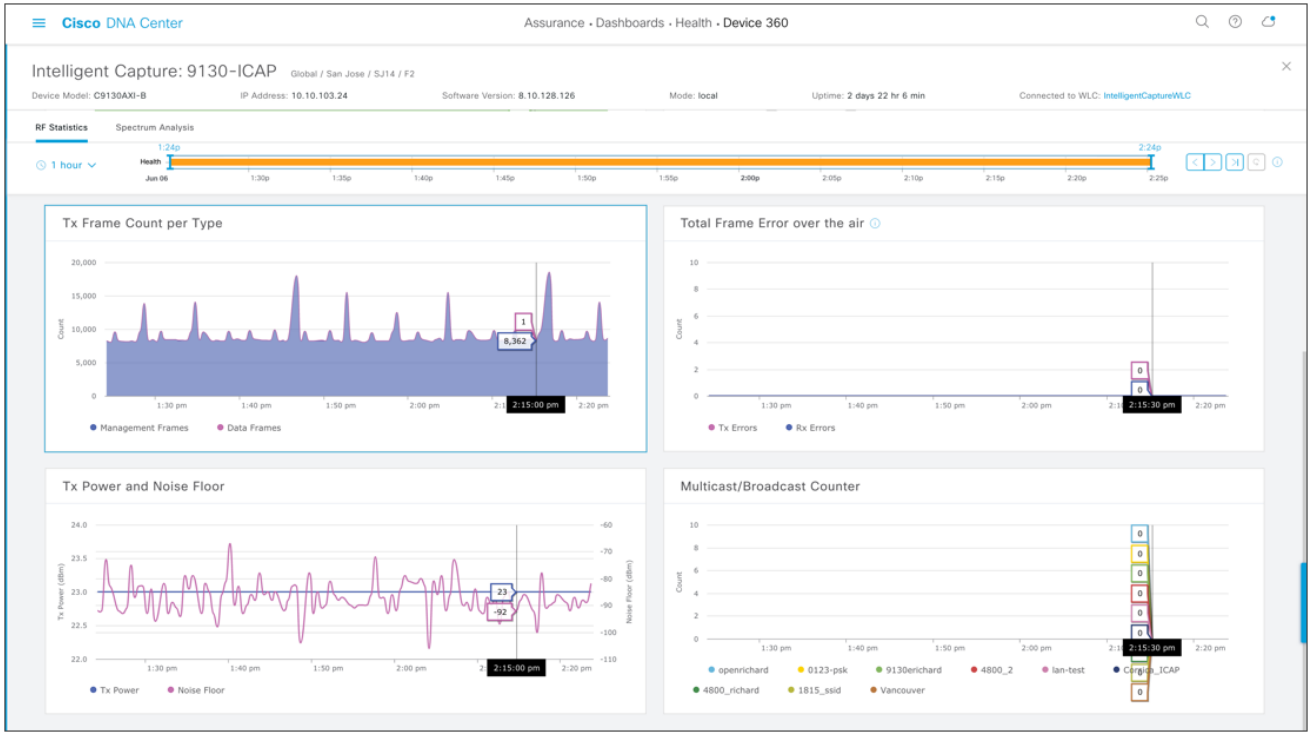
Client intelligent capture

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

Intelligent capture

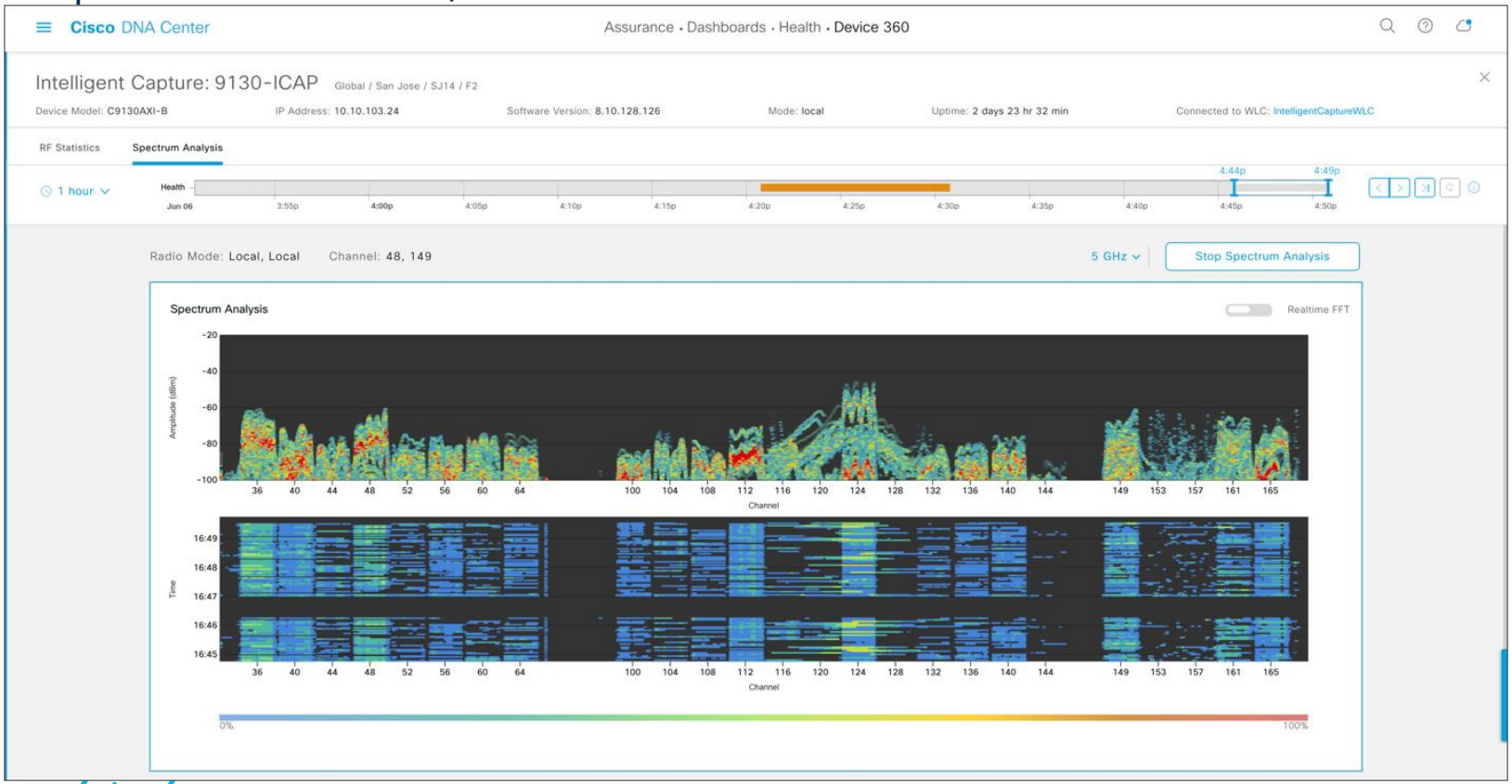
Cisco DNA Center RF stats

RF stats can be enabled globally or on specific APs



Intelligent capture

The power of Cleanair / RF Asic



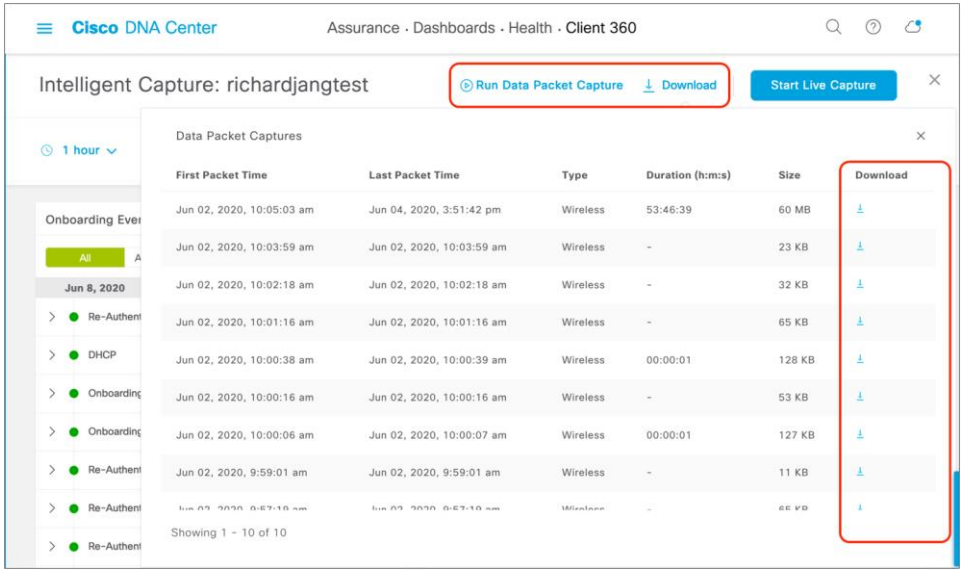
Intelligent capture

Client intelligent capture

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

Intelligent capture

Client intelligent capture

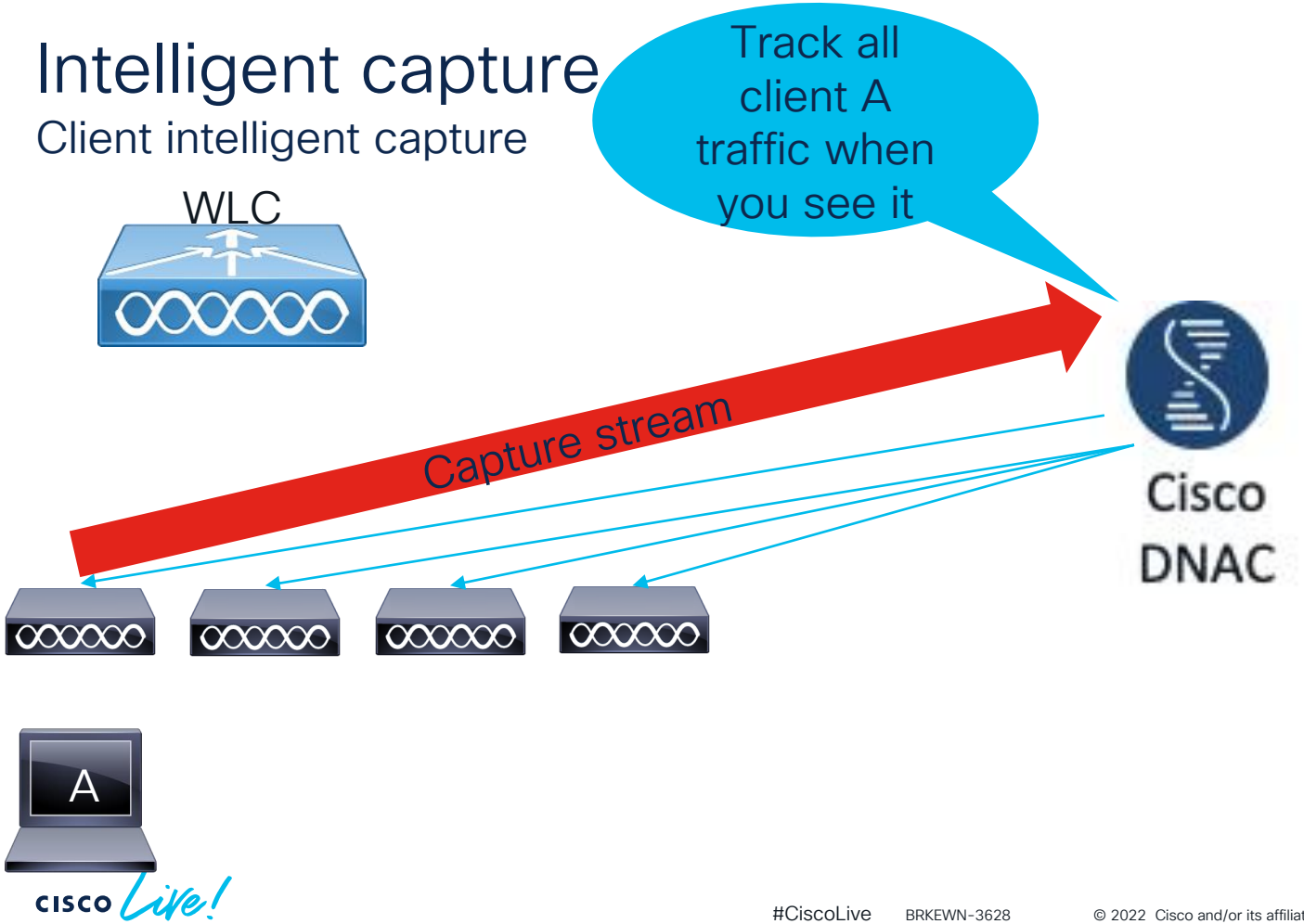


Data packet capture supported on 4800 and 9130

Live Capture (onboarding) on all other AP models

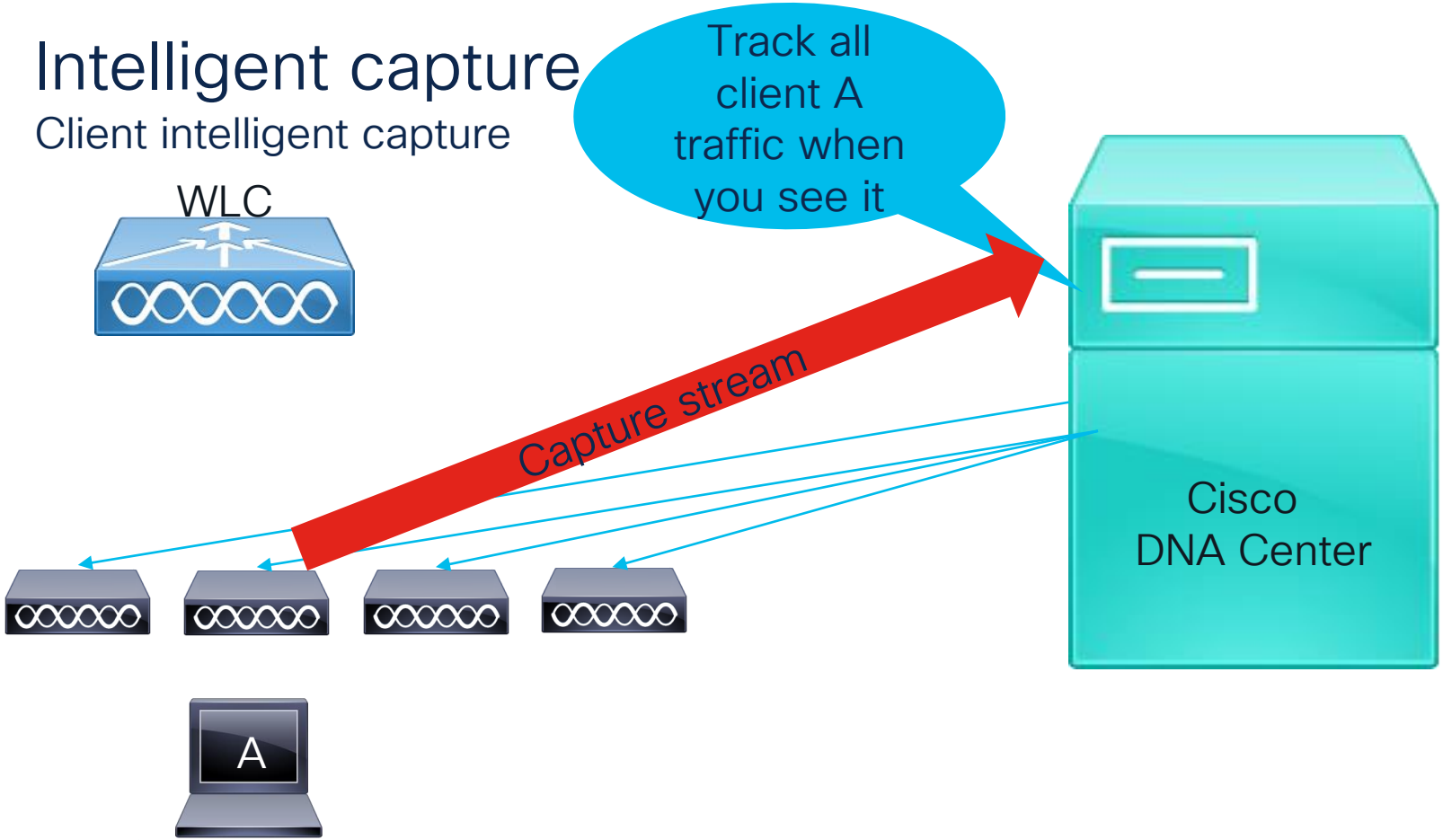
Intelligent capture

Client intelligent capture



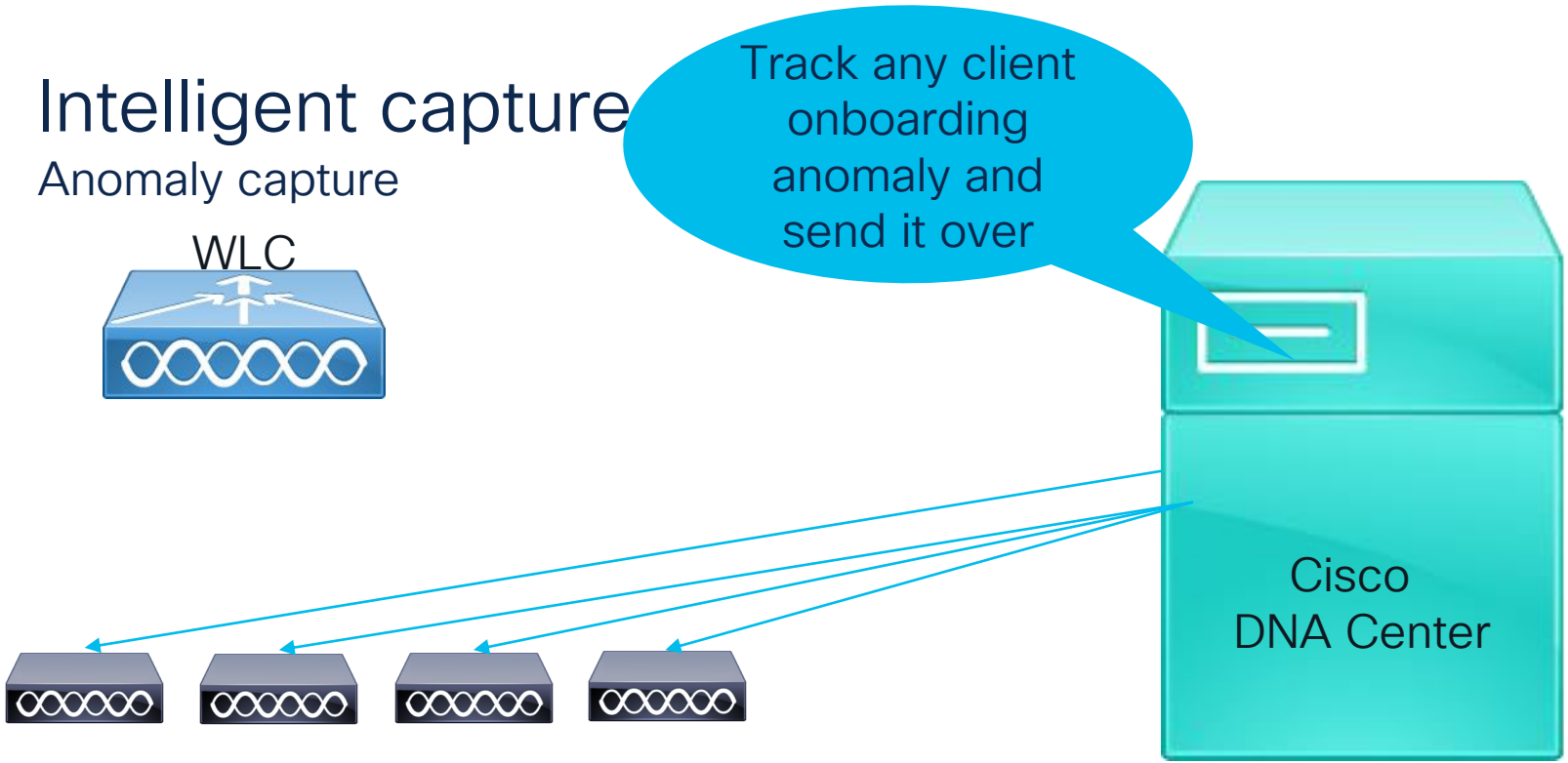
Intelligent capture

Client intelligent capture



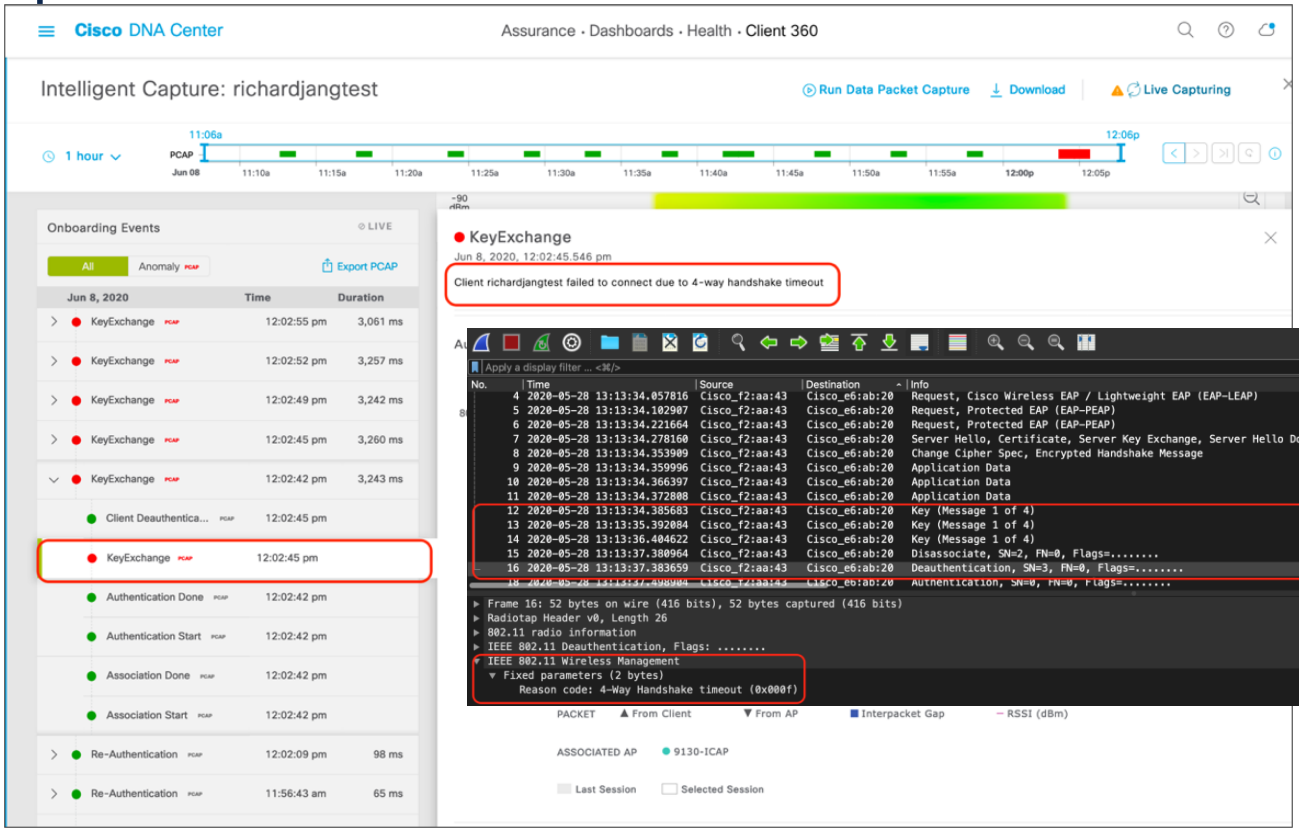
Intelligent capture

Anomaly capture



Intelligent capture

Anomaly capture



AP Join/AP Flap

AP cannot join the WLC

- AP with radio mac <AP_radiomac1> and AP ethernet mac <AP_ethermac1> is not able to join the wireless network
- All or a handful of APs dropped from the C9800 11 AM and recovered
- AP cannot join post SSO or HA failover

OR

- A replacement AP will not join C9800

AP Not Able to Join WLC – Basics

- Is Layer 3 Connectivity established between AP and Wireless Management Interface (WMI) of C9800?
- How are the APs being primed?
- Are UDP ports 5246 and 5247 allowed along the path from AP to WLC?
- Is the network between AP and WLC is stable and uncongested?

Specific AP is not joining the WLC

- Syslogs from WLC and AP
- Always-on Traces and RadioActive traces from AP
- TechTip: RA trace for AP join requires both radio mac and ethernet mac to be debugged for a wholistic view
- EPC is also a good tool especially if ports blocked along the path are not obvious

AP Join Troubleshooting

For Your Reference

show wireless stats ap discovery

Discovery requests received from total number of APs : 3

AP Radio MAC	AP Ethernet MAC	IP Address	Last Success time	Last failure type	Last failure time
0062.ecaa.de80	0042.68a0.ee78	192.168.26.101	05/28/19 10:00:02	None	NA
00a3.8ec2.da00	002c.c899.b9ac	192.168.25.102	05/28/19 10:00:02	None	NA
cc16.7e30.3980	58ac.78de.891e	192.168.26.102	05/28/19 10:00:09	Non-wireless Mgmt interface	NA

- Single view for all Aps that tried to find the controller

AP cannot join the WLC

- AP with radio mac <AP_radiomac1> and AP ethernet mac <AP_ethermac1> is not able to join the wireless network
- All or a handful of APs dropped from the C9800 11 AM and recovered
- AP cannot join post SSO or HA failover

OR

- A replacement AP will not join C9800

AP Join Troubleshooting

show ap uptime

Number of APs: 3

AP Name	Ethernet MAC	Radio MAC	AP Up Time	Association Up Time
ap3800i-r2-sw1-te0-1	0042.68a0.ee78	0062.ecaa.de80	1 day 0 hour 37 minutes	1 day 0 hour 21
ap2800-r2-sw1-2-0-4	002c.c899.b9ac	00a3.8ec2.da00	1 day 0 hour 38 minutes	5 hour 30
ap3800i-r2-sw1-te0-2	58ac.78de.891e	cc16.7e30.3980	1 day 0 hour 36 minutes	1 day 0 hour 21

AP Join Troubleshooting

Show wireless stats ap join summary

```
Number of APs: 600

Base MAC     Ethernet MAC    AP Name      IP Address    Status  Last Failure Phase   Last Disconnect Reason
-----------------------------------------------------------------------------------------------
RadioMAC1    EthernetMAC1    E1-F2-AP1    10.1.1.244     Joined      Run              Heart beat timer expiry
RadioMAC2    EthernetMAC2    C3-F1-AP3    10.2.1.56      Joined      Run              DTLS close alert from peer
RadioMAC3    EthernetMAC3    C1-F4-AP2    10.1.1.121     Joined      Join             DTLS close alert from peer
RadioMAC4    EthernetMAC4    C5-F2-AP4    10.3.1.235     Joined      Run              DTLS close alert from peer
RadioMAC5    EthernetMAC5    M1-F19-AP1   10.3.1.237     Joined      Run              DTLS close alert from peer
RadioMAC6    EthernetMAC6    P4-F10-AP1   10.3.4.202     Joined      Run              DTLS close alert from peer
RadioMAC7    EthernetMAC7    C3-F1-AP6    10.3.2.158     Joined      Run              DTLS close alert from peer
```

AP Join Troubleshooting

For Your Reference

show wireless dtls connections

AP Name	Local Port	Peer IP	Peer Port	Version	Ciphersuite
APD4E8.8019.49E0	Capwap_Ctrl	170.85.125.43	5250	DTLSv1.0	TLS_NUM_RSA_WITH_AES_128_CBC_SHA
EDU_BR_01_00_01_1852	Capwap_Ctrl	170.85.142.18	5264	DTLSv1.0	TLS_NUM_RSA_WITH_AES_128_CBC_SHA
EDU_BR_01_00_02_3702	Capwap_Ctrl	170.85.125.14	56998	DTLSv1.0	TLS_NUM_RSA_WITH_AES_128_CBC_SHA
EDU_BR_01_00_03_1832	Capwap_Ctrl	170.85.145.85	5264	DTLSv1.0	TLS_NUM_RSA_WITH_AES_128_CBC_SHA
EDU_BR_01_00_10_1832	Capwap_Ctrl	170.85.151.11	5272	DTLSv1.0	TLS_NUM_RSA_WITH_AES_128_CBC_SHA
EDU_BR_01_00_13_3702	Capwap_Ctrl	170.85.125.20	62903	DTLSv1.0	TLS_NUM_RSA_WITH_AES_128_CBC_SHA

- Single view:
  - Connections per AP
  - Ciphers in use
  - Source ports for NAT/PAT problems
  - Mobility will show here

AP Join Troubleshooting

Show wireless stats ap history mac address <AP_Ethernet_MAC >

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

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

- Unfiltered output
  - Time Stamp of Incident
  - APs affected
  - Disconnect Reason

Mapping AP to a WNCd instance

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

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

AP cannot join the WLC

- AP with radio mac <AP_radiomac1> and AP ethernet mac <AP_ethermac1> is not able to join the wireless network
- All or a handful of APs dropped from the C9800 11 AM and recovered
- AP cannot join post SSO or HA failover

OR

- A replacement AP will not join C9800

AP State Across Components

For Your Reference

show ap summary

Number of APs: 1

AP Name	Slots	AP Model	Ethernet MAC	Radio MAC	Location	Country	IP Address	State
AP4C77.6D9E.6162	3	4800	4c77.6d9e.6162	7069.5a51.4ec0	default location	BE	192.168.79.249	Registered

show platform software capwap chassis active R0

Tunnel ID	AP MAC	Type	IP	Port
0x90000004	7069.5a51.4ec0	Data	192.168.79.249	5272
0xa0000001	0000.0000.0000	Mobility Data	10.48.71.113	16667

AP State Across Components

For Your Reference

show platform software capwap chassis active F0

```
Tunnel ID  AP MAC          Type          IP              Port      AOM ID  Status
-------------------------------------------------------------------------------------
0x90000004  7069.5a51.4ec0  Data          192.168.79.249    5272        567  Done
0xa0000001  0000.0000.0000  Mobility Data  10.48.71.113     16667       519  Done
```

show platform hardware chassis active qfp feature wireless capwap cpp-client summary

```
cpp_if_hdl    pal_if_hdl      AP MAC          Src IP          Dst IP       Dst Port  Tun Type
-------------------------------------------------------------------------------------------
   0X33       0XA0000001   0000.0000.0000    10.48.39.30      10.48.71.113    16667    MOBILITY
   0X34       0X90000004   7069.5a51.4ec0    10.48.39.30      192.168.79.249  5272     DATA
```

AP State Across components

For Your Reference

show platform hardware chassis active qfp feature wireless capwap datapath summary

Vrf	Src Port	Dst IP	Dst Port	Input Uidb	Output Uidb	Instance Id
0	5247	192.168.79.249	5272	65490	65484	3
0	16667	10.48.71.113	16667	65491	65485	0

AP Join/AP Flap – AP View

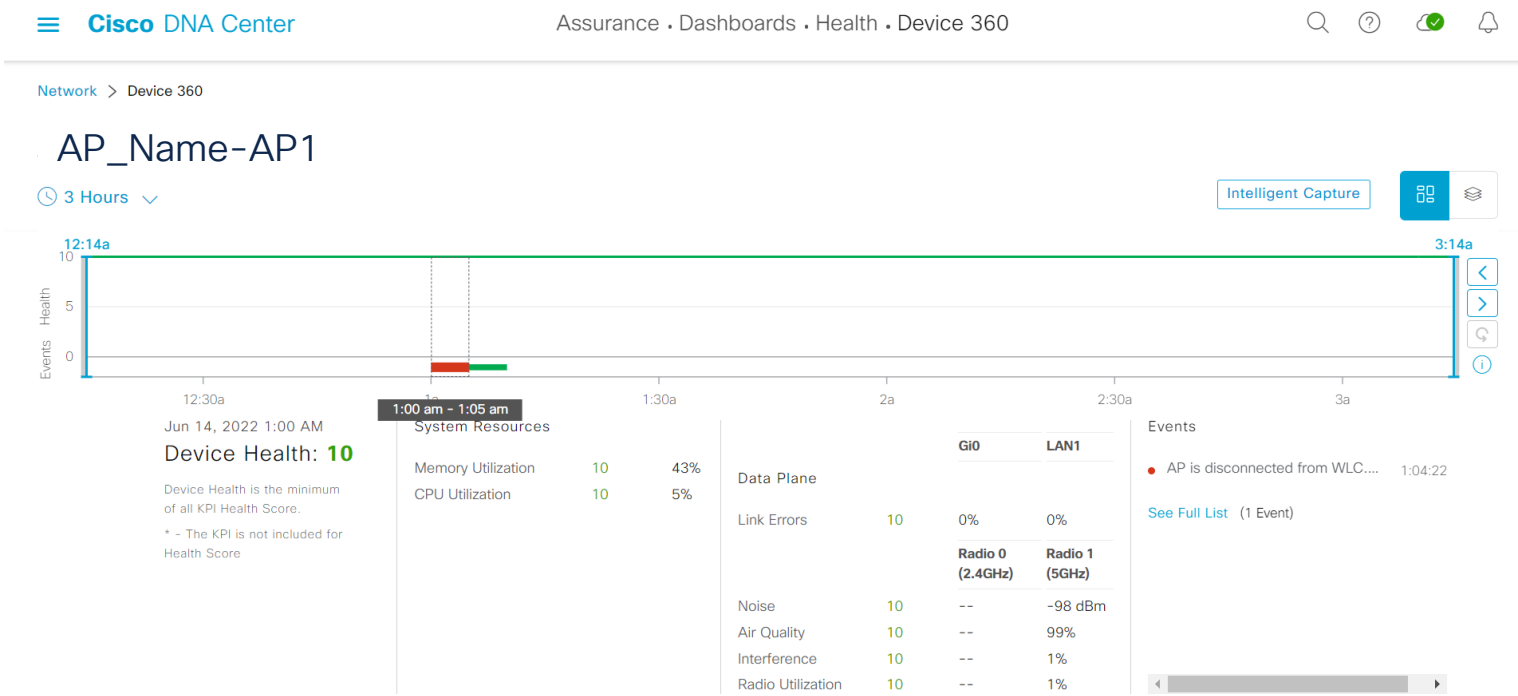
CAPWAP debugging on AP

For Your Reference

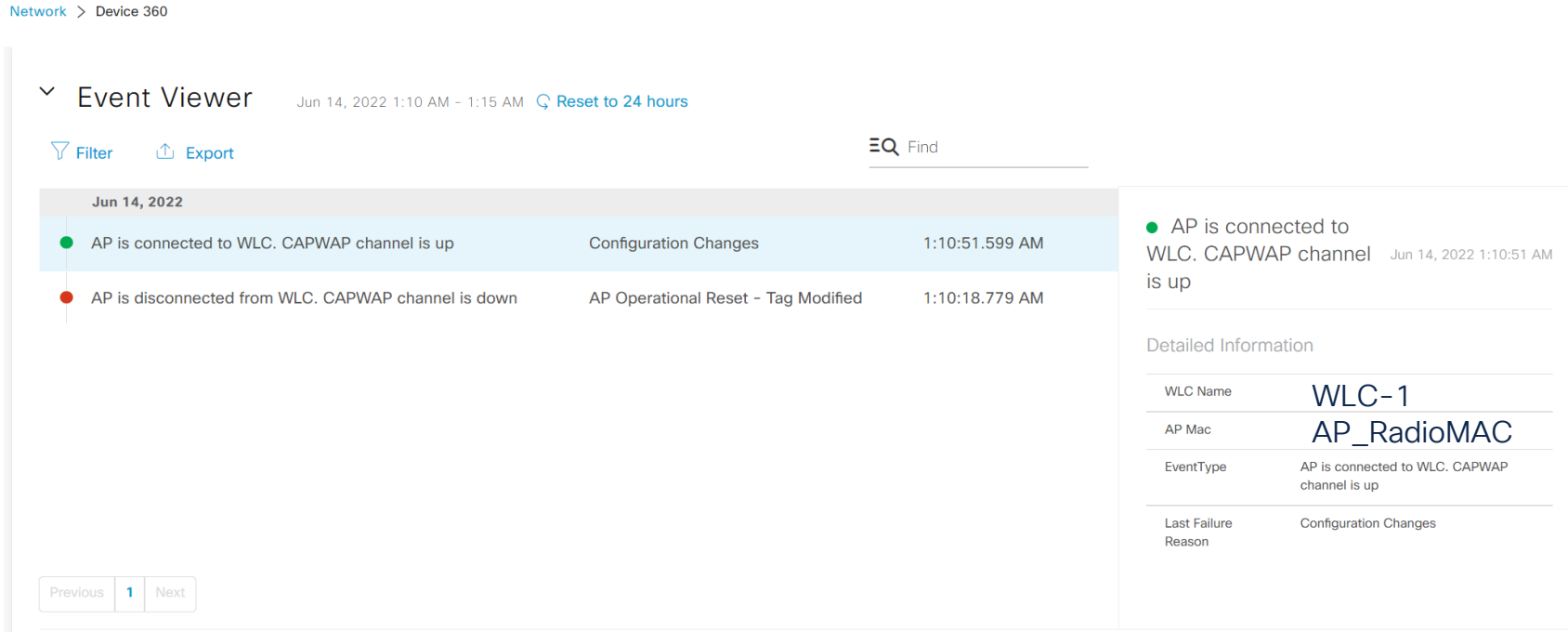
- Show capwap client config
- Show capwap client rcb
- Debug capwap client events
- Debug capwap client errors
- Debug capwap client payload

AP Join/AP Flap – DNA Center View

AP 360



AP Event Viewer



Data Plane Troubleshooting

Port-Asic Troubleshooting

- Show interface <>
- Show platform hardware port <> ezman statistics
- Show platform hardware port <> ezman info

TIP: Ensure PHY and ROMMON versions are updated to latest available for the specific C9800 platform.

Example of port drops

Backpressure indicators - data plane not able to process fast enough resulting in random drops

- show platform hardware port 0/1/0 ezman statistics

```
RX Counters
  MAC Filter drop:0  Unknown Vlan Drop:0
  High Priority
   Pass Pkt:93191         Bytes:16243813
   Drop Pkt:0             Bytes:0
  Low Priority
   Pass Pkt:8447296407    Bytes:6805697149012
   Drop Pkt:172546135654  Bytes:139012797667814
TX Counters
  High Priority
   Pass Pkt:0             Bytes:0
   Drop Pkt:0             Bytes:0
  Low Priority
   Pass Pkt:15182029085   Bytes:22497843030408
   Drop Pkt:0             Bytes:0
```

- show interfaces TenGigabitEthernet0/0/5

```
<snip>
 Input queue: 0/375/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 9090609000 bits/sec, 1410628 packets/sec
  5 minute output rate 1435073000 bits/sec, 121063 packets/sec
     1814427777729 packets input, 146180407969360 bytes, 0 no
buffer
     Received 1865 broadcasts (7052 multicasts)
     0 runts, 0 giants, 0 throttles
     1174099533 input errors, 0 CRC, 0 frame, 1174099533
overrun, 0 ignored
     0 watchdog, 7052 multicast, 0 pause input
     15220486562 packets output, 22554826373594 bytes, 0
underruns
```

Packet Tracer

- Enables to view processing of each packet that enters the C9800 from its ingress to egress from the system
- Feature Invocation Array (FIA) tracing , if enabled , provides a feature-by-feature processing including time spent at processing at each feature

```
Feature: CAPWAP_ENCAP_FEATURE
  Entry       : Output - 0x7001446c
  Input       : VLAN-CPPIF-2256
  Output      : CAPWAP-IF-0x0090c000a8
  Lapsed time : 330 ns
Feature: CAPWAP_OUTPUT_FRAG_FEATURE
  Entry       : Output - 0x70014474
  Input       : VLAN-CPPIF-2256
  Output      : CAPWAP-IF-0x0090c000a8
  Lapsed time : 288 ns
Feature: CAPWAP_ENCAP_IP_FEATURE
  Entry       : Output - 0x7001448c
  Input       : VLAN-CPPIF-2256
  Output      : CAPWAP-IF-0x0090c000a8
  Lapsed time : 1077 ns
```

Packet Tracer

For Your Reference

- Clear any preexisting packet-tracer configuration

```
#clear platform hardware chassis active qfp feature packet-trace

#clear platform condition all
```

- Choose interface to run packet-tracer `#debug platform condition interface [internal-RP | tenGigE | port-channel] both`
- Enable fia tracing with circular buffer up to 8192 packets
- `#debug platform packet-trace packet 8192 fia-trace circular`
- Copy the entire packet contents for review

```
#debug platform packet-trace copy packet both l2 size 256
```

Packet Tracer

For Your Reference

- To start the packet-tracer

```
#debug platform condition start
```

- To stop the packet-tracer

```
#debug platform condition stop
```

- To view list of packets captured

```
#show platform hardware chassis active qfp feature packet-trace summary
```

- To view a specific packet

```
#show platform hardware chassis active qf feature packet-trace packet <pkt-id>
```

- To export packet contents

```
#show platform hardware chassis active qfp feature packet-tracer packet all
decode | redirect bootflash:<FILENAME>.txt
```

Data Plane Statistics – Utilization

show platform hardware chassis active qfp datapath utilization

```
Load for five secs: 5%/0%; one minute: 7%; five minutes: 8%
Time source is NTP, 10:54:24.256 PDT Tue Jun 14 2022
```

CPP 0: Subdev 0		5 secs	1 min	5 min	60 min
Input: Priority	(pps)	2398	2485	2552	2596
	(bps)	6883896	7111224	7519936	7352072
Non-Priority	(pps)	249051	262694	266819	253358
	(bps)	1742384176	1844201472	1883472592	1781806512
Total	(pps)	251449	265179	269371	255954
	(bps)	1749268072	1851312696	1890992528	1789158584
Output: Priority	(pps)	2238	2423	2431	2851
	(bps)	5947440	5858904	6005016	6728544
Non-Priority	(pps)	241605	247387	263266	247080
	(bps)	1669812808	1699537320	1836281784	1739971064
Total	(pps)	243843	249810	265697	249931
	(bps)	1675760248	1705396224	1842286800	1746699608
Processing: Load	(pct)	4	4	4	4

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

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

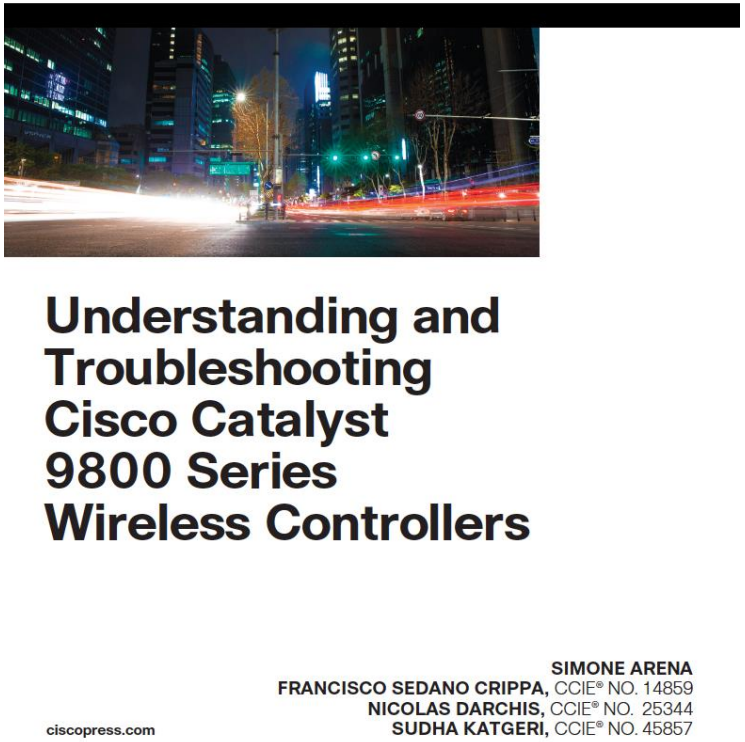
Statistics Commands

For Your Reference

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

Conclusion

[Amazon link to purchase]



Appendix

High CPU Troubleshooting

C9800 High CPU – Show commands

- CPU cores used by IOS

```
#show process cpu sorted
```

- CPU cores used by BinOS processes

```
#show process cpu platform sorted
```

- Traffic Punted to CPU

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

- CPU Queues and Policers

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

C9800 High CPU – CPU PCAP

- CPU PCAP ores used by IOS

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

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

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

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

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

Memory Troubleshooting

Memory Leak Troubleshooting

- 3 types of memory management
  - IOS Memory Allocation
  - BinOS Memory Allocation
  - Database Memory Allocation
- Validate memory leak and rate of leak along with process that is experiencing memory leak

```
#show platform software process slot chassis active R0 monitor |
include Mem
#show processes memory platform sorted
```

Memory Leak Troubleshooting

- Identify the callsite

```
#show processes memory platform accounting
```

- collect

```
#show platform software memory <PROCESS_NAME> chassis active R0 alloc callsite brief
#debug platform software memory <PROCESS_NAME> chassis active R0 alloc callsite clear
#debug platform software memory<PROCESS_NAME> chassis active R0 alloc backtrace  start <CALL_SITE> depth 10
#show platform software memory <PROCESS_NAME> chassis active R0 alloc backtrace
#debug platform software memory <PROCESS_NAME> chassis active R0 alloc callsite stop
```

- To view database memory

```
#show platform software memory database <PROCESS_NAME> chassis active R0 {brief | summary | callsite}
```

Mobility Happy Hour

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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

cisco Live!

Thank you


cisco Live!
ALL IN