cisco Live!

Let's go

The bridge to possible

Troubleshoot Cisco Catalyst 9800 Wireless Controllers

Lakshmi Kasturi – Technical Leader

BRKEWN-3628

Cisco Webex App

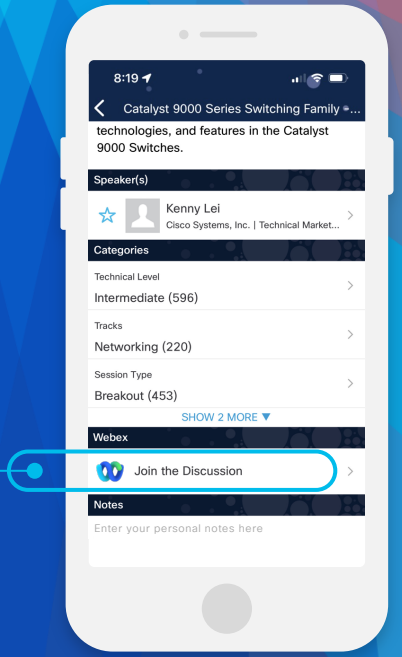
Questions?

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

How

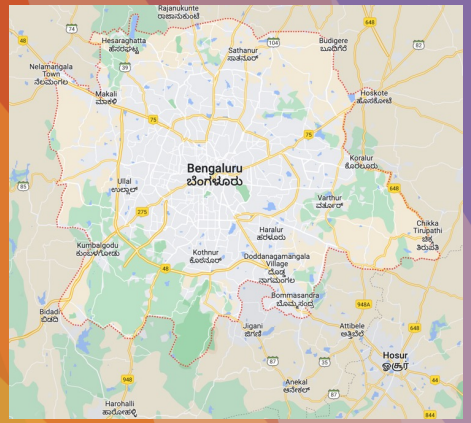
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



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

About Lakshmi



CISCO™

10 Years

ZOOPHILIST

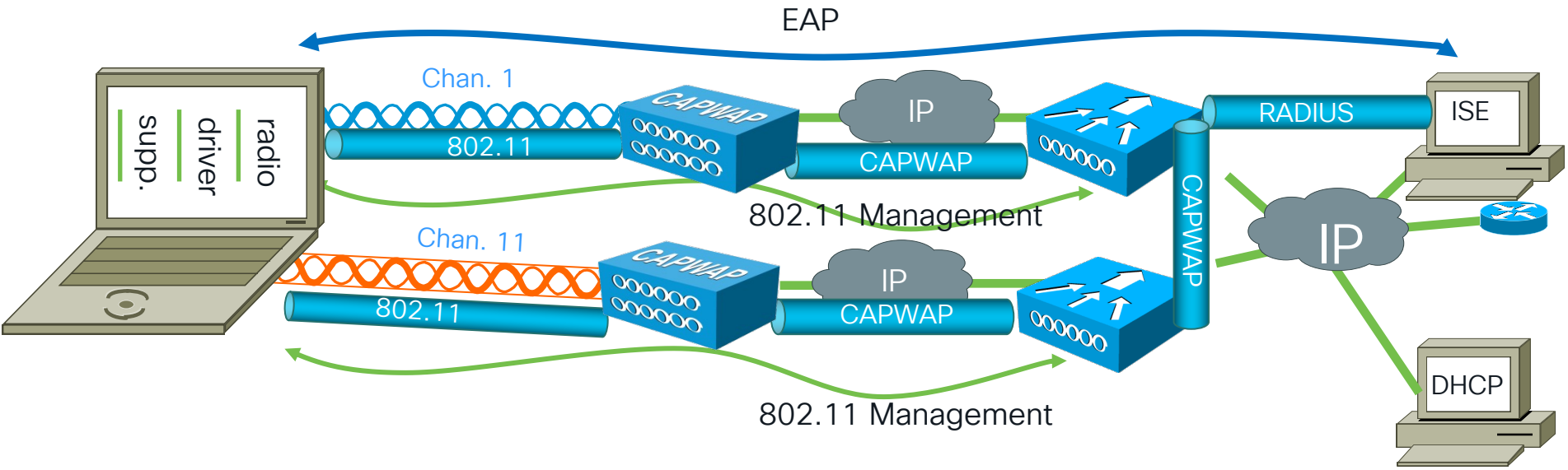
a lover of animals

cisco Live!

Agenda

- Data Collection Principles
- Hardware & Software Architecture
- Troubleshooting Techniques
- KPI Monitoring
- Automate Troubleshooting

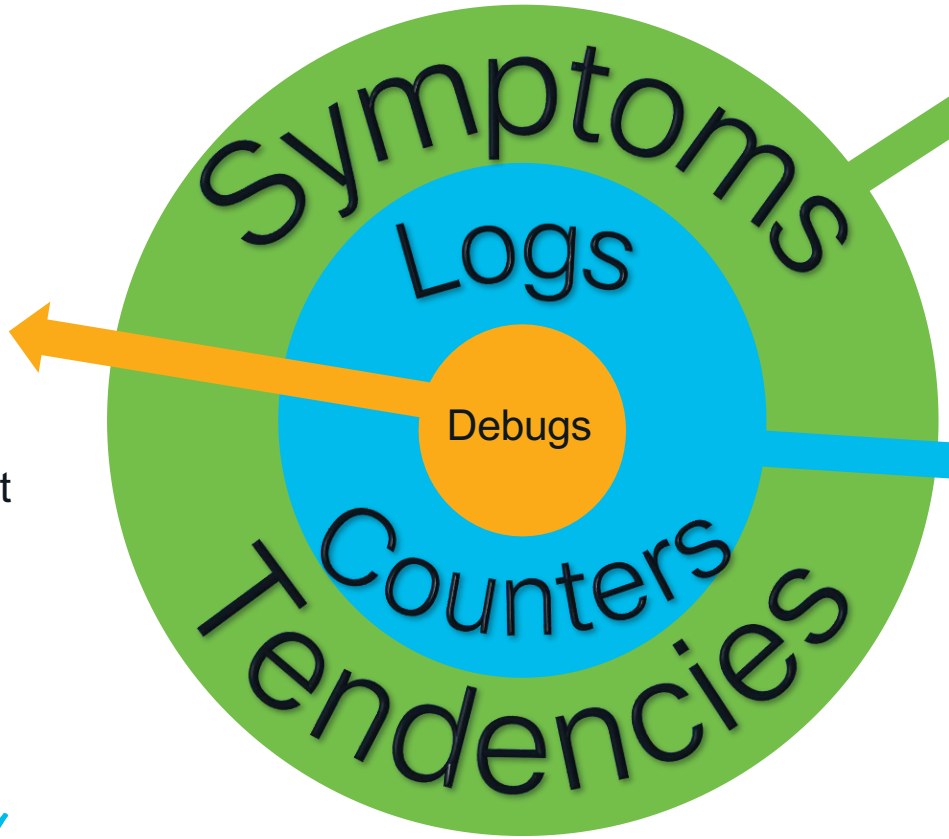
Where do we start?



Wireless Link = Complex multi-variable equation

✓ Isolate and remove the variables

Data Collection Principles



Catalyst Center (DNAC)

- Network Wide
- Issues not triggers

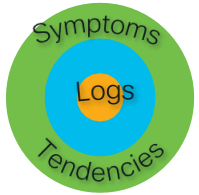
Low Level

- Root Cause
- Fix development

Controller/AP

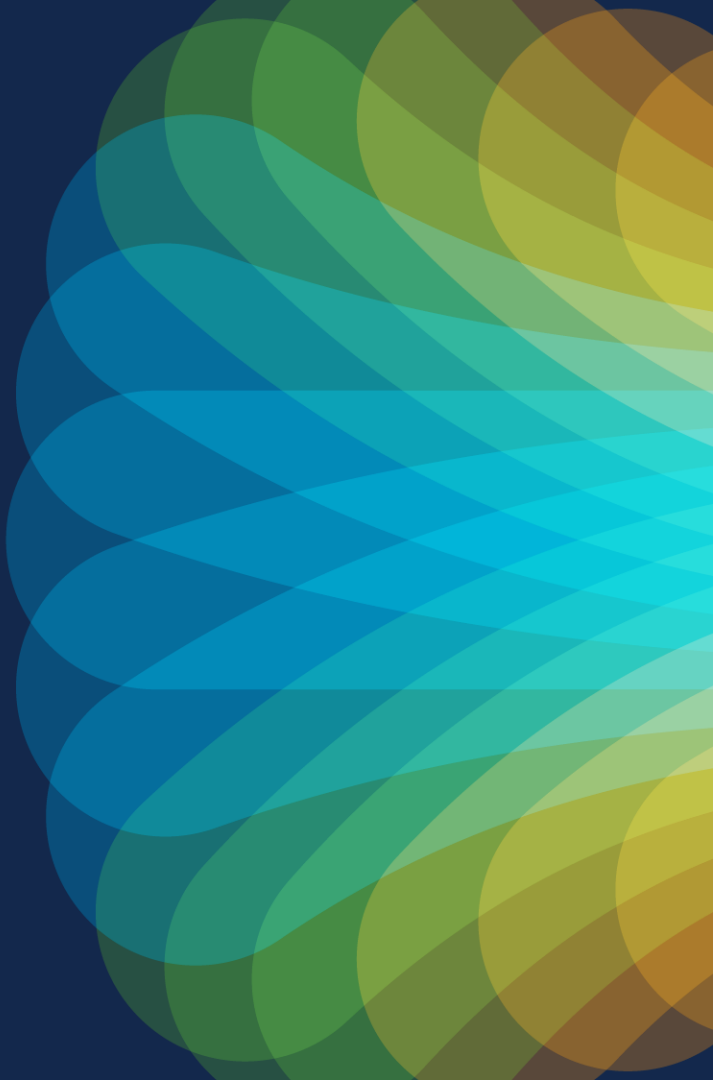
- Component Isolation
- Fault Triggers

Applying Tools



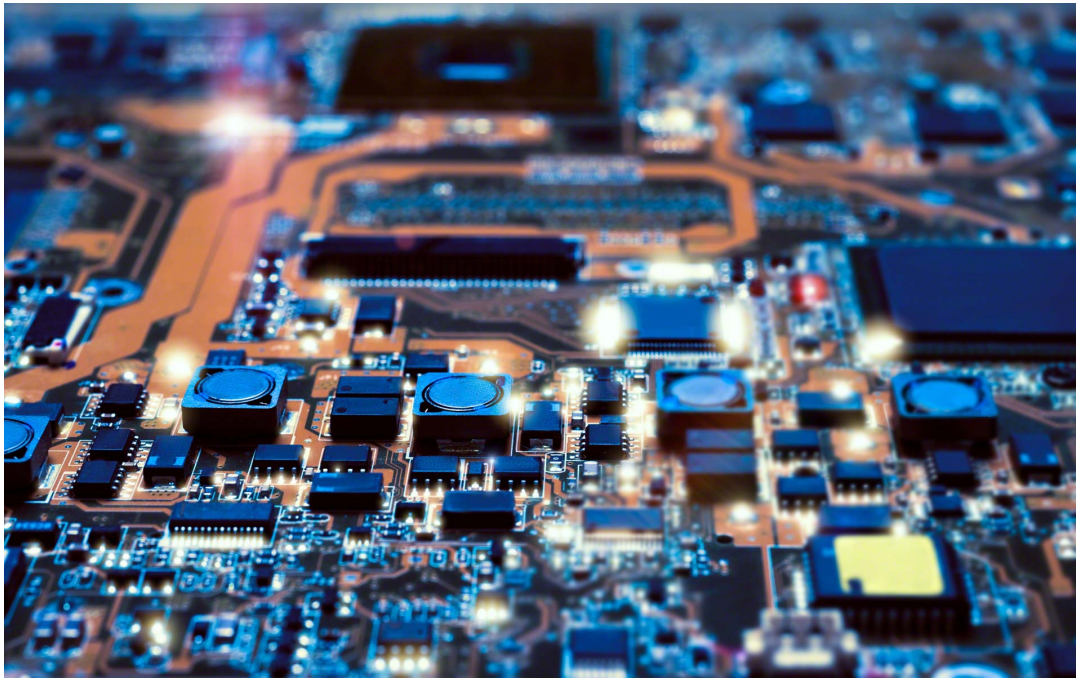
	DNAC 360	Show	Wireless Sniffer	Debug WLC	Debug AP	WiFi Hawk	WCAE	WLAN Poller
General Problems								
Client Issues								
Client Roaming								
Device Issues								
RF Analysis								
Configuration Analysis								

C9800 WLC Architecture



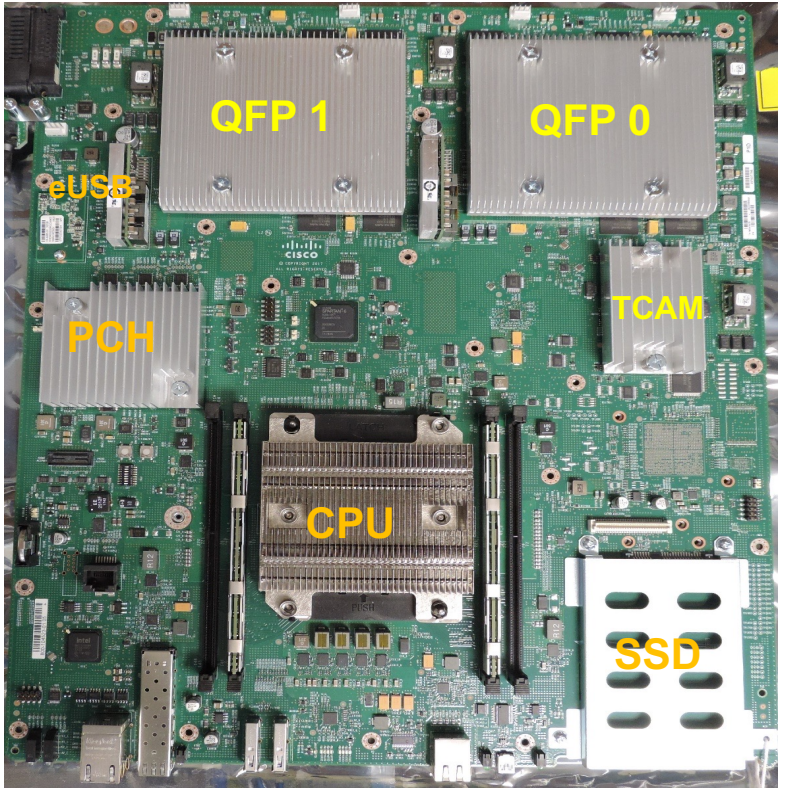
C9800 Architecture

- Hardware Architecture
- Software Architecture



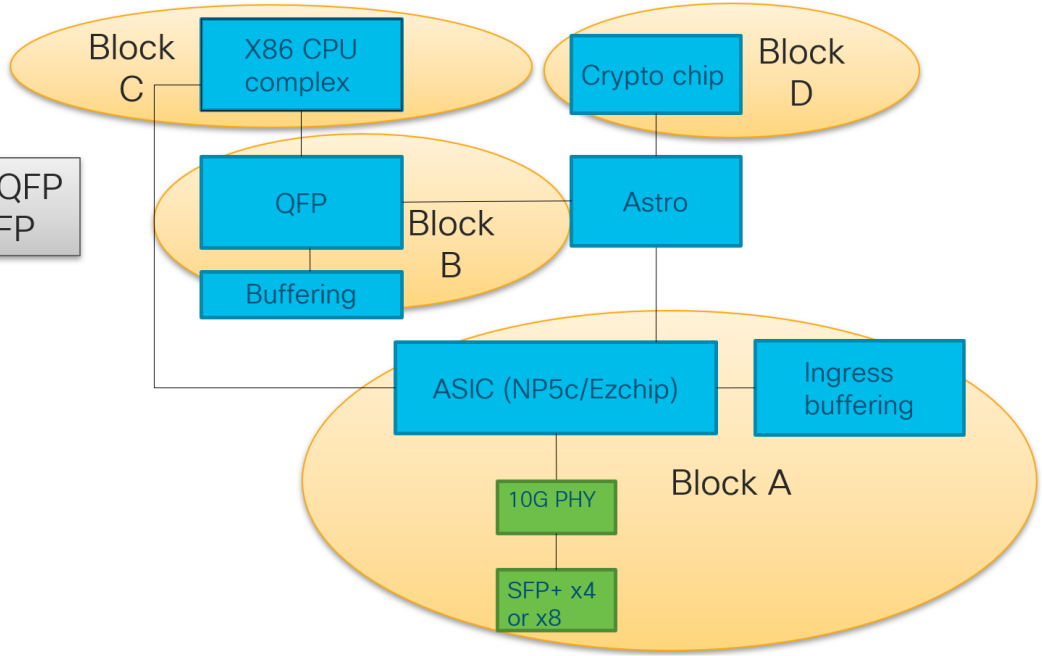
C9800 Hardware Architecture

- 9800-80 capable of 80Gbps throughput
- 2 Load balanced QFP (1 in 9800-40)
- 1 Crypto Chip



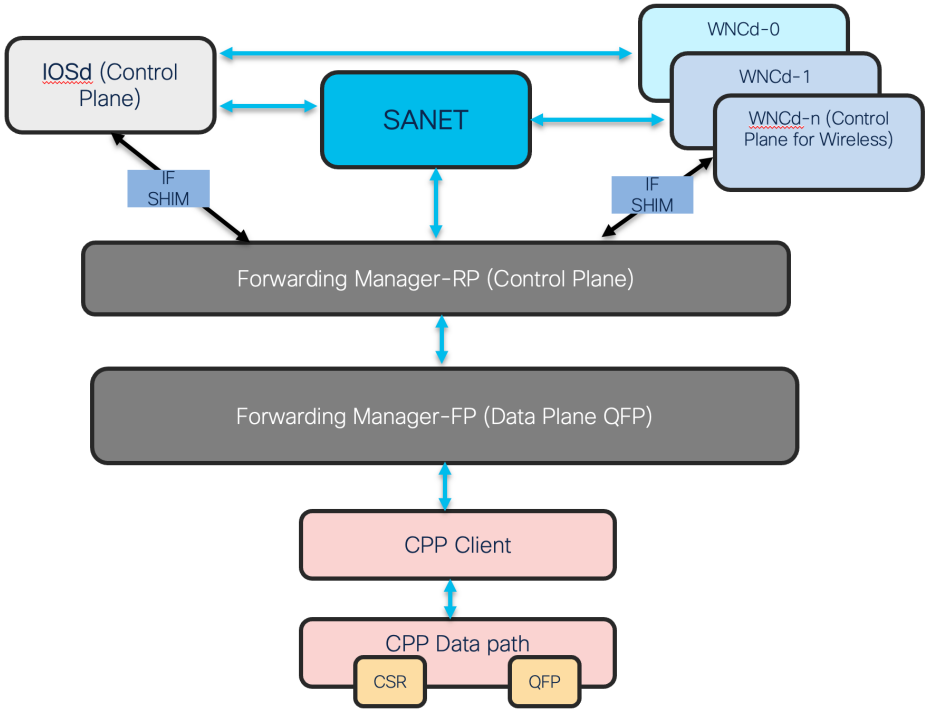
C9800 WLC Hardware Appliance High Level Block Diagram

C9800-40: Single QFP
C9800-80: Dual QFP



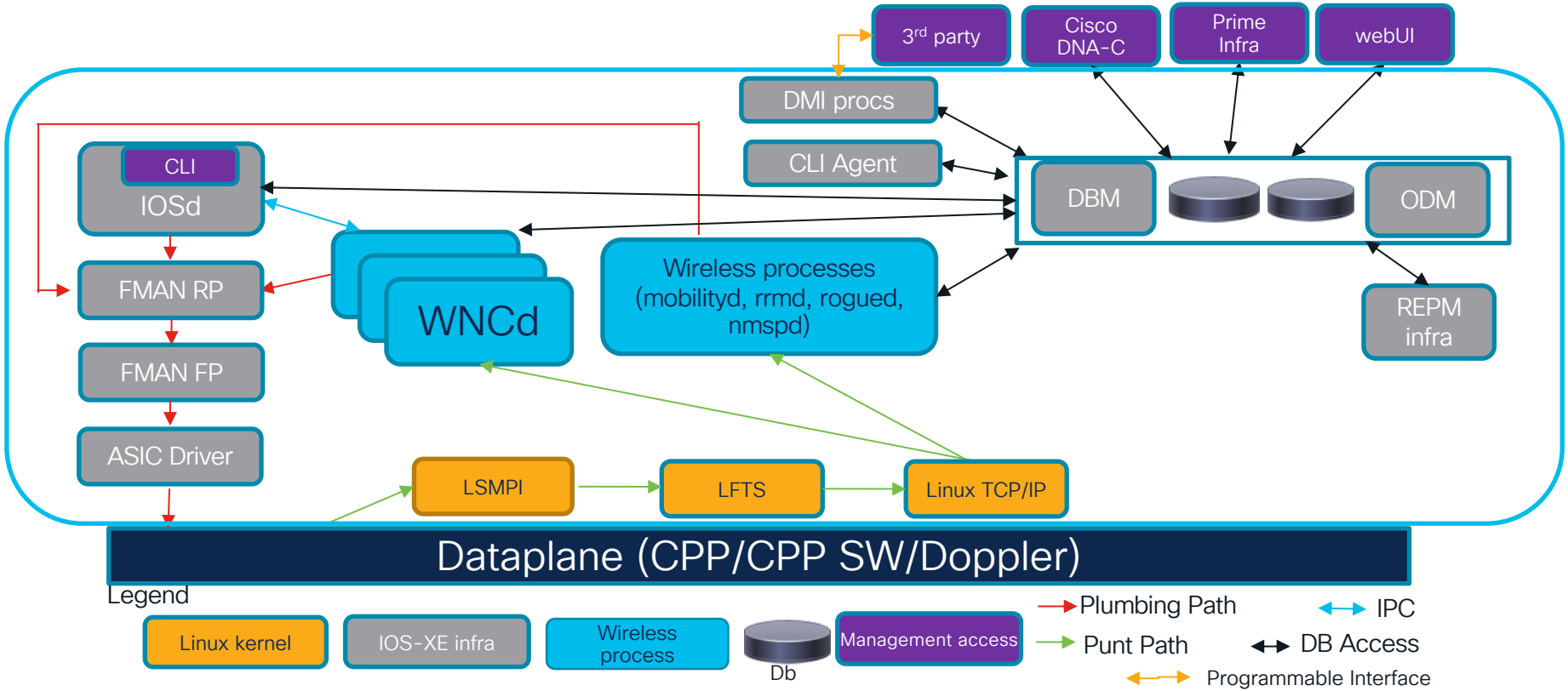
Software Architecture

C9800 Software Architecture
Simplified View



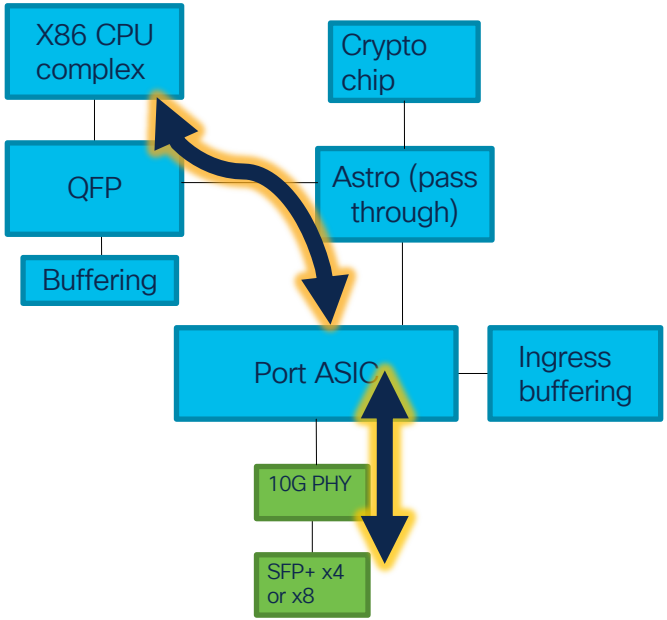
C9800 Software Architecture

Let me Complicate

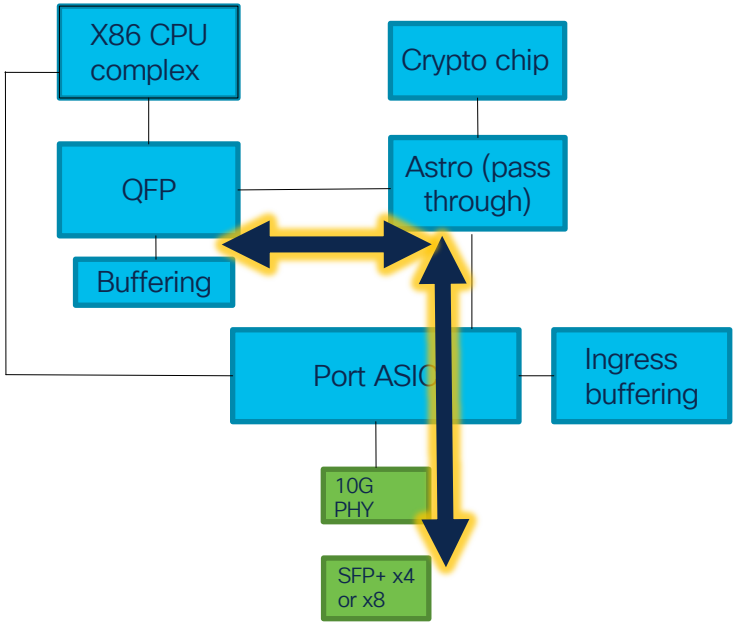


What's the Packet Flow ?

Let's combine – Hardware & Software Architecture

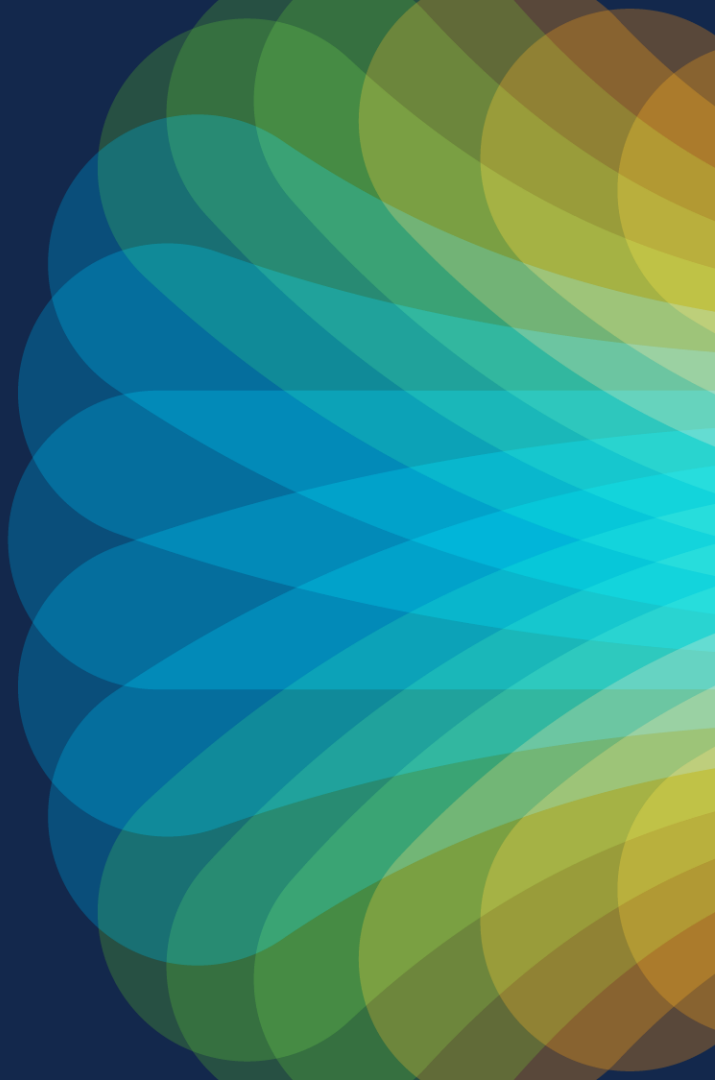


Control Plane Packet (Punt/Inject)



Data Plane Packet

9800 Troubleshooting



C9800 Troubleshooting

- Control Plane
- Embedded Packet Capture

Troubleshooting Control Plane

Where to start ?

- IOSd Logging
  - Traditional – Syslog
- Always On Tracing
  - Real time data for all relevant events
- Radioactive / Conditional Debugging
  - Per IP/MAC address debugging
- Archive Bundle

IOSd Logging

- Syslog – #show logging
  - Good Starting Point
  - System details
    - Client delete
    - AP Join/Disjoin
    - Memory / CPU
    - GUI Connections

IOSd Logging

- AP Join

May 22 2023 09:34:31.251 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Capwap2, changed state to up
May 22 2023 09:34:31.249 UTC: %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1 R0/0: wncd: AP Event: AP Name: **C9120_1**, MAC: 0042.68a0.ee78 Joined
May 22 2023 09:36:19.548 UTC: %CAPWAPAC_SMGR_TRACE_MESSAGE-3-EWLC_GEN_ERR: Chassis 1 R0/0: wncd: Error in Session-IP: 192.168.25.101[5264] Mac: 00a3.8ec2.da00 Heartbeat timer expiry for AP. **Close CAPWAP DTLS session**

- Admin UI

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'

Always on Tracing CLI

- Simplified View
- Generate per process for last 10mins

```
# show logging process <process daemon> to-file <Always_on_process.txt>
# more bootflash:Always_on_process.txt
# copy bootflash:Always_on_process.txt tftp://<ServerIP>/Path or
ftp://user:password@ServerIP/Path
```

Always on Tracing CLI

Specify – MAC/IP

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

Specify – Timelines

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

Failure condition snapshot

```
# show logging profile wireless trace-on-failure
# show logging profile wireless filter uuid <UUID Derived from summary> to-file
bootflash:Trace_on_Failure.txt
```

Always on - Successful client connection

RA tracing OFF

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

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

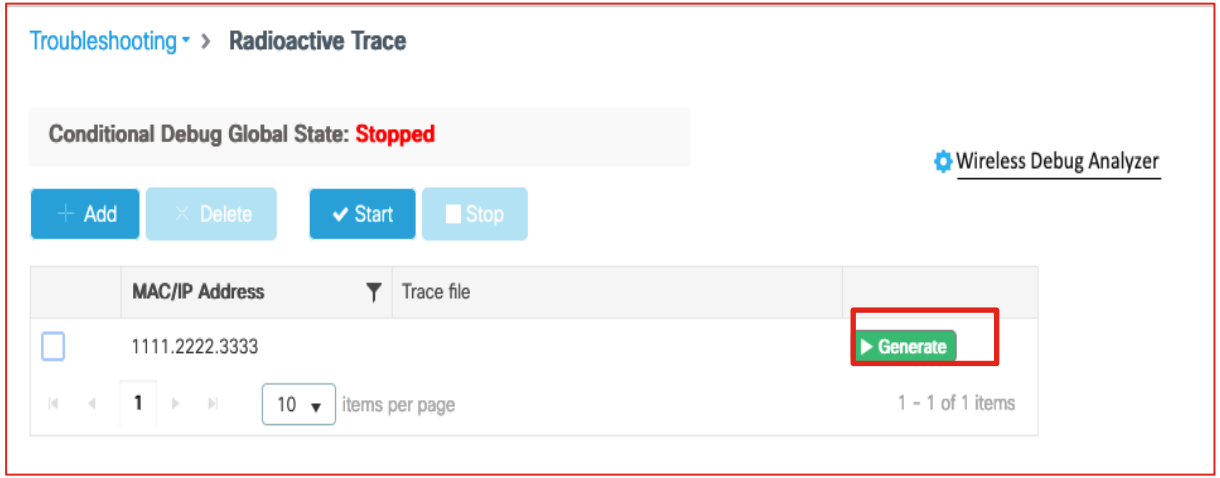
Radioactive Tracing

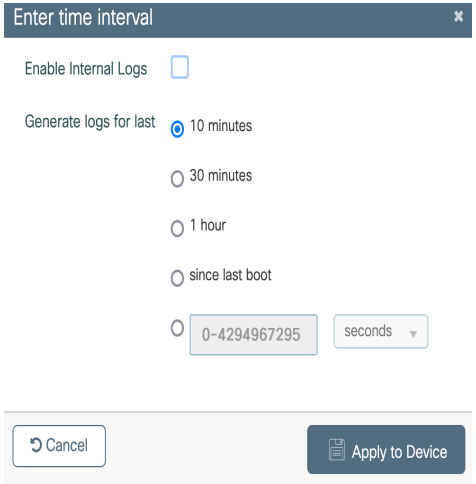
Enables all debugs automatically for given MAC/IP Address

“Generate” decodes on-flash binary logs to readable format

#debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x} {monitor-time} {N-sec} internal level verbose

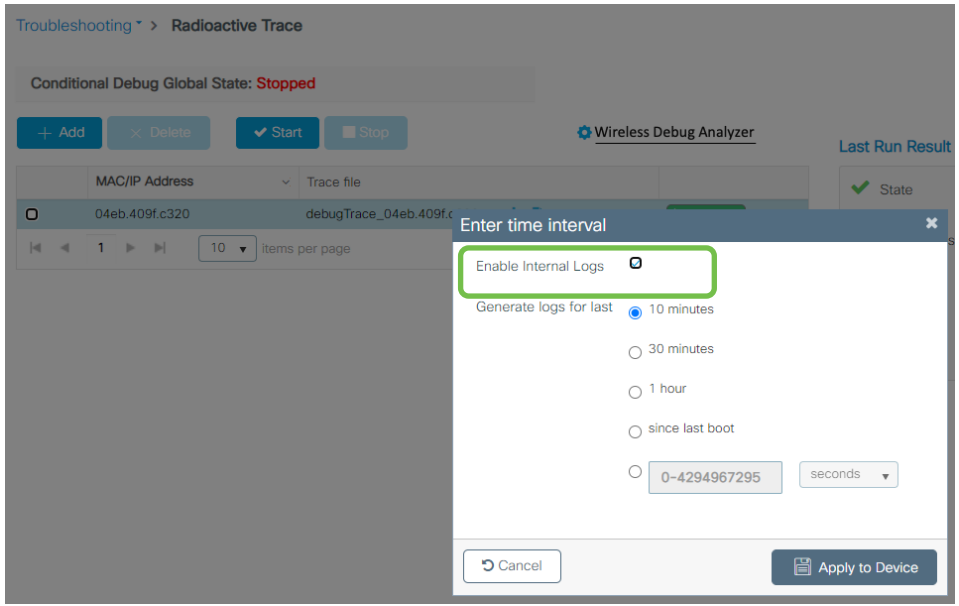
#no debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x} → Disable & Generate logs





Radioactive Tracing – Internal

Let me complicate



- Enable – Internal Logs
- Extremely verbose
- RA Trace: 400 lines
- RA Trace + Internal: 3000 lines

RadioActive Trace – Failed Authentication

- Group Key Update

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

Conditional Debugging

Further Complicate

- Specific Process
- Specific Use Cases

```
# set platform software trace {Process Name} wireless chassis active R0 {Modules | all-modules } {level}
# show platform software trace level {Process Name} chassis active R0
# show logging process {Process Name} to-file bootflash:Process_Logs.txt
```

E.g. set platform software trace wncd wireless chassis active R0 sisf verbose

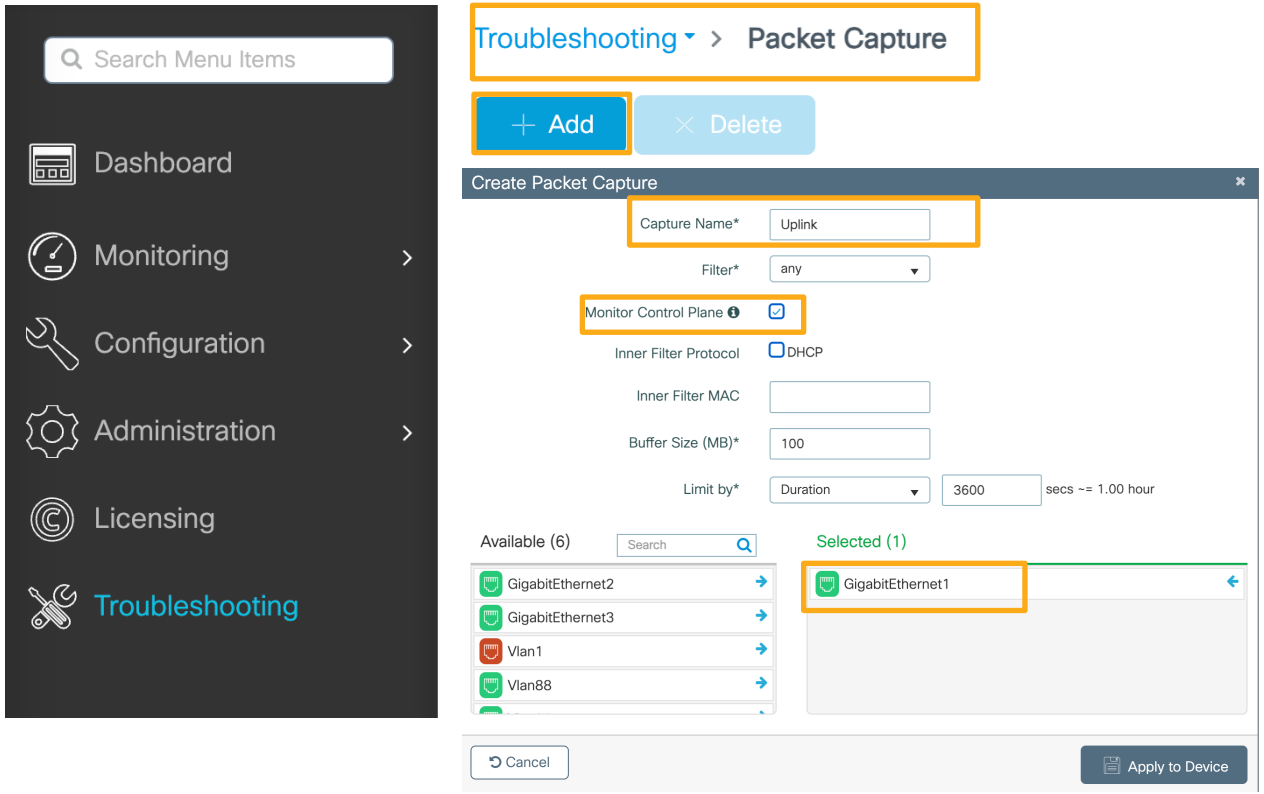
Archive Bundle

- Generates tar file
- Combines all available logs per process

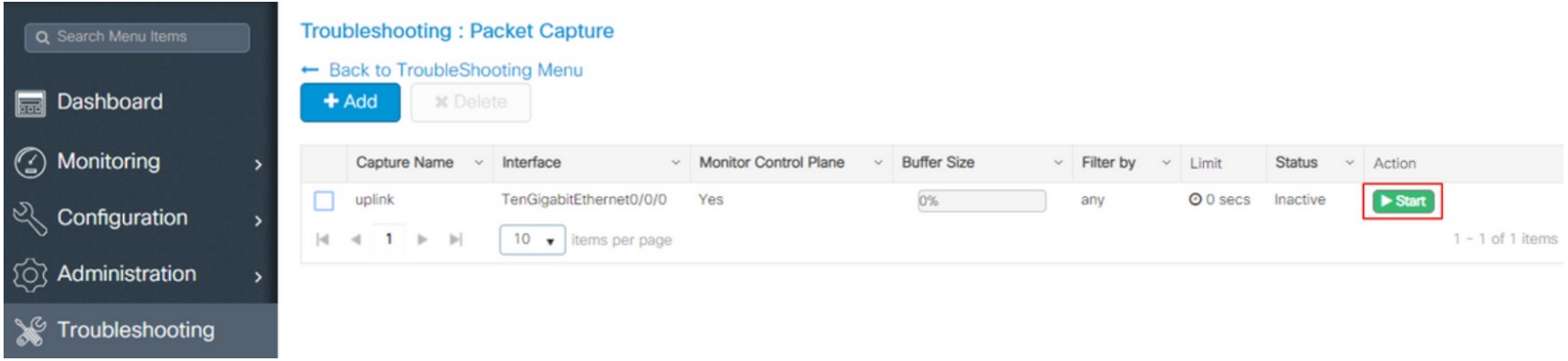
```
# request platform software trace archive last <No of days> to-file
bootflash:<Archive_file>
```

Embedded Packet Capture

Embedded Packet Capture

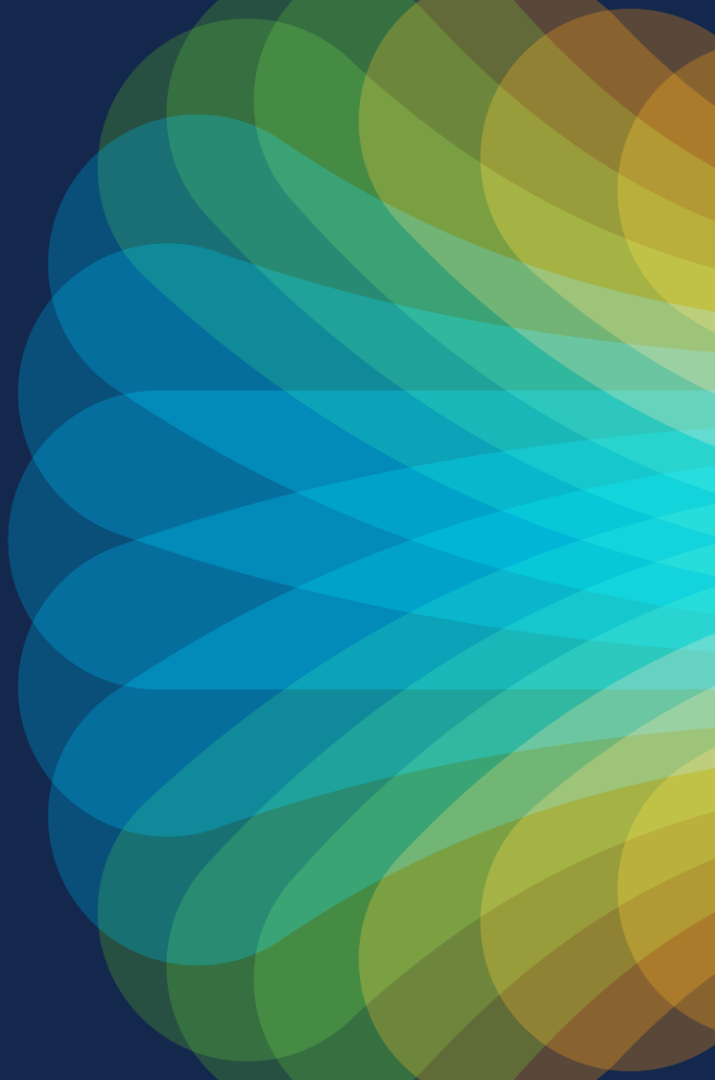


Embedded Packet Capture



1	2019-01-21 05:27:40.996942	10.104.172.169	10.65.34.206	TLSv1.2	804	Application Data
2	2019-01-21 05:27:41.035993	Vmware_9a:a8:65	Broadcast	ARP	60	Who has 10.104.172.89? Tell 10.104.172.29
3	2019-01-21 05:27:41.045987	10.65.34.206	10.104.172.169	TCP	54	64125 → 443 [ACK] Seq=1 Ack=751 Win=257 Len=0
4	2019-01-21 05:27:41.108987	Apple_33:a6:8b	Broadcast	ARP	60	Who has 10.104.172.1? Tell 10.104.172.46
5	2019-01-21 05:27:41.460974	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x546730d8
6	2019-01-21 05:27:41.563966	9.12.64.230	255.255.255.255	CAPWAP-Cont…	260	CAPWAP-Control - Discovery Request
7	2019-01-21 05:27:41.563966	9.12.64.230	255.255.255.255	CAPWAP-Cont…	260	CAPWAP-Control - Discovery Request
8	2019-01-21 05:27:41.563966	9.12.64.19	9.12.64.230	CAPWAP-Cont…	136	CAPWAP-Control - Discovery Response
9	2019-01-21 05:27:41.672954	0.0.0.0	255.255.255.255	DHCP	324	DHCP Discover - Transaction ID 0x6a200c34
10	2019-01-21 05:27:41.686960	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x48056849

KPI Monitoring



KPI Monitoring

Device checks

- Uptime – self & peer
- AP Uptime & Connection status
- Switchover counters

System Monitoring

- CPU & Memory monitoring
- Core & system report

Other Device connectivity

- Mobility
- Telemetry

Client Connectivity

- Client Status
- Client Deauth stats

Device Checks

Generic Check

Install Mode - Faster boot, lower memory footprint, uptime

```
#show version | i uptime|Installation mode|Cisco IOS Software
Cisco IOS Software [Amsterdam], C9800 Software (C9800_IOSXE-K9), Version 17.9.4, RELEASE
SOFTWARE (fc2)
Gladius1 uptime is 2 weeks, 5 days, 21 hours, 30 minutes

Installation mode is INSTALL
```

Hardware Check - Only for 9800-40/80/L

```
#show environment
Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     0
```

AP Health Status

Crashed or Disconnected ?

Expectation:
AP Uptime = Association Uptime = Last controller connection

 # show ap uptime

Number of APs:8

AP Name	Ethernet MAC	Radio MAC	AP Up Time	Association Up
AP1	0042.68a0.fc4a	0062.ecf3.8310	26 days 0 hour 57 minutes 41 seconds	26 days 0 hour 57 minutes
AP2	7069.5a74.7a50	7069.5a78.7780	26 days 0 hour 57 minutes 41 seconds	20 days 10 hour 20 minutes
AP3	04eb.409e.1d28	04eb.409f.4fa0	18 minutes 15 seconds	18 minutes 13 seconds

AP Crashed - What's next ?

#show ap crash-file

File Location: BOOTFLASH

AP Name	Crash File	Radio Slot 0	Radio Slot 1
AP3	Ap3-1_0062ecaade80.crash		

#dir bootflash: | in crash

```
54   -rw-   50476   May 9 2023 13:07:34 +02:00   Ap3-1_0062ecaade80.crash
66   -rw-   120276  Jan 26 2023 11:46:55 +01:00  Ap4-9_d4e88019f140.crash
```

AP Disconnections

Who has failed ?

 # show wireless stats ap join summary

Number of APs: 8

Base MAC	Ethernet MAC	AP Name	IP Address	Status	Last Failure Phase	Last Disconnect Reason
04eb.409e.d660	04eb.409e.0e00	AP6	9.12.89.213	Joined	Join	AP Auth Failure
0cd0.f894.78e0	0cd0.f894.0250	AP7	9.12.89.242	Joined	NA	NA
58bc.2793.6830	f866.f267.7f0e	AP8	9.12.89.222	Not Joined	Dtls-Handshake	Certificate verify failed

AP Disconnections

Why ?

#show wireless stats ap mac-address h.h.h join detailed | b AP re

AP reported disconnect detail

Disconnect reason from AP	: NA
AP reported reboot detail	
Reboot reason from AP	: No reboot reason

Last AP disconnect details

Last Disconnect Phase	: Dtls-Handshake
Last Disconnect Reason	: DTLS handshake expired
Last Disconnect Time	: 09/24/2023 20:31:26
Current Join Status	: Not Joined

AP Radio Reset

- Radio resets – Channel change or Radar

show ap auto-rf dot11 5ghz | i Channel changes due to radar|AP Name|Channel Change Count

```
AP Name                                 : Lakshmi-9117-2
    Channel changes due to radar              : 0
AP Name                                 : Lakshmi_9120_1
    Channel changes due to radar              : 0
    Channel Change Count                      : 6
```

HA Checks

- Basic HA status

#show redundancy | i uptime|Location|Current Software state|Switchovers

Available system uptime = 2 weeks, 1 day, 2 hours, 48 minutes
Switchovers system experienced = 1
Active Location = slot 1
Current Software state = ACTIVE
Uptime in current state = 7 hours, 10 minutes
Standby Location = slot 2
Current Software state = STANDBY HOT
Uptime in current state = 7 hours, 4 minutes

- Per Chassis and stack status
- Switchover count

HA Checks

My HA pair keeps failing over regularly !

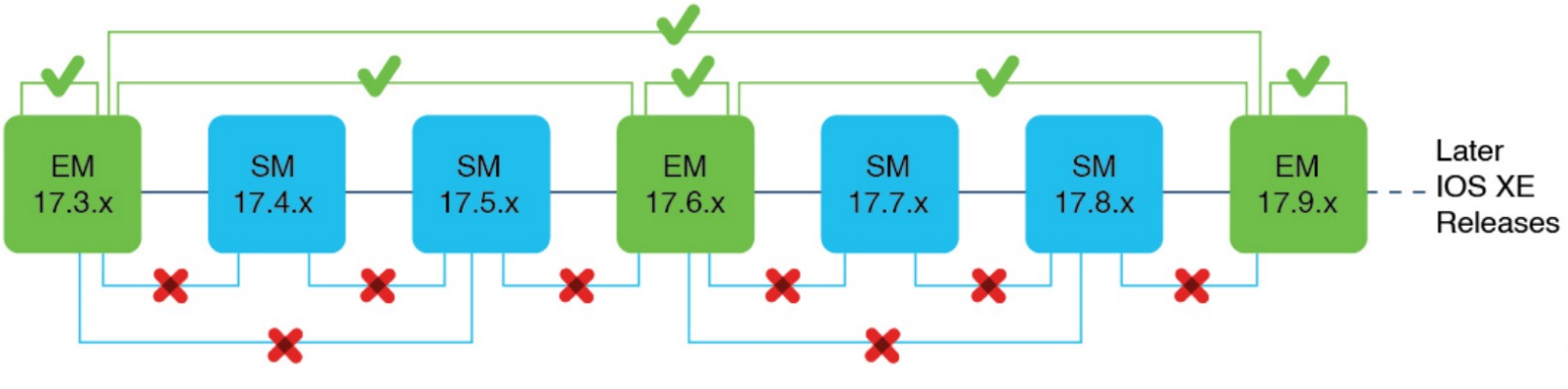
#show redundancy switchover history

Index	Previous active	Current active	Switchover reason	Switchover time
8	2	1	active unit removed	14:06:05 CEST Tue May 29 2023
9	1	2	active unit removed	14:25:29 CEST Tue May 29 2023
10	2	1	Active RMI port down	11:00:22 CEST Thu May 30 2023
11	1	2	active unit removed	11:08:53 CEST Thu Jun 30 2023
12	2	1	active unit removed	11:18:47 CEST Thu Jun 30 2023
13	1	2	active unit removed	11:34:32 CEST Thu Jun 30 2023
14	2	1	active unit removed	11:51:34 CEST Thu Jul 30 2023

ISSU Upgrade

Why use ISSU upgrade ?

- Upgrade during production
- Reduces downtime
- Supported between all main releases



Upgrade Failed ? – Let's troubleshoot

#show redundancy config-sync failures historic mcl

Mismatched Command List

-snmp-server enable traps hsrp

#show install summary

Type St Filename/Version

IMG C 17.09.03.0.4111

APSP C bootflash:C9800-CL-universalk9.17.09.03.CSCwf67455.SPA.apsp.bin

Upgrade Failed ? – Let's troubleshoot

#show install log

```
[8|install_commit(CONSOLE, )]: Committing SMU
[8|install_commit(INFO, )]: Executing .install_pre_smu_activation.sh from /bootflash/C9800-CL-
universalk9.17.09.03.CSCwf67455.SPA.apsp.bin
[8|install_commit(INFO, )]: SUCCESS: Prescript execution done
[8|install_commit(INFO, )]: Executing .install_pre_smu_activation.sh from /bootflash/C9800-CL-
universalk9.17.09.03.CSCwf67455.SPA.apsp.bin done.
[8|install_commit(CONSOLE, )]:
[8|install_commit(INFO, )]: [1]: Performing verify_smu SUCCESS: verify_smu finished
[remote|install_commit]: END SUCCESS
 Wed Sep 27 00:21:47 UTC 2023
[remote|install_commit(INFO, )]: cleanup_trap  remote_invocation 1 operation install_commit .. 0 .. 0
[8|install_commit(INFO, )]: [1]: Performing SMU_COMMIT
  SUCCESS: SMU_COMMIT finished
[8|install_commit(INFO, )]: Remote output from chassis 1/R0
[8|install_commit(INFO, )]:
[8|install_commit]: END SUCCESS /bootflash/C9800-CL-universalk9.17.09.03.CSCwf67455.SPA.apsp.bin
```

Crashes & System reports

- Process impacted, timestamp

9800-40/80 – Harddisk
9800-L/CL - Bootflash

#dir harddisk:/core/ | i core|system-report
Directory of harddisk:/core/

3661831 -rw- 11260562 Mar 25 2023 22:07:12 +01:00
Gladius1_1_RP_0_wncd_16574_20230325-220708-CET.core.gz
3661830 -rw- 48528 Mar 25 2023 21:57:20 +01:00 Gladius1_1_RP_0-system-report_20230325-215658-CET-info.txt
3661829 -rw- 126548098 Mar 25 2023 21:57:10 +01:00 Gladius1_1_RP_0-system-report_20230325-215658-CET.tar.gz

System Monitoring

Memory Utilization

show platform resources

**State Acronym: H - Healthy, W - Warning, C - Critical

Resource	Usage	Max	Warning	Critical	State
RP0 (ok,active)					H
Control Processor	5.00%	100%	80%	90%	H
DRAM	4425MB(28%)	15567MB	88%	93%	H
ESP0(ok, active)					H
QFP					H
DRAM	244364KB(13%)	1835008KB	85%	95%	H
IRAM	414KB(20%)	2048KB	85%	95%	H
CPU Utilization	0.00%	100%	90%	95%	H

Memory Utilization

Gladius # **show process memory platform sorted**
System memory: 8087340K total, 4777004K used, 3310336K free,
Lowest: 3278648K

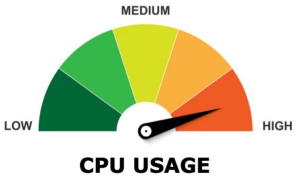
Pid	Text	Data	Stack	Dynamic	RSS	Name
23439	390426	1301000	136	460	1301000	linux_iosd-imag
18048	990	409416	328	16112	409416	wncd_0
17201	181	380860	3956	5200	380860	wncmgrd
23351	526	327388	136	45476	327388	dbm
28496	89	258616	136	18608	258616	pubd

Memory Debugging

Gladius1#**show process memory platform accounting**

```
process                callsite_ID(bytes)  max_diff_bytes   callsite_ID(calls)
max_diff_calls              tracekey                  timestamp(UTC)

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

cli_agent_rp_0      2160919555  8914627 2160919555  23228
1#5abb66956d7547e01f8250be345b11fe      2023-07-08 02:26

wncd_0_rp_0         2160919555        2598253       146453505        5018
1#8844b0be9c7c328d18ad34424c5ef556      2023-07-08 02:25
```

CPU Utilization

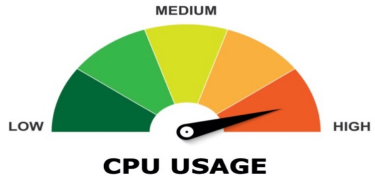


- “High CPU” can happen on any single CPU core if a single process is causing it.

- CPU utilization within IOSd :

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

CPU Utilization



- Per Process CPU utilization

Gladius1#**show processes cpu platform sorted | ex 0% 0% 0%**

CPU utilization for five seconds: 14%, one minute: 16%, five minutes: 16%

Core 0:	CPU utilization	for five	seconds:	10%,	one minute:	7%,	five	minutes:	11%
Core 1:	CPU utilization	for five	seconds:	6%,	one minute:	28%,	five	minutes:	12%
Core 2:	CPU utilization	for five	seconds:	48%,	one minute:	55%,	five	minutes:	68%
Core 3:	CPU utilization	for five	seconds:	20%,	one minute:	8%,	five	minutes:	11%
Core 4:	CPU utilization	for five	seconds:	38%,	one minute:	13%,	five	minutes:	17%
Core 5:	CPU utilization	for five	seconds:	14%,	one minute:	11%,	five	minutes:	13%
Core 6:	CPU utilization	for five	seconds:	9%,	one minute:	20%,	five	minutes:	23%
Core 7:	CPU utilization	for five	seconds:	5%,	one minute:	8%,	five	minutes:	18%

Pid	PPid	5Sec	1Min	5Min	Status	Size	Name
19056	19037	99%	99%	99%	R	7525896	wncd_0
21922	21913	96%	77%	79%	R	127488	smand
19460	19451	37%	34%	33%	R	6363828	wncd_2
19604	19596	18%	19%	18%	R	4556132	wncd_3

Ignore ucode_pkt_PPE0 for 9800-CL/9800-L

Datapath Utilization

- Exception : 9800-CL & 9800-L
- Both have dedicated CPU cores DP

#show platform hardware chassis active qfp datapath utilization sum

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

Dataplane Statistics

#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

Other Device Connectivity

Connectivity – Mobility

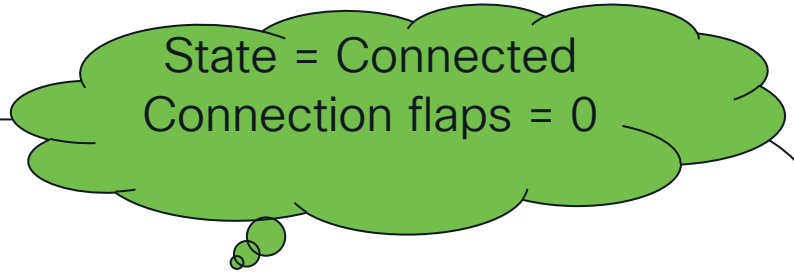
#sh wireless mobility summary

Wireless Management VLAN: 25
Wireless Management IP Address: 192.168.25.25
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: eWLC3
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility MAC Address: 001e.f62a.46ff
Mobility Domain Identifier: 0x2e47

Controllers configured in the Mobility Domain:

IP	Public Ip	MAC Address	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU
192.168.25.25	N/A	001e.f62a.46ff	eWLC3	0.0.0.0	::	N/A	N/A
192.168.5.35	192.168.5.35	00b0.e1f2.f480	9800-2	0.0.0.0	::	Up	1385
192.168.25.23	192.168.25.23	706d.1535.6b0b	Vewlc	0.0.0.0	::	Control And Data Path Down	
192.168.25.33	192.168.25.33	f4bd.9e57.ff6b	8500	0.0.0.0	::	Up	1005

Connectivity – Telemetry



Vewlc#show telemetry connection all

Telemetry connections

Index	Peer Address	Port	VRF	Source Address	State	State Description
84	192.168.0.105	25103	0	192.168.40.10	Active	Connection up

Vewlc #show telemetry internal connection 84 detail

Telemetry protocol manager stats:

Con str : 192.168.0.1Te05:25103:0:192.168.40.10
Sockfd : 103
Protocol : tls-native
State : CNDP_STATE_CONNECTED
..
Version : TLSv1.2
..
Msgs Received : 0
Creation time: : Wed Dec 14 18:19:43:761

Last connected time: : Wed Dec 14 18:19:43:910
Last disconnect time: :
Last error: :
Connection flaps: : 0
Last flap Reason: :
Keep Alive Timeouts: : 0
Last Transport Error : No Error

Client Status

Client Stats

9800-cl#sh wireless stats client detail

```
Total Number of Clients : 30
----------------------------------------
Protcol                Client Count
 802.11b                   : 0
 802.11g                   : 0
 802.11a                   : 0
 802.11n-2.4GHz            : 0
 802.11n-5 GHz             : 0
 802.11ac                  : 0
 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 : 0
Excluded Clients: 0
Disabled Clients: 0
Foreign Clients : 0
Anchor Clients  : 0
Local Clients   : 0
Idle Clients    : 0
Locally Administered MAC Clients: 0
```

```
client state statistics:
------------------------------------------------

Average Time in Each State (ms)
  Associated State    : 1
  L2 State       : 16
  Mobility State : 6
  IP Learn State : 386
  L3 Auth State   : 0


------------------------------
AP Deletes
------------------------------
When client is sending disassociation                    : 0
Idle timeout                                             : 11
Client ACL mismatch                                      : 0
AP authentication stop                                   : 0
Association expired at AP                                : 0
4-way handshake failed                                   : 0
DHCP timeout                                             : 0
Reassociation timeout                                    : 0
SA query timeout                                         : 0
Intra AP roam                                            : 0
Channel switch at AP                                     : 0
Bad AID                                                  : 0
```

Client Delete Reasons

vewlc3#show wireless stats client delete reasons

Total client delete reasons

Controller deletes

Datapath plumb	: 0
WPA key exchange timeout	**: 107**
802.11w MAX SA queries reached	: 0
DOT11 invalid FT IE	: 2
IP-LEARN connection timeout	**: 690**
WPA group key update timeout	: 15

Client Tech Support

vewlc3#show tech-support wireless client mac-address <Client MAC>

- Client Detail
- Mobility Stats
- Radius Stats
- Control & Dataplane Stat
- Plumbing drops

Client Tech Support

```
---------- show wireless client mac-address 001C.BFF6.2E30 stats mobility ----------

Mobility event statistics:
    Joined as                          :
        Local                          : 1
        Foreign                        : 0
        Export foreign                 : 0
        Export anchor                  : 0
    Delete                             :
        Local                          : 0
        Remote                         : 0
    Role changes                       :
        Local to anchor                : 0
        Anchor to local                : 0
    Roam stats                         :
        L2 roam count                  : 0
        L3 roam count                  : 0
        Flex client roam count         : 0
        Inter-WNCd roam count          : 0
        Intra-WNCd roam count          : 0
        Remote cntrl move count        : 0
        Remote inter-cntrl roam count  : 0
        Remote WebAuth pending roams   : 0
    Anchor Request                     :
        Sent                           : 0
          Grant received               : 0
          Deny received                : 0
        Received                       : 0
          Grant sent                   : 0
          Deny  sent                   : 0
    Handoff Status Received            :
        Success                        : 0
        Group mismatch                 : 0
        Client unknown                 : 0
        Client blacklisted             :
        SSID mismatch                  : 0
        Denied                         : 0
        L3 Vlan Override               : 0
        Unknown peer                   : 0
```

```
------------------- show radius statistics -------------------

                                      Auth.       Acct.       Both
          Maximum inQ length:           NA          NA          0
        Maximum waitQ length:           NA          NA          2
        Maximum doneQ length:           NA          NA          0
        Total responses seen:            0           0          0
     Packets with responses:             0           0          0
  Packets without responses:             5           0          5
  Access Rejects           :             0
  Access Accepts           :             0
 Average response delay(ms):             0           0          0
 Maximum response delay(ms):             0           0          0
  Number of Radius timeouts:            26           0         26
       Radius Timers Started:           27           0         27
       Radius Timers Created:           27           0         27
Radius Timers Create Failed:             0           0          0
       Radius Timers Stopped:           26           0         26
  Radius Timers Stop Failed:             0           0          0
  Radius Timers Outstanding:             1           0          1
        Radius Timers Added:            27           0         27
   Radius Timers Add Failed:             0           0          0
    Radius Timers Jitterred:             0           0          0
Radius Timers Jitter Failed:             0           0          0
       Duplicate ID detects:             0           0          0
 Buffer Allocation Failures:             0           0          0
Maximum Buffer Size (bytes):           414           0        414
Malformed Responses        :             0           0          0
Bad Authenticators         :             0           0          0
Unknown Responses          :             3           0          3
 Source Port Range: (2 ports only)
 1645 - 1646
 Last used Source Port/Identifier:
 1645/0
```

```
Client Details for client cpp_if_handle: 0x40
  Name                  : WLCLIENT-IF-0x00a0000001
  Mac Addr              : 001c.bff6.2e30
  pal_if_handle         : 0xa0000001
  Mobility State        : LOCAL
  Multicast Action      : FORWARD
  MDNS Mode             : DROP
  Auth State            : RUN
  Vlan                  : 90
  SSID                  : C65_Open
  Point of Attachment   : CAPWAP-IF-0x90000005
  EoGRE Client          : N
  Link-local Enabled    : false
  Link-local Vlan       : 0
  Instance id           : 3
  Client Type           : NORMAL
  Mcast Vlan            : 0
  Point of Presence     : NULL
  BSSID Mac             : d4e8.8019.f060
  Radio Id              : 0
  Global WLAN ID        : 1
  VLAN Override         : false
  IPSG Flag             : 0
  P2P Type              : BLOCKING DISABLE
  iPSK Tag              : 0
  Zone ID               : 0
  Input UIDB            : 0X176C3
  Output UIDB           : 0X176C0
  WLAN Input UIDB       : 0XFFFFFFFF
  WLAN Output UIDB      : 0XFFFFFFFF
  AVC enable            : false
  FQDN filter enable    : false
  FQDN filter Id        : 0
  Umbrella Profile Id   : 0
  sgacl enforcement     : false
```

Client Debug bundle

Client Debug Bundle

- Client RA + Client Tech Support

 # debug wireless bundle client <Client mac 1 .... Client mac 5>
no debug wireless bundle client <Client mac 1 .... Client mac 5>

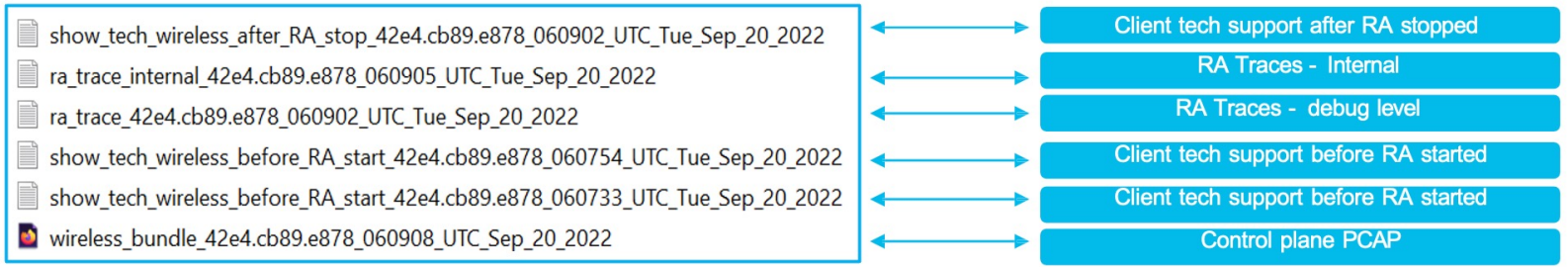
- With EPC Capture

 # debug wireless bundle start epc monitor-time <seconds>
debug wireless bundle client stop-all collect-all

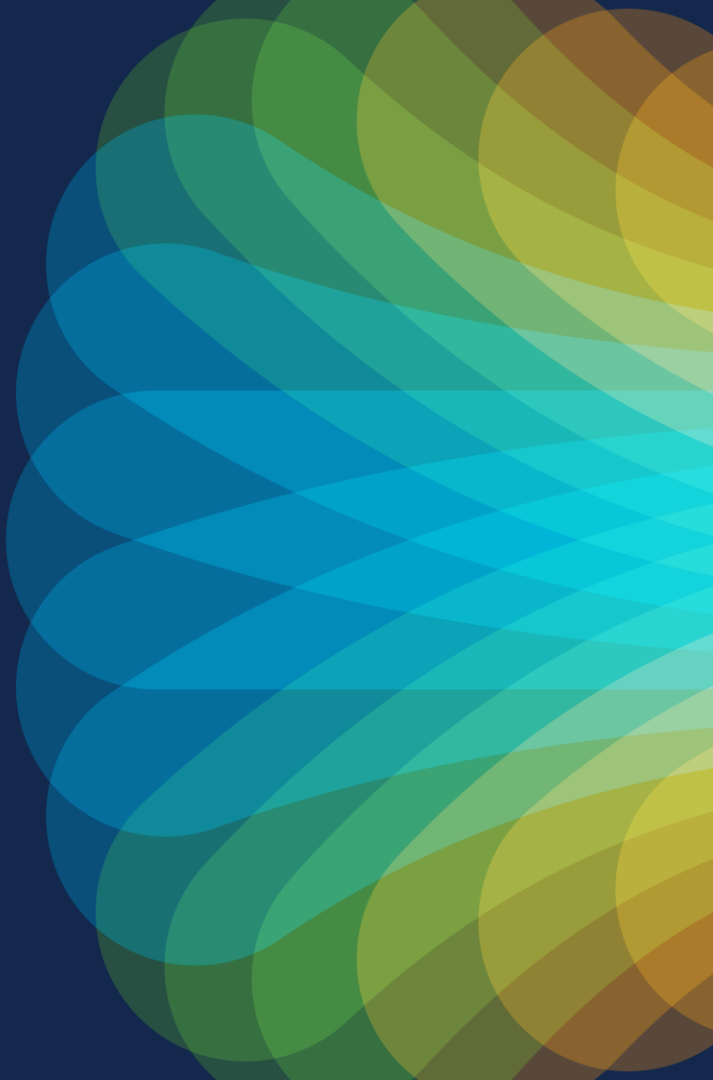
Note : Client mac should be in xxxx.xxxx.xxxx format
Bundle name is highlighted by wlc, when 'no debug' is run

Bundle Contents

- RA traces
- Show tech support for client
- WLC Control Plane Capture



Automate Troubleshooting



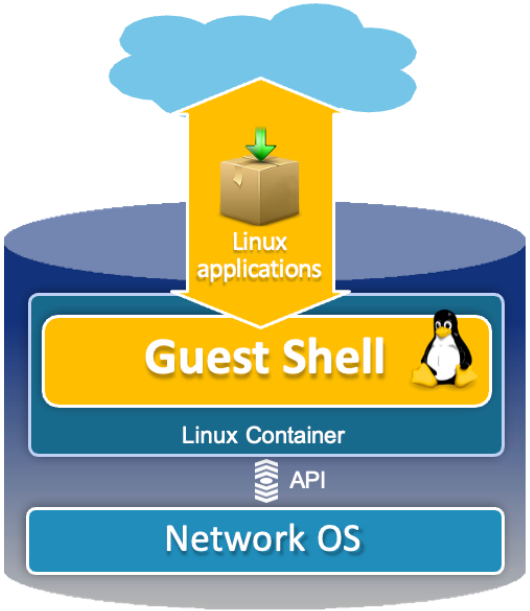
Automation

- KPI can be scripted
- Simple TTL or EEM or Automation using Python
- WLAN Poller
- Advantages –
  - Memory – Leak, Buffer shortage
  - Queue drops
  - Data Plane drops
  - Data Plane – Control Plane communication drops
  - Many other unknown issues

Guestshell & EEM

What is Guestshell ?

- 64-bit Linux environment running on IOS XE and NX-OS platforms
- Install, update and operate 3rd party Linux apps (e.g., Puppet, Chef, Splunk)
- Bundled with Python
- Intended for agent or script hosting

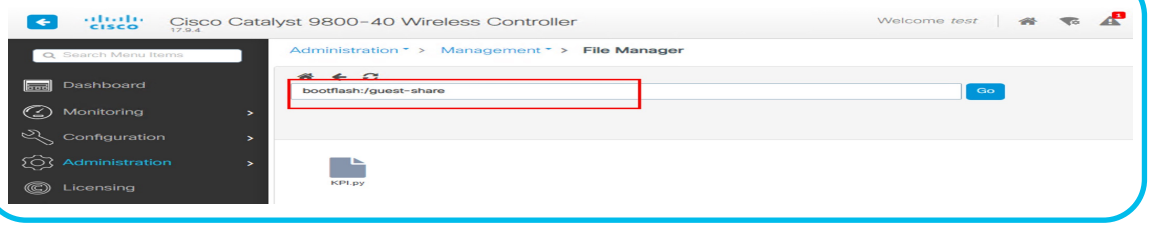


How to Set it Up ? – 3 Simple Steps !!

Enable

```
iox
    app-hosting appid guestshell
    app-vnic management guest-interface 0
    end
```

Copy



Execute

Gladius1#*guestshell run python3 /bootflash/guest-share/KPI.py*
Exported files Gladius1-Oct-07-2023-18-26.txt to destination tftp://192.168.10.45/lkasturi/

Event Manager

- Available in switches/routers and now in 9800 WLCs trigger-based scripts.
- Workarounds
- Automate data-collection
- Combine outputs or create commands

Documentation :

General Information

IOS-XE EEM

Best Practices

Combination of Guestshell & EEM

- Combine EEM with Guestshell using EEM trigger-based scripts
- Create Scripts to automate data-collection
- Run script periodically or On-Demand

Script to capture continuous PCAP from WLC

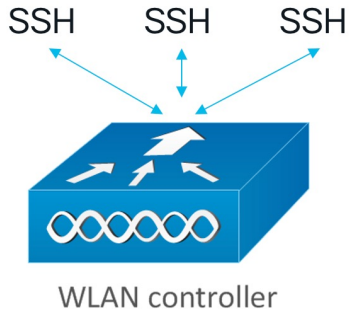
```
event manager applet Continuous_packet_capture
event timer watchdog name timer time 120
action 0.5 cli command "enable"
action 1.0 cli command "guestshell run python3 /bootflash//guest-
share/Continuous_packet_capture.py"
```

WLAN Poller

What is WLAN Poller

- Task automation against Controller/APs
- Simplify data collection across large groups of Aps/controllers
- Fully customizable
- Python bundle: No install required
- Not official product: Just for data collection, not for permanent use

Features



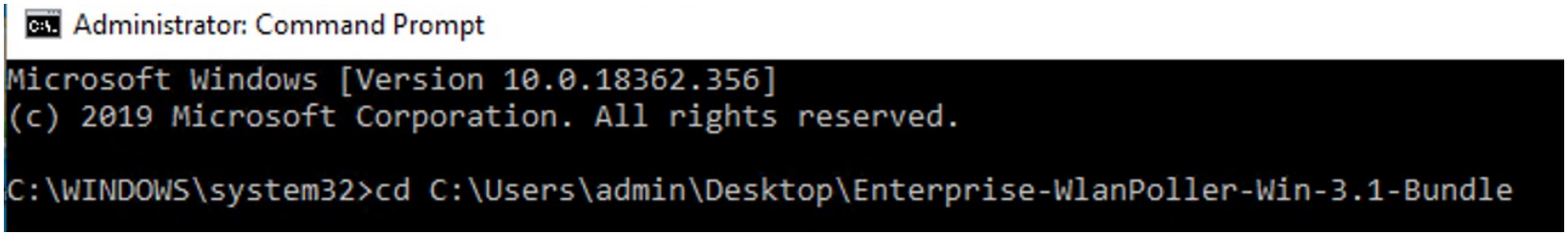
- Support for AireOS/9800 and any AP IOS/COS
- Bulk data/debug collection, including core/crashes, etc
- Command execution at regular intervals.
- AP/WLC DFS statistics and debug collection
- AP Flash health check
- AP cert check report
- Upgrade debug images on selected Aps
- Migrations support

How to Use ?

- Pick your Platform – Windows/MAC

  https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!wlan-poller-wlan-poller/download

- Windows
- In CMD,
  - Go to Filepath → Run wlanpoller.exe

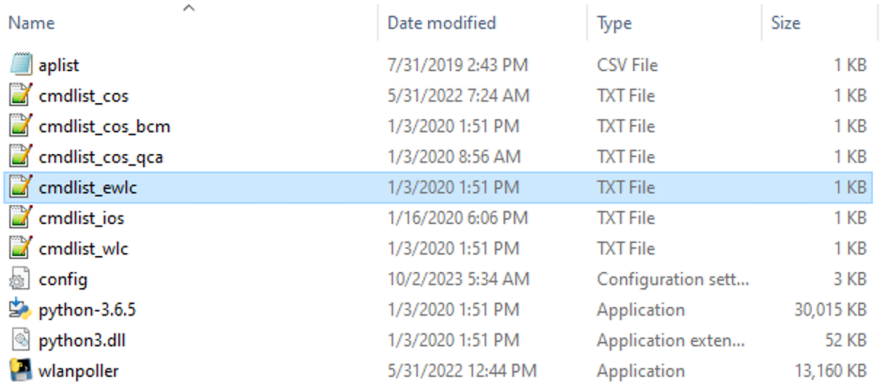


Configure – Config.ini

```
[General]
# Label
label = test

; active value should be based on 1 == AirOS WLC, 2 == eWLC and False for failure.

wlc_type: 2

; config global mode for WLC and AP connection: "ssh" or "telnet"
mode: ssh
ap_mode: ssh

; set global WLC credentials
wlc_user: Test
wlc_pasw: 12345!
wlc_enable: 12345!

; set global AP credentials
ap_user: test
ap_pasw: 12345
ap_enable: 12345

; syslog address
syslog_server: self
; WLC sections must be named as [WLC-<wlcname>]
[WLC-1]
active: True
ipaddr: 10.104.172.194
mode: ssh

; tftp
tftp_addr: self
; data poller command lists
;cmdlist_wlc = cmdlist_wlc.txt
cmdlist_ewlc = cmdlist_ewlc.txt
;cmdlist_ios = cmdlist_ios.txt
;cmdlist_cos = cmdlist_cos.txt
;cmdlist_cos_qca = cmdlist_cos_qca.txt
;cmdlist_cos_bcm = cmdlist_cos_bcm.txt
```

Modify Command list

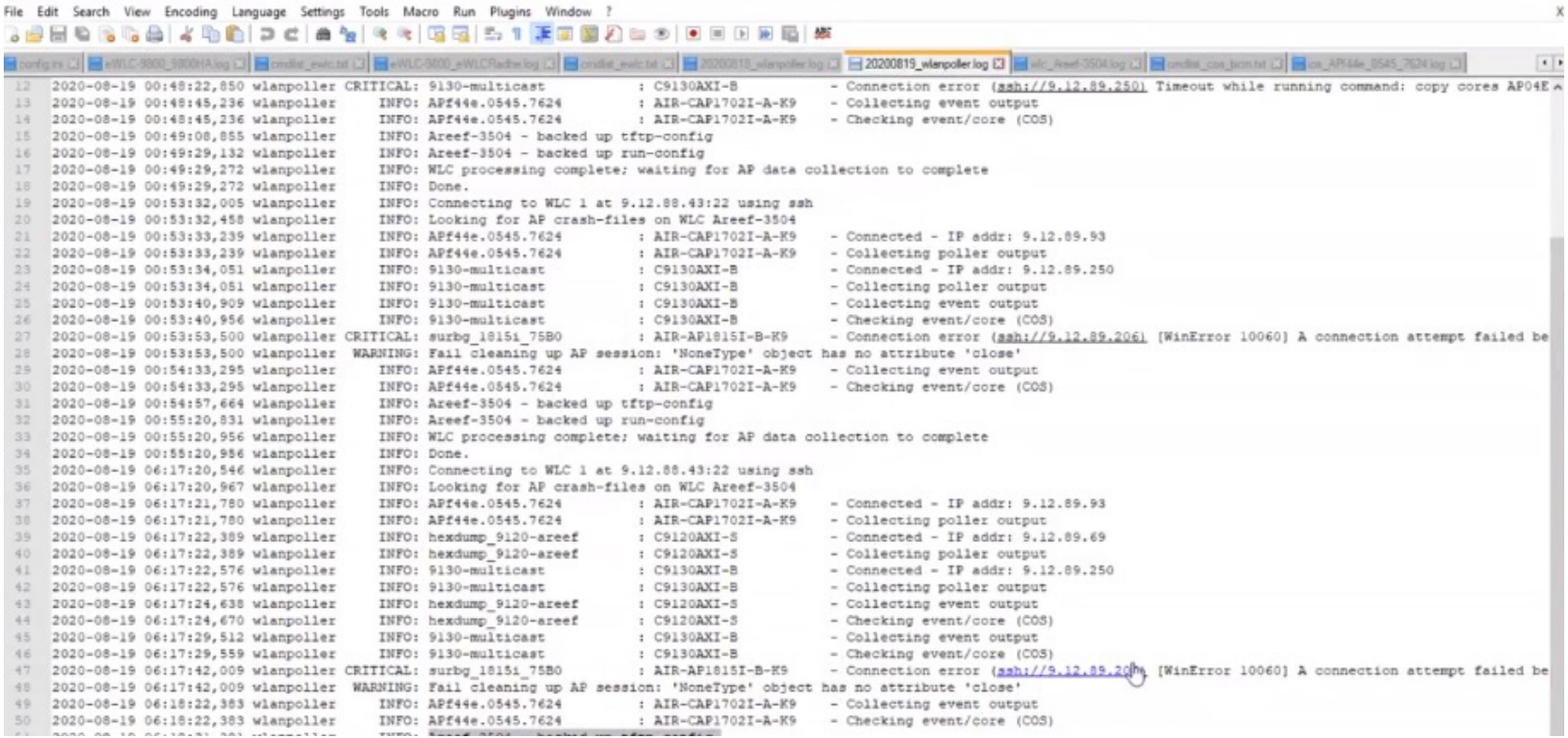
- Open corresponding “cmdlist_x.txt” file
- Add necessary commands



Name	Date modified	Type	Size
aplist	7/31/2019 2:43 PM	CSV File	1 KB
cmdlist_cos	5/31/2022 7:24 AM	TXT File	1 KB
cmdlist_cos_bcm	1/3/2020 1:51 PM	TXT File	1 KB
cmdlist_cos_qca	1/3/2020 8:56 AM	TXT File	1 KB
cmdlist_ewlc	1/3/2020 1:51 PM	TXT File	1 KB
cmdlist_ios	1/16/2020 6:06 PM	TXT File	1 KB
cmdlist_wlc	1/3/2020 1:51 PM	TXT File	1 KB
config	10/2/2023 5:34 AM	Configuration sett...	3 KB
python-3.6.5	1/3/2020 1:51 PM	Application	30,015 KB
python3.dll	1/3/2020 1:51 PM	Application exten...	52 KB
wlanpoller	5/31/2022 12:44 PM	Application	13,160 KB

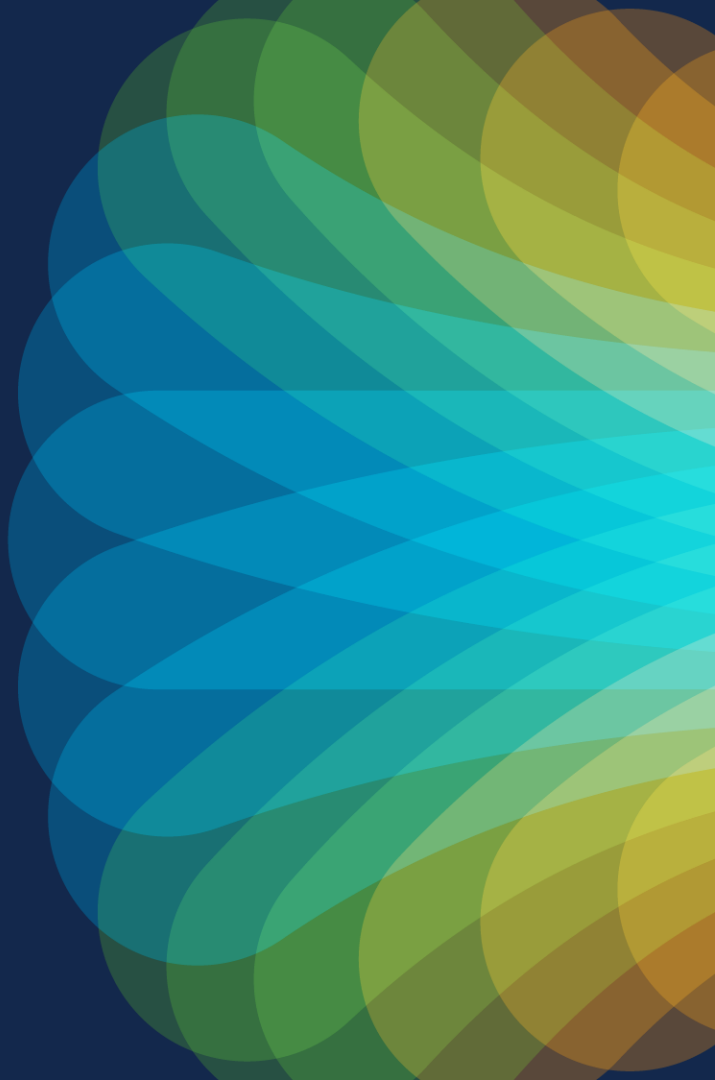
```
show clock
show memory summary
show memory details
show ap summary
show wireless stats ap join summary
show ap uptime
show ap crash-file
show wireless client summary
show wireless vlan details
show wlan summary
show ap config general
show interfaces summary
```

Wlan Poller Output Logs



```
2020-08-19 00:48:22,850 wlanpoller CRITICAL: 9130-multicast          : C9130AXI-B          - Connection error (ssh://9.12.89.250) Timeout while running command: copy cores AP04E
2020-08-19 00:48:45,236 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Collecting event output
2020-08-19 00:48:45,236 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Checking event/core (COS)
2020-08-19 00:49:08,855 wlanpoller     INFO: Areef-3504 - backed up tftp-config
2020-08-19 00:49:29,132 wlanpoller     INFO: Areef-3504 - backed up run-config
2020-08-19 00:49:29,272 wlanpoller     INFO: WLC processing complete; waiting for AP data collection to complete
2020-08-19 00:49:29,272 wlanpoller     INFO: Done.
2020-08-19 00:53:32,005 wlanpoller     INFO: Connecting to WLC 1 at 9.12.88.43:22 using ssh
2020-08-19 00:53:32,458 wlanpoller     INFO: Looking for AP crash-files on WLC Areef-3504
2020-08-19 00:53:33,239 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Connected - IP addr: 9.12.89.93
2020-08-19 00:53:33,239 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Collecting poller output
2020-08-19 00:53:34,051 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Connected - IP addr: 9.12.89.250
2020-08-19 00:53:34,051 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Collecting poller output
2020-08-19 00:53:40,909 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Collecting event output
2020-08-19 00:53:40,956 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Checking event/core (COS)
2020-08-19 00:53:53,500 wlanpoller CRITICAL: surbg_1815i_75B0        : AIR-AP1815I-B-K9    - Connection error (ssh://9.12.89.206) [WinError 10060] A connection attempt failed be
2020-08-19 00:53:53,500 wlanpoller  WARNING: Fail cleaning up AP session: 'NoneType' object has no attribute 'close'
2020-08-19 00:54:33,295 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Collecting event output
2020-08-19 00:54:33,295 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Checking event/core (COS)
2020-08-19 00:54:57,664 wlanpoller     INFO: Areef-3504 - backed up tftp-config
2020-08-19 00:55:20,831 wlanpoller     INFO: Areef-3504 - backed up run-config
2020-08-19 00:55:20,956 wlanpoller     INFO: WLC processing complete; waiting for AP data collection to complete
2020-08-19 00:55:20,956 wlanpoller     INFO: Done.
2020-08-19 06:17:20,546 wlanpoller     INFO: Connecting to WLC 1 at 9.12.88.43:22 using ssh
2020-08-19 06:17:20,967 wlanpoller     INFO: Looking for AP crash-files on WLC Areef-3504
2020-08-19 06:17:21,780 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Connected - IP addr: 9.12.89.93
2020-08-19 06:17:21,780 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Collecting poller output
2020-08-19 06:17:22,389 wlanpoller     INFO: hexdump_9120-areef      : C9120AXI-S          - Connected - IP addr: 9.12.89.69
2020-08-19 06:17:22,389 wlanpoller     INFO: hexdump_9120-areef      : C9120AXI-S          - Collecting poller output
2020-08-19 06:17:22,576 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Connected - IP addr: 9.12.89.250
2020-08-19 06:17:22,576 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Collecting poller output
2020-08-19 06:17:24,638 wlanpoller     INFO: hexdump_9120-areef      : C9120AXI-S          - Collecting event output
2020-08-19 06:17:24,670 wlanpoller     INFO: hexdump_9120-areef      : C9120AXI-S          - Checking event/core (COS)
2020-08-19 06:17:29,512 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Collecting event output
2020-08-19 06:17:29,559 wlanpoller     INFO: 9130-multicast          : C9130AXI-B          - Checking event/core (COS)
2020-08-19 06:17:42,009 wlanpoller CRITICAL: surbg_1815i_75B0        : AIR-AP1815I-B-K9    - Connection error (ssh://9.12.89.206) [WinError 10060] A connection attempt failed be
2020-08-19 06:17:42,009 wlanpoller  WARNING: Fail cleaning up AP session: 'NoneType' object has no attribute 'close'
2020-08-19 06:18:22,383 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Collecting event output
2020-08-19 06:18:22,383 wlanpoller     INFO: APf44e.0545.7624        : AIR-CAP1702I-A-K9   - Checking event/core (COS)
```

Automate Log analysis



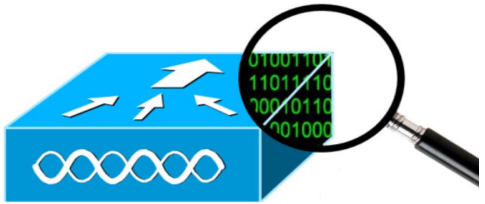
Tools to Automate Analysis

- Wireless Config Analyzer Express – WCAE
- Debug Analyzer
- WiFi Hawk
- WalkMe – On device Intelligence

WCAE -Wireless Config Analyzer Express

Wireless Config Analyzer Express

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



Wireless Config Analyzer Express

Wireless Health Check

- Best Practices Score
- Configuration Highlights
- Upgrade Advisor
- Tag/Policy usage
- Log Summarization
- Ap inventory
- AP Config view

RRM Health

- RF Health Analysis
- RF Stats Summarization
- Channel Stats
- RRM analysis
- NDP AP summarization
- AP RF view

Client Audit

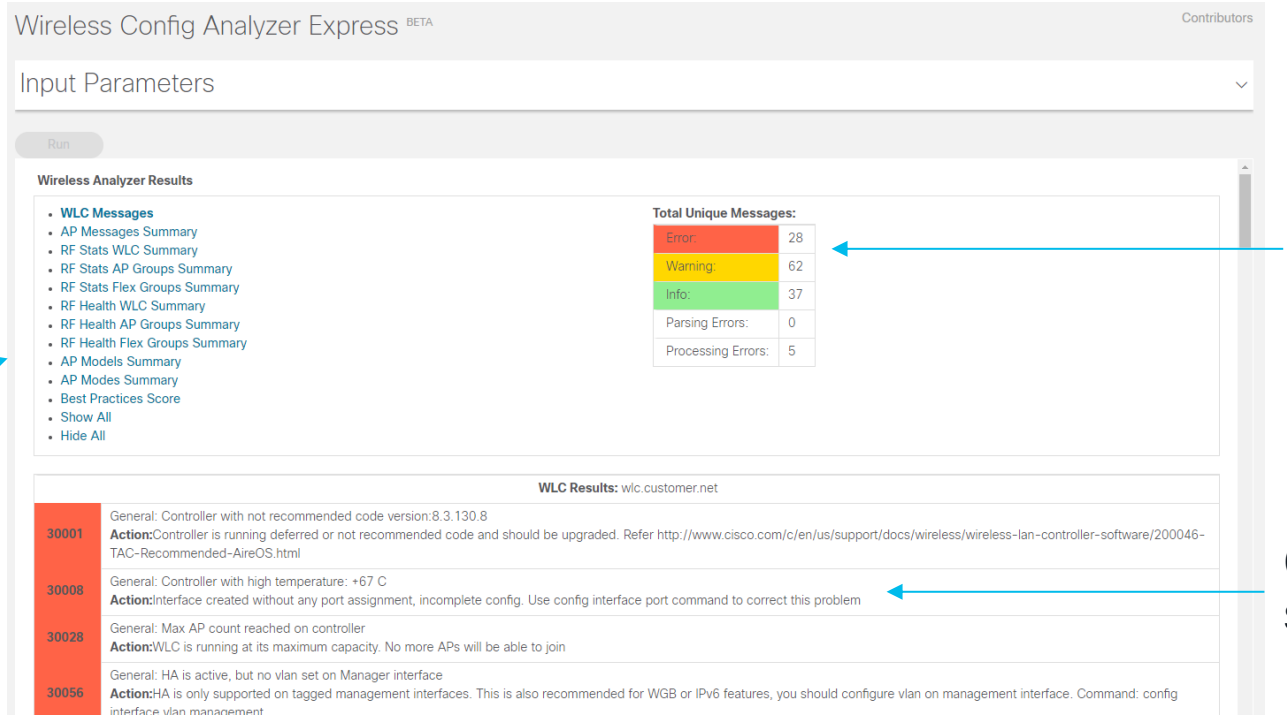
- 8821
- iPhone
- Drager
- Vocera
- Spectralink

Input Files – Best Methods

You can upload a Zip!

- Tool supports:
  - “sh run-config” ← AireOS
  - “sh tech wireless” ← 9800/EWC
- In AireOS
  - SSH with config paging disabled
  - Use: transfer upload datatype run-config (max 32MB)
- In IOS-XE
  - SSH and collect all output
  - Debug bundle, add the command “show tech wireless”

WCAE Interface



Menu Area

Message Counts

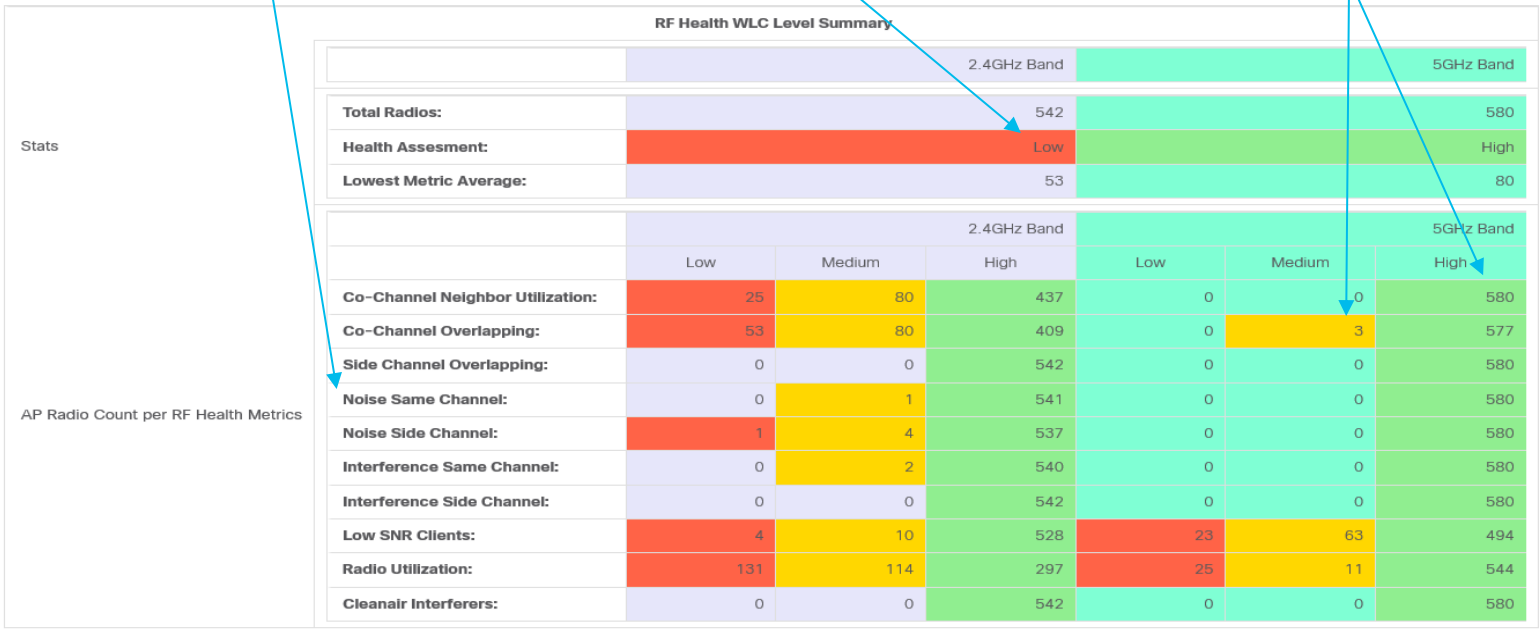
Open summary

WCAE – RF Health

Individual Metrics

General Evaluation

Total Radios per level



RF Health WLC Level Summary

Stats

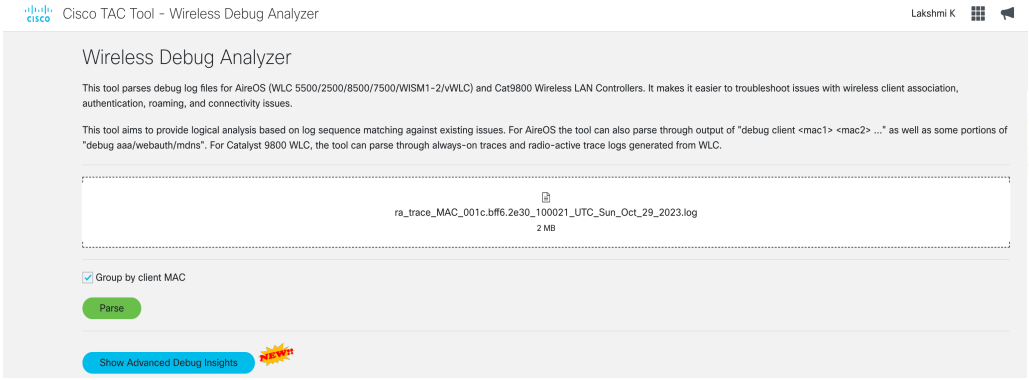
	2.4GHz Band	5GHz Band
Total Radios:	542	580
Health Assesment:	Low	High
Lowest Metric Average:	53	80

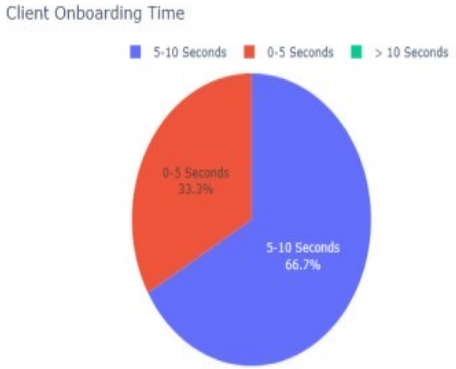
AP Radio Count per RF Health Metrics

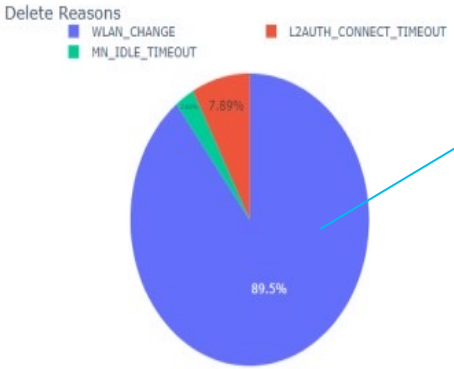
	2.4GHz Band			5GHz Band		
	Low	Medium	High	Low	Medium	High
Co-Channel Neighbor Utilization:	25	80	437	0	0	580
Co-Channel Overlapping:	53	80	409	0	3	577
Side Channel Overlapping:	0	0	542	0	0	580
Noise Same Channel:	0	1	541	0	0	580
Noise Side Channel:	1	4	537	0	0	580
Interference Same Channel:	0	2	540	0	0	580
Interference Side Channel:	0	0	542	0	0	580
Low SNR Clients:	4	10	528	23	63	494
Radio Utilization:	131	114	297	25	11	544
Cleanair Interferers:	0	0	542	0	0	580

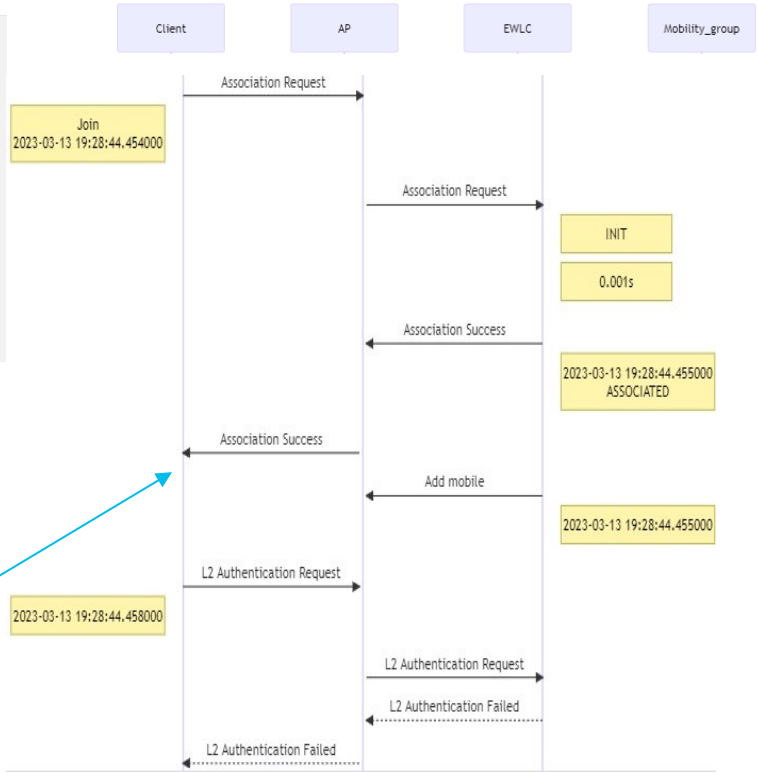
Debug Analzyer

Debug Analyzer









WiFi Hawk

Bird’s Eye view on Features

- Expert System to identify problems over from a wireless capture
  - Hard to see issues found in huge files
  - Low level protocol analysis
  - Interoperability problem
- Generate a summary of events per client and AP WLANs

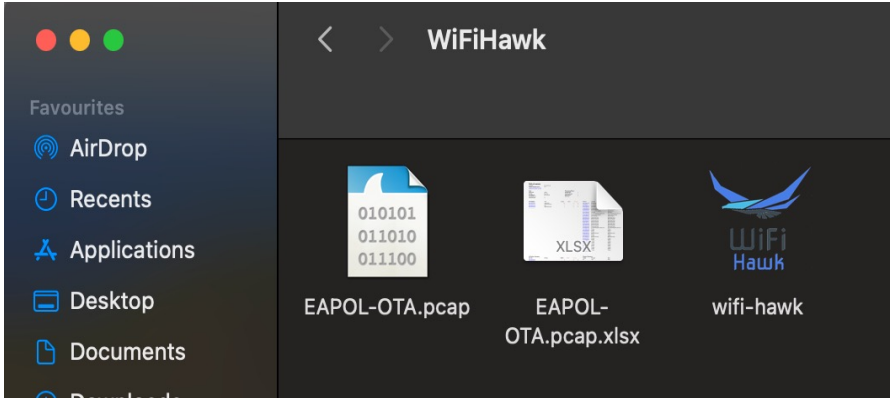
“Loose State Machine”

- Client has state machine to detect error transitions
  - No authentication
  - PSK failures
  - EAPoL negotiation errors
- Works even when capture is incomplete, or have missing frames

Desktop Version

WebEx Room

How to Use ?



	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 Measurement 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

Detecting easy to miss problems

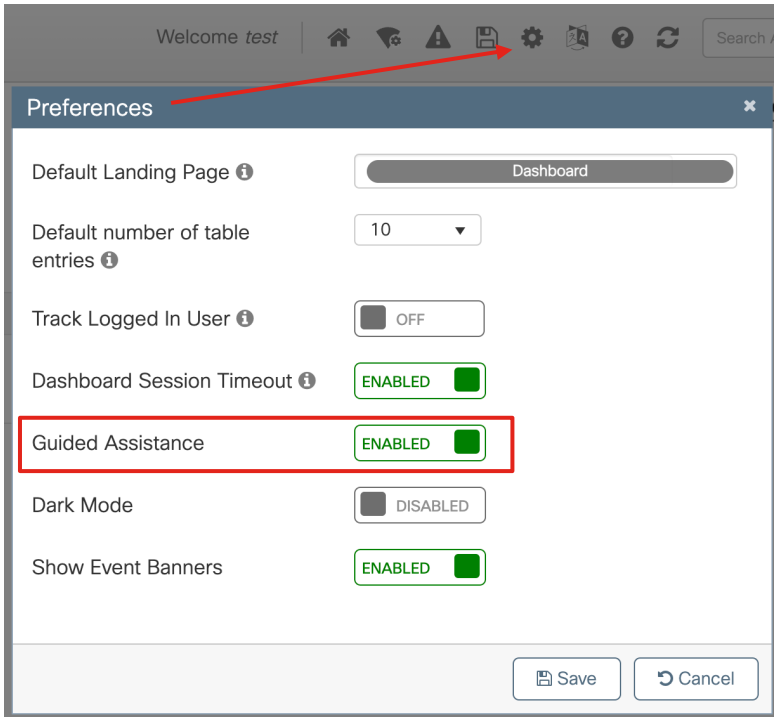
- Simplify finding issues across large captures
  - Unencrypted traffic leak (Client/AP)
  - Beacon loss
  - High Co-channel interference
  - Incorrect Data rates

Event Flow

Direction	Type	Severity	Frame	Time	Info
------	High Channel Utilization	Warning	1	Fri, 15 Mar 2019 21:05:05 CET	Current Channel utilization: 94
>>>>>>	First Beacon	Info	1	Fri, 15 Mar 2019 21:05:05 CET	
>>>>>>	Beacon loss	Warning	2	Fri, 15 Mar 2019 21:05:06 CET	Beacon loss detected, Time delta:0.824816
------	High Channel Utilization	Warning	2	Fri, 15 Mar 2019 21:05:06 CET	Current Channel utilization: 95
>>>>>>	Beacon loss	Warning	3	Fri, 15 Mar 2019 21:05:08 CET	Beacon loss detected, Time delta:1.427207
------	High Channel Utilization	Warning	3	Fri, 15 Mar 2019 21:05:08 CET	Current Channel utilization: 95
>>>>>>	Beacon loss	Warning	9	Fri, 15 Mar 2019 21:05:11 CET	Beacon loss detected, Time delta:3.523894
------	High Channel Utilization	Warning	9	Fri, 15 Mar 2019 21:05:11 CET	Current Channel utilization: 94
>>>>>>	Beacon loss	Warning	13	Fri, 15 Mar 2019 21:05:16 CET	Beacon loss detected, Time delta:4.612270
<<<<<<	EAP KEY RX	Info	6c:8b:d3:3b:8a:a0	1269 Thu, 21 Jan 2021 00:51:56 CET	EAPoL M1
<<<<<<	EAP KEY RX	Info	6c:8b:d3:3b:8a:a0	1271 Thu, 21 Jan 2021 00:51:56 CET	EAPoL M1
<<<<<<	EAP KEY RX	Info	6c:8b:d3:3b:8a:a0	1273 Thu, 21 Jan 2021 00:51:56 CET	EAPoL M1
>>>>>>	EAP KEY TX	Info	6c:8b:d3:3b:8a:a0	1330 Thu, 21 Jan 2021 00:51:56 CET	EAPoL M2
<<<<<<	Unencrypted AP TX Traffic	Error	6c:8b:d3:3b:8a:a0	1333 Thu, 21 Jan 2021 00:51:56 CET	AP defect, traffic sent without encryption
<<<<<<	EAP KEY RX	Info	6c:8b:d3:3b:8a:a0	1334 Thu, 21 Jan 2021 00:51:56 CET	EAPoL M3

Walk Me
On-Device Intelligence

WalkMe – Guided Conceptual Assistance

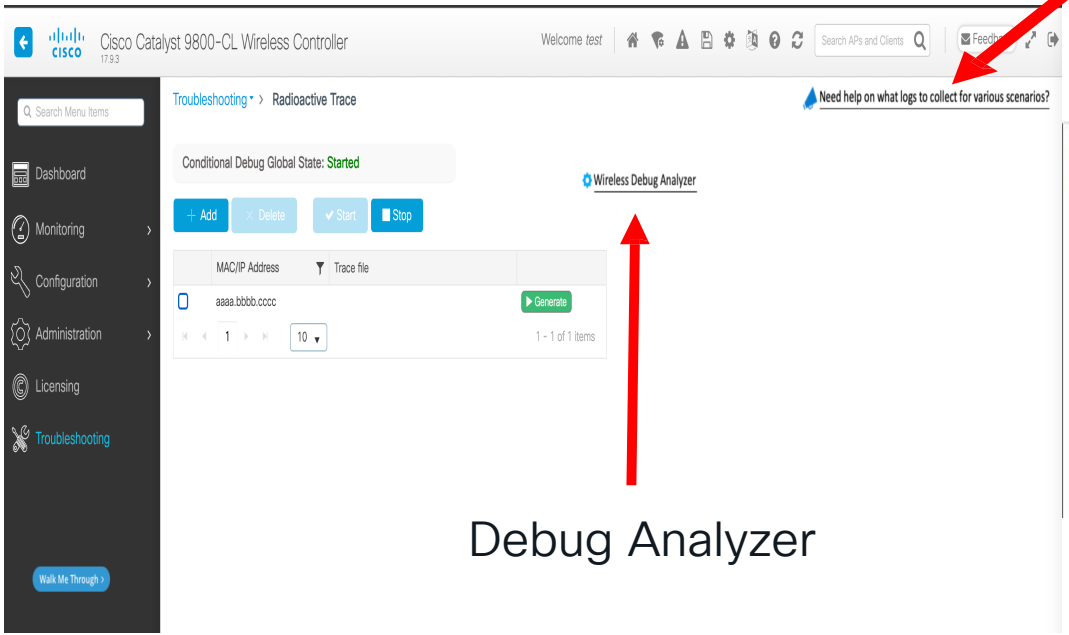


WalkMe – Guided Conceptual Assistance

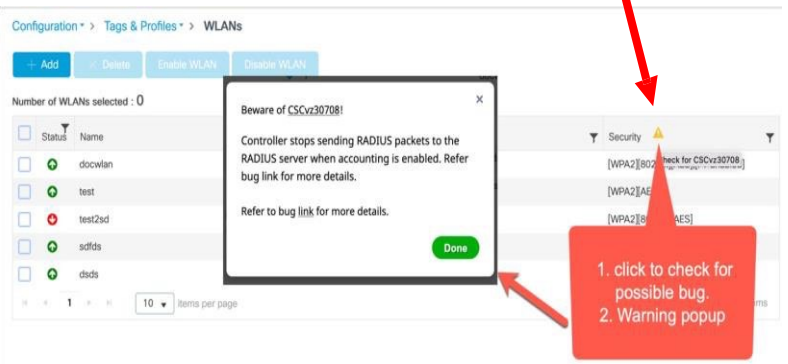
Enhancements & Warnings

Log Advisor

Critical Bug Warning



Debug Analyzer



Key Take Away

- Architecture
- Troubleshooting Techniques
  - Always on Tracing
  - RA & Conditional
- KPI Monitoring
  - Device
  - System
  - Client
- Automating Monitoring & Troubleshooting
  - Data Collection
    - Guestshell & EEM Scripts
    - WLAN Poller
  - Log Analysis Automation Tools
    - WCAE
    - Debug Analyzer
    - WiFi Hawk

cisco Live!

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am – 4:00pm**
Friday	**10:30am – 1:30pm**

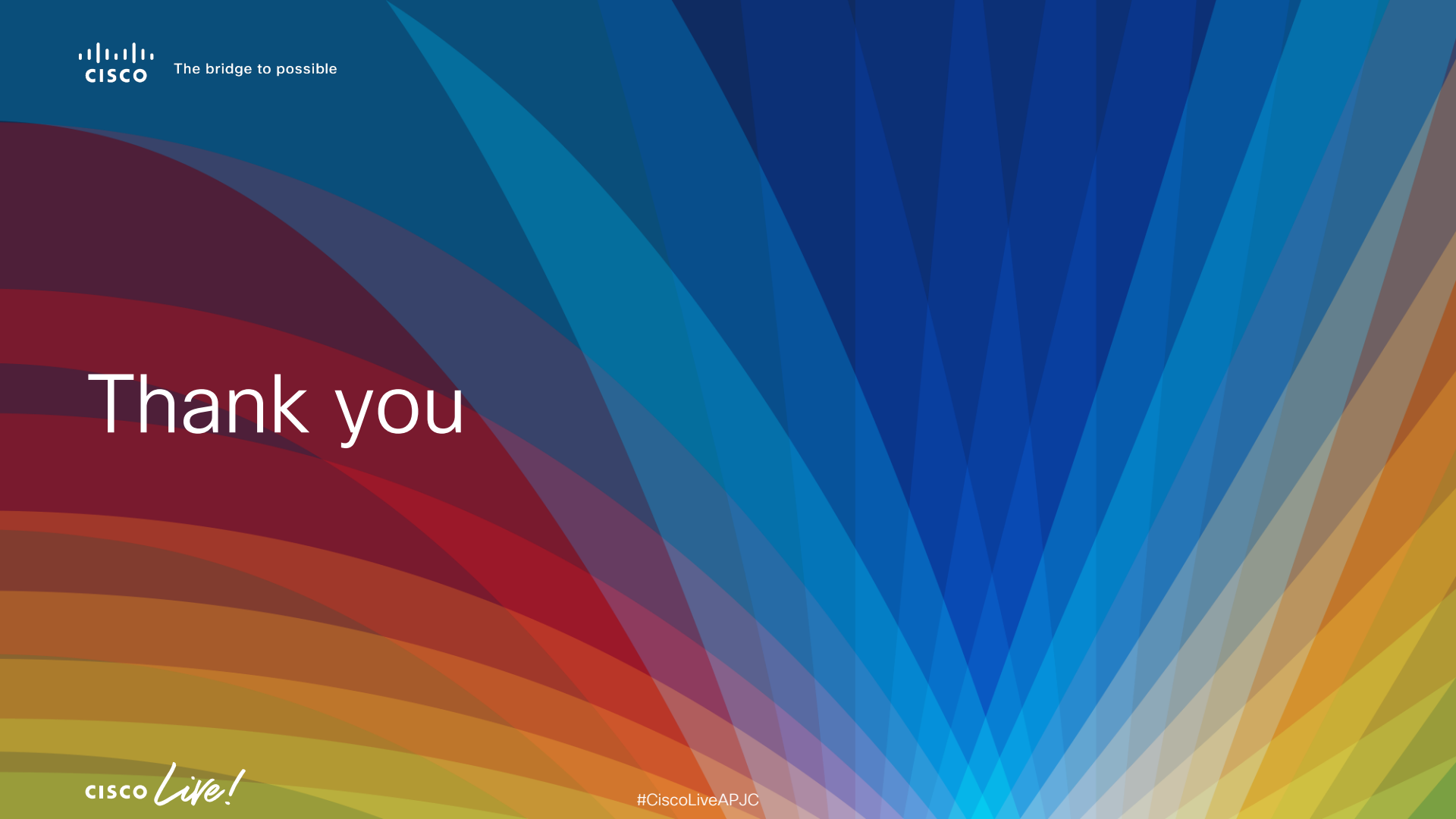
Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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
The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC

cisco Live!

Let's go

#CiscoLiveAPJC

Reference Slide

- Guestshell & EEM - https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!9800-guestshelleem-scripts-9800-guestshelleem-scripts/automated-archive-request-and-export
- WCAE - https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!wireless-config-analyzer-express/wireless-config-analyzer-express
- Wifi Hawk - https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!wifi-hawk