Mastering SD-Access Fabric Enabled Wireless

cisco Live !

Packet Walk and Deep Dive Troubleshooting – Like a TAC Engineer

Lakshmi Ganesh Kondaveeti
Senior Technical Leader, SDA/CATC

BRKEWN-3515

Webex App

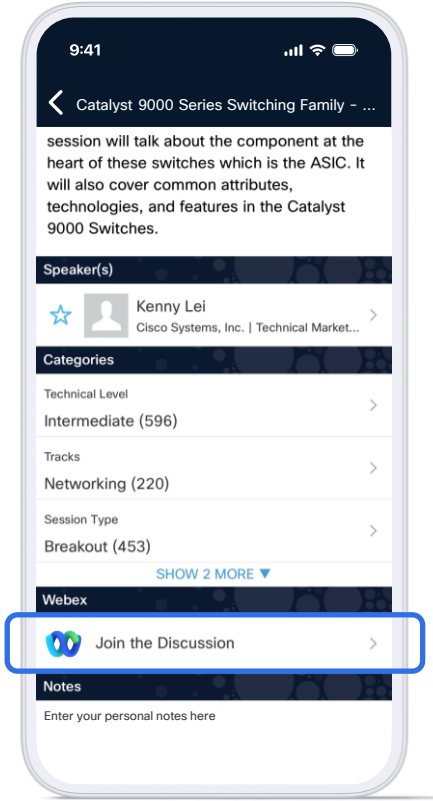
Questions?

Use Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 27, 2026.



Lakshmi Ganesh Kondaveeti (**LG**)

Professional Experience

- Overall 20 years with 15 years of TAC experience.
- Deep expertise in Enterprise Switching ,Routing and Cisco Catalyst Centre, SDA Fabric including wired and wireless
- Dual CCIE certified: Enterprise Infrastructure & Service Provider

Professional Role

- Senior Technical Leader - SDA Fabric , Catalyst Centre
- Passionate about building scalable, resilient, and future-ready networks

Key Highlight

- Cisco Inventor, 4 issued patents, with a strong focus on innovation and engineering excellence.

CISCO CERTIFIED CCIE ENTERPRISE

CISCO CERTIFIED CCIE SERVICE PROVIDER

CISCO INVENTOR -4-

WHY HOW WHAT

Please download the slides

Agenda

Architecture Overview

- Best Practices
- Design and Deployment

Basic Workflows and Troubleshooting

- AP Join
- Client Onboarding
- Client Roaming

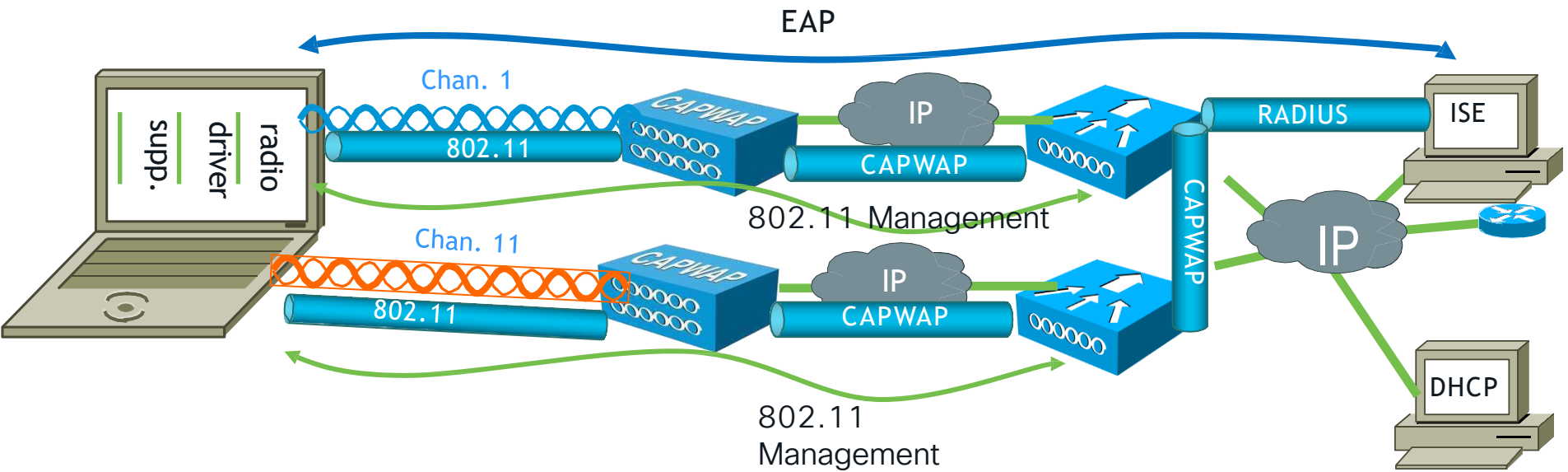
Some troubleshooting tools

*Some scenarios, useful commands & tools

*Appendix

Where do we start? Legacy Network?

Where do we start?



- ✓ Ease of Deployment
- ✓ Stretching the VLANs – Mobility
- ✓ Deploying the policy irrespective of IPs/IP Pools
- ✓ Network Segmentation

Overlay uses **alternate forwarding** attributes to provide additional services **Policy** is applied **irrespectively of network constructs** (VLAN, subnet, IP) Easily implement **Network Segmentation** (w/o implementing MPLS) Provide **L2 and L3 flexibility** (w/o stretching VLANs)

WITH A FABRIC…

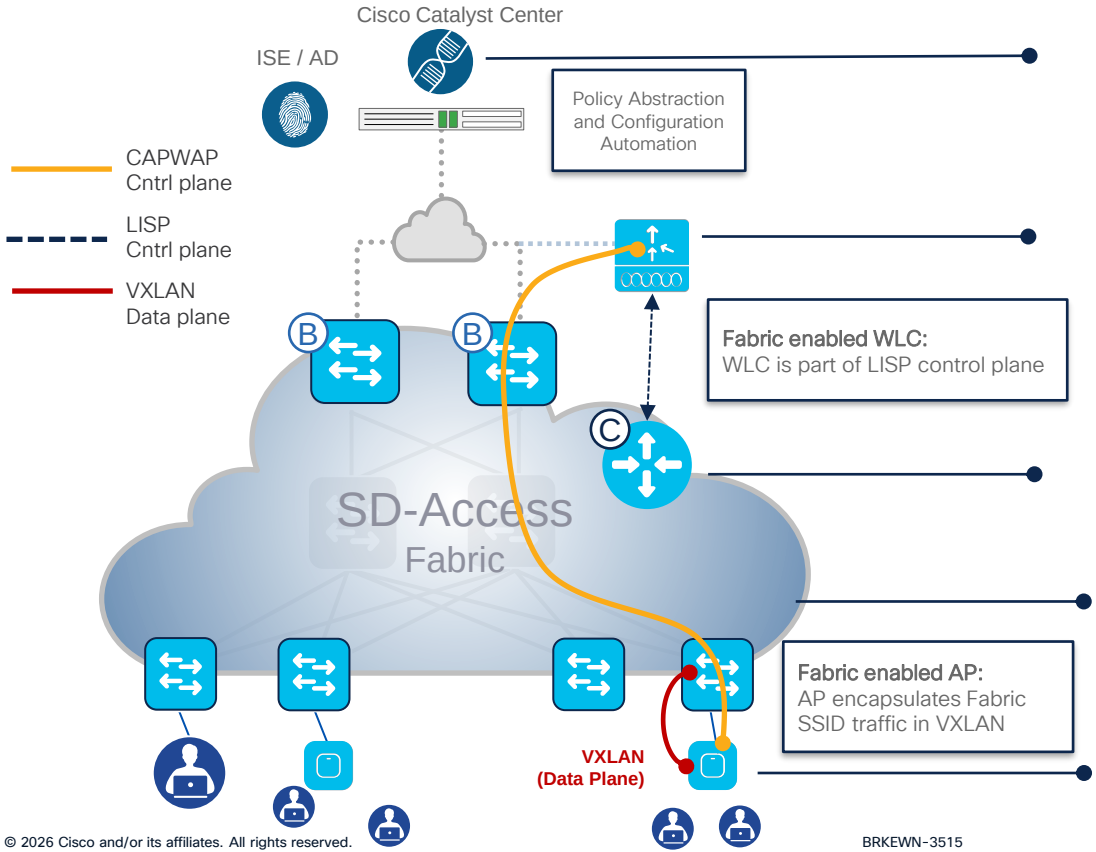
Key Assertion

If we could **“break the dependence”** between IP addressing and policy, we could **greatly simplify** networks – and make networks **much more functional.**

Brief intro of SDA Wireless Architecture

SD-Access Wireless Architecture

Simplify Control Plane and Optimizing the Data Plane



Automation
- Cisco Catalyst Center simplifies the Fabric deployment,
- Including the wireless integration component

Centralized Wireless Control Plane
- WLC still provides client session management
- AP Mgmt, Mobility, RRM, etc.
- Same operational advantages of CUWN

LISP control plane Management
- WLC integrates with LISP control plane
- WLC updates the CP for wireless clients
- Mobility is integrated in Fabric thanks to LISP CP

Optimized Distributed Data Plane
- Fabric overlay with Anycast GW + Stretched subnet
- VLAN extension with no complications
- All roaming is Layer 2

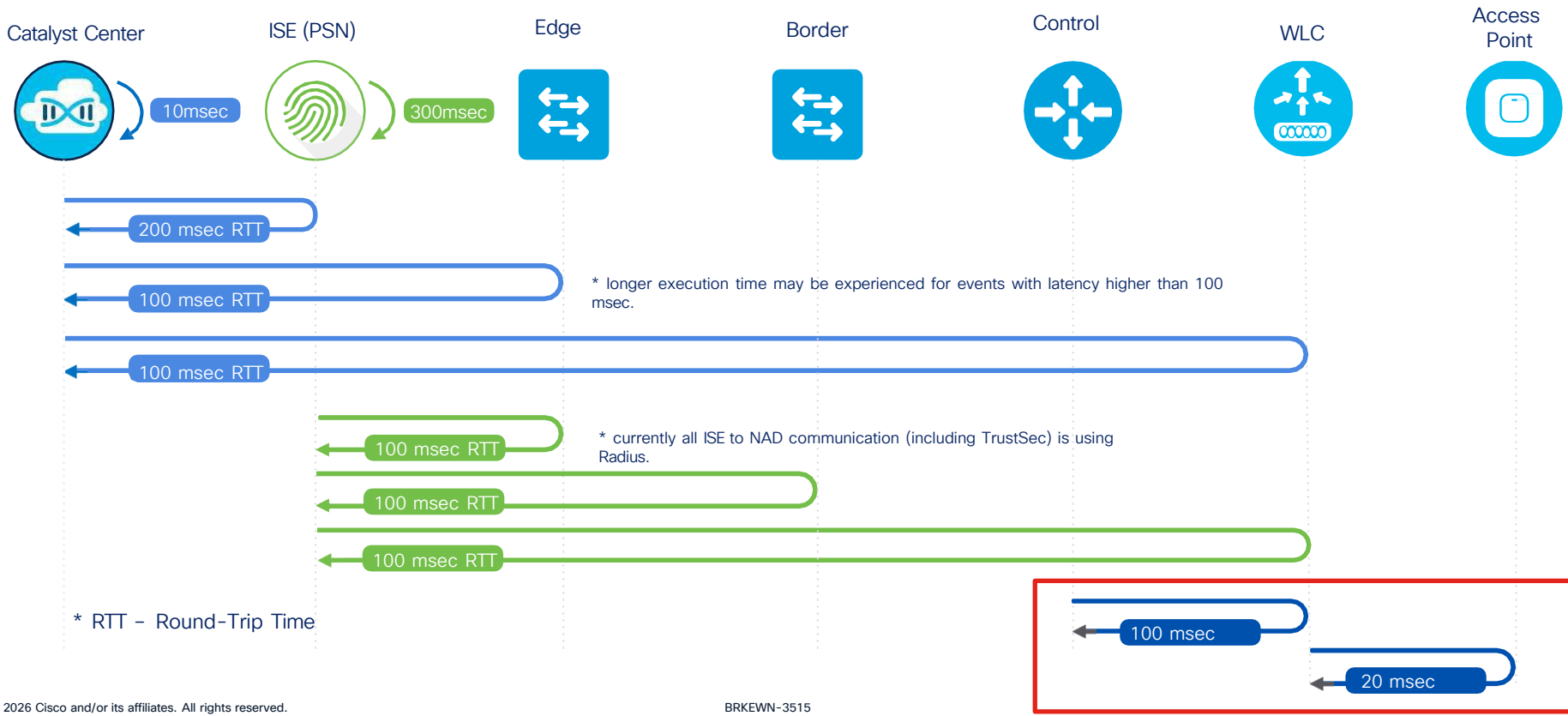
VXLAN from the AP
- Carrying hierarchical policy segmentation starting from the edge of the network

Quick overview of the design and deployment

Best practices

Cisco SD-Access Network Requirements

Latency Requirements (RTT)



Best Practices

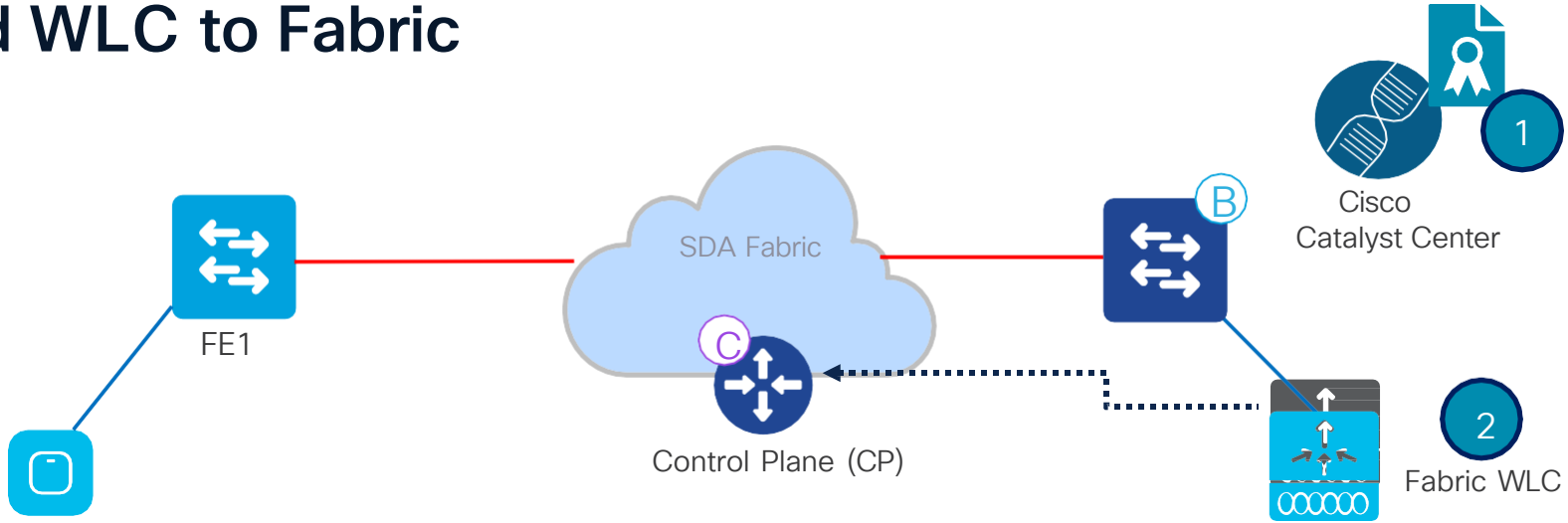
Quick verifications

There is a series of requirements in SD-access scenarios that is often a source of mistakes, so please verify first that these requirements are met .

- You have a specific route (and not using the default one) pointing to the WLC on the LISP control plane node
- Your APs are in the Infra VN, using the global routing table
- APs have connectivity to the WLC by pinging the WLC from the AP itself
- The fabric status of the control plane on the WLC is up
- The Wireless network profile and SSID is configured properly from Cisco Catalyst Center
- The Wireless IP Pools, AP and Client pools, are mapped against the respective Virtual Network (VN).
- The WLC and AP Provisioning is done.
- The APs are in fabric-enabled state.

Design and Deployment

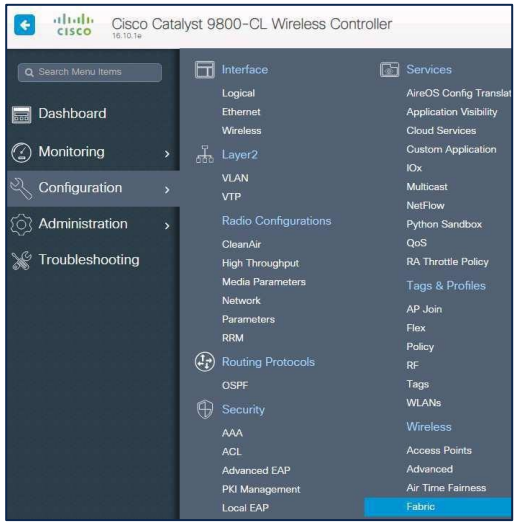
Add WLC to Fabric



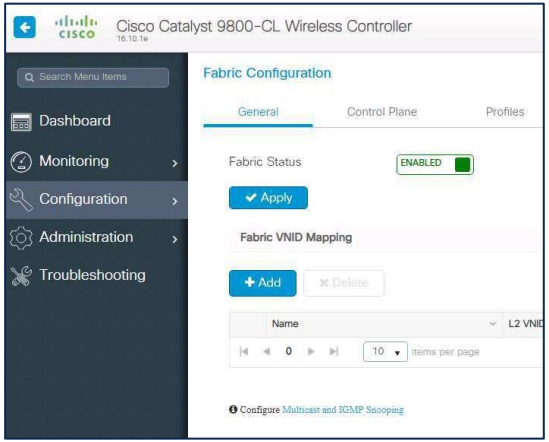
1. In Cisco Catalyst Center, first create the design, network settings, Wireless settings, discover, provision the WLC and then add it to the Fabric site
2. Fabric configuration is pushed to WLC. WLC becomes Fabric aware. Most importantly WLC is configured with credentials to established a secure connection to CP
3. WLC is ready to participate in SD-Access Wireless. Once AP(s) join the WLC and provisioned then those would be also part of SD-Access Wireless.

Add WLC to Fabric – Verify settings

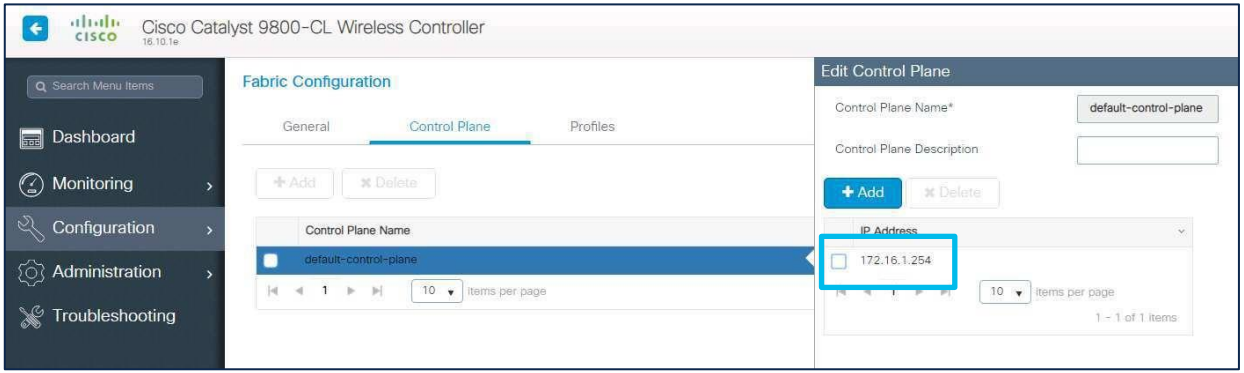
Configuration > Wireless > Fabric



Fabric status is enabled



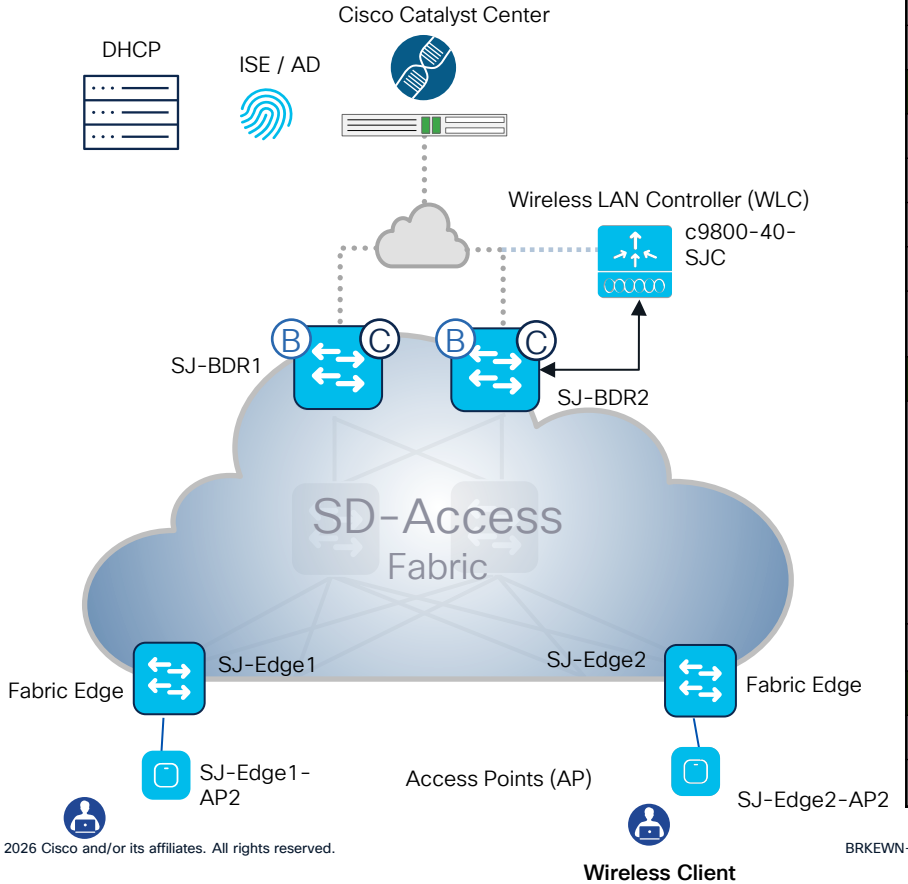
CP is correctly configured



SD-Access Wireless Basic Workflows

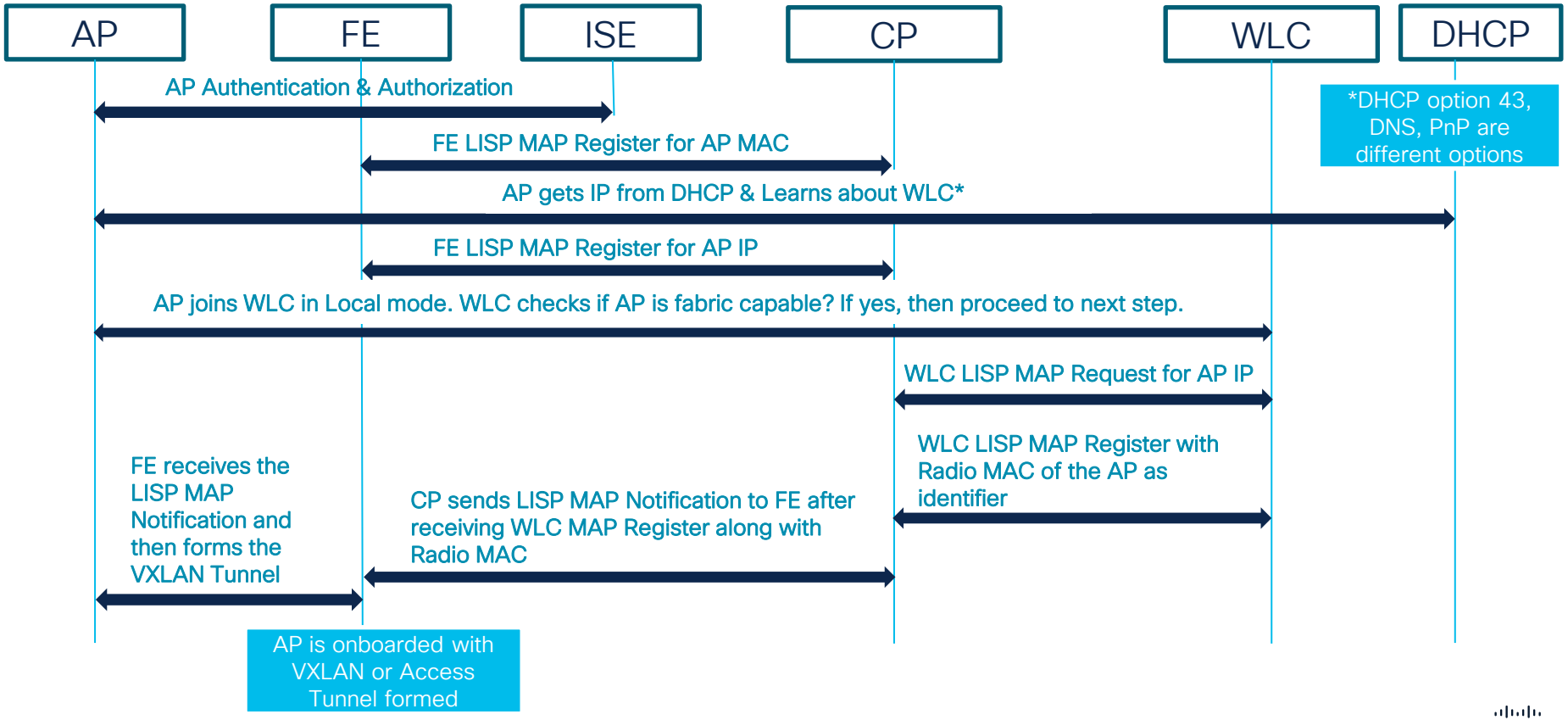
AP Join/Onboarding Flow

SD-Access Wireless Topology

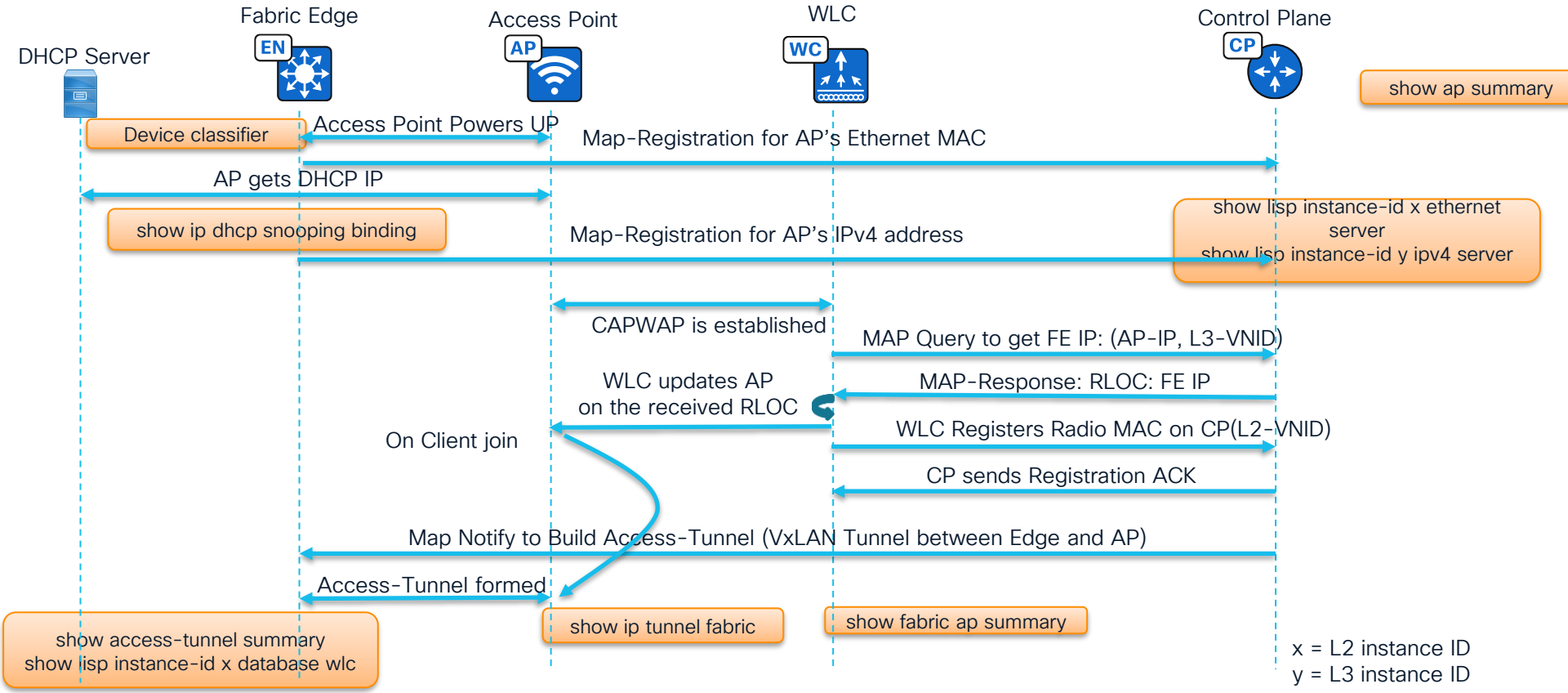


Nodes/Devices Details	IP/MAC Details
Cisco Catalyst Center (CatC)	10.127.84.3
Cisco Identity Services Engine (ISE)	10.127.84.5
DHCP	10.127.84.8
Fabric Devices	
Border/Control Plane - SJ-BDR1	10.127.84.100
Border/Control Plane - SJ-BDR2	10.127.84.101
Fabric Edge - SJ-Edge1	10.127.84.104
Fabric Edge - SJ-Edge2	10.127.84.105
Wireless LAN Controller (WLC) c9800-40-SJC	10.127.84.21
Access Points	
SJ-Edge2-AP2 (Connected to SJ-Edge2)	IP: 10.127.85.85 **Ethernet MAC:** 1006.edfc.2cdc **Radio MAC:** 889c.ade7.9880 (Used for AP Join) 889c.ade7.9881 (Fabric SSID)
SJ-Edge1-AP2 (Connected to SJ-Edge1)	IP: 10.127.85.83
Wireless Client	
IP Details	10.127.85.51
MAC Details	d037.45b7.5027

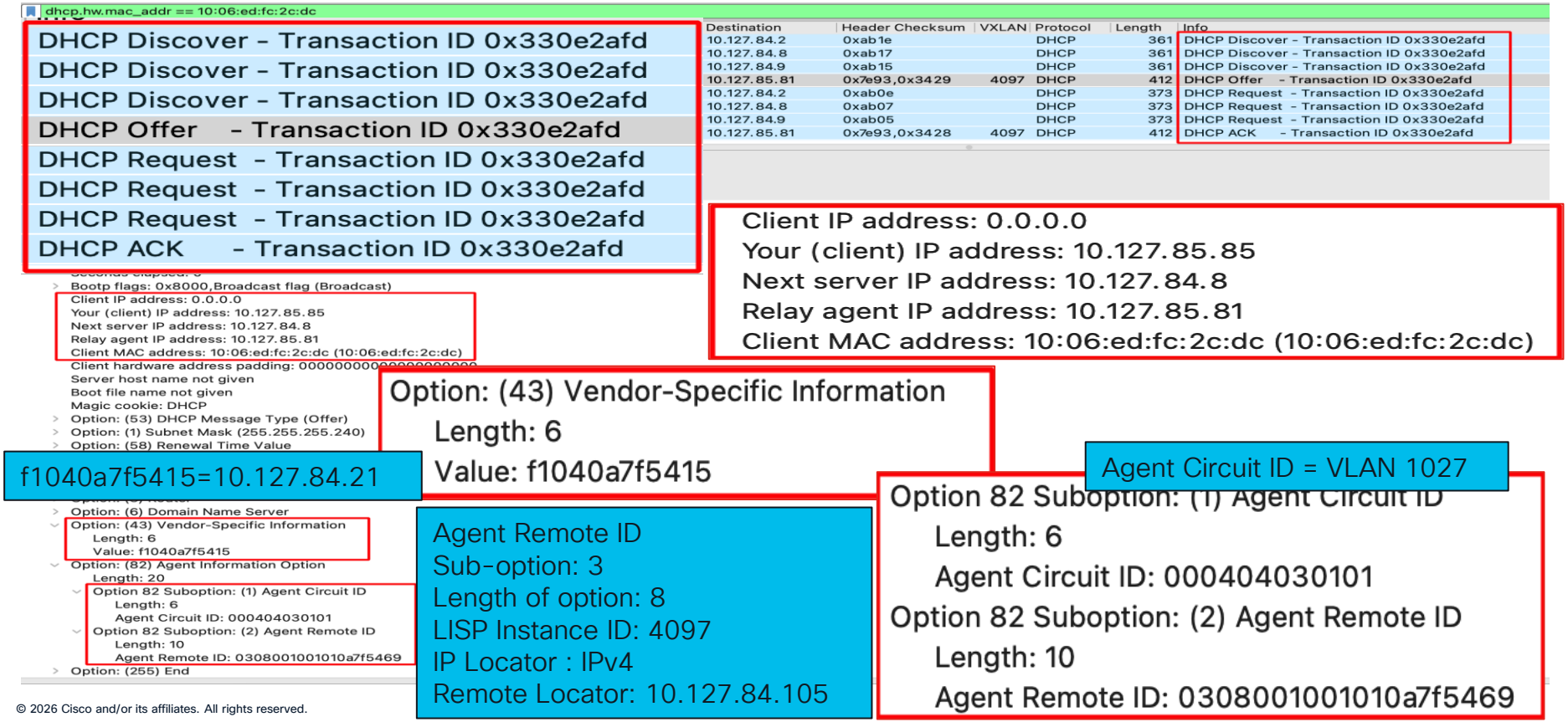
AP Onboarding Flow



Fabric AP Join Process



AP DHCP Flow – FE Uplink Captures



AP Joining WLC - WLC Captures

13912	2024-10-02 16:19:24.437965	0.265977s	10.127.85.85	10.127.84.21	0x628f	CAPWA...	298	CAPWAP-Control - Discovery Request[Malformed Packet]
13913	2024-10-02 16:19:24.437965	0.000000s	10.127.85.85	10.127.84.21	0x628f	CAPWA...	298	CAPWAP-Control - Discovery Request[Malformed Packet]
13914	2024-10-02 16:19:24.438972	0.001007s	10.127.84.21	10.127.85.85	0xbe8d	CAPWA...	147	CAPWAP-Control - Discovery Response
13915	2024-10-02 16:19:24.438972	0.000000s	10.127.84.21	10.127.85.85	0xbe8d	CAPWA...	151	CAPWAP-Control - Discovery Response
14362	2024-10-02 16:19:33.899947	0.243991s	10.127.85.85	10.127.84.21	0x6235	DTLSv1.2	272	Client Hello
14363	2024-10-02 16:19:33.899947	0.000000s	10.127.85.85	10.127.84.21	0x6235	DTLSv1.2	272	Client Hello
14364	2024-10-02 16:19:33.900939	0.000992s	10.127.84.21	10.127.85.85	0xb5a1	DTLSv1.2	94	Hello Verify Request
14365	2024-10-02 16:19:33.900939	0.000000s	10.127.84.21	10.127.85.85	0xb5a1	DTLSv1.2	98	Hello Verify Request
14366	2024-10-02 16:19:33.901946	0.001007s	10.127.85.85	10.127.84.21	0x6220	DTLSv1.2	292	Client Hello
14367	2024-10-02 16:19:33.901946	0.000000s	10.127.85.85	10.127.84.21	0x6220	DTLSv1.2	292	Client Hello
14368	2024-10-02 16:19:33.903944	0.001998s	10.127.84.21	10.127.85.85	0xb3cf	DTLSv1.2	558	Server Hello,Certificate (Fragment)
14369	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3cf	DTLSv1.2	562	Server Hello,Certificate (Fragment)
14370	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3ce	DTLSv1.2	558	Certificate (Fragment)
14371	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3ce	DTLSv1.2	562	Certificate (Fragment)
14372	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3cd	DTLSv1.2	558	Certificate (Fragment)
14373	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3cd	DTLSv1.2	562	Certificate (Fragment)
14374	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3cc	DTLSv1.2	558	Certificate (Fragment)
14375	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3cb	DTLSv1.2	558	Certificate (Reassembled),Server Key Exchange (Fragment)
14376	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3cc	DTLSv1.2	562	Certificate[Reassembly error,protocol DTLS: New fragment overlaps old data (retransmission?)]
14377	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3cb	DTLSv1.2	562	Certificate[Reassembly error,protocol DTLS: New fragment overlaps old data (retransmission?)]
14378	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3eb	DTLSv1.2	525	Server Key Exchange (Reassembled),Certificate Request,Server Hello Done
14379	2024-10-02 16:19:33.903944	0.000000s	10.127.84.21	10.127.85.85	0xb3eb	DTLSv1.2	529	Server Key Exchange[Reassembly error,protocol DTLS: New fragment overlaps old data (retransmissi
14380	2024-10-02 16:19:34.272980	0.369036s	10.127.85.85	10.127.84.21	0x60df	DTLSv1.2	590	Certificate (Fragment)
14381	2024-10-02 16:19:34.272980	0.000000s	10.127.85.85	10.127.84.21	0x60df	DTLSv1.2	590	Certificate (Fragment)
14382	2024-10-02 16:19:34.273972	0.000992s	10.127.85.85	10.127.84.21	0x60de	DTLSv1.2	590	Certificate (Reassembled),Client Key Exchange (Fragment)
14383	2024-10-02 16:19:34.273972	0.000000s	10.127.85.85	10.127.84.21	0x60de	DTLSv1.2	590	Certificate[Reassembly error,protocol DTLS: New fragment overlaps old data (retransmission?)]
14392	2024-10-02 16:19:34.584961	0.132989s	10.127.85.85	10.127.84.21	0x6147	DTLSv1.2	459	Client Key Exchange (Reassembled),Certificate Verify,Change Cipher Spec,Encrypted Handshake Mes
14393	2024-10-02 16:19:34.584961	0.000000s	10.127.85.85	10.127.84.21	0x6147	DTLSv1.2	459	Client Key Exchange[Reassembly error,protocol DTLS: New fragment overlaps old data (retransmissio
14394	2024-10-02 16:19:34.585968	0.001007s	10.127.84.21	10.127.85.85	0xb412	DTLSv1.2	121	Change Cipher Spec,Encrypted Handshake Message
[illegible]	[illegible]	[illegible]s	10.127.84.21	10.127.85.85	0xb412	DTLSv1.2	125	Change Cipher Spec,Encrypted Handshake Message
[illegible]	[illegible]	[illegible]s	10.127.85.85	10.127.84.21	0x5cea	DTLSv1.2	1483	Application Data
[illegible]	[illegible]	[illegible]s	10.127.85.85	10.127.84.21	0x5d13	CAPWA...	1442	CAPWAP-Control - Join Request[Malformed Packet]
14418	2024-10-02 16:19:35.804951	0.003998s	10.127.84.21	10.127.85.85	0xae86	DTLSv1.2	1460	Application Data
14419	2024-10-02 16:19:35.804951	0.000000s	10.127.84.21	10.127.85.85	0xae72	DTLSv1.2	1484	Application Data

AP Joins in Local Mode

Fabric Edge (FE) MAP Register for AP MAC & IP
FE Uplink Captures

lisp-tcp

No.	Time	DeltaTime	Source	Destination	Header Checksum	V)	Protocol	Length	Info
7685	2024-10-02 05:25:42.909...	0.001282s	10.127.84.105	10.127.84.100	0x42a3		LISP	176	[TCP ACKed unseen segment] ; Msg: 331,Registration for [8193] 10:06:ed:fc:2c:dc/48
7686	2024-10-02 05:25:42.909...	0.000178s	10.127.84.105	10.127.84.101	0x9231		LISP	176	Msg: 331,Registration for [8193] 10:06:ed:fc:2c:dc/48
7689	2024-10-02 05:25:42.910...	0.000159s	10.127.84.100	10.127.84.105	0x85f4		LISP	165	Msg: 432,Registration ACK; Msg: 433,Mapping Notification
7690	2024-10-02 05:25:42.910...	0.000249s	10.127.84.101	10.127.84.105	0x67b2		LISP	165	Msg: 382,Registration ACK; Msg: 383,Mapping Notification
7729	2024-10-02 05:25:44.407...	0.005552s	10.127.84.105	10.127.84.101	0x9217		LISP	200	Msg: 332,Registration for [4097] fe80::58a2:46ff:b89a:2e9f/128
7730	2024-10-02 05:25:44.407...	0.000084s	10.127.84.105	10.127.84.100	0x4289		LISP	200	Msg: 332,Registration for [4097] fe80::58a2:46ff:b89a:2e9f/128
7731	2024-10-02 05:25:44.408...	0.000572s	10.127.84.101	10.127.84.105	0x67f5		LISP	97	Msg: 384,Registration ACK
7734	2024-10-02 05:25:44.408...	0.000005s	10.127.84.100	10.127.84.105	0x8637		LISP	97	Msg: 434,Registration ACK
7924	2024-10-02 05:25:53.205...	0.000684s	10.127.84.105	10.127.84.101	0x91a9		LISP	308	Msg: 333,Registration for [4097] 10.127.85.85/32; Msg: 334,Registration for [4097] 10.127.85.85/32
7925	2024-10-02 05:25:53.205...	0.000273s	10.127.84.105	10.127.84.100	0x421b		LISP	308	Msg: 333,Registration for [4097] 10.127.85.85/32; Msg: 334,Registration for [4097] 10.127.85.85/32
7926	2024-10-02 05:25:53.206...	0.000456s	10.127.84.101	10.127.84.105	0x6795		LISP	192	Msg: 385,Registration ACK; Msg: 386,Registration ACK; Msg: 387,Mapping Notification
7927	2024-10-02 05:25:53.206...	0.000452s	10.127.84.100	10.127.84.105	0x85d7		LISP	192	Msg: 435,Registration ACK; Msg: 436,Registration ACK; Msg: 437,Mapping Notification
9030	2024-10-02 05:26:47.976...	0.001700s	10.127.84.100	10.127.84.105	0x85ce		LISP	200	Msg: 438,Mapping Notification
9031	2024-10-02 05:26:47.977...	0.000030s	10.127.84.101	10.127.84.105	0x678c		LISP	200	Msg: 388,Mapping Notification

Msg: 331,Registration for [8193] 10:06:ed:fc:2c:dc/48

Msg: 333,Registration for [4097] 10.127.85.85/32; Msg: 334,Registration for [4097] 10.127.85.85/32

Msg: 333,Registration for [4097] 10.127.85.85/32; Msg: 334,Registration for [4097] 10.127.85.85/32

WLC to CP MAP Request & Reply - WLC Captures

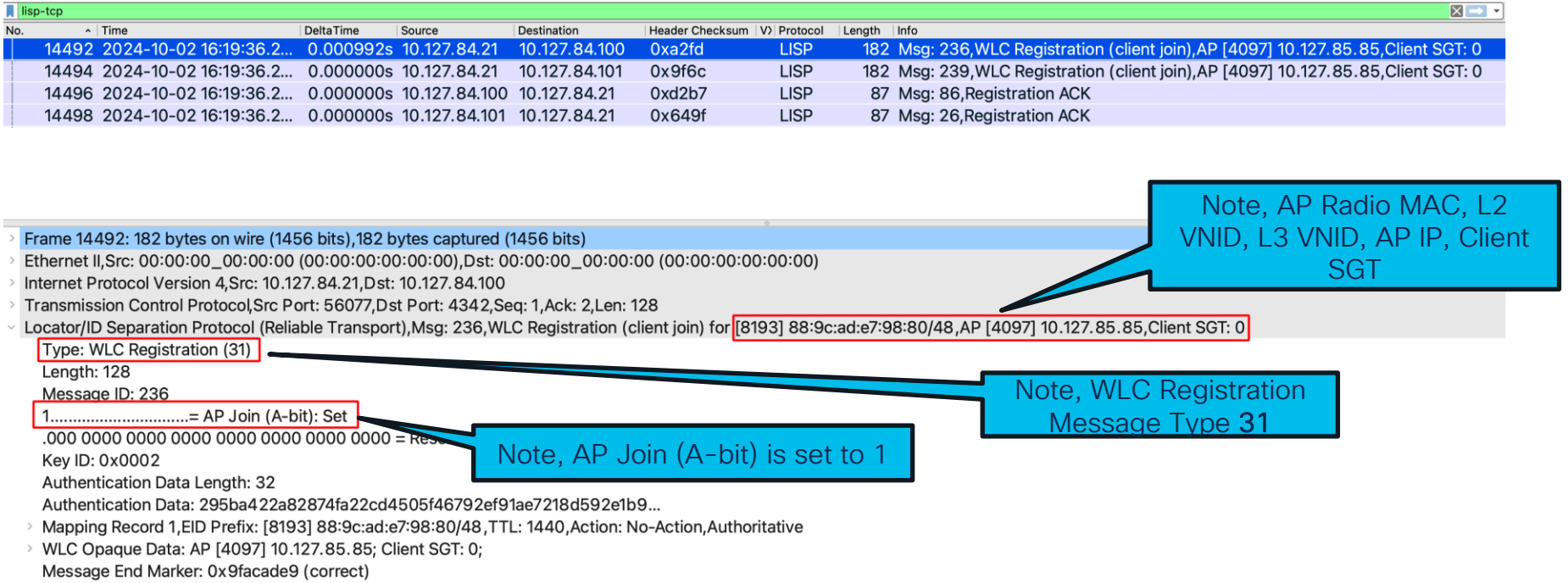
lisp

No.	Time	DeltaTime	Source	Destination	Header Checksum	V)	Protocol	Length	Info
14484	2024-10-02 16:19:36.2...	0.000000s	10.127.84.21	10.127.85.85	0xc25b,0xf...		LISP	130	Encapsulated Map-Request for [4097] 10.127.85.85/32
14485	2024-10-02 16:19:36.2...	0.000000s	10.127.84.21	10.127.85.85	0xc25b,0xf...		LISP	134	Encapsulated Map-Request for [4097] 10.127.85.85/32
14486	2024-10-02 16:19:36.2...	0.000000s	10.127.84.21	10.127.85.85	0xd020,0x...		LISP	130	Encapsulated Map-Request for [4097] 10.127.85.85/32
14487	2024-10-02 16:19:36.2...	0.000000s	10.127.84.21	10.127.85.85	0xd020,0x...		LISP	134	Encapsulated Map-Request for [4097] 10.127.85.85/32
14488	2024-10-02 16:19:36.2...	0.000000s	10.127.84.100	10.127.84.21	0xed40		LISP	94	Map-Reply for [4097] 10.127.85.85/32
14489	2024-10-02 16:19:36.2...	0.000000s	10.127.84.100	10.127.84.21	0xed40		LISP	94	Map-Reply for [4097] 10.127.85.85/32
14490	2024-10-02 16:19:36.2...	0.000000s	10.127.84.101	10.127.84.21	0xdc5a		LISP	94	Map-Reply for [4097] 10.127.85.85/32
14491	2024-10-02 16:19:36.2...	0.000000s	10.127.84.101	10.127.84.21	0xdc5a		LISP	94	Map-Reply for [4097] 10.127.85.85/32

```
Internet Protocol Version 4,Src: 10.127.84.100,Dst: 10.127.84.21
User Datagram Protocol,Src Port: 4342,Dst Port: 57850
Locator/ID Separation Protocol
    0010 ....................= Type: Map-Reply (2)
    ....0....................= P bit (Probe): Not set
    .....0...................= E bit (Echo-Nonce locator reachability algorithm enabled): Not set
    ......0..................= S bit (LISP-SEC capable): Not set
    .......0 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0x76ba7d48a59644eb
  Mapping Record 1,EID Prefix: [4097] 10.127.85.85/32,TTL: 1440,Action: No-Action,Not Authoritative
      Record TTL: 1440
      Locator Count: 1
      EID Mask Length: 32
      000.............= Action: No-Action (0)
      ...0 ............= Authoritative bit: Not set
      .....000 0000 0000 = Reserved: 0x000
      0000 ............= Reserved: 0x0
      ....0000 0000 0000 = Mapping Version: 0
      EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    EID Prefix: [4097] 10.127.85.85
    Locator Record 1,RLOC: 10.127.84.105,Reachable,Priority/Weight: 10/10,Multicast Priority/Weight: 10/10
        Priority: 10
        Weight: 10
        Multicast Priority: 10
        Multicast Weight: 10
      Flags: 0x0001
        AFI: IPv4 (1)
        Locator: 10.127.84.105
```

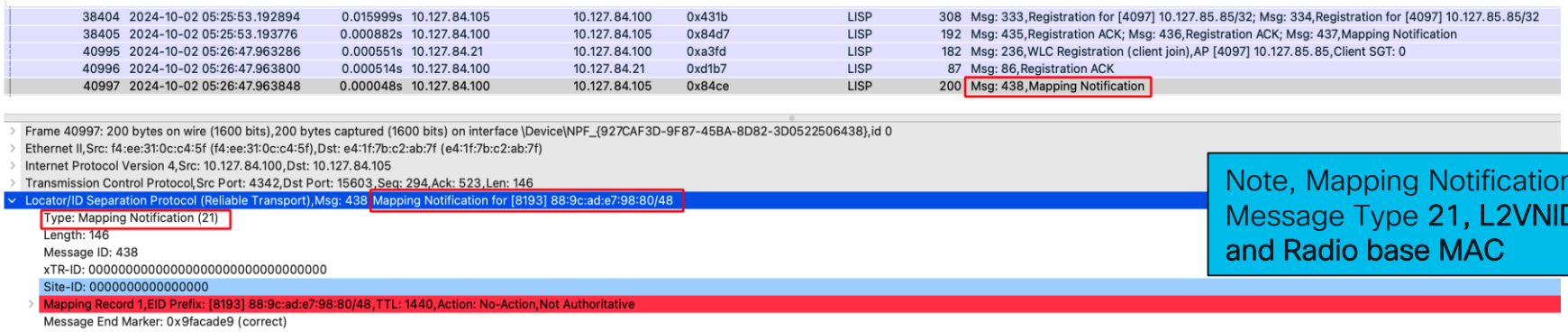
RLOC IP in MAP Reply

WLC LISP MAP Register to CP - WLC Captures



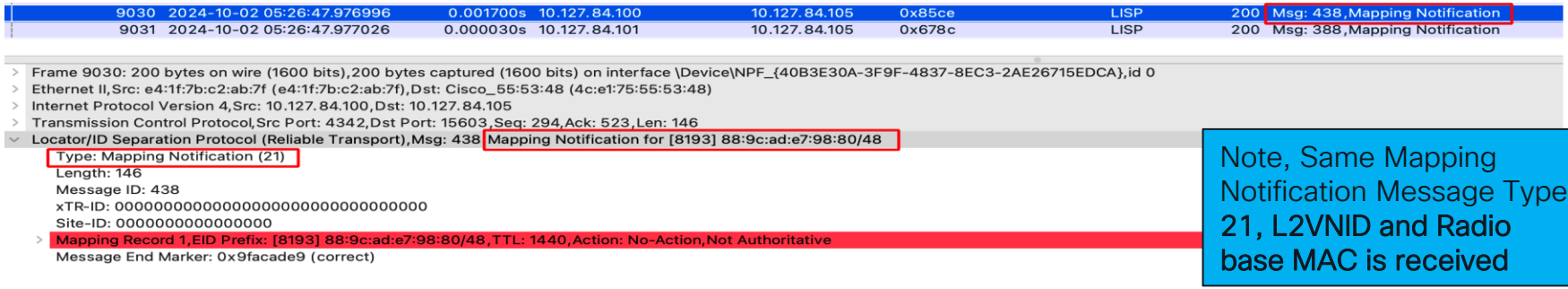
VxLAN Tunnel Formation

CP sends the MAP Notification to FE – Control Plane Captures



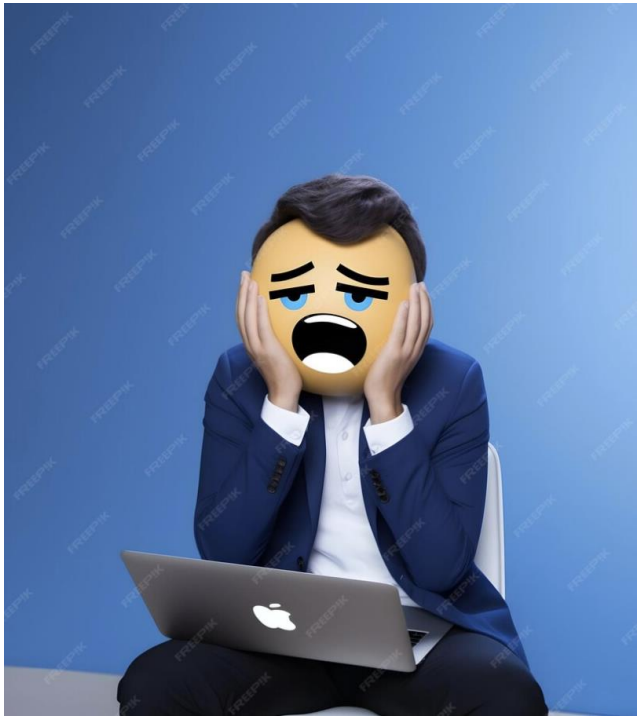
Note, Mapping Notification Message Type 21, L2VNID and Radio base MAC

FE receives the MAP Notification and then forms the VXLAN Tunnel – FE Uplink Captures



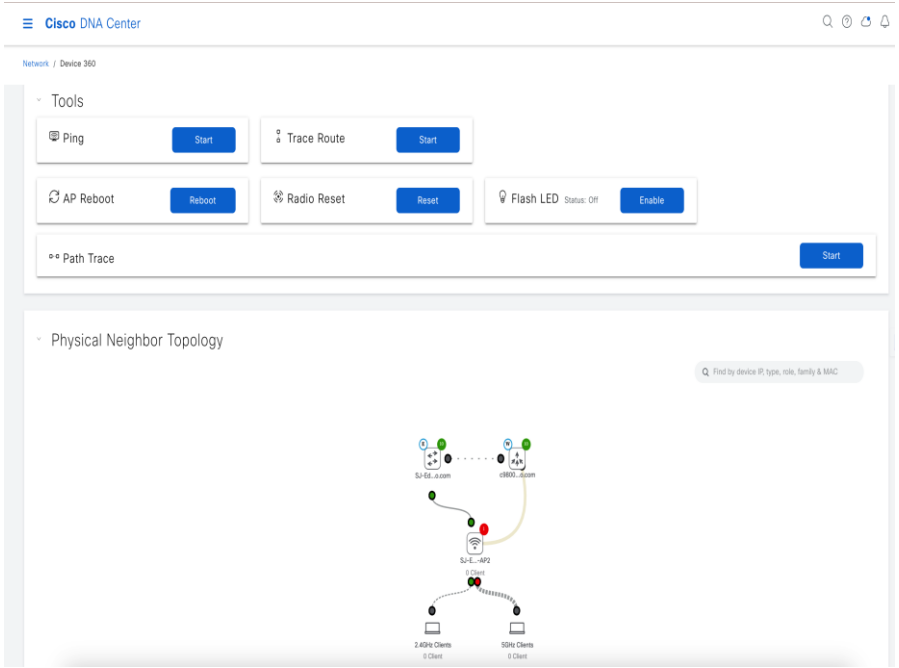
Note, Same Mapping Notification Message Type 21, L2VNID and Radio base MAC is received

When something breaks ....



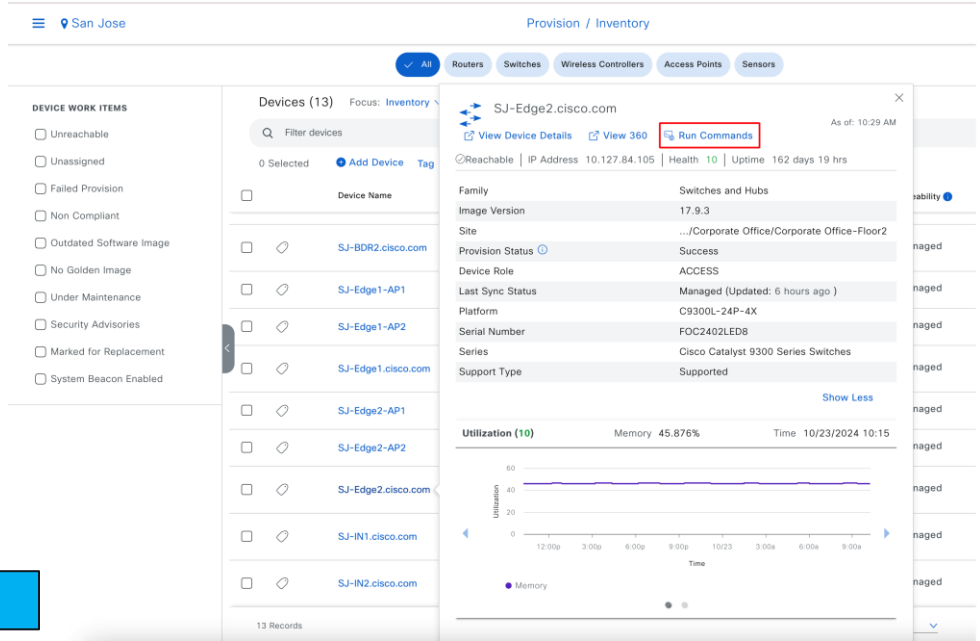
AP Join Troubleshooting

Catalyst Center Checks

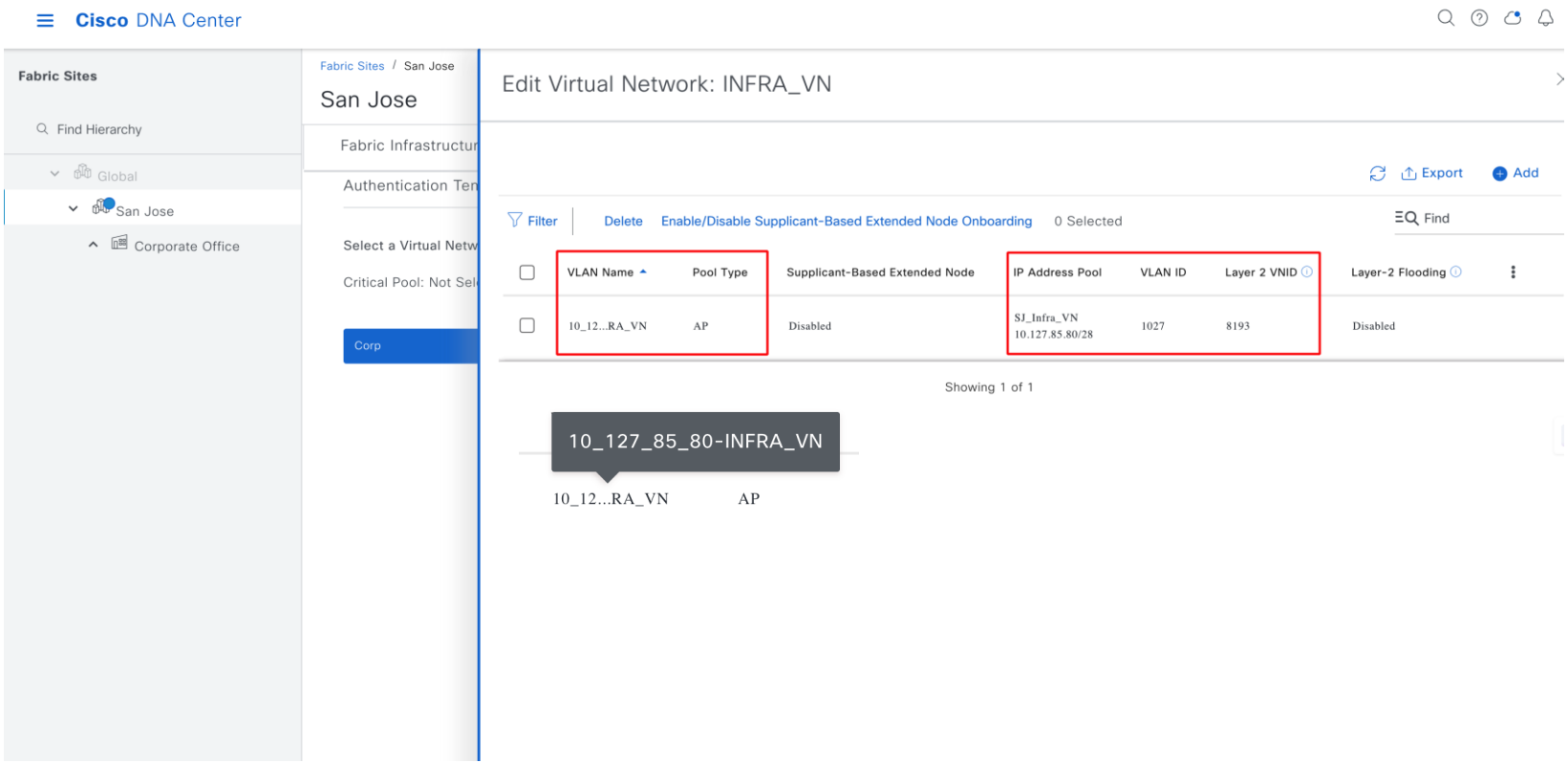


Assurance > Dashboards > Health > Network > Device 360

Provision > Inventory > Device > Run Commands



Catalyst Center Checks

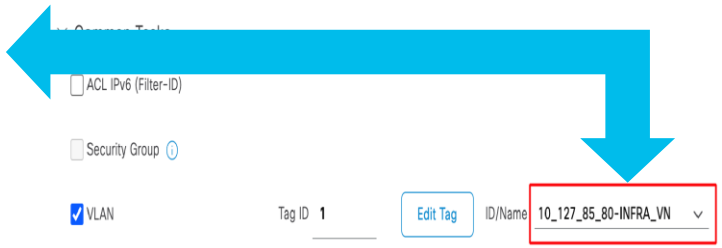


Fabric Edge Checks

```
SJ-Edge2#show vlan
<snip>
1027 10_127_85_80-INFRA_VN          active    L2LI0:8193, Gi1/0/1, Gi1/0/24
<snip ends>

SJ-Edge2#show run int Vlan 1027
<snip>
interface Vlan1027
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.ffdd
 ip address 10.127.85.81 255.255.255.240
 ip helper-address global 10.127.84.2
 ip helper-address global 10.127.84.8 => This is our DHCP server
 ip helper-address global 10.127.84.9
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 10_127_85_80-INFRA_VN-IPV4
end
<snip ends>
```

Identity Services Engine

Policy / Policy Elements



Note the VLAN, VLAN Name. We should use same VLAN Name in the ISE Authorization Profile

1) Note the IP Address, Subnet mask, DHCP Server IPs.

2) LISP mobility is configured for dynamic EIDs to be learnt

Fabric Edge Checks

```
SJ-Edge2#show run | s router lisp
router lisp
<snip>
 instance-id 4097
  remote-rloc-probe on-route-change
  dynamic-eid 10_127_85_80-INFRA_VN-IPV4
   database-mapping 10.127.85.80/28 locator-set rloc_b99de326-de2f-4125-9f35-40fcf2d020c7
   exit-dynamic-eid
  !
  service ipv4
   eid-table default
   exit-service-ipv4
  !
  exit-instance-id
  !
 instance-id 8193
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1027
   database-mapping mac locator-set rloc_b99de326-de2f-4125-9f35-40fcf2d020c7
   exit-service-ethernet
<snip ends>
```

Note the corresponding configured L3, L2 instance IDs, IP Pool and the VLAN

Fabric Edge Checks

```
SJ-Edge2#show run | i dhcp
<snip>
ip dhcp relay information option
ip dhcp snooping vlan 1025,1027
ip dhcp snooping

SJ-Edge2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
10:06:ED:FC:2C:DC   10.127.85.85      7755659     dhcp-snooping  1027  GigabitEthernet1/0/1

SJ-Edge2#show access-tunnel summary

Name    RLOC IP(Source)    AP IP(Destination)      VRF ID  Source Port  Destination Port
------  ---------------  ------------------  ------  -----------  ----------------
Ac1     10.127.84.105      10.127.85.85              0        N/A        4789

Name   IfId          Uptime
------ ----------  --------------------
Ac1    0x00000046 0 days, 02:58:45
<snip ends>
```

Ensure that DHCP configuration is present, and snooping is enabled for AP VLAN

Ensure we have DHCP snooping entry

Note the “Uptime” of the access-tunnel

Fabric Edge Checks

```
SJ-Edge2#show platform software fed switch active ifm interfaces access-tunnel
Interface                   IF_ID                State
------------------------------------------------------------------------
Ac0                         0x0000003d           READY
Ac1                         0x00000046           READY

SJ-Edge2#show platform software access-tunnel switch active R0
Name     SrcIp              DstIp              DstPort   VrfId      lif_id
------------------------------------------------------------------------
Ac0      10.127.84.105      10.127.85.88       0x12b5    0x0000     0x00003d
Ac1      10.127.84.105      10.127.85.85       0x12b5    0x0000     0x000046

SJ-Edge2#show platform software access-tunnel switch active F0
Name     SrcIp              DstIp              DstPort   VrfId      lif_id          Obj_id       Status
------------------------------------------------------------------------------------------------------
Ac0      10.127.84.105      10.127.85.88       0x12b5    0x000      0x00003d        0x05a99e     Done
Ac1      10.127.84.105      10.127.85.85       0x12b5    0x000      0x000046        0x05a99f     Done
```

Access-Tunnel should be in ”READY” state

Entry should remain stable, and parameters should match with earlier CLIs.

Entry should remain stable, match above CLIs and in “Done” status

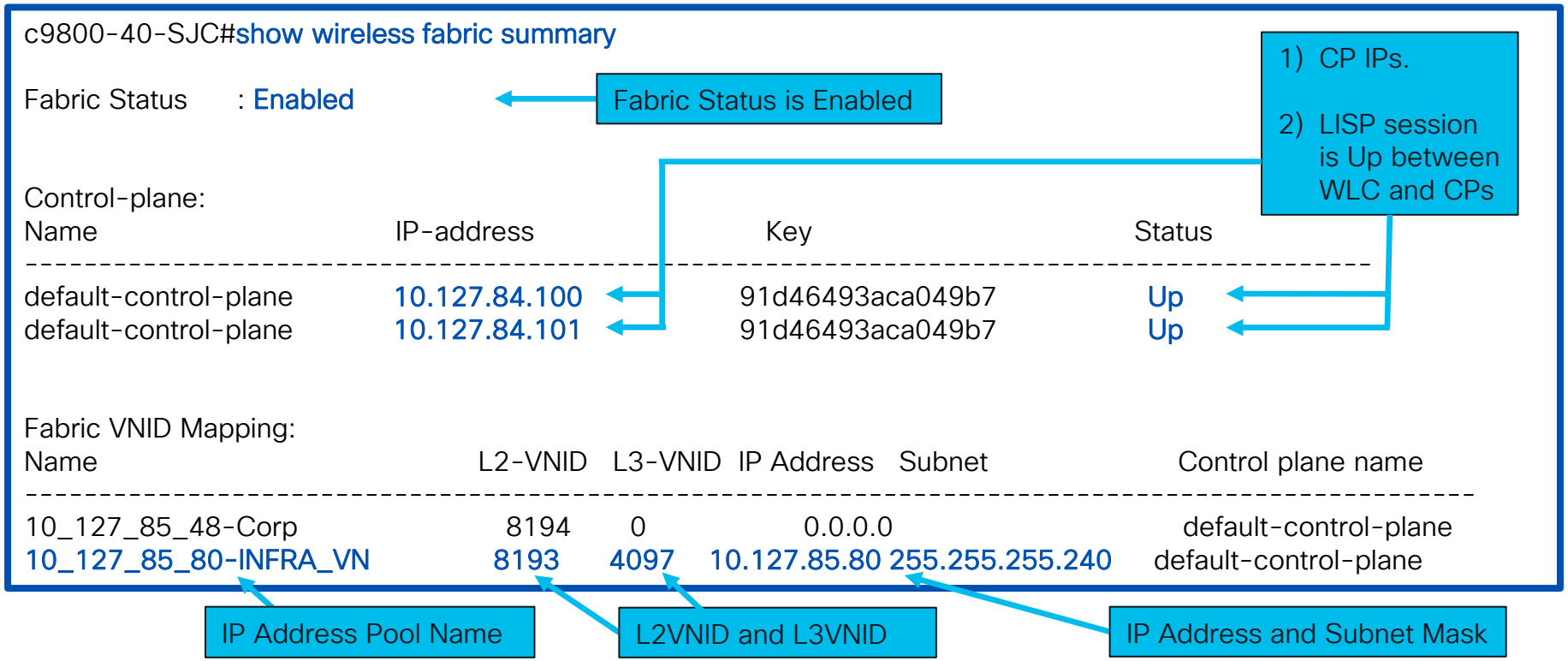
Fabric Edge Checks

```
SJ-Edge2#show platform software access-tunnel switch active R0 statistics
Access Tunnel          Counters (Success/Failure)
----------------------------------------
Create                      20/0
Create Obj Download         20/0
Delete                      18/0
Delete Obj Download         18/0
NACK                         0/0

SJ-Edge2#show platform software access-tunnel switch active F0 statistics
Access Tunnel     Counters (Success/Failure)
----------------------------------------
Create                   20/0
Delete                   18/0
HW Create                20/0
HW Delete                18/0
Create Ack               20/0
Delete Ack               18/0
NACK Notify               0/0
```

There should not be any failures

There should not be any failures

WLC Checks



WLC Checks

Note the AP Name, Model, Ethernet MAC, Radio MAC, Country, IP Address, State

```
c9800-40-SJC#show fabric ap summary
Number of Fabric AP : 4

AP Name          Slots  AP Model        Ethernet MAC    Radio MAC       Location         Country  IP Address
State
-------------------------------------------------------------------------------------------------------------
-----------------------------------
SJ-Edge1-AP1     3      C9130AXE-D      00df.1d9a.0e38  24d7.9c20.2d60  default location  US       10.127.85.83
Registered
SJ-Edge1-AP2     3      C9130AXI-D      6c71.0df2.4c04  2c57.4158.71a0  default location  US       10.127.85.84
Registered
SJ-Edge2-AP1     3      C9130AXI-D      1006.edfc.2c1c  889c.ade7.9280  default location  US       10.127.85.82
Registered
SJ-Edge2-AP2     3      C9130AXI-D      1006.edfc.2cdc  889c.ade7.9880  default location  US       10.127.85.85
Registered
```

Control Plane (CP) Checks

```
SJ-BDR1#show lisp session

Sessions for VRF default, total: 16, established: 11
Peer                    State    Up/Down    In/Out                Users
10.127.84.21:56077      Up       5d07h      143/87                2
10.127.84.100:4342      Up       17w3d      21485363/16095310     6
10.127.84.100:27272     Up       17w3d      16095310/21485363     4
10.127.84.101:4342      Up       17w3d      21460827/16095308     6
10.127.84.101:52967     Up       17w3d      16095019/21462324     4
10.127.84.104:51559     Up       5w3d       390/478               10
10.127.84.105:15603     Up       5w1d       335/439               8
SJ-BDR1#
```

Note the LISP session with WLC and the Fabric Edge(s)

Control Plane (CP) Checks

```
SJ-BDR1#show lisp instance-id 8193 ethernet server address-resolution
<snip>
Address-resolution data for router lisp 0 instance-id 8193

L3 InstID    Host Address                Hardware Address
    4097     10.127.85.85/32               1006.edfc.2cdc

SJ-BDR1#show lisp site
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last          Up       Who Last                Inst      EID Prefix
               Register                Registered              ID
site_uci       never         no        --                     4097      0.0.0.0/0
               04:11:13      yes#     10.127.84.105:15603     4097      10.127.85.85/32
```

Note the Host Address (AP IP), L3 InstID, AP Hardware Address

Note the Last Register, Up, Who Last Registered (FE Loopback IP), Inst ID, EID Prefix (AP IP)

AP Checks

```
SJ-Edge2-AP2#show ip interface brief
Interface              IP-Address      Method  Status         Protocol Speed      Duplex
wired0                 10.127.85.85    DHCP    up             up       1000       full

SJ-Edge2-AP2#show controllers wired 0
wired0    Link encap:Ethernet  HWaddr 10:06:ED:FC:2C:DC
          inet addr:10.127.85.85  Bcast:10.127.85.95  Mask:255.255.255.240
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1

SJ-Edge2-AP2#show ip tunnel fabric
Fabric GWs Information:
Tunnel-Id     GW-IP       GW-MAC                  Adj-Status   Encap-Type  Packet-In  Bytes-In    Packet-Out
Bytes-out
        1     10.127.84.105     00:00:0C:9F:FF:DD     Forward      VXLAN       25746      5325422     3077
401508
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC
SJ-Edge2-AP2#
```

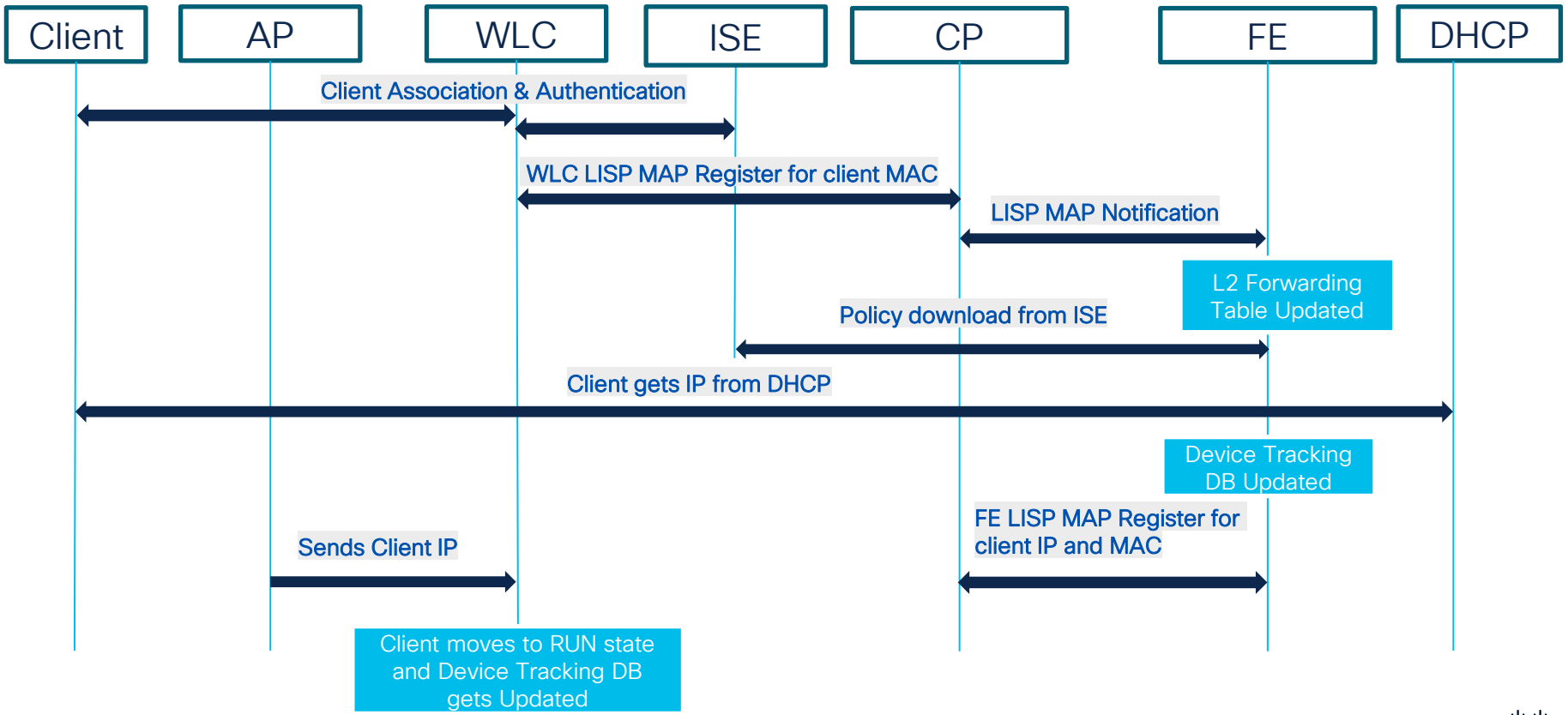
Note the wired0 interface of the AP

Note the IP, Hwaddr, “UP” status

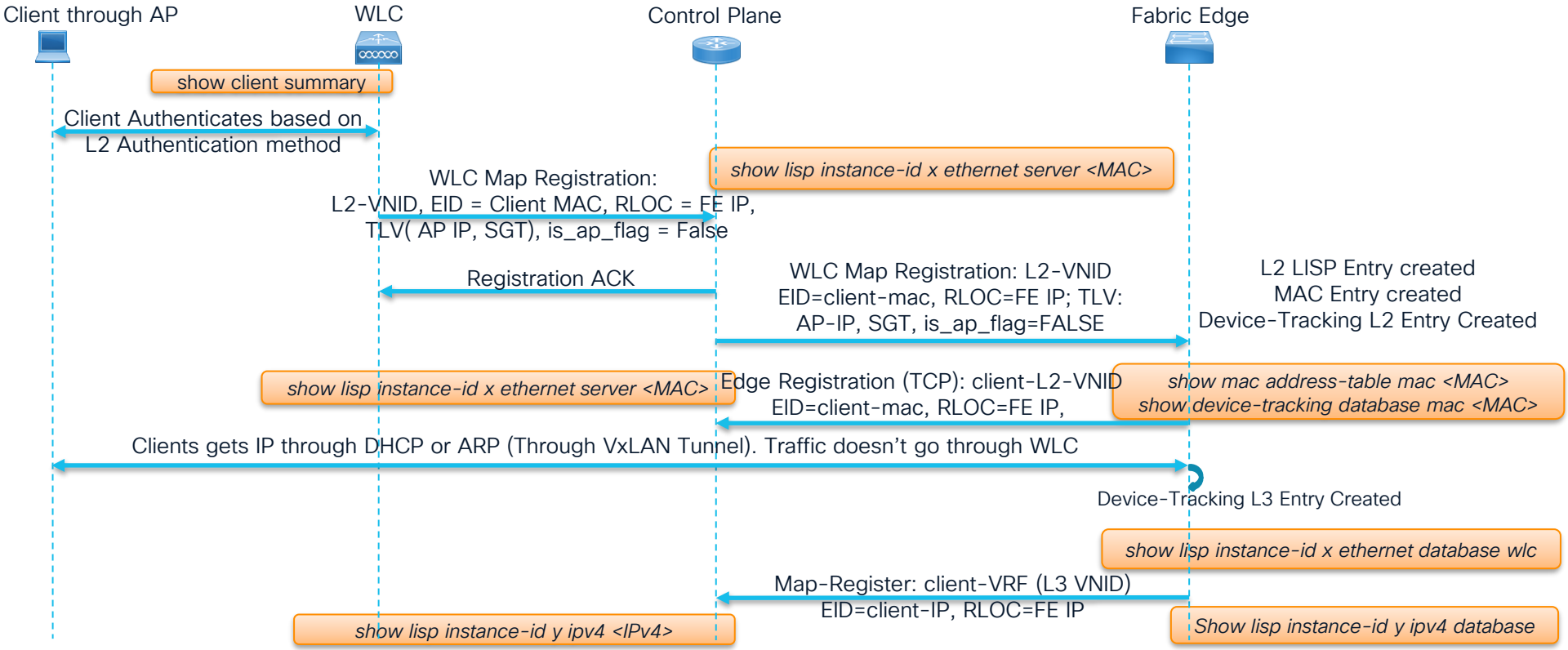
Note the access-tunnel is formed with the Edge 10.127.84.105. Encap-Type is “VXLAN” and Adj-Status is “Forward”.

Client Onboarding Flow

Client Onboarding Flow



Fabric Client Join Process



x = L2 instance ID
y = L3 instance ID

Client Onboarding Flow

Client Association & Authentication – WLC Captures

Note Association Request, Response, Request Identity, Response Identity

wlan.sa == d0:37:45:b7:50:27 || wlan.da == d0:37:45:b7:50:27 || radius

No.	Time	DeltaTime	Source	Destination	Header Checksum	VXLAN	Protocol	Length	Info
6903	2024-09-30 14:01:10.955944	0.230991s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x37ad		802.11	255	Association Request,SN=33,FN=0,Flags=.....,SSID=SJ_Corp_SSID
6904	2024-09-30 14:01:10.955944	0.000000s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x37ad		802.11	255	Association Request,SN=33,FN=0,Flags=.....,SSID=SJ_Corp_SSID
6905	2024-09-30 14:01:10.957943	0.001999s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe5f0		802.11	189	Association Response,SN=0,FN=0,Flags=.....
6906	2024-09-30 14:01:10.957943	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe5f0		802.11	193	Association Response,SN=0,FN=0,Flags=.....
6929	2024-09-30 14:01:10.964946	0.003006s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe64c		EAP	91	Request,Identity
6930	2024-09-30 14:01:10.964946	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe64c		EAP	95	Request,Identity
6939	2024-09-30 14:01:10.997934	0.030989s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x3861		EAP	138	Response,Identity
6940	2024-09-30 14:01:10.997934	0.000000s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x3861		EAP	138	Response,Identity
7062	2024-09-30 14:01:13.794957	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe197		EAP	129	Request,Protected EAP (EAP-PEAP)
7065	2024-09-30 14:01:13.804951	0.005997s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x3855		EAP	138	Response,Protected EAP (EAP-PEAP)
7066	2024-09-30 14:01:13.804951	0.000000s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x3855		EAP	138	Response,Protected EAP (EAP-PEAP)
7067	2024-09-30 14:01:13.805958	0.001007s	10.127.84.21	10.127.84.5	0xecfb		RADIUS	528	Access-Request id=175
7068	2024-09-30 14:01:13.805958	0.000000s	10.127.84.21	10.127.84.5	0xecfb		RADIUS	532	Access-Request id=175,Duplicate Request
7069	2024-09-30 14:01:13.819949	0.013991s	10.127.84.5	10.127.84.21	0x068b		RADIUS	402	Access-Accept id=175
7070	2024-09-30 14:01:13.819949	0.000000s	10.127.84.5	10.127.84.21	0x068b		RADIUS	402	Access-Accept id=175,Duplicate Response
7071	2024-09-30 14:01:13.819949	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe1ae		EAP	90	Success
7072	2024-09-30 14:01:13.819949	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe1ae		EAP	94	Success
7073	2024-09-30 14:01:13.822955	0.003006s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe13b		EAPOL	203	Key (Message 1 of 4)
7074	2024-09-30 14:01:13.822955	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe13b		EAPOL	207	Key (Message 1 of 4)
7075	2024-09-30 14:01:13.828951	0.005996s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x3806		EAPOL	213	Key (Message 2 of 4)
7076	2024-09-30 14:01:13.828951	0.000000s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x3806		EAPOL	213	Key (Message 2 of 4)
7077	2024-09-30 14:01:13.828951	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe116		EAPOL	237	Key (Message 3 of 4)
7078	2024-09-30 14:01:13.828951	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:...	0xe116		EAPOL	241	Key (Message 3 of 4)
7079	2024-09-30 14:01:13.833956	0.005005s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x381e		EAPOL	191	Key (Message 4 of 4)
7080	2024-09-30 14:01:13.833956	0.000000s	Tp-LinkT_b7:50:27	88:9c:ad:e7:98:81	0x381e		EAPOL	191	Key (Message 4 of 4)

Note EAP Request, Success, Radius Access-Request, Access-Accept and EAPOL Messages

cisco

Client Onboarding Flow

LISP MAP Register for client MAC from WLC – WLC Captures

lisp-tcp

No.	Time	DeltaTime	Source	Destination	Header Checksum	VXLAN	Protocol	Length	Info
7089	2024-09-30 14:01:13.836947	0.001999s	10.127.84.21	10.127.84.100	0xba78		LISP	182	Msg: 214,WLC Registration (client join),AP [4097] 10.127.85.85,Client SGT: 4
7091	2024-09-30 14:01:13.836947	0.000000s	10.127.84.21	10.127.84.101	0xb6e7		LISP	182	Msg: 217,WLC Registration (client join),AP [4097] 10.127.85.85,Client SGT: 4
7093	2024-09-30 14:01:13.837954	0.001007s	10.127.84.100	10.127.84.21	0xea28		LISP	87	Msg: 71,Registration ACK
7095	2024-09-30 14:01:13.837954	0.000000s	10.127.84.101	10.127.84.21	0x7c10		LISP	87	Msg: 11,Registration ACK

Msg: 214,WLC Registration (client join),AP [4097] 10.127.85.85,Client SGT: 4

Note, WLC Registration Message, Type (31), L3VNID, AP IP, L2VNID, Client MAC Address and Client SGT Assigned (4)

```
Frame 7089: 182 bytes on wire (1456 bits),182 bytes captured (1456 bits)
Ethernet II,Src: 00:00:00_00:00:00 (00:00:00:00:00:00),Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4,Src: 10.127.84.21,Dst: 10.127.84.100
Transmission Control Protocol,Src Port: 56077,Dst Port: 4342,Seq: 1,Ack: 2,Len: 128
Locator/ID Separation Protocol (Reliable Transport),Msg: 214,WLC Registration (client join) for [8194] d0:37:45:b7:50:27/48,AP [4097] 10.127.85.85,Client SGT: 4
  Type: WLC Registration (31)
  Length: 128
  Message ID: 214
  0...............................= AP Join (A-bit): Not set
  .000 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0x00000000
  Key ID: 0x0002
  Authentication Data Length: 32
  Authentication Data: 1044f3cf58b93585defd39975998bf32ca878ae8f5c4
  Mapping Record 1,EID Prefix: [8194] d0:37:45:b7:50:27/48,TTL: 1440,Actio
    Record TTL: 1440
    Locator Count: 1
    EID Mask Length: 48
    000.............= Action: No-Action (0)
    ...1 ............= Authoritative bit: Set
    .....000 0000 0000 = Reserved: 0x000
    0000 ............= Reserved: 0x0
    ....0000 0000 0000 = Mapping Version: 0
    EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
    EID Prefix: [8194] d0:37:45:b7:50:27
    Locator Record 1,Local RLOC: 10.127.84.105,Reachable,Priority/Weight: 0/0,Multicast Priority/Weight: 0/0
  WLC Opaque Data: AP [4097] 10.127.85.85; Client SGT: 4;
  Message End Marker: 0x9facade9 (correct)
```

Locator/ID Separation Protocol (Reliable Transport),Msg: 214,WLC Registration (client join) for [8194] d0:37:45:b7:50:27/48,AP [4097] 10.127.85.85,Client SGT: 4

Type: WLC Registration (31)

EID Prefix: [8194] d0:37:45:b7:50:27

Locator Record 1,Local RLOC: 10.127.84.105,Reachable,Priority/Weight: 0/0,Multicast Priority/Weight: 0/0

WLC Opaque Data: AP [4097] 10.127.85.85; Client SGT: 4;

cisco

Client Onboarding Flow – RA Traces from WLC

Client Association & Authentication

2024/09/30 14:01:10.957037338 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (debug): MAC: d037.45b7.5027 Received Dot11 association request. Processing started,SSID: SJ_Corp_SSID, Policy profile: SJ_Corp_SSID_profile, AP Name: SJ-Edge2-AP2, Ap Mac Address: 889c.ade7.9880BSSID MAC0000.0000.0000wlan ID: 18RSSI: -60, SNR: 37

2024/09/30 14:01:10.958102013 {wncd_x_R0-0}{1}: [dot11] [15082]: (info): MAC: d037.45b7.5027 dot11 send association response. Sending assoc response of length: 115 with resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS

2024/09/30 14:01:10.964660337 {wncd_x_R0-0}{1}: [dot1x] [15082]: (info): [d037.45b7.5027:capwap_90000008] Dot1x authentication started for (d037.45b7.5027)
2024/09/30 14:01:10.999026952 {wncd_x_R0-0}{1}: [wncd_0] [15082]: (debug): AAA/BND(00000000): Received aaa Authentication request, list handle 0x5600002b. Ownership changed from Unknown to AAA

2024/09/30 14:01:13.820176010 {wncd_x_R0-0}{1}: [radius] [15082]: (info): RADIUS: Received from id 1812/175 10.127.84.5:0, Access-Accept, len 360

Note the client association request, WLAN/SSID and AP associated. We shall see similar logs.

Note the Radius “Access-Accept” received from the ISE

RA Traces from WLC -Continued

Note the M1, M2, M3 and M4 Messages

2024/09/30 14:01:13.823605836 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (info): MAC: d037.45b7.5027
EAP key M1 Sent successfully
2024/09/30 14:01:13.829479061 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (info): MAC: d037.45b7.5027
M2 Status: EAP key M2 validation success
2024/09/30 14:01:13.829671267 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (info): MAC: d037.45b7.5027
EAP key M3 Sent successfully
2024/09/30 14:01:13.834630804 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (info): MAC: d037.45b7.5027
M4 Status: EAP key M4 validation is successful
2024/09/30 14:01:13.834890467 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (debug): MAC: d037.45b7.5027
L2 Authentication of station is successful., L3 Authentication : 0

WLC MAP Register for client MAC and WLC MAP Notification

2024/09/30 14:01:13.837449848 {wncd_x_R0-0}{1}: [lisp-agent-internal] [15082]: (note): MAC: d037.45b7.5027
Successfully sent the map register message to map server IPV4 10.127.84.101 with message id 217 client delete 0

2024/09/30 14:01:13.837460566 {wncd_x_R0-0}{1}: [lisp-agent-db] [15082]: (debug): MAC: d037.45b7.5027
Successfully inserted the CLIENT history node with details VNID: 8194, SGT: 4, for AP MAC MAC: 889c.ade7.9880 ,
XTR-IP: 10.127.84.105 ,MS-IP: 10.127.84.101

Note the LISP Map register sent for the client MAC to WLC and the subsequent MAP notification with L2 VNID, SGT and FE IP

Client Onboarding Flow

LISP MAP Register from WLC and CP's LISP MAP Notification – CP Captures

Note, The same WLC Registration Message is received on the Control Plane (CP) Node

lisp-tcp

Source	Destination	Protocol	Length	Info
10.127.84.21	10.127.84.100	LISP	182	[TCP ACKed unseen segment] ; Msg: 214,WLC Registration (client join),AP [4097] 10.127.85.85,Client SGT: 4
10.127.84.100	10.127.84.21	LISP	87	Msg: 71,Registration ACK
10.127.84.100	10.127.84.105	LISP	192	[TCP ACKed unseen segment] ; Msg: 319,Mapping Notification

DHCP Flow (DORA Process) – Fabric Edge Uplink Captures

bootp.hw.mac_addr == d0:37:45:b7:50:27

No.	Time	DeltaTime	Source	Destination	Header Checksum	VXLAN	Protocol	Length	Info
1678	2024-09-30 03:08:36.872326	0.002693s	10.127.85.49	10.127.84.8	0xa448,0xbc82	4099	DHCP	416	DHCP Discover - Transaction ID 0x23b5875
1679	2024-09-30 03:08:36.872444	0.000118s	10.127.85.49	10.127.84.9	0xa447,0xbc80	4099	DHCP	416	DHCP Discover - Transaction ID 0x23b5875
1680	2024-09-30 03:08:36.873034	0.000590s	10.127.84.8	10.127.85.49	0x7e9c,0x61f2	4099	DHCP	404	DHCP Offer - Transaction ID 0x23b5875
1681	2024-09-30 03:08:36.878286	0.005252s	10.127.85.49	255.255.255.255	0x33e7,0x1b14		DHCP	432	DHCP Offer - Transaction ID 0x23b5875
1682	2024-09-30 03:08:36.887952	0.009666s	0.0.0.0	255.255.255.255	0x33d3,0x841e		DHCP	448	DHCP Request - Transaction ID 0x23b5875
1683	2024-09-30 03:08:36.890834	0.002882s	10.127.85.49	10.127.84.8	0xa42c,0xbc65	4099	DHCP	442	DHCP Request - Transaction ID 0x23b5875
1684	2024-09-30 03:08:36.890955	0.000121s	10.127.85.49	10.127.84.9	0xa42b,0xbc63	4099	DHCP	442	DHCP Request - Transaction ID 0x23b5875
1685	2024-09-30 03:08:36.891748	0.000793s	10.127.84.8	10.127.85.49	0x7e97,0x61ec	4099	DHCP	409	DHCP ACK - Transaction ID 0x23b5875
1687	2024-09-30 03:08:36.899061	0.000071s	10.127.85.49	255.255.255.255	0x33df,0x1b0c		DHCP	437	DHCP ACK - Transaction ID 0x23b5875

```
Frame 1678: 416 bytes on wire (3328 bits),416 bytes captured (3328 bits) on interface \Device\NPF_{40B3E30A-3F9F-4837-8EC3-2AE26715EDCA},id 0
Ethernet II,Src: Cisco_55:53:46 (4c:e1:75:55:53:46),Dst: e4:1f:7b:eb:60:1f (e4:1f:7b:eb:60:1f)
Internet Protocol Version 4,Src: 10.127.84.105,Dst: 10.127.84.100
User Datagram Protocol,Src Port: 5177,Dst Port: 4789
Virtual eXtensible Local Area Network
    Flags: 0x8848,GBP Extension,Don't Learn,VXLAN Network ID (VNI),Policy Applied
    Group Policy ID: 2
    VXLAN Network Identifier (VNI): 4099
    Reserved: 0
Ethernet II,Src: Cisco_55:53:46 (4c:e1:75:55:53:46),Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
Internet Protocol Version 4,Src: 10.127.85.49,Dst: 10.127.84.8
User Datagram Protocol,Src Port: 67,Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
```

Note, The SGT (2) and L3VNID

Client Onboarding Flow

DHCP Offer packet – Note Option 82 – Fabric Edge Uplink Captures

bootp.hw.mac_addr == d0:37:45:b7:50:27

No.	Time	DeltaTime	Source	Destination	Header Checksum	VXLAN	Protocol	Length	Info
1678	2024-09-30 03:08:36.872326	0.002693s	10.127.85.49	10.127.84.8	0xa448,0xbc82	4099	DHCP	416	DHCP Discover - Transaction ID 0x23b5875
1679	2024-09-30 03:08:36.872444	0.000118s	10.127.85.49	10.127.84.9	0xa447,0xbc80	4099	DHCP	416	DHCP Discover - Transaction ID 0x23b5875
1680	2024-09-30 03:08:36.873034	0.000590s	10.127.84.8	10.127.85.49	0x7e9c,0x61f2	4099	DHCP	404	DHCP Offer - Transaction ID 0x23b5875
1681	2024-09-30 03:08:36.878286	0.005252s	10.127.85.49	255.255.255.255	0x33e7,0x1b14		DHCP	432	DHCP Offer - Transaction ID 0x23b5875
1682	2024-09-30 03:08:36.887952	0.009666s	0.0.0.0	255.255.255.255	0x33d3,0x841e		DHCP	448	DHCP Request - Transaction ID 0x23b5875
1683	2024-09-30 03:08:36.890834	0.002882s	10.127.85.49	10.127.84.8	0xa42c,0xbc65	4099	DHCP	442	DHCP Request - Transaction ID 0x23b5875
1684	2024-09-30 03:08:36.890955	0.000121s	10.127.85.49	10.127.84.9	0xa42b,0xbc63	4099	DHCP	442	DHCP Request - Transaction ID 0x23b5875
1685	2024-09-30 03:08:36.891748	0.000793s	10.127.84.8	10.127.85.49	0x7e97,0x61ec	4099	DHCP	409	DHCP ACK - Transaction ID 0x23b5875
1687	2024-09-30 03:08:36.899061	0.000071s	10.127.85.49	255.255.255.255	0x33df,0x1b0c				

```
    VXLAN Network Identifier (VNI): 4099
    Reserved: 0
> Ethernet II, Src: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
> Internet Protocol Version 4, Src: 10.127.84.8, Dst: 10.127.85.49
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x023b5875
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.127.85.51
    Next server IP address: 10.127.84.8
    Relay agent IP address: 10.127.85.49
    Client MAC address: Tp-LinkT_b7:50:27 (d0:37:45:b7:50:27)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (1) Subnet Mask (255.255.255.240)
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (51) IP Address Lease Time
  > Option: (54) DHCP Server Identifier (10.127.84.8)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  v Option: (82) Agent Information Option
      Length: 20
    v Option 82 Suboption: (1) Agent Circuit ID
        Length: 6
        Agent Circuit ID: 000404010d02
    v Option 82 Suboption: (2) Agent Remote ID
        Length: 10
        Agent Remote ID: 0308001003010a7f5469
  > Option: (255) End
```

```
v Option: (82) Agent Information Option
    Length: 20
  v Option 82 Suboption: (1) Agent Circuit ID
      Length: 6
      Agent Circuit ID: 000404010d02
  v Option 82 Suboption: (2) Agent Remote ID
      Length: 10
      Agent Remote ID: 0308001003010a7f5469
```

Decode of Option 82

For the Agent Circuit-ID:

000404010d02

00 => Sub-option 1 = Vlan/Module/Port

04 => Length of option

0401 => Vlan 1025 (0x401)

0d => Module 13

02 => Port 2

For the Agent Remote-ID:

0308001003010a7f5469

03 => Sub-option LISP

08 => 8 = Length of option

001003 => 4099 in decimals = L3 LISP Instance ID 4099

01 => IPV4 locator (IPv6 would be 02)

0a.7f.54.69 => 10.127.84.105 Remote locator (Loopback 0 of xTR)

Client Onboarding Flow

Fabric Edge LISP MAP Register for client IP and MAC – CP Downlink Captures

10.127.84.105	10.127.84.100	LISP	176	Msg: 212,Registration for [8194] d0:37:45:b7:50:27/48
10.127.84.100	10.127.84.105	LISP	225	Msg: 320,Registration ACK; Msg: 321,Mapping Notification
10.127.84.105	10.127.84.100	LISP	200	Msg: 213,Registration for [4099] fe80::3f71:d25b:36d0:f039/128
10.127.84.100	10.127.84.105	LISP	97	Msg: 322,Registration ACK
10.127.84.105	10.127.84.100	LISP	308	Msg: 214,Registration for [4099] 10.127.85.51/32; Msg: 215,Registration for [4099] 10.127.85.51/32
10.127.84.100	10.127.84.105	LISP	192	Msg: 323,Registration ACK; Msg: 324,Registration ACK; Msg: 325,Mapping Notification

After AP Sends Client IP – WLC Captures

Source	Destination	Header Checksum	VXLAN	Protocol	Length	Info
Tp-LinkT_b7:50:27	Broadcast	0x3207		ARP	120	ARP Announcement for 10.127.85.51

```
> Frame 2203: 120 bytes on wire (960 bits),120 bytes captured (960 bits)
> Ethernet II,Src: Cisco_52:cc:c3 (f4:bd:9e:52:cc:c3),Dst: 90:eb:50:85:2a:2b (90:eb:50:85:2a:2b)
> Internet Protocol Version 4,Src: 10.127.85.85,Dst: 10.127.84.21
> User Datagram Protocol,Src Port: 5264,Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data,Flags: .....T
> Logical-Link Control
> Address Resolution Protocol (ARP Announcement)
```

Client Onboarding Flow – RA Traces from WLC

AP Sends Client IP

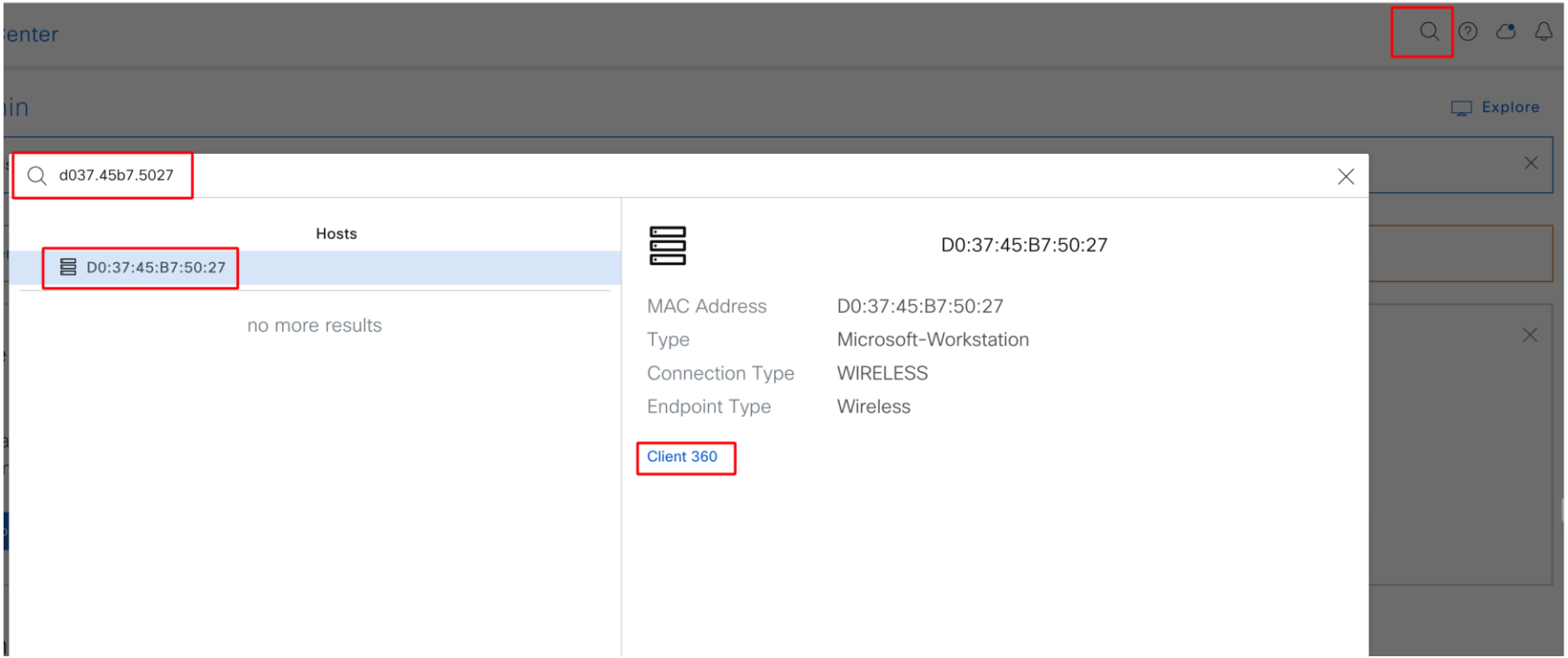
2024/09/30 14:01:14.921276911 {wncd_x_R0-0}{1}: [client-iplearn] [15082]: (debug): MAC: d037.45b7.5027 sisf binding table event cb. SISF Binding event STATE_CHANGE IP 10.127.85.51 vnid 8194 state REACHABLE origin PK4
2024/09/30 14:01:14.921279853 {wncd_x_R0-0}{1}: [client-iplearn] [15082]: (debug): MAC: d037.45b7.5027 sisf binding table event cb. SISF move to Run state
2024/09/30 14:01:14.921282021 {wncd_x_R0-0}{1}: [client-iplearn] [15082]: (note): MAC: d037.45b7.5027 Client IP learn successful. Method: IP Snooping IP:10.127.85.51

2024/09/30 14:01:14.910081521 {wncd_x_R0-0}{1}: [client-orch-fabric] [15082]: (debug): MAC: d037.45b7.5027 Sanet Resolved VNID Policy Name = 10_127_85_48-Corp
2024/09/30 14:01:14.910081835 {wncd_x_R0-0}{1}: [client-orch-fabric] [15082]: (debug): MAC: d037.45b7.5027 VNID Overrride Name From Sanet (Shouldnt be empty): = 10_127_85_48-Corp
2024/09/30 14:01:14.910086007 {wncd_x_R0-0}{1}: [client-orch-fabric] [15082]: (debug): MAC: d037.45b7.5027 VNID Mapping record L2-VNID Value = 8194
2024/09/30 14:01:14.910086301 {wncd_x_R0-0}{1}: [client-orch-fabric] [15082]: (debug): MAC: d037.45b7.5027 Value from VNID Mapping Table in case of override = 8194
2024/09/30 14:01:14.910086795 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (debug): MAC: d037.45b7.5027 vlan_mode_api: switching_mode Local-swtiching vnid 8194

Note the Client IP being learned successfully while associating it with L2VNID

Client Onboarding Troubleshooting

Catalyst Center Checks



WLC Checks

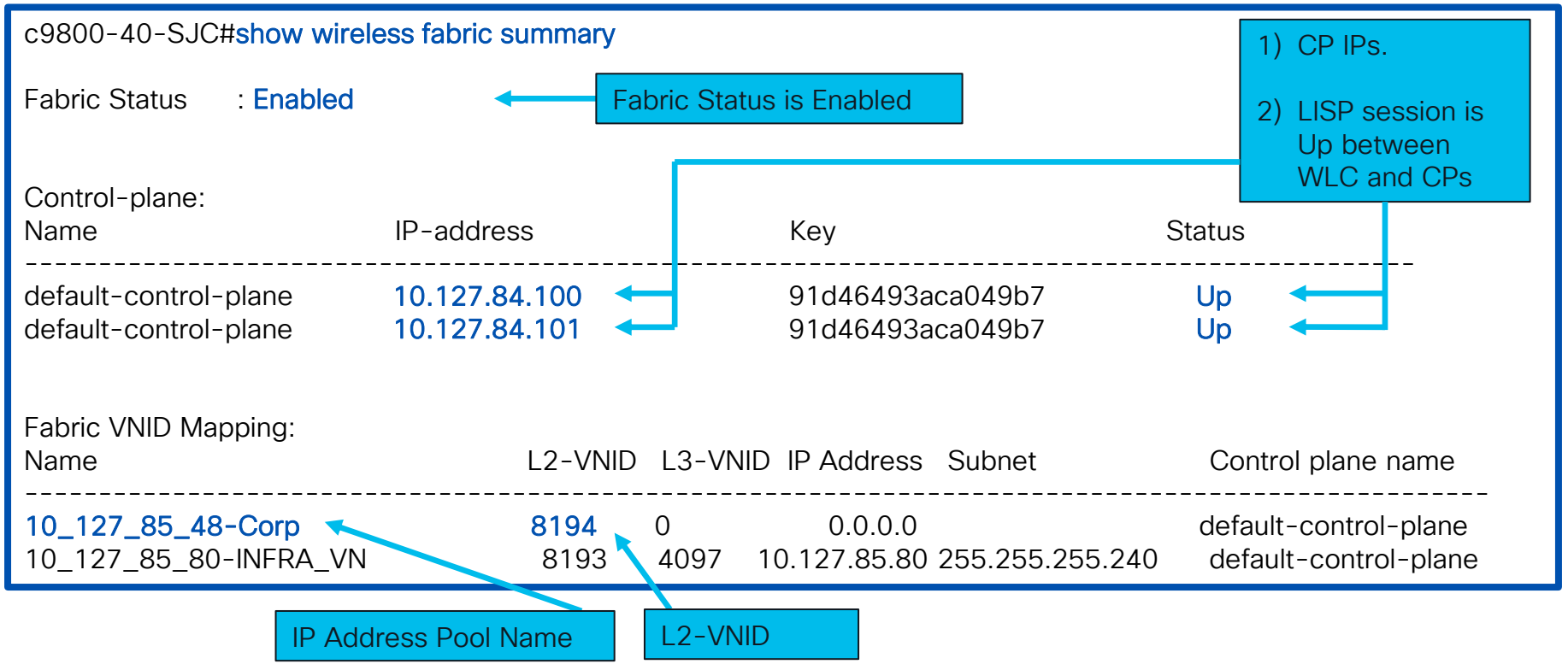
```
c9800-40-SJC#show wireless client summary
Number of Clients: 1

MAC Address       AP Name          Type   ID   State          Protocol Method   Role
--------------------------------------------------------------------------------------
d037.45b7.5027    SJ-Edge2-AP2     WLAN   18   Run            11n(2.4) Dot1x    Local

c9800-40-SJC#show wireless client mac d037.45b7.5027 detail | sec Fabric
Fabric status : Enabled
  RLOC    : 10.127.84.105
  VNID    : 8194
  SGT     : 4
  Control plane name  : default-control-plane

c9800-40-SJC#show wireless device-tracking database mac
  MAC             VLAN  IF-HDL      IP
  ------------------------------------------------------------
  d037.45b7.5027  1     0x90000008  10.127.85.51
c9800-40-SJC#show wireless device-tracking database ip
  IP                      ZONE-ID          STATE        DISCOVERY          MAC
------------------------------------------------------------------------------------
10.127.85.51              0x00000000       Reachable    IPv4 DHCP          d037.45b7.5027
```

1) Client in “Run” state?
2) Note AP Name

1) Note the RLOC, VNID, SGT
2) Same info is passed to CP

1) Device-Tracking Database is finally updated

WLC Checks

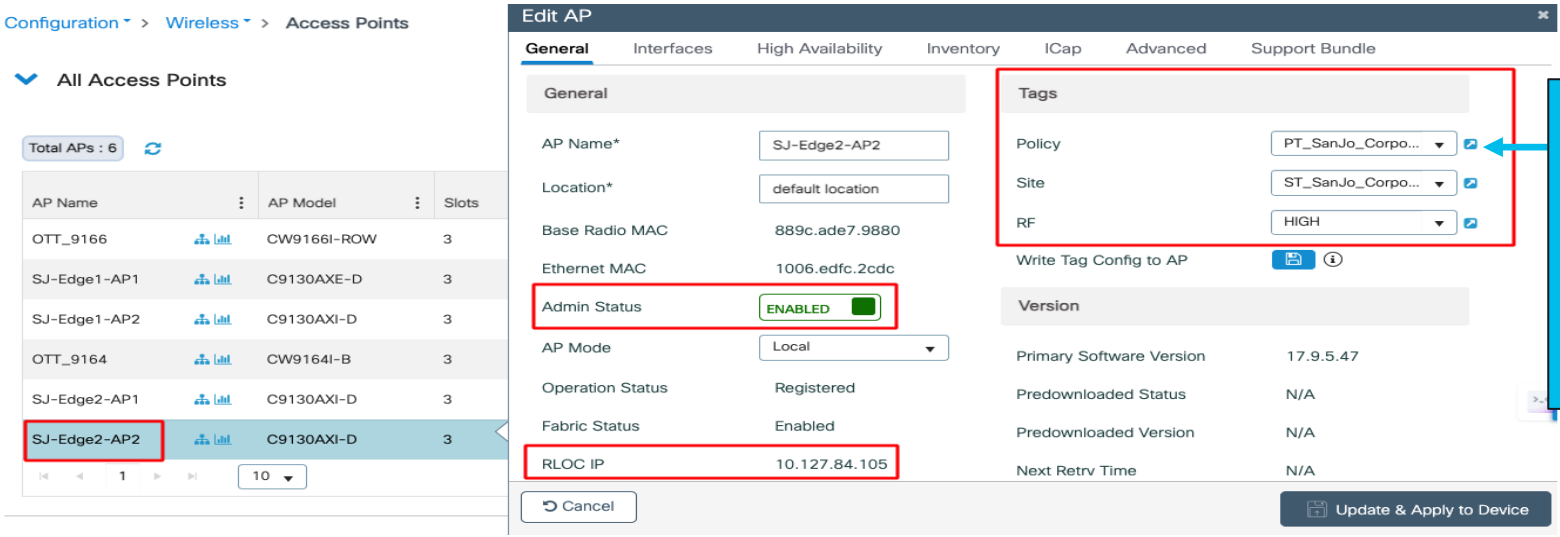


WLC Checks

Ensure basic configuration is present on WLC

Tags configurations are pushed from the Catalyst Center.

Configuration > Wireless > Access Points (Click the AP > General – Notice the Tags and other fields)



WLC Checks

On WLC we can see the details in the following command output

```
c9800-40-SJC#show ap tag summary
Number of APs: 6

AP Name          AP Mac          Site Tag Name              Policy Tag Name                          RF Tag Name
Misconfigured    Tag Source
-----------------------------------------------------------------------------------------------------------
....
SJ-Edge1-AP1     00df.1d9a.0e38    ST_SanJo_Corporat_9248f_0  PT_SanJo_Corpo_Corporat_78519     HIGH
No               Static
SJ-Edge1-AP2     6c71.0df2.4c04    ST_SanJo_Corporat_9248f_0    PT_SanJo_Corpo_Corporat_78519     HIGH
No               Static
SJ-Edge2-AP1     1006.edfc.2c1c    ST_SanJo_Corporat_9248f_0    PT_SanJo_Corpo_Corporat_78519     HIGH
No               Static
SJ-Edge2-AP2     1006.edfc.2cdc    ST_SanJo_Corporat_9248f_0    PT_SanJo_Corpo_Corporat_78519     HIGH
No               Static
```

SSH, Username, Password needs to be enabled in the AP Join Profile

AP Checks

```
SJ-Edge2-AP2#show controllers Dot11Radio 0 wlan
wifi0     Link encap:Ethernet  HWaddr 88:9C:AD:E7:98:80
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3647 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1333 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:2699
          RX bytes:316177 (308.7 KiB)  TX bytes:118081 (115.3 KiB)

radio vap id              mac         ssid state
    0      0 88:9C:AD:E7:98:80      EEC_Exp    UP
    0      1 88:9C:AD:E7:98:81 SJ_Corp_SSID    UP
...
...
...

VAP-ID         SSID   Bridging Type
     0      EEC_Exp CAPWAP-Tunneled
     1 SJ_Corp_SSID Fabric-Tunneled
```

SSH, Username, Password needs to be enabled in the AP Join Profile

Take note of Fabric SSID and state

SSID Bridging Type should be “Fabric-Tunneled”

Fabric Edge(s) Checks

```
SJ-Edge2#show cdp neighbors
Device ID            Local Intrfce     Holdtme    Capability  Platform      Port ID
SJ-Edge2-AP2     Gig 1/0/1         122              R T       C9130AXI- Gig 0

SJ-Edge2#show device-tracking database | inc 1/0/1
DH4 10.127.85.85  1006.edfc.2cdc  Gi1/0/1    1027    0024    8s  REACHABLE 239 s(6093071 s)

SJ-Edge2#show access-tunnel summary

Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 2

Name    RLOC IP(Source)    AP IP(Destination)     VRF ID  Source Port    Destination Port
------  ---------------  ------------------  ------  -----------  ----------------
Ac0       10.127.84.105     10.127.85.88             0       N/A             4789
Ac1       10.127.84.105     10.127.85.85             0       N/A             4789

Name   IfId          Uptime
------ ---------- --------------------
Ac0    0x0000003D 6 days, 23:36:15
Ac1    0x00000046 6 days, 23:36:13
```

Note the AP in the CDP

AP should be reachable

Note the “Uptime” of the access-tunnel

Fabric Edge(s) Checks

```
SJ-Edge2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
10:06:ED:FC:2C:1C   10.127.85.87     58401       dhcp-snooping  1027  GigabitEthernet1/0/24
D0:37:45:B7:50:27   10.127.85.51     8640112     dhcp-snooping  1025  AccessTunnel0
10:06:ED:FC:2C:DC   10.127.85.85     57106       dhcp-snooping  1027  GigabitEthernet1/0/1
Total number of bindings: 3

SJ-Edge2#show lisp instance-id 8194 ethernet database wlc

WLC clients/access-points information for router lisp 0 IID 8194

Hardware Address   Type    Sources   Tunnel Update

----------------  ------  -------  -------------
d037.45b7.5027     client  2        Signalled

SJ-Edge2#
```

Note the IP address and the MAC of the client

Note the client should be in “Signalled” Tunnel Update state. Same is signalled by WLC via Control Plane node

Fabric Edge(s) Checks

```
SJ-Edge2#show cts role-based permissions
IPv4 Role-based permissions default:
        Deny IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 4:Employee to group Unknown:
        Permit IP-00


SJ-Edge2#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor  HW-Monitor
*       *       0          27477      0           0           0           0
0       0       0          0          0           17913110    0           0
2       0       0          0          0           8213220     0           0
4       0       0          0          0           7813220     0           0
```

Note the required permissions are present for the corresponding SGTs

Note the HW-Permitt or SW-Permitt is happening and HW-Denied is not incrementing

Fabric Edge(s) Checks

```
SJ-Edge2#show vlan

VLAN Name                                        Status    Ports
---- ----------------------------------- --------- -------------------------------
1025 10_127_85_48-Corp                           active    L2LI0:8194,
1027 10_127_85_80-INFRA_VN                       active    L2LI0:8193, Gi1/0/1, Gi1/0/24

SJ-Edge2#show run | s  instance-id 8194
 instance-id 8194
  service ethernet
   eid-table vlan 1025
   database-mapping mac locator-set rloc_b99de326-de2f-4125-9f35-40fcf2d020c7
   exit-service-ethernet
  !
  exit-instance-id
SJ-Edge2#
```

Note the Vlans, client IP pool and AP IP pool names along with L2 VNID instances

Vlan 1025 is mapped to L2 LISP instance-id 8194

Fabric Edge(s) Checks

```
SJ-Edge2#show run interface Vlan1025
interface Vlan1025
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f48b
 vrf forwarding Corp
 ip address 10.127.85.49 255.255.255.240
 ip helper-address 10.127.84.8
 ip helper-address 10.127.84.9
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 10_127_85_48-Corp-IPV4
end

SJ-Edge2#show run interface Loopback0
interface Loopback0
 description Fabric Node Router ID
 ip address 10.127.84.105 255.255.255.255
 ip router isis
 clns mtu 1400
end
```

Note the configuration is deployed by the Catalyst Center. Please take note of the VRF, IP Pool and DHCP details.

Note the Loopback0 IP of the Edge

Fabric Edge(s) Checks

```
SJ-Edge2#show ip interface Vlan1025
Vlan1025 is up, line protocol is up
  Internet address is 10.127.85.49/28
  ...
  MTU is 9100 bytes
  Helper addresses are 10.127.84.8
                       10.127.84.9
  ...
  VPN Routing/Forwarding "Corp"

SJ-Edge2#show lisp session

Sessions for VRF default, total: 2, established: 2
Peer                    State     Up/Down      In/Out    Users
10.127.84.100:4342      Up        2w6d         169/124   10
10.127.84.101:4342      Up        2w6d         169/124   10
```

Note the SVI is in up/up state, MTU is 9100, DHCP Helper addresses are present, VRF

Note the LISP session is “Up” with the CPs

Control Plane (CP) Node Checks

```
SJ-BDR1#show lisp session

Sessions for VRF default, total: 16, established: 11
Peer                    State     Up/Down     In/Out     Users
10.127.84.21:59391      Up        2w6d        57/46      2
10.127.84.105:15603     Up        2w6d        124/169    8
SJ-BDR1#
SJ-BDR1#show lisp instance-id 8194 ethernet server registration-history reverse
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event

Timestamp (UTC)         Instance  Proto     Roam    WLC     Source
                                                            EID prefix / Locator
*Sep 30 15:00:59.750    8194      TCP       No      No      10.127.84.105
                                                          + d037.45b7.5027/48
```

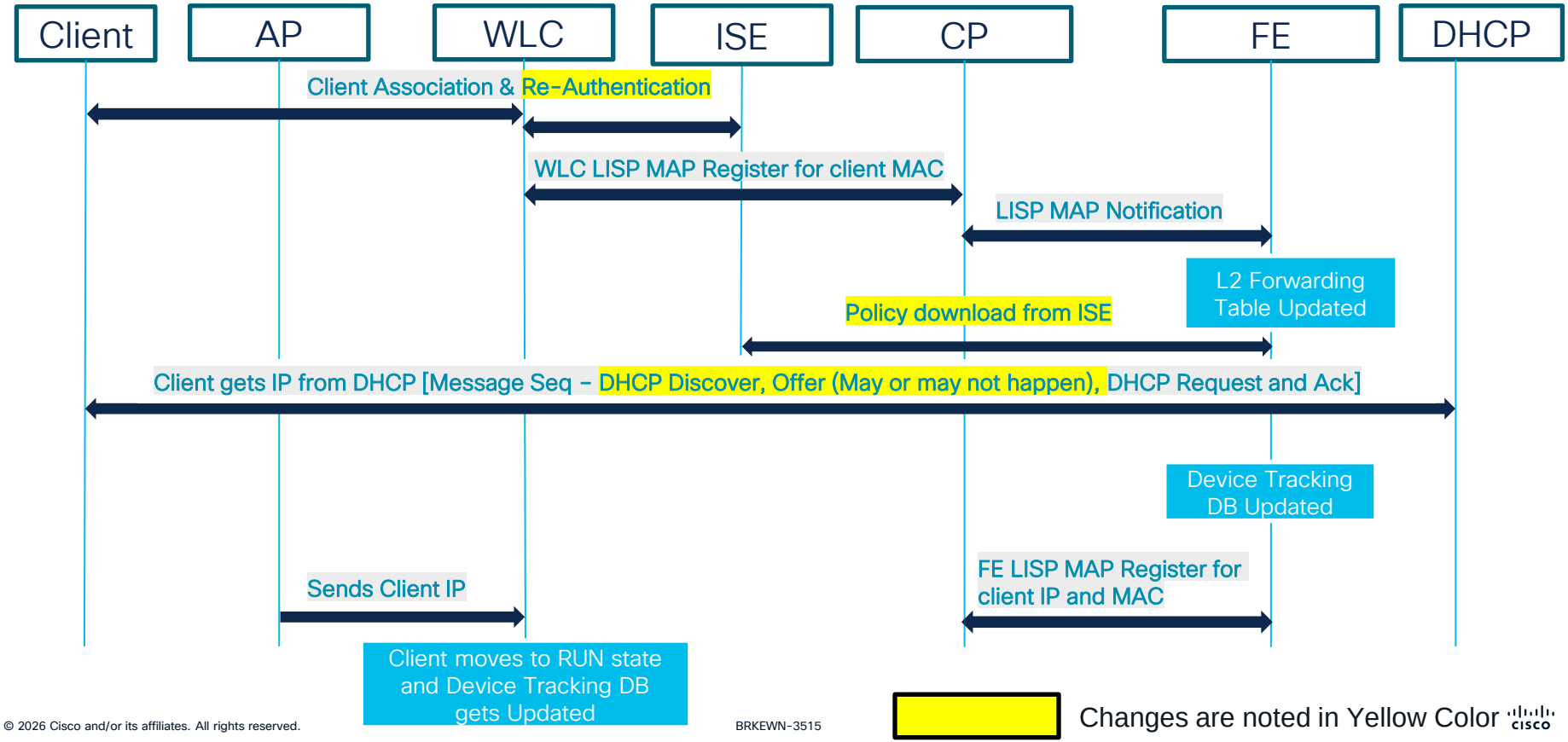
Note the LISP sessions being “Up” with the WLC and Edge.

Note the LISP registration history and + symbol

Client Roaming Flow

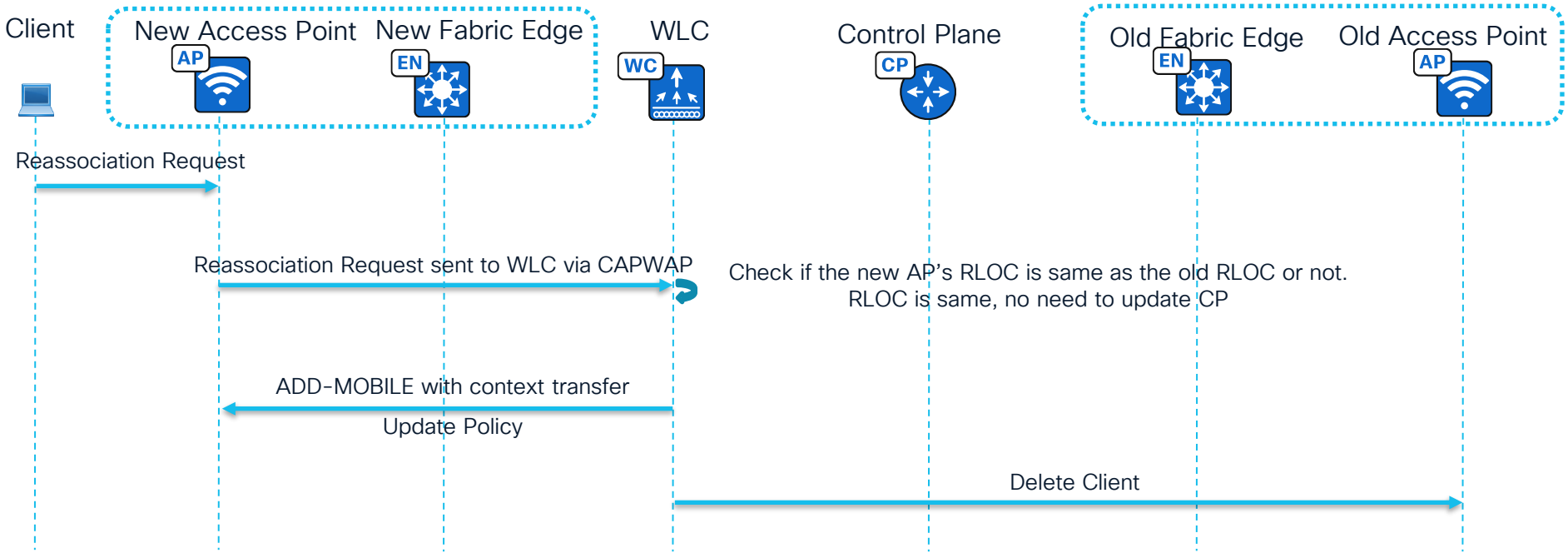
Client Roaming Flow

Changes w.r.t Client Onboarding – Client moves from one AP to other

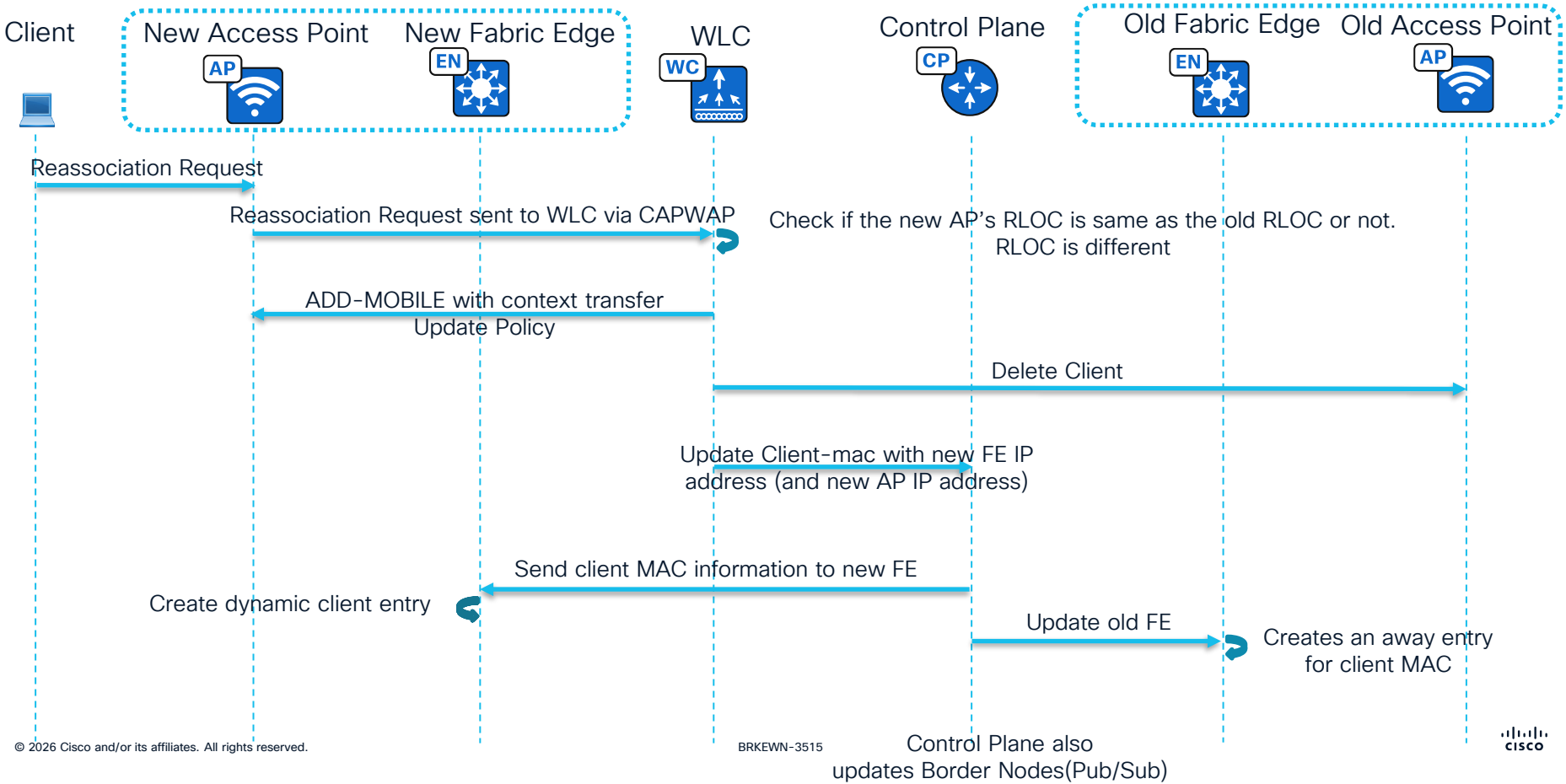


Changes are noted in Yellow Color

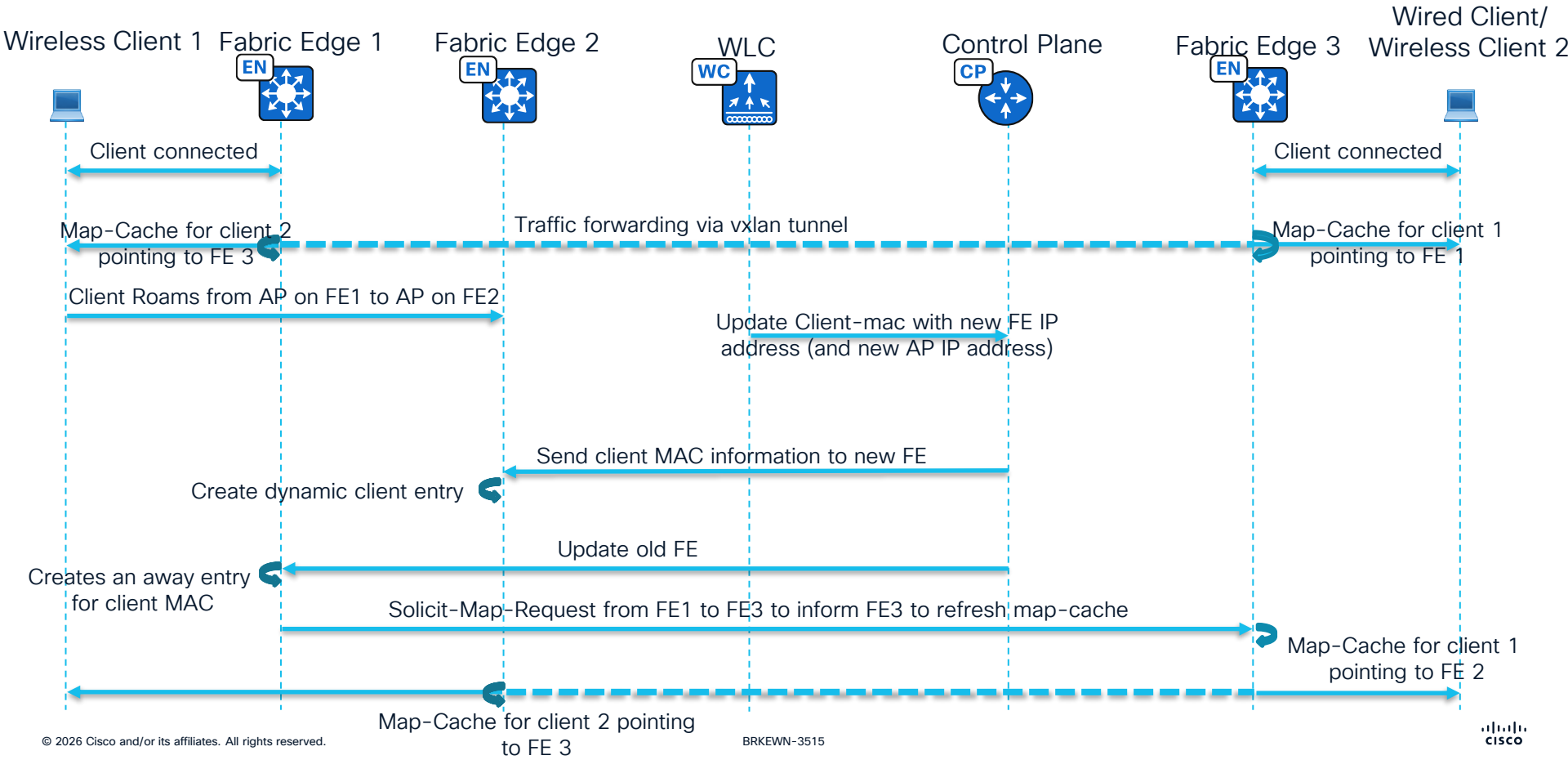
Fabric Client Roaming across AP on Same Fabric Edge



Fabric Client Roaming across AP on Different Fabric Edge



Traffic convergence with Fabric Client Roaming



cisco

Client Roaming Flow – RA Traces

Note the reassociation received, IP Learn complete and Roam Success Messages

Client Reassociation

2024/09/30 15:17:58.739820062 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: d037.45b7.5027 **Re-Association received.** BSSID 2c57.4158.71a1, WLAN SJ_Corp_SSID_profile, Slot 0 AP 2c57.4158.71a0, SJ-Edge1-AP2, Site tag ST_SanJo_Corporat_9248f_0, Policy tag PT_SanJo_Corpo_Corporat_78519, Policy profile SJ_Corp_SSID_profile, Switching Local, Socket delay 0ms

2024/09/30 15:17:58.743611610 {wncd_x_R0-0}{1}: [sisf-gleaner] [15082]: (note): **Wireless reassociation received from CO for mac: d037.45b7.5027**, Vlan: 1, Zone-id: 0x00000000, if_handle : 0x90000015

2024/09/30 15:17:58.743717084 {wncd_x_R0-0}{1}: [client-iplearn] [15082]: (debug): MAC: d037.45b7.5027 Client event to WSA from EWLC_CLIENT_FSM_IPLEARN: **State from: S_IPLEARN_COMPLETE to: S_IPLEARN_COMPLETE on: E_IPLEARN_INTRA_WNCD_ROAM**

2024/09/30 15:17:58.743728958 {wncd_x_R0-0}{1}: [wsa-clt-evt] [15082]: (debug): WSA CLT FSM EVT create Populate: **Skipping duplicate event reason Mac:d037.45b7.5027, Event:WSA_CL_EVENT_INVALID, Reason: WSA_CL_EVT_REASON_INTRA_CTRL_ROAM_SUCCESS**

Client Roaming Troubleshooting

WLC Checks

Note the client mobility history

```
c9800-40-SJC#show wireless client mac d037.45b7.5027 mobility history

Recent association history (most recent on top):

AP Name          BSSID          AP Slot  Assoc Time           Instance  Mobility Role  Run Latency (ms)  Dot11 Roam Type
-------------------------------------------------------------------------------------------------------------------
SJ-Edge2-AP2     889c.ade7.9881  0       09/30/2024 20:30:26  0         Local          318               802.11i Slow
SJ-Edge1-AP2     2c57.4158.71a1  0       09/30/2024 20:10:26  0         Local          393               802.11i Slow

c9800-40-SJC#
```

Control Plane (CP) Checks

SJ-BDR1#show lisp instance-id 8194 ethernet server registration-history reverse
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event

Timestamp (UTC)	Instance	Proto	Roam	WLC	Source EID prefix / Locator
*Sep 30 15:00:59.750	8194	TCP	No	No	10.127.84.105 + d037.45b7.5027/48
*Sep 30 15:00:59.748	8194	TCP	No	No	10.127.84.104 - d037.45b7.5027/48
*Sep 30 15:00:59.745	8194	TCP	Yes	Yes	10.127.84.21 + d037.45b7.5027/48 / 10.127.84.105
*Sep 30 14:41:00.082	8194	TCP	No	No	10.127.84.104 + d037.45b7.5027/48
*Sep 30 14:41:00.081	8194	TCP	No	Yes	10.127.84.21 + d037.45b7.5027/48 / 10.127.84.104

Note the LISP registration history for the client
+, -

Some troubleshooting tools

Cisco WLC and Monitoring Catalyst Center

Scenario : Obtain insights, assurance information, collect troubleshooting command outputs and various reports

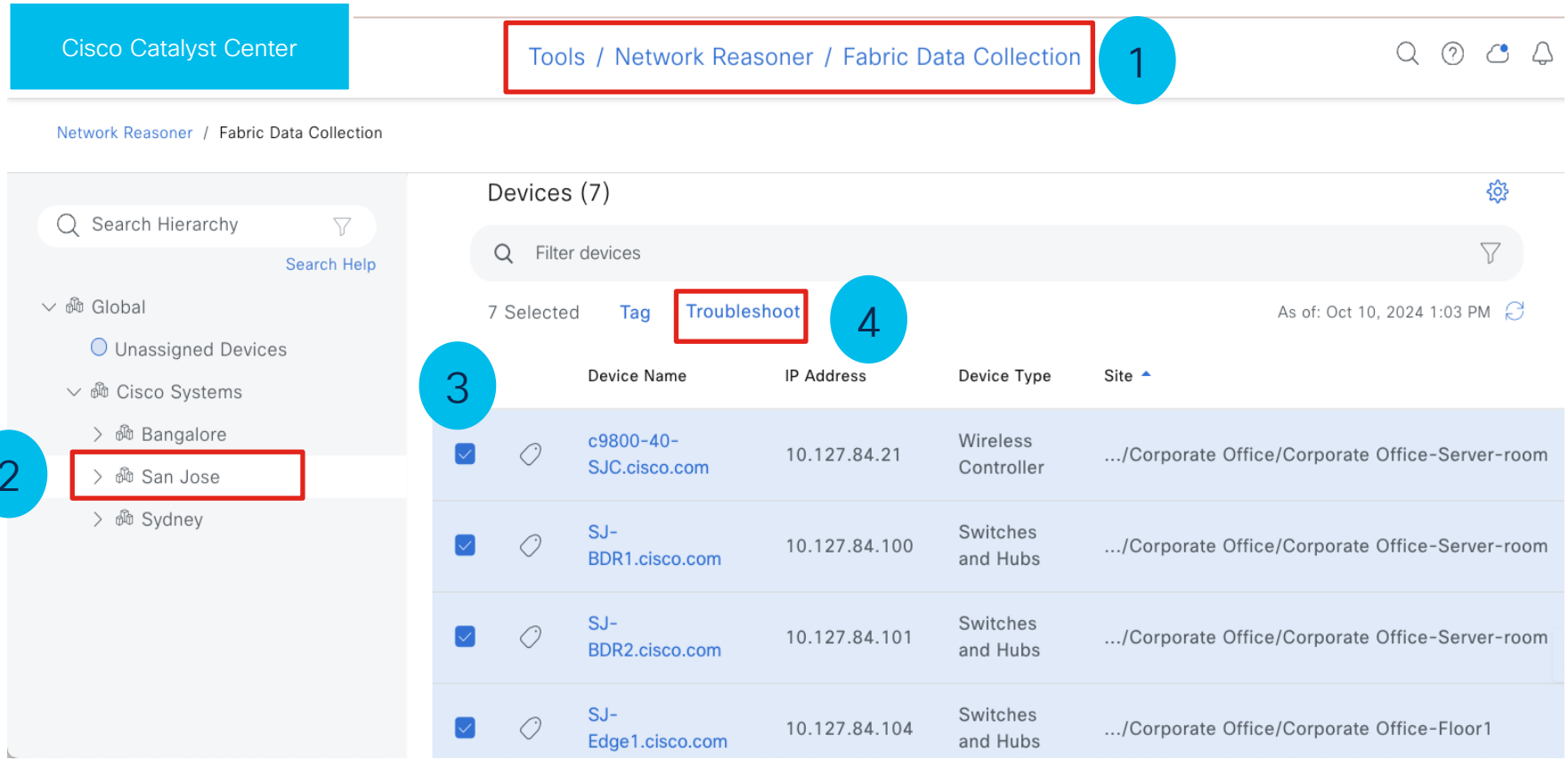
Catalyst Centre

- Leverage CatC for 360 troubleshooting of networks and clients.
- Example : Network Reasoner, Reports, Assurance

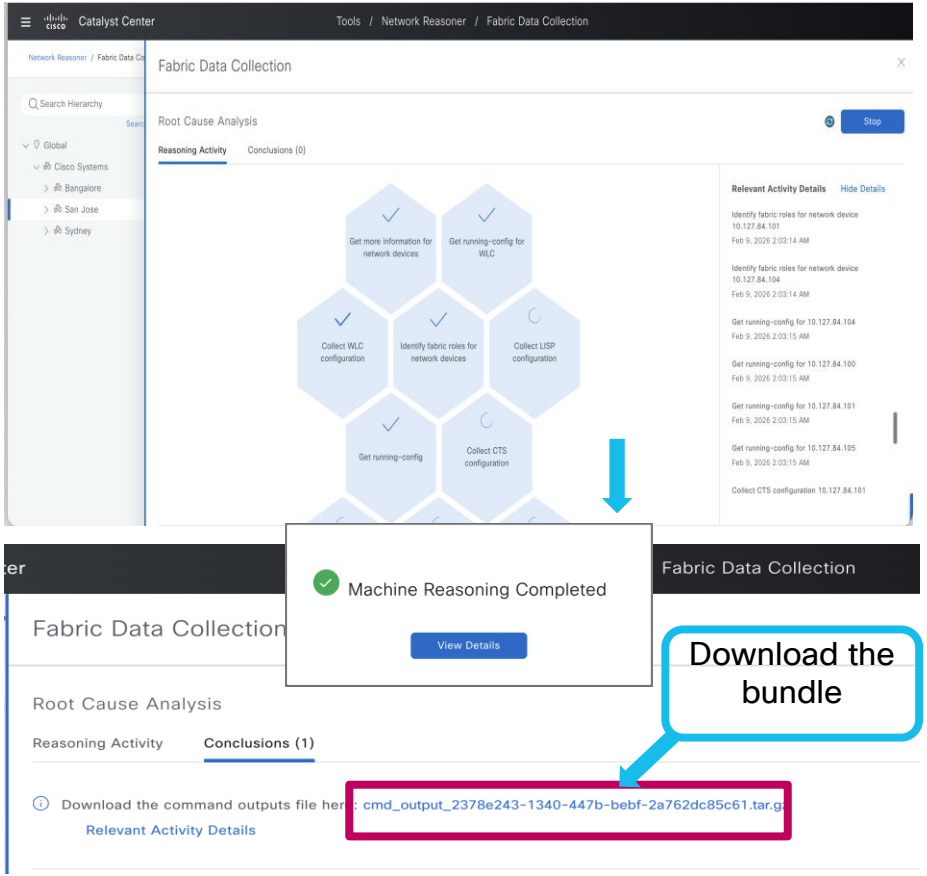
Cisco WLC

- Troubleshooting tools from Cisco WLC
- Example : Packet Captures, Debug bundle, Radioactive Traces

Network Reasoner - Fabric Data Collection



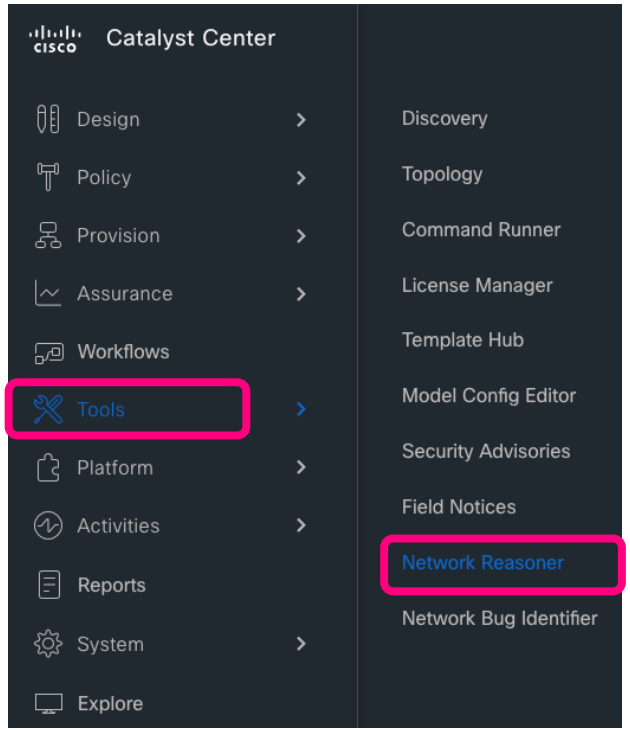
Network Reasoner - Fabric Data Collection



Download the SDA_Digger tool from https://github.com/michelpe/SDA_Digger . Unzip the SDA_Digger file and it shall unzip into a folder. Analyse as following :-

```
gkondave@GKONDAVE-M-56JK SDA_Digger-master % python3 SDA_Digger.py -b ../cmd_output_2378e243-1340-447b-bebf-2a762dc85c61/
Starting SDA Digger tool
Session Analysis: Checked LISP sessions on 4 nodes towards 2 CP nodes. Found 8 sessions, missing 0, failures 0
LISP Database Analysis: 192.168.4.1/32 : In LISP database on SJ-BDR1(10.127.84.100) CP node: SJ-BDR1 reports RLOC 10.127.84.101
LISP Database Analysis: 192.168.4.1/32 : In LISP database on SJ-BDR1(10.127.84.100) CP node: SJ-BDR1 reports RLOC 10.127.84.101
LISP Database Analysis: 192.168.4.1/32 : In LISP database on SJ-BDR2(10.127.84.101) CP node: SJ-BDR2 reports RLOC 10.127.84.100
LISP Database Analysis: 192.168.4.1/32 : In LISP database on SJ-BDR2(10.127.84.101) CP node: SJ-BDR2 reports RLOC 10.127.84.100
LISP Database Analysis: Number of EID checked 28, failed 2
LISP Database Analysis: Number of Local EID 8
LISP Database Analysis: Number of Devices checked 4
MTU Analysis: System MTU in fabric 9100, configured on 4 devices, misconfigured on 0 devices
Device-tracking analysis: Verified 2 edge devices with SVI info, 4 success, 0 mismatches 0 info missing
Authentication Analysis: client 0caf.31ff.3820 on GigabitEthernet1/0/19 SJ-Edge2 not showing an IPv4 Address
Authentication Analysis: client 0caf.31ff.3824 on GigabitEthernet1/0/20 SJ-Edge2 not showing an IPv4 Address
Authentication Analysis: client 0caf.31ff.3828 on GigabitEthernet1/0/21 SJ-Edge2 not showing an IPv4 Address
Authentication Analysis: client 0caf.31ff.382c on GigabitEthernet1/0/22 SJ-Edge2 not showing an IPv4 Address
Authentication Analysis: client 0caf.31ff.3830 on GigabitEthernet1/0/19 SJ-Edge1 not showing an IPv4 Address
Authentication Analysis: client 0caf.31ff.3834 on GigabitEthernet1/0/20 SJ-Edge1 not showing an IPv4 Address
Authentication Analysis: client 0caf.31ff.3838 on GigabitEthernet1/0/21 SJ-Edge1 not showing an IPv4 Address
Authentication Analysis: client 0caf.31ff.383c on GigabitEthernet1/0/22 SJ-Edge1 not showing an IPv4 Address
Authentication Analysis: Verified 10 sessions on 2 edges
Authentication Analysis: Found 0 Failed Authentication sessions
Reachability Analysis: Fabric Edge Devices with full (/32) reachabily 4, devices without full reachability 0, not checked 0
CTS Permissions Analysis: Verified 2 permissions entries on 2 devices with 0 failures
CTS Analysis: verified CTS on 4 nodes, 0 failures found
SVI Analysis: Verified 2 edge devices with SVI info, 2 consistent , 0 inconsistent, 0 border devices with inconsistent SVI info
Access-Tunnel Analysis: Verified 2 devices:3 Access tunnels up 0 were not up on platform side, 0 edges were skipped
Duplicate Addresses Analysis:Checked 12 addresses in LISP databases, found 0 duplicate addresses
Reachability Analysis: Fabric Edge Devices with full (/32) reachabily 4, devices without full reachability 0, not checked 0
gkondave@GKONDAVE-M-56JK SDA_Digger-master %
```

Network Reasoner



1 **Wireless AP Data Collection**

Collect show output, logs, and PCAP for an Access Point (AP) on its associated Catalyst 9800 WLC and via SSH to the AP for up to 30 minutes

Network Performance Impact: Medium

CX

2 **Wireless Client Data Collection**

Collect show output, logs, and PCAP for a Wireless Client on 1-2 Catalyst 9800 WLCs and up to 5 APs via SSH for up to 30 minutes

Network Performance Impact: Medium

CX

Running Machine Reasoning – AP Data Collection

Reasoner Inputs

Troubleshoot Duration (5-30 minutes)*
5

Two AP MAC address (A,B)*
a49b.cd5a.b160,a49b.cd47.f474

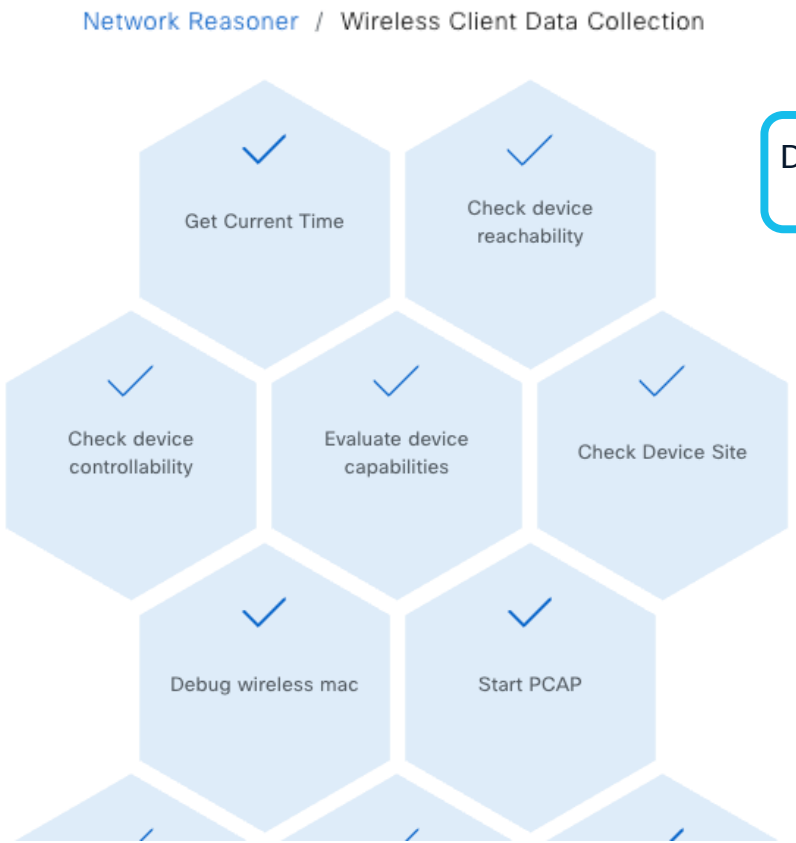
PCAP Interface
GigabitEthernet0

AP IP address*
10.107.79.18

AP Name*
9120AP

Run Machine Reasoning

Network Reasoner Activity - Client



Detailed insights of activities

Relevant Activity Details Hide Details

Check if the device f45a3cc3-d96c-46d1-a33d-7ecc147e6fe9 is provisioned or assigned to a site.
Sep 13, 2025 11:32:38 PM

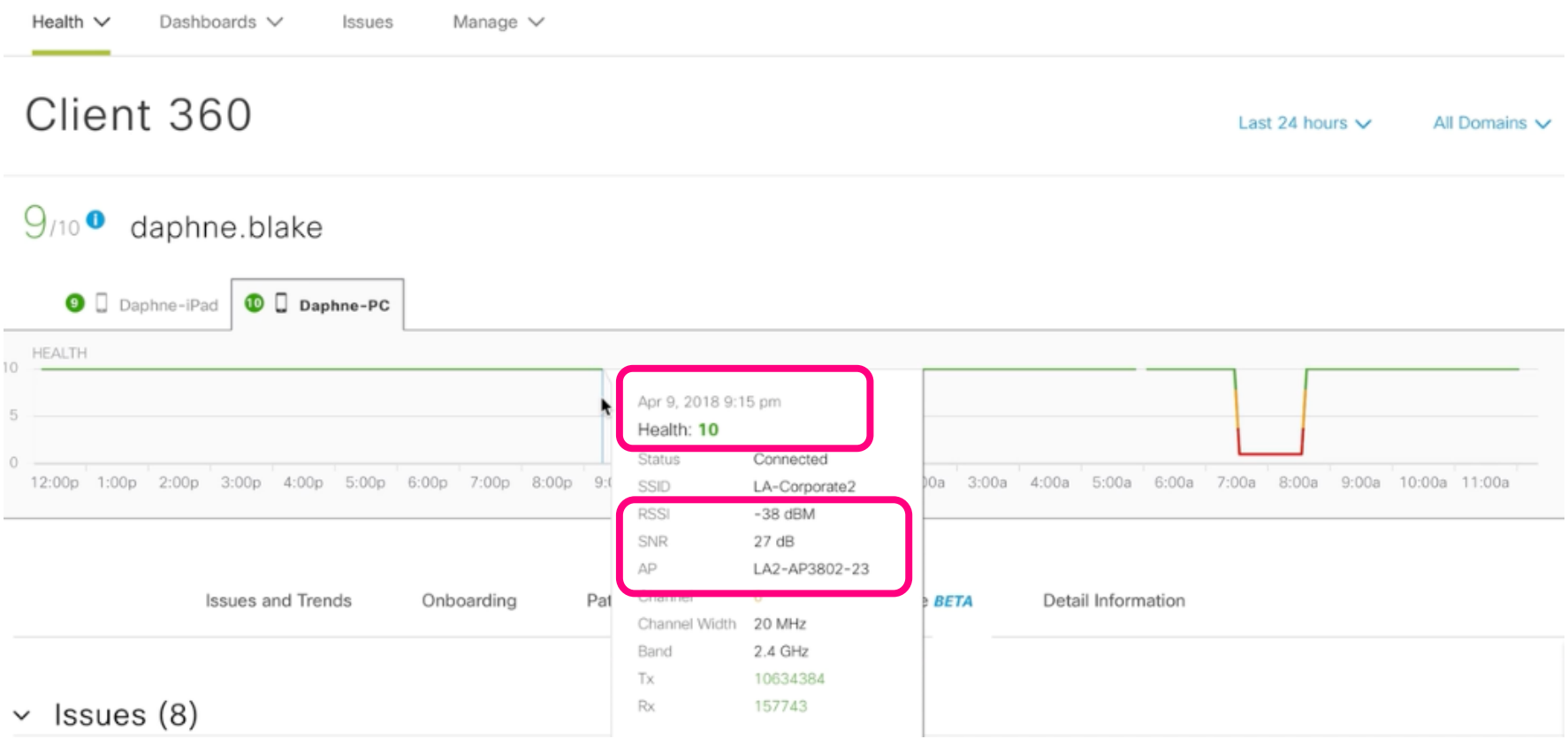
Debug wireless mac
Sep 13, 2025 11:32:44 PM

Get Current Time
Sep 13, 2025 11:32:44 PM

Starting Client PCAP session mre_client_pcap_1757786564883 with filter ec63.d7fc.f729 on interface GigabitEthernet0
Sep 13, 2025 11:32:45 PM

Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.84.21 for filename: c9800-40-SJC.cisco.com-ec63.d7fc.f729-1757786555655.txt

Client 360



Client 360 – Issues Insights

- Client A took longer to authenticate due to network delay.
- Network latency for Netflix application above 387ms.
- Client B connectivity issue due to RF at AP location B.

Issues (4)

Onboarding

Wireless client took a long time to connect (SSID: LA-Corporate2, AP: LA2-AP3802-23, Band: 2.4 GHz) - Excessive time for Authentication due to AAA server or Network delays

Total occurrences: 9

Application

Network Latency for Application 'netflix' is Above the Threshold Value of 387ms.

Total occurrences: 16

Application

Network Latency for Application 'disney-web-portal' is Above the Threshold Value of 262ms.

Total occurrences: 11

Onboarding

Wireless client took a long time to connect (SSID: LA-Corporate2, AP: LA2-AP3802-23, Band: 2.4 GHz, Site: Global/USA/SM/Level1) - Excessive time due to RF issues

Total occurrences: 4

Detailed insights of the issue

Wireless client took a lon
delays
Total occurrences: 9

Application
Network Latency for App
Total occurrences: 16

Application
Network Latency for App
Total occurrences: 11

Onboarding
Wireless client took a lon
Total occurrences: 4

Onboarding

Status: Open

Description

This client is taking longer than expected time to connect to 'LA-Corporate2' SSID due to excessive authentication time.

- Onboarding took 36.4 seconds (expected time should be less than 10.0 seconds).
- Association took less than a second (expected time should be less than 2.0 seconds)
- Authentication and Key Exchange took 30.8 seconds (expected time should be less than 3.0 seconds)
- IP Addressing took 0 seconds (expected time should be less than 5.0 seconds)

Onboarding Transaction Log

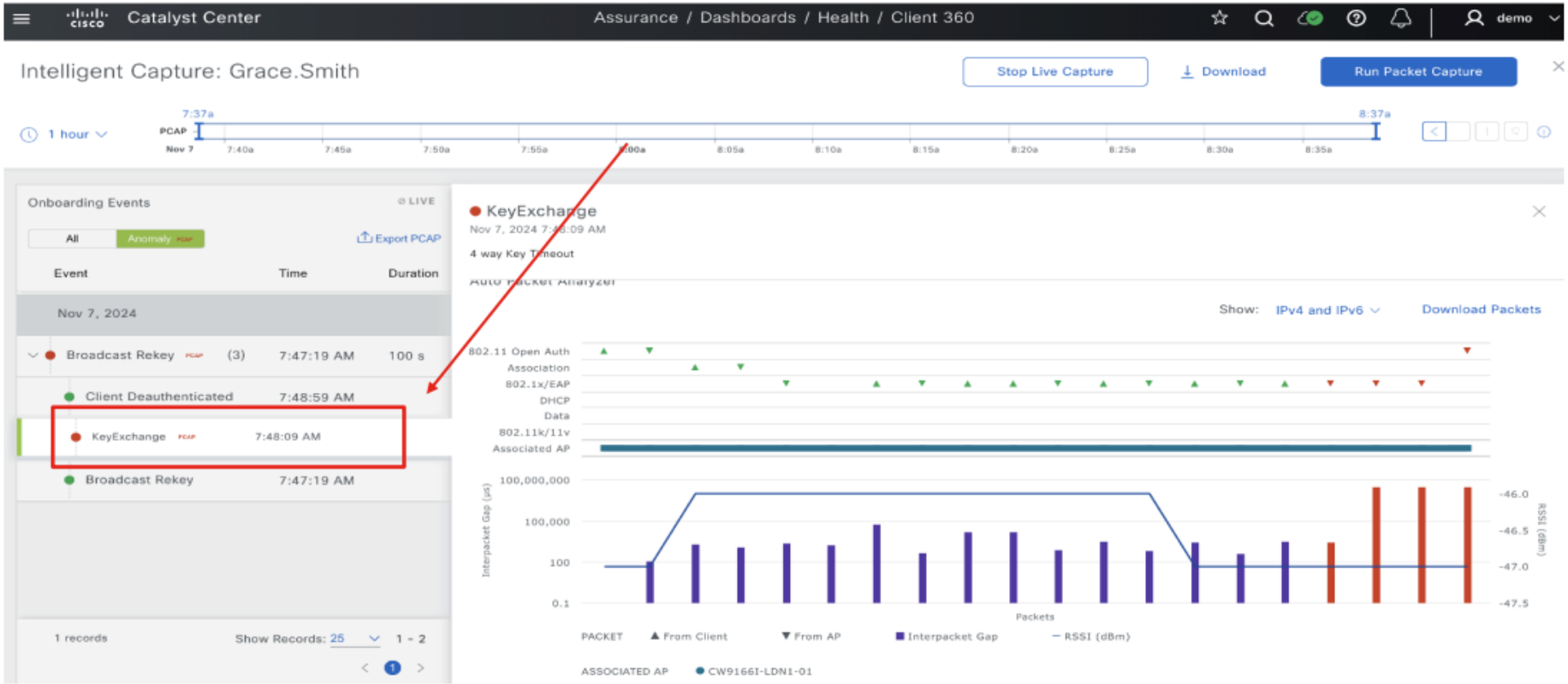
Find

Event	Reason	Date / Duration
Failure	4 Way Key Timeout	5.55 sec
Success		30.85 sec

Event	Reason
Auth Start	PMK Cache Expired
Auth Done	dot1x Full Auth
L2Key Done	4 Way Key Timeout
Send Deauth	

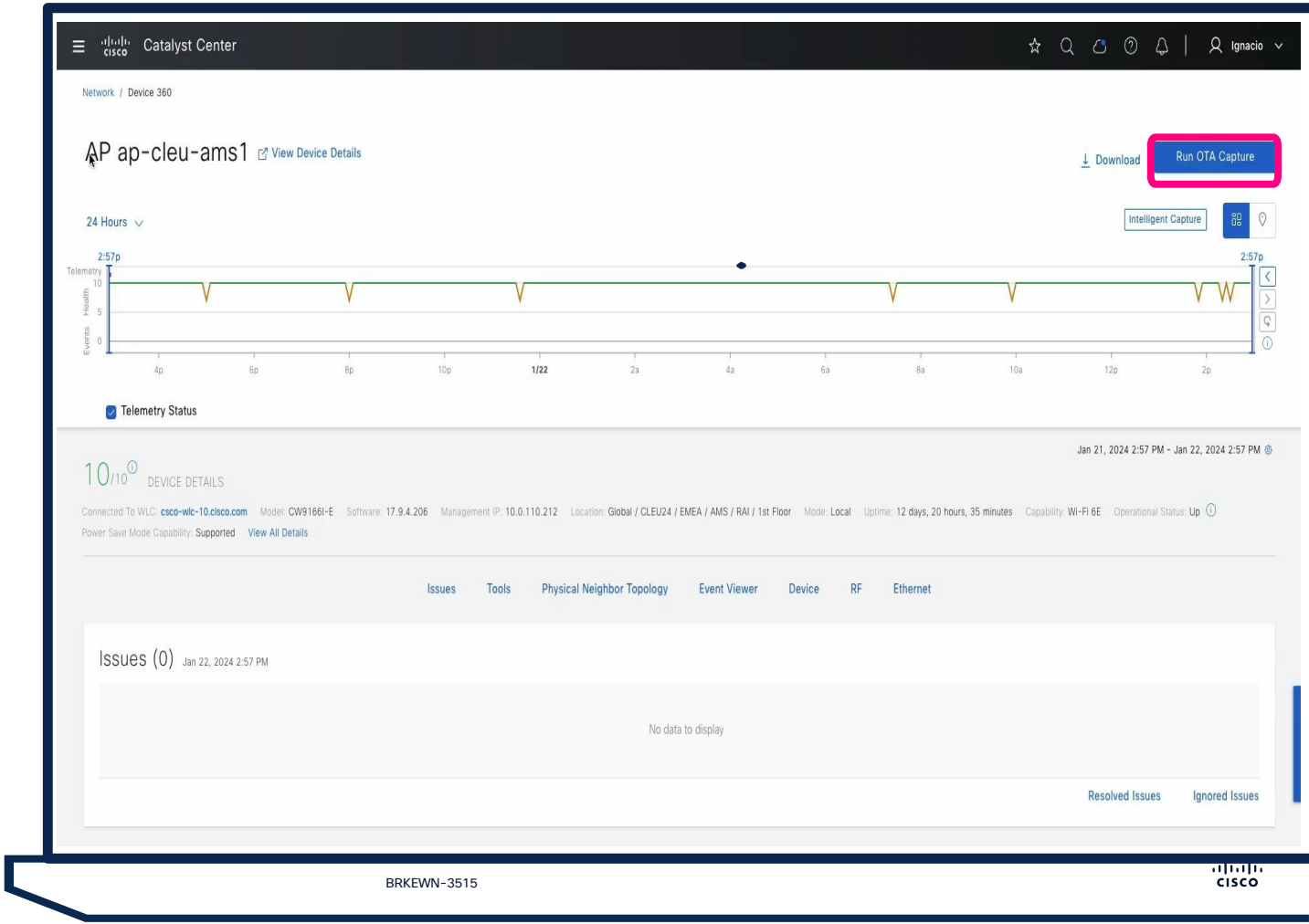
Failure due to – 4 way handshake key timeout

ICAP (Intelligent Capture) in Catalyst Center – Client 360



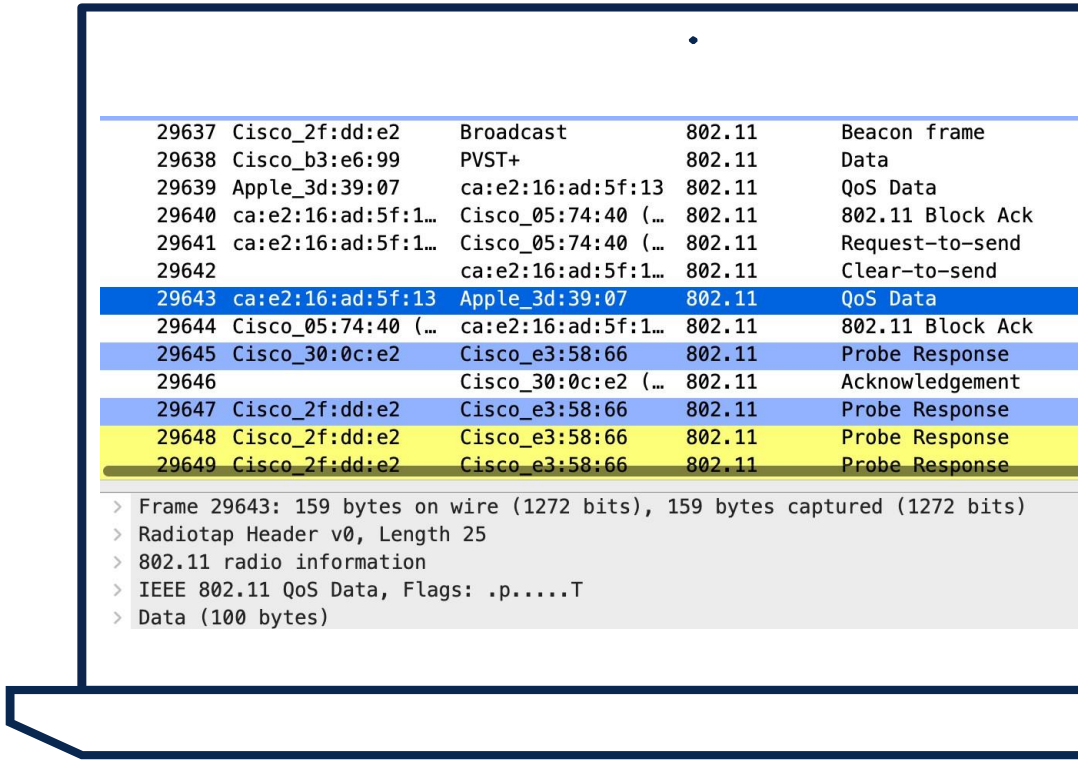
OTA capture

- Go to AP Device 360 View
- Run OTA Capture
- Select band, radio, channel width and channel



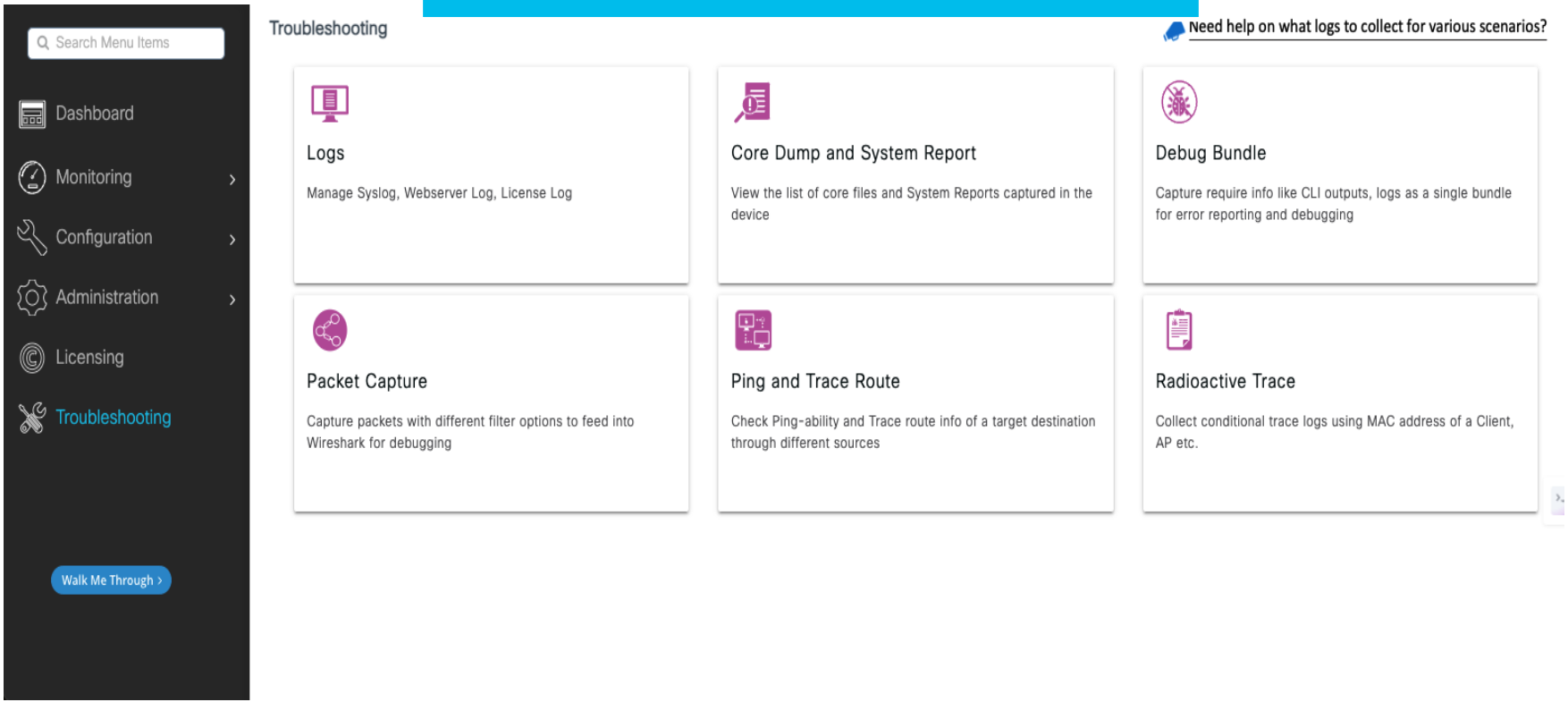
AP Packet Capture Type

- OTA Sniffer
  - Turns radio into Sniffer mode, no client serving capability
  - Captures all packets on specific channel
  - Requires 17.11 and 2.3.7

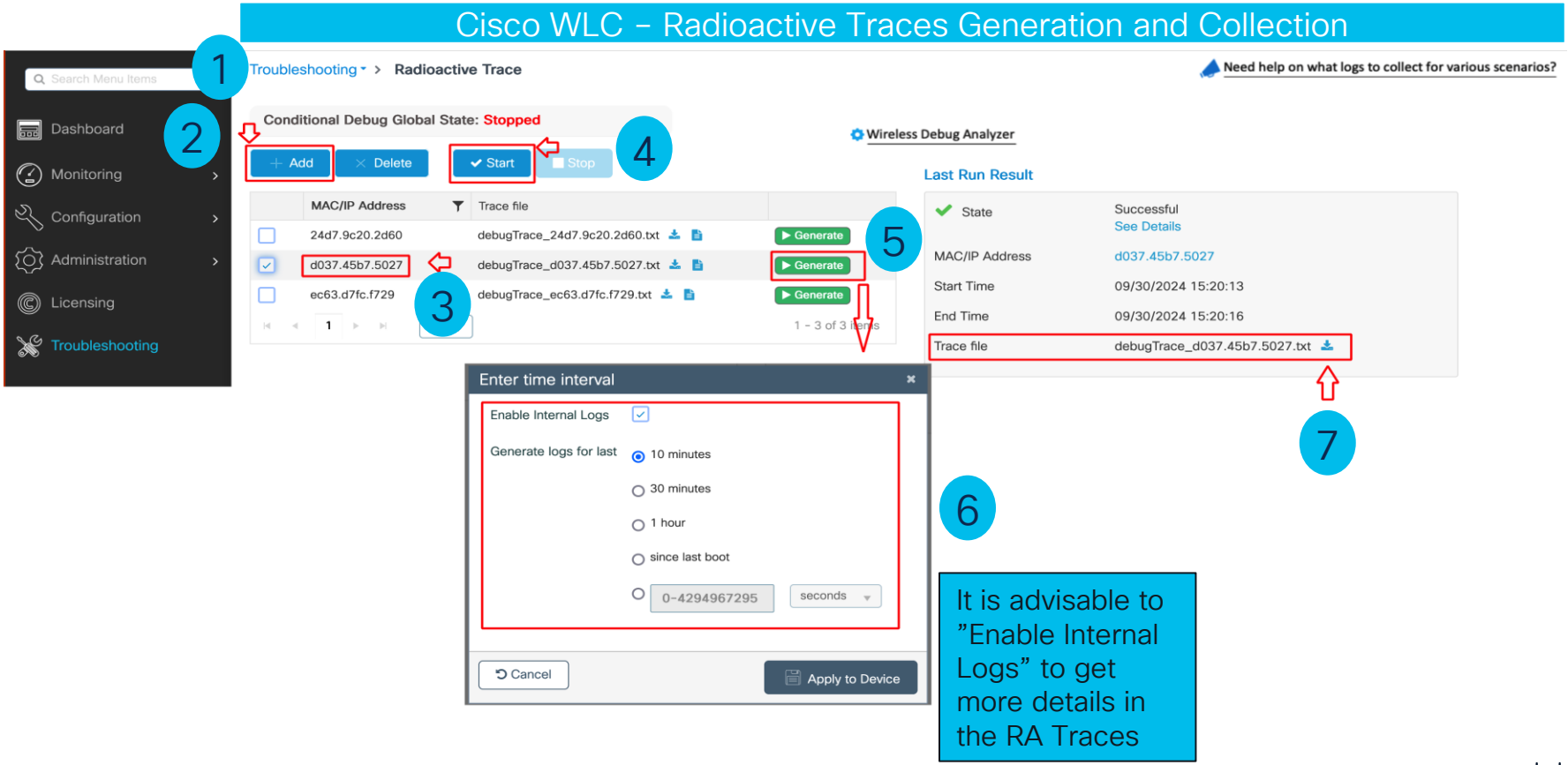


Cisco WLC – Troubleshooting Tools

Cisco WLC – Troubleshooting Tools



Cisco WLC – Radioactive Traces Generation and Collection



Some Tools

1) Assurance Dashboards, Client 360 - Cisco Catalyst Center
2) Network Reasoner – Cisco Catalyst Center

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/b_collect_data_from_sda_fabric.html

3) OTA Captures – Cisco Catalyst Center

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/catalyst-center-assurance/2-3-7/b_cisco_catalyst_assurance_2_3_7_ug/b_cisco_catalyst_assurance_2_3_6_ug_chapter_01110.html

4) SPAN Captures – Switches

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9500-series-switches/218111-verify-span-and-erspan-on-catalyst-9000.html

5) Wireless Troubleshooting Tools

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

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

Some More Tools

1) OTA Captures – Cisco Catalyst Center

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/catalyst-center-assurance/2-3-7/b_cisco_catalyst_assurance_2_3_7_ug/b_cisco_catalyst_assurance_2_3_6_ug_chapter_01110.html

2) SPAN Captures – Switches

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9500-series-switches/218111-verify-span-and-erspan-on-catalyst-9000.html

3) Wireless Troubleshooting Tools

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

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

Recap

Architecture Overview

- Best Practices
- Design and Deployment

Basic Workflows and Troubleshooting

- AP Join
- Client Onboarding
- Client Roaming

Some troubleshooting tools

*Some scenarios, useful commands & tools

*Appendix

Complete your session surveys

Complete your surveys in the Cisco Events App.

Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Contact me at: Webex space

Thank you

cisco Live !

Appendix

Some scenarios and the list of useful commands

Scenario -1 - AP is not joining

Dynamic AP Profile is not matching on the ISE and misconfiguration in the policy set, authorization profile

ISE Checks

Policy Sets→ MAB

Policy > Policy Set
Ensure the configuration is correct

Reset | Reset Policyset Hitcounts | Save

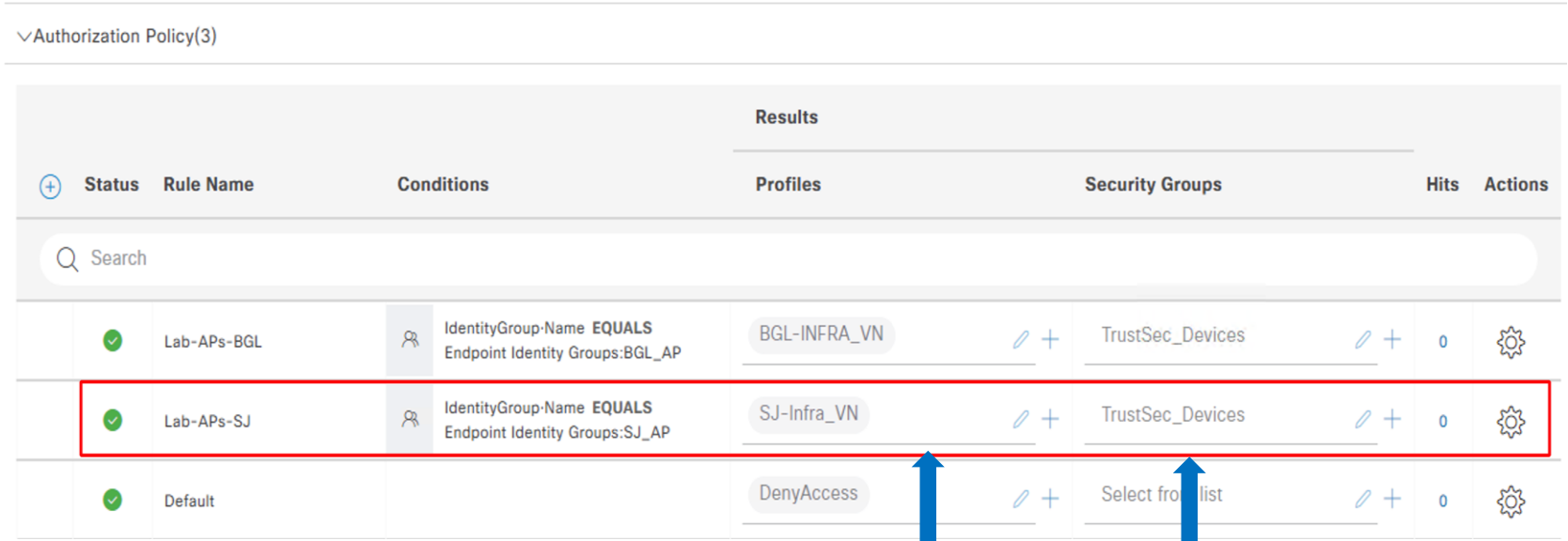
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search					
✓	MAB		OR Normalised Radius·RadiusFlowType EQUALS WiredMAB Normalised Radius·RadiusFlowType EQUALS WirelessMAB	Default Network Access	0

Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
Search					
✓	MAB	OR Normalised Radius·RadiusFlowType EQUALS WiredMAB Normalised Radius·RadiusFlowType EQUALS WirelessMAB	Internal Users Options	0	⚙

Scenario – 1 – Contd

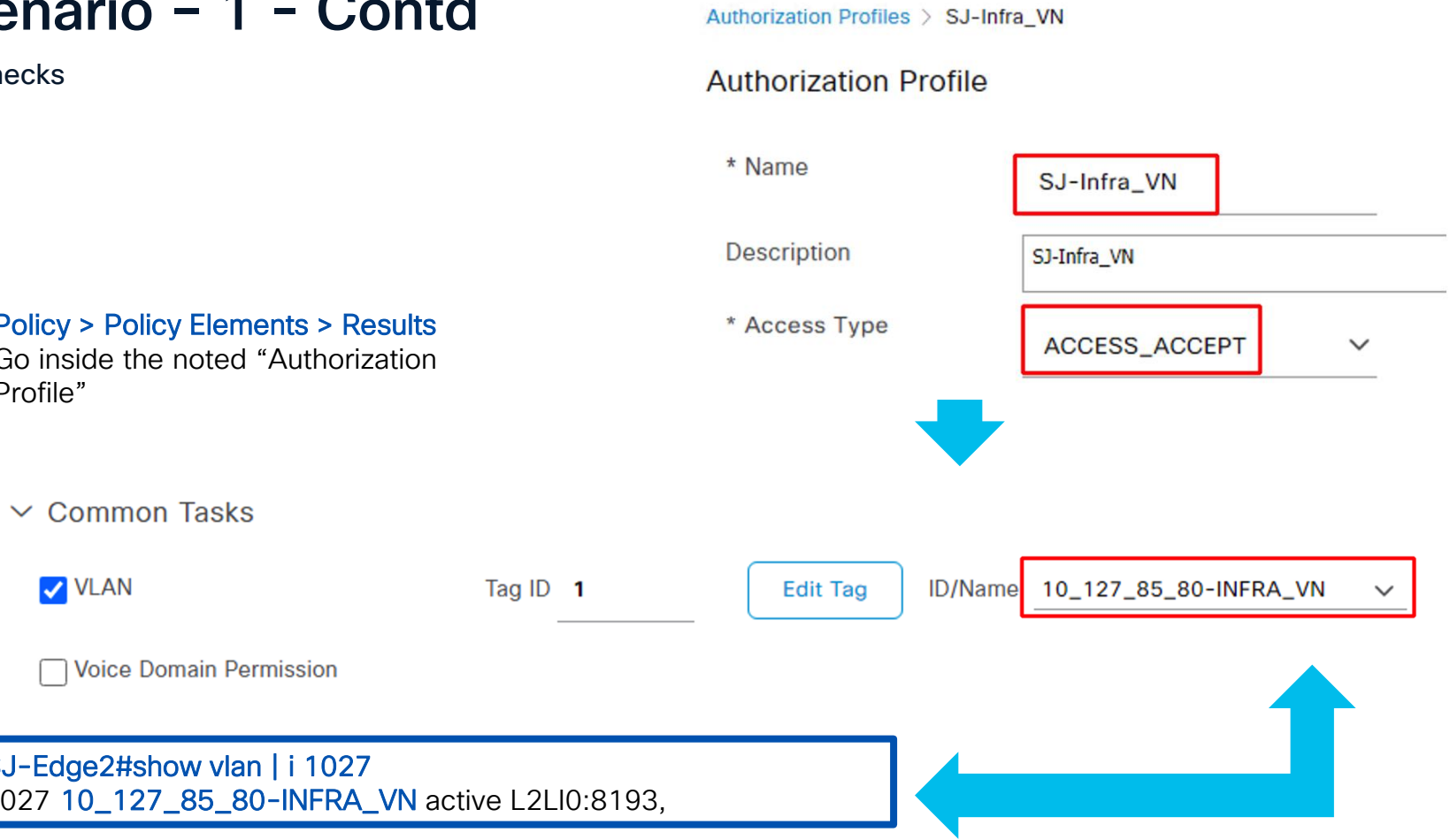
ISE Checks



Scenario – 1 – Contd

ISE Checks

Policy > Policy Elements > Results
Go inside the noted “Authorization Profile”



Scenario – 2

Client stuck in IP Learn – Client abandoned Auth

MAB Authentication is successful, and client is in IP learn state.

IT IS NOT ALWAYS THE NETWORK PROBLEM !! ☺

Client has not initiated the DHCP process

00:28:29.484 {wncd_x_R0-0}{1}: [client-orch-sm] [20578]: (note): MAC: d453.83da.cd5c Association received

00:28:29.487 {wncd_x_R0-0}{1}: [radius] [20578]: (info): RADIUS: Started 5 sec timeout

00:28:29.997 {wncd_x_R0-0}{1}: [dot11] [20578]: (debug): MAC: d453.83da.cd5c send association response.

Note: The clients also have timers and will not move forward if the association takes longer than 200-350 ms. We need to troubleshoot on client side.

Useful commands and debugs

Useful commands and debugs

These are the command cheat sheet for fabric on Control Node, Edge Node, Wireless Lan Controller (WLC), and Access Point (AP).

Control Node:
- **show lisp instance-id <L2 ap instance id> ethernet server** - MAC to Endpoint Identification (EID) Mapping
- **show lisp instance-id <L3 ap instance id> ipv4 server** - IP to EID Mapping
- **show lisp instance-id 8188 ethernet server address-resolution** - MAC to IP Mapping for a specific instance ID
- **show lisp site**
- **show tech-support**
- **show tech-support lisp**

Debugs
- debug lisp control-plane all
- debug platform software l2lisp events
- debug cts all

Edge Node:
- **show lisp instance-id <L2 ap instance id> ethernet database wlc**
- **show lisp instance-id <L2 client instance id> ethernet database wlc**
- **show access-tunnel summary**
- **show platform software fed switch active ifm interfaces access-tunnel**
- **show platform software access-tunnel switch active R0**

Useful commands and debugs

- show platform software access-tunnel switch active R0 statistics
- show platform software access-tunnel switch active F0
- show platform software access-tunnel switch active F0 statistics
- show platform software object-manager switch active F0 statistics
- show platform software object-manager switch active F0 pending-issue-update
- show platform software object-manager switch active F0 pending-ack-update
- show platform software object-manager switch active F0 error-object
- show tech-support
- show tech-support lisp

- Debugs
- debug device-tracking
- debug lisp control-plane all
- debug platform fhs all
- debug platform software l2lisp events
- debug matm all
- debug cts all
- debug access-tunnel detail

Useful commands and debugs

WLC (IOS-XE)
- show ap summary
- show fabric ap summary
- show wireless fabric summary
- show wireless client summary
- show tech-support wireless
- show tech-support wireless fabric
- show tech-support lisp (If Fabric in a box or Embedded wireless running on 9300/9400/9500)
- show tech-support (If Fabric in a box or Embedded wireless running on 9300/9400/9500)

Debugs

debug wireless mac <mac address> internal
debug capwap-idb error
debug capwap-idb info
debug capwap-idb packet

Access Point:
- show ip tunnel fabric
- show tech-support

Diagnostic Tools

Scenario : Troubleshooting AP Join, Best Practices, Client Connectivity, PCAPs

AP/WLC Debugs

- Correlating AP and WLC side of debugs
- Example : AP join issues

WCAE

- Gain insights on best practices, warnings, RF, performance issues
- Example : Checking WLC Performance

Debug Analyzer

- Analyze client RA traces in table, graphical format for quick and easy consumption with various statistics
- Example : Client connectivity

WiFi-Hawk (OTA)

- Get insights on over the air packet capture, outputs from AP
- Example : Debugging an RF Issue

Correlating AP Debugs & WLC Traces

- **AP side debugs** : In AP CLI : **“debug capwap client events”** and **“debug capwap client error”**
- **WLC side** : In WLC : **RA trace** for AP mac address from WLC : **Troubleshooting > RA trace**

1. Discovery Phase

AP Debugs :

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1638] CAPWAP State: Discovery

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1666] Discovery Request sent to 10.127.84.20, discovery type STATIC_CONFIG(1)

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1877] Discovery Response from 10.127.84.20

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1879] Found Configured MWAR 'c9800-40-BGL' (respIdx 0).

WLC RA Trace :

2025/09/07 12:57:47.156982498 {wncmgrd_R0-0}{1}: [capwapac-discovery] [14867]: (note): MAC: 1416.9d2a.bf80 IP:10.127.85.77[5256], Discovery Request received

2025/09/07 12:57:47.157593433 {wncmgrd_R0-0}{1}: [capwapac-discovery] [14867]: (note): MAC: 1416.9d2a.bf80 IP:10.127.85.77[5256], Discovery Response sent

Correlating AP Debugs & WLC Traces

2. DTLS Phase

AP Debugs :

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.0099] CAPWAP State: DTLS Setup

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.0240] DTLS connection created sucessfully local_ip: 10.127.85.77 local_port: 5256 peer_ip: 10.127.84.20 peer_port: 5246, app_tag: 2C5741582524 CN:Cisco Manufacturing CA III

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.0649] dtls_verify_server_cert: Controller certificate verification successful

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.4022] Dtls Session Established with the AC 10.127.84.20, port 5246

WLC RA Trace :

2025/09/07 12:57:47.222608830 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (note): MAC: 1416.9d2a.bf80 DTLS session create callback received.

2025/09/07 12:57:47.284328730 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [15069]: (info): Remote Host: 10.127.85.77[5256] MAC: 1416.9d2a.bf80 Completed cert verification, status:CERT_VALIDATE_SUCCESS

Correlating AP Debugs & WLC Traces

3. Join Phase

AP Debugs :

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.4135] CAPWAP State: Join

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3521] Sending Join request to 10.127.84.20 through port 5256, packet size 1376

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3565] Join Response from 10.127.84.20, packet size 1397

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3873] Starting Post Join timer

WLC RA Trace :

2025/09/07 12:57:48.550108207 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [15069]: (note): MAC: 1416.9d2a.bf80 Received CAPWAP join request

2025/09/07 12:57:48.553214349 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [15069]: (note): MAC: 1416.9d2a.bf80 Successfully processed Join request. AP name: BGL-Edge1-AP1, Model: C9130AXE-D, radio slots: 3, rlan slots: 0, site tag name: ST_Banga_BGL18_caba6_0, policy tag name: PT_Banga_BGL18_BGL18-Se_52ab9, rf tag name: TYPICAL

2025/09/07 12:57:48.553368425 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (info): MAC: 1416.9d2a.bf80 Join Response generated with MTU 1485, as per MTU payload, update flag: 0

2025/09/07 12:57:48.553386207 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (note): MAC: 1416.9d2a.bf80 Join processing complete. AP in joined state

Correlating AP Debugs & WLC Traces

4. Image

AP Debugs :

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3962] CAPWAP State: Image Data

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3968] AP image version 17.9.5.47 backup 17.9.3.50, Controller 17.9.5.47

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3969] CAPWAP Image Data: MWAR Controller image running version 17.9.5.47 is accepted.

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3969] Version is the same, do not need update.

WLC RA Trace :

2025/09/07 12:57:48.554127571 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [15069]: (info): 1416.9d2a.bf80 Retrieved AP SW version: 17.9.5.47, for AP model: C9130AXE-D, AP image type: ap1g6a, site-tag: ST_Banga_BGL18_caba6_0

Correlating AP Debugs & WLC Traces

5. Configure & Run

AP Debugs :

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.5007] CAPWAP State: Configure

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.8400] Configuration Status sent to 10.127.84.20 (part 0)

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.8434] Configuration Status Response from 10.127.84.20

Sep 7 12:57:49 kernel: [*09/07/2025 12:57:49.3048] CAPWAP State: Run

Sep 7 12:57:49 kernel: [*09/07/2025 12:57:49.3395] CAPWAP data tunnel ADD to forwarding SUCCEEDED

Sep 7 12:57:49 kernel: [*09/07/2025 12:57:49.3543] **AP has joined controller c9800-40-BGL**

WLC RA Trace :

2025/09/07 12:57:49.038381077 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [15069]: (note): MAC: 1416.9d2a.bf80 Received CAPWAP config status request

2025/09/07 12:57:49.038455973 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (note): MAC: 1416.9d2a.bf80 Successfully handled Config status request.

2025/09/07 12:57:49.040192648 {wncd_x_R0-0}{1}: [lisp-agent-api] [15069]: (info): **AP Join Successful for MAC: 1416.9d2a.bf80**

Wireless Config Analyzer Express (WCAE)

- How to leverage WCAE

WCAE – Cloud Version

Download Full Report

Wireless Analyzer Results

- WLC Messages
- AP Message Summary
- RF Stats WLC Level Summary
- RF Stats AP Site Summary
- RF Stats Flex Profile Summary
- RF Health WLC Level Summary
- RF Health AP Site Summary
- RF Health Flex Profile Summary
- AP Models Summary
- AP Modes Summary
- WLC Logs Summary
- Show All
- Hide All

Total Unique Messages

Message Type	Count
Error	4
Warning	28
Info	16
Parsing Errors	0
Processing Errors	0

230038	Management: To prevent WebUI issues while using some large GUI options (VLANs for example), it is advisable to increase the VTY count to 50 **Action:** Use the command 'line vty 0 50' to increase the VTY count
230044	Security: Management over Wireless is enabled, this is not recommended from a security point of view **Action:** Management over wireless should be used with care, only enable if absolutely required. Check 9800 Best practices guide for more information
230056	Management: Service tcp-keepalive in/out, should be enabled to reduce lingering inactive connections to management points **Action:** Add: service tcp-keepalives in/service tcp-keepalives out to configuration
60020	RF: WLC has 80.0% of APs with failed Interference Profile for 2.4GHz Band **Action:** None

RF Health WLC Level Summary

		2.4GHz Band			5GHz Band		
Stats	Total Radios			15			74
	Health Assessment						
	Lowest Metric Average			0			0
		Low	Medium	High	Low	Medium	High
AP Radio Count per RF Health Metrics	Co-Channel Neighbor Utilization	0	0	15	0	2	72
	Co-Channel Overlapping	0	1	14	16	2	56
	Side Channel Overlapping	0	0	15	0	0	74
	Noise Same Channel	0	0	15	0	0	74
	Noise Side Channel	0	0	15	0	0	74
	Interference Same Channel	0	0	15	0	0	74

WCAE –Excel Download

Table of contents

Generated: 2025-09-12 12:28
WCAE Version: 0.41

Total Message Counts
Errors: 12
Warnings: 39
Informational: 23

Program Execution
Parsing Errors: 4
Processing Errors: 680

Debug Data

Back to Content tab

	A	B	C	D	E
1				Back to Content Tab	
2	Type	Count	Log Signature		Explanation
3	Client 8021x Fail(ed/ures)	348223	CO_CLIENT_DELETE_REASON_CLIENT_8021X_FAILURE	May happen during Normal Onboarding	Client reported authentication error on deauth frame
4	Inter Instance Roam Success	251715	CO_CLIENT_DELETE_REASON_INTER_WNCD_ROAM_SUCCESS	May happen during Normal Onboarding	Client roamed across WNCD instances. This is normal scenario for default tag, or roaming across tags
5	Incorrect Credentials	121346	CO_CLIENT_DELETE_REASON_CLIENT_CREDENTIAL_FAILURE	May need validation	Wrong username or password
6	Client Eap Timeout	114699	CO_CLIENT_DELETE_REASON_CLIENT_EAP_TIMEOUT_FAILURE	May happen during Normal Onboarding	Client reported EAP error on deauth frame
7	L2-auth Connection Timeout	104621	CO_CLIENT_DELETE_REASON_L2AUTH_CONNECT_TIMEOUT	May happen during Normal Onboarding	Client did not complete L2 auth like PSK or 802.1x, in time. Could be normal if client roamed or went out of coverage
8	Mic Validation Fail(ed/ures)	60916	CO_CLIENT_DELETE_REASON_KEY_MGMT_MIC_VALIDATION	May need validation	if WLAN is PSK, possible invalid password. For 802.1x, this is client side supplicant issue
9	L3 Authentication Fail(ed/ures)	59426	CO_CLIENT_DELETE_REASON_L3AUTH_FAIL	May need validation	Security processing for a L3 Auth failed (Webauth/guest)
10	Inter Controller Roam Success	50018	CO_CLIENT_DELETE_REASON_INTER_CTRL_ROAM_SUCCESS	May happen during Normal Onboarding	Successful inter controller client roam
11	Due To Mobility Fail(ed/ures)	18204	CO_CLIENT_DELETE_REASON_MOBILITY_FAILURE	May happen during Normal Onboarding	Client delete, either due to roaming while on IP learning state, or due to policy configuration mismatch
12	Client Miscellaneous Reason	12607	CO_CLIENT_DELETE_REASON_CLIENT_MISC_REASON	May happen during Normal Onboarding	Client reported generic reason in deauth frame
13	Wpa Group Key Update Timeout	10186	CO_CLIENT_DELETE_REASON_GROUP_KEY_UPDATE_TIMEOUT	May need validation	Client did not complete Broadcast key rotation. This may happen if client was sleeping or out of coverage
14	Supplicant Request(s)	10084	CO_CLIENT_DELETE_REASON_USER_REQUEST	May happen during Normal Onboarding	Client deleted due to supplicant sending EAP Logoff. This may happen during machine authentication
15	Due To Ssid Change	8476	CO_CLIENT_DELETE_REASON_WLAN_CHANGE	May happen during Normal Onboarding	Client changed WLANs/SSID
16	Ip-learn Connection Timeout	8163	CO_CLIENT_DELETE_REASON_IPLEARN_CONNECT_TIMEOUT	May happen during Normal Onboarding	Controller did not learn client IP address in the allowed time
17	Dot11r Pre-authentication Fail(ed/ures)	5454	CO_CLIENT_DELETE_REASON_FT_AUTH_RESPONSE	May happen during Normal Onboarding	Client failed pre-authentication during FT roaming
18	Mac Authentication Fail(ed/ures)	5074	CO_CLIENT_DELETE_REASON_MAB_FAILED	May happen during Normal Onboarding	Client failed Mac Authentication Bypass
19	Wpa Key Exchange Timeout	4599	CO_CLIENT_DELETE_REASON_KEY_XCHNG_TIMEOUT	May happen during Normal Onboarding	This can happen during normal scenarios. Client deleted due to EAPoL M1 retries. Possible client side issue, or it roamed during a
20	Wrong Psk	3528	CO_CLIENT_DELETE_REASON_EXCLUDE_WRONG_PSK	Possible defect or config error	Client excluded due to wrong PSK password

Client delete reasons breakup

Configuration Checks:

Controller Checks Results
APs Checks Results

Controller: 9800WLC

Data Summary
Log Summary
Upgrade Advisor
Best Practices
WLAN Summary
Interface Summary
RF Profiles 2.4 GHz
RF Profiles 5 GHz
RF Profiles 6 GHz
Site Tags
Hardware State
Resources
Client Stats

WNCD Load Distribution
Client Delete Reasons
Tag/Policy Usage
RF Stats 2.4GHz
RF Stats 5GHz
RF Stats 6GHz
RF Health 2.4GHz
RF Health 5GHz
RF Health 6GHz
Channel Stats 2.4GHz
Channel Stats 5GHz
Channel Stats 6GHz
Rogue Report
RF Neighborhood 2.4GHz
RF Neighborhood 5GHz
RF Neighborhood 6GHz

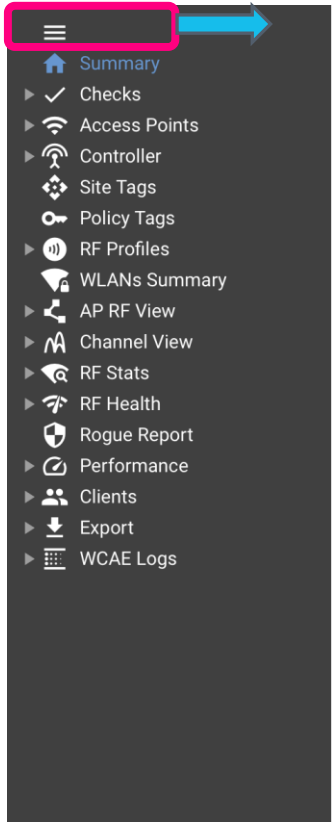
Client Audit

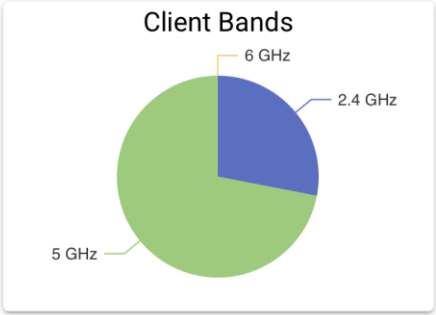
Apple IOS
Cisco 8821
Drager
Spectralink
Vocera

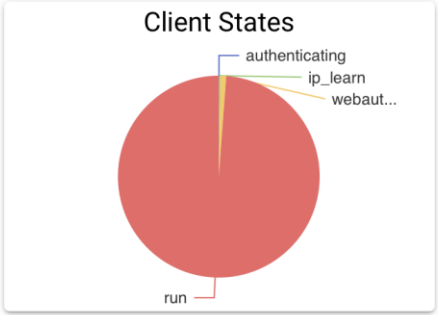
AP Information

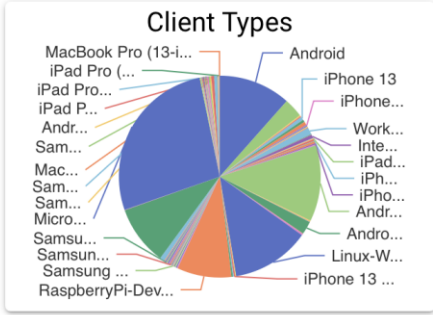
APs Configuration
APs Slot Configuration
APs Interface Status
APs RF Summary 2.4GHz
APs RF Summary 5GHz
APs RF Summary 6GHz
APs RF Health Details
APs NDP Summarization 2.4GHz
APs NDP Summarization 5GHz
APs NDP Summarization 6GHz
APs RF Neighbors 2.4GHz
APs RF Neighbors 5GHz
APs RF Neighbors 6GHz

Wireless Config Analyzer Express (WCAE) – Summary







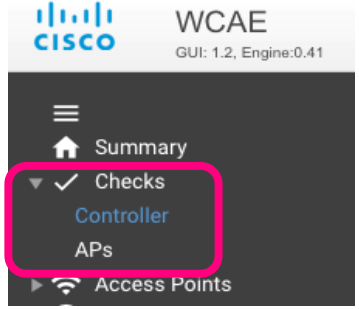


Total Messages	Count
Controller Messages	44
APs Messages	31
Processing Errors	4967
Parsing Errors	4
AP Missing Config	0
AP Missing RF Data	0

Controller Information	
Model	C9800-80-K9
Serial	FOX2803P0TQ
Version	17.15.3
Rommon Version	17.12(2r)
Days Uptime	1
System Name	9800_WLC

General Info	
AP Count	1577
Active Clients	5103
Site Tags	16
Policy Tags	147
Redundancy	Duplex
Multicast/Broadcast	Disabled/Disabled

WCAE – WLC and AP Checks



WLC Checks

Level	Category	Feature	Message	Action
Error	Operational	HW	Controller has a ROMMON version lower than the recommended for the platform	Check ROMMON Software section for your controller, in the Cisco Software Download page, and upgrade to latest version available, otherwise this may prevent future IOS-XE upgrade scenarios
Warning	Operational	RF	WLC has 13.0% of APs with high channel utilization for 2.4GHz Band	
Warning	Operational	RF	WLC has 32.1% of APs with failed Interference Profile for 2.4GHz Band	
Info	Config Error	Tags	More than 100 Site tags detected. Large counts are supported, but they may have a performance impact on some conditions	

AP Checks

Low coverage detected, action on AP placement recommended

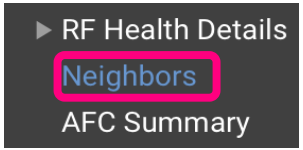
+	60029	Warning	Operational	RF	AP shows low coverage (all neighbors < -75 dBm) on 5GHz band. This could affect roaming and be indication of poor RF design or NDP issues	This message is intended to flag APs that don't have a smooth coverage transition to other APs. This may be result of AP physical placement

RF Summarization

Path : Access Points > RF Summary/ RF Health Details/Neighbors or Rogue Report in home page

For every AP :
- Channel, Power, Utilization, Interference
- Number of RX/TX Neighbors, Number of clients at SNR X

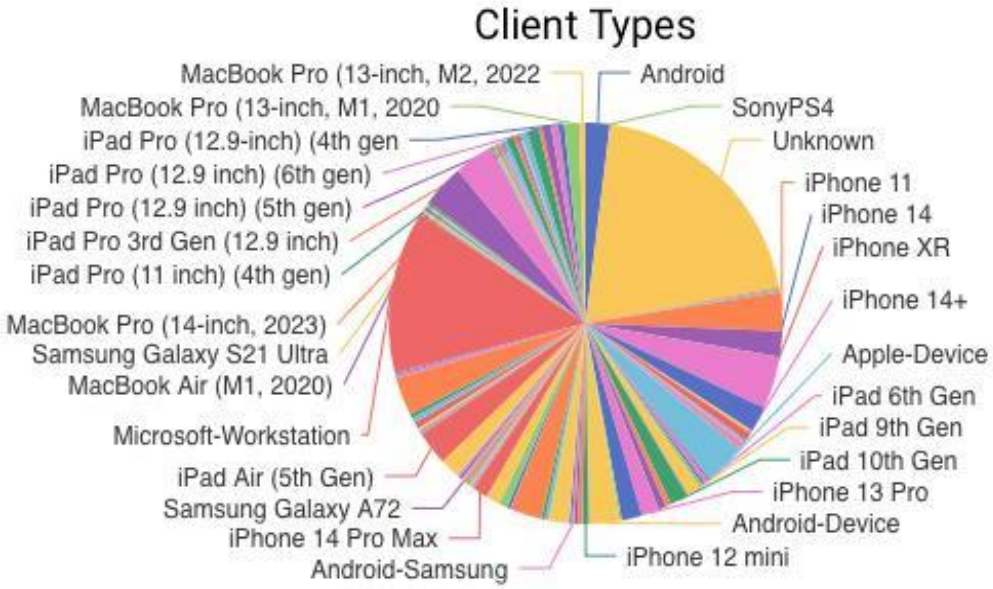
For every AP :
- Health score(0 to 100), co-channel utilization/noise



For every AP :
- Neighbor info – names with channel, width, power

For every Rogue :
- Rogue MAC, Number of detecting APs, strongly heard AP
- Classification, Heard RSSI, Channel, Band

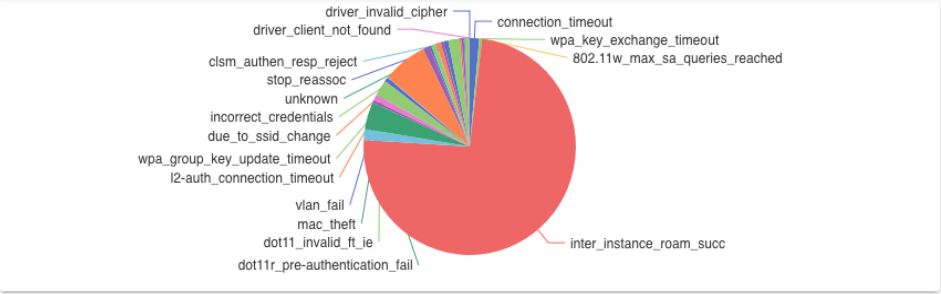
Client Types And Count



Client Type	Count
Android	297
SonyPS4	2
Unknown	3005
iPhone 7	20
iPhone 8	29
HP-Device	1
iPhone 11	467
iPhone 12	310
iPhone 13	634
iPhone 14	304
iPhone 7+	10
iPhone 8+	23
iPhone XR	108
iPhone XS	28

Client Delete Reasons

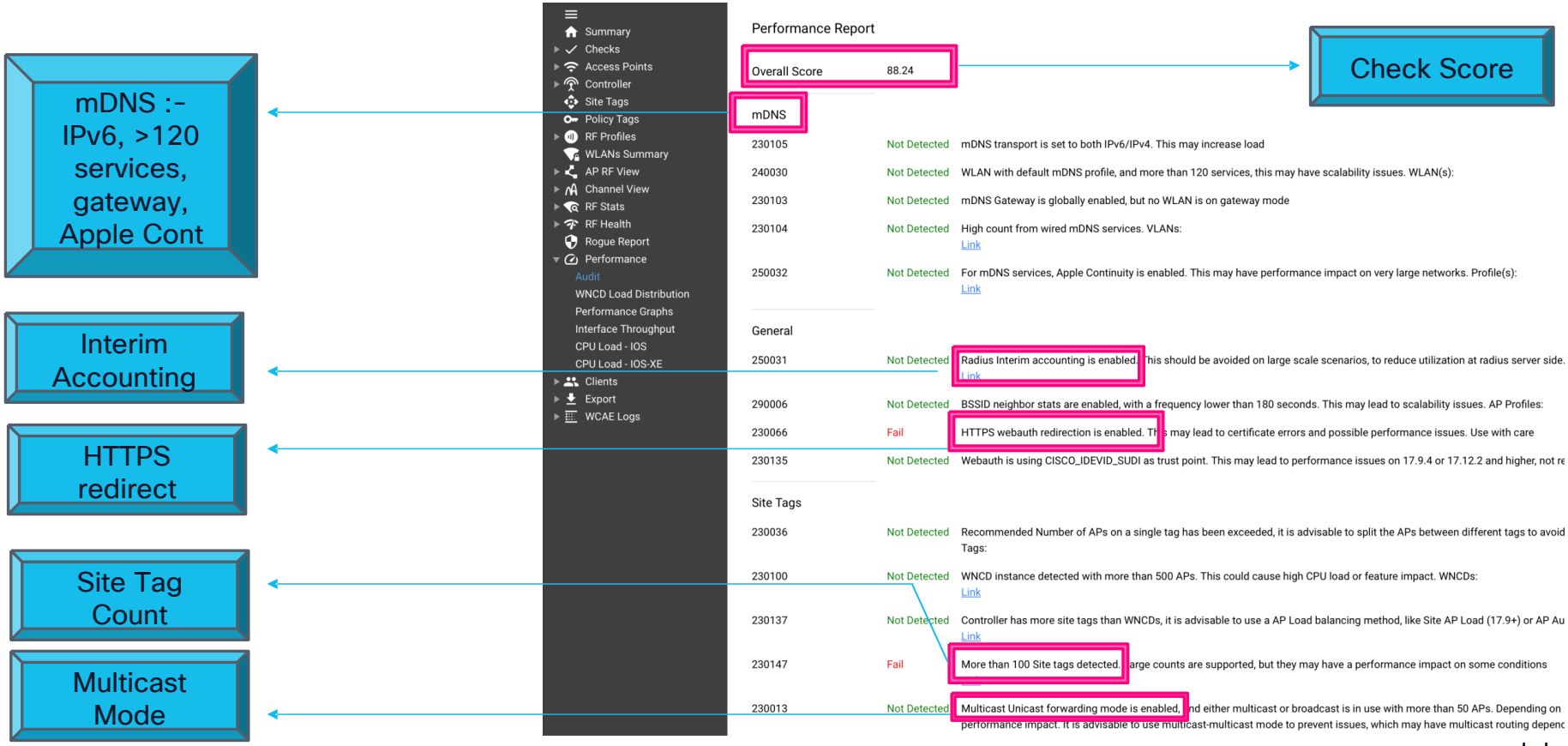
Client Delete Reasons



- Count per delete reason
- Reason
- Explanation

Delete Reason	Count	Log Signature	Level	Explanation
Connection Timeout	3314	CO_CLIENT_DELETE_REASON_CONNECT_TIMEOUT	May need validation	Client associated to Flex AP, and did not complete onboarding process, may be triggered if client v
Wpa Key Exchange Timeout	942	CO_CLIENT_DELETE_REASON_KEY_XCHNG_TIMEOUT	May happen during Normal Onboarding	This can happen during normal scenarios. Client deleted due to EAPoL M1 retries. Possible client
802.11w Max Sa Queries Reached	2	CO_CLIENT_DELETE_REASON_MAX_SAQUERIES	May happen during Normal Onboarding	For PMF clients, triggered when client did not reply to SA queries and reached max retries. Could b
Inter Instance Roam Success	169437	CO_CLIENT_DELETE_REASON_INTER_WNCD_ROAM_SUCCESS	May happen during Normal Onboarding	Client roamed across WNCD instances. This is normal scenario for default tag, or roaming across
Due To Mobility Fail(ed/ures)	3699	CO_CLIENT_DELETE_REASON_MOBILITY_FAILURE	May happen during Normal Onboarding	Client delete, either due to roaming while on IP learning state, or due to policy configuration mism
Dot11r Pre-authentication Fail(ed/ures)	9219	CO_CLIENT_DELETE_REASON_FT_AUTH_RESPONSE	May happen during Normal Onboarding	Client failed pre-authentication during FT roaming
Dot11 Fail(ed/ures)	2	CO_CLIENT_DELETE_REASON_DOT11_UNSPECIFIED_FAILURE	May need validation	Association response creation fail, possible due to client malformed request
Dot11 Invalid Akm	1030	CO_CLIENT_DELETE_REASON_DOT11_AKMP_INVALID	Possible defect or config error	Client requested invalid Authentication Key Management during association
Dot11 Received Invalid Pmkid In The Received Rsn Ie	1950	CO_CLIENT_DELETE_REASON_DOT11_INVALID_PMKID	Possible defect or config error	Controller could not validate PMKID provided by client. This may have different triggers
Dot11 Invalid Mdie	1	CO_CLIENT_DELETE_REASON_DOT11_INVALID_MDIE	May need validation	802.11r(FT) client sent invalid mobility domain
Dot11 Invalid Ft Ie	5353	CO_CLIENT_DELETE_REASON_DOT11_INVALID_FTIE	May need validation	Failure during FT processing for client. This may have different triggers
Client Eap Id Timeout	55	CO_CLIENT_DELETE_REASON_CLIENT_EAP_ID_TIMEOUT	May happen during Normal Onboarding	Client did not reply to EAP requests in the specified retries/time
Wrong Replay Counter	44	CO_CLIENT_DELETE_REASON_MN_AP_WRONG_REPLAY_COUNTER	May need validation	Invalid replay counter received during EAPoL negotiation. Client should recover on new attempt
Mic Validation Fail(ed/ures)	4	CO_CLIENT_DELETE_REASON_KEY_MGMT_MIC_VALIDATION	May need validation	if WLAN is PSK, possible invalid password. For 802.1x, this is client side supplicant issue

Usecase : Troubleshooting High WNCd Utilization



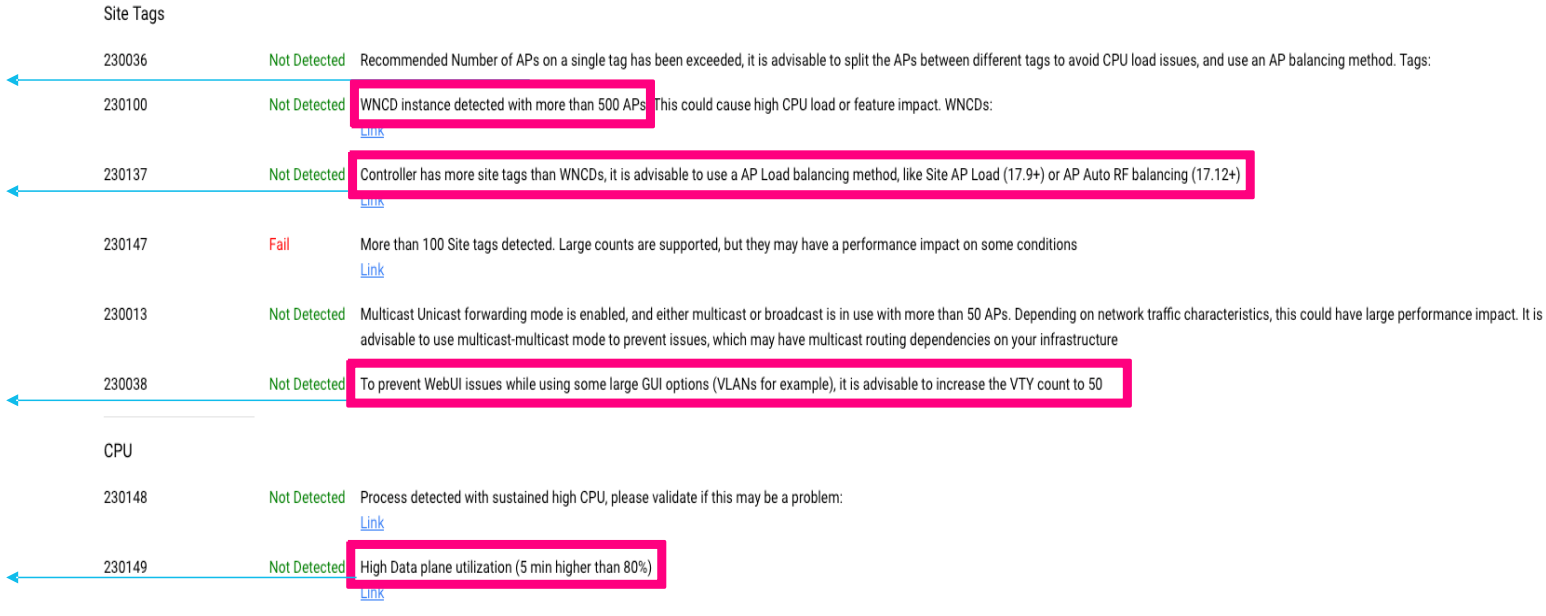
Troubleshooting High WNCd Utilization (Continued..)

WNCd – AP count

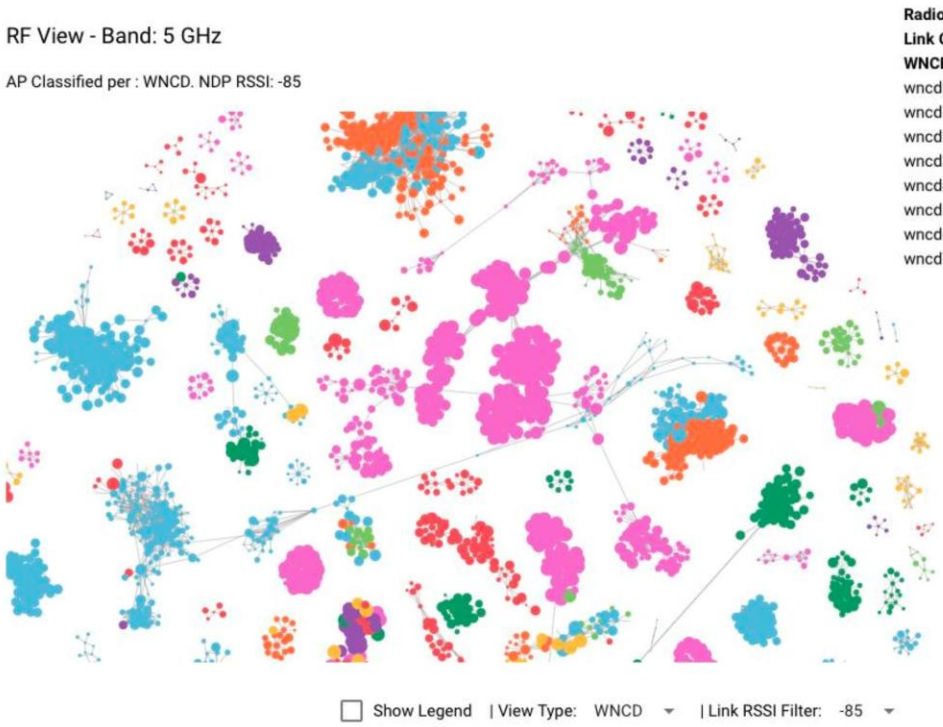
Load Balancing

GUI Latency

Data Plane Util



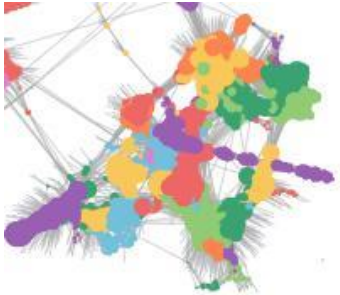
WNCd view



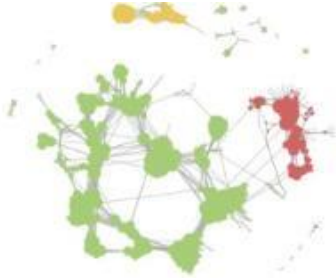
Radio Count: 3498
Link Count: 14740

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

High Inter WNCd expected(expensive)



Fairly balanced WNCds



WNCd Load Balancing Options

17.3.X:

- The controller load balances the site-tags across the WNCds in a **round robin fashion**
- not always optimal for large networks.

17.9.3 and higher:

- To prevent unbalanced site-tag assignment to WNCds, the **site load command** was introduced in 17.9.3 and higher.
- This allows administrators to predefine the expected load of each site tag.

17.12.X and higher:

- The RF based **Automatic AP Load Balancing** feature uses **Radio Resource Management (RRM)** neighbor report-based AP grouping and load-balancing across WNCd instances.
- When this feature is enabled, it forms AP clusters based on the RSSI received from AP neighbor reports. These clusters or neighborhoods are further split into sub-neighborhoods and smaller areas.
- The resulting groups of APs are then distributed evenly across the WNCd processes

Debug Analyzer

- RA Trace Analyzer
- Obtain quick insights

Simplified Data Collection – Debug Bundle

Log collection in a single command :

RA Traces & Client Tech Support

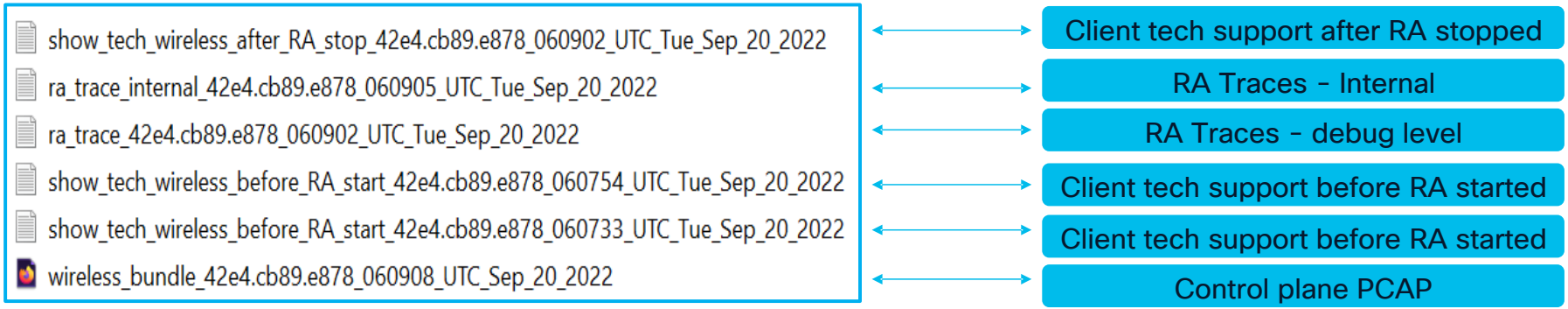
- This collects and captures both RA traces(debug level) and internal RA for the configured clients
- Show tech wireless client MAC of two instances, one before RA trace is enabled and once after RA trace is stopped are captured
- C9800# debug wireless bundle client <client_mac1 ...client_mac5>

Packet Capture

- Packet captures at the WLC control plane is collected for the clients
- C9800# debug wireless bundle include epc client <client_mac1 ...client_mac5>

Bundle Contents

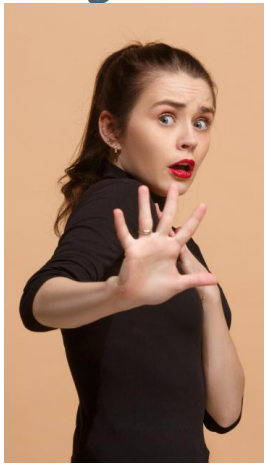
i. Two sets of RA traces for all the clients
   ii. Two sets of clients tech support
      iii. WLC control plane captures



RA Trace – Raw File

~/Downloads/debugTrace_ec63.d7fc.f729 (2).txt

```
Logging display requested on 2025/06/23 12:00:04 (IST) for Hostname: [c9800-40-SJC], Model: [C9800-40-K9        ], Version: [17.09.05], SN: [JAE271507TK], MD_SN: [TTM265101FM]
2025/06/20 18:28:15.073514051 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Association received. BSSID 889c.ade7.9281, WLAN SJ_Corp_SSID_profile, Slot 0 AP 889c.ade7.9280, SJ-E
2025/06/20 18:28:15.073746134 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
2025/06/20 18:28:15.074469577 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729  Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
2025/06/20 18:28:15.074852467 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
2025/06/20 18:28:15.075299006 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  ADD MOBILE sent. Client state flags: 0x41  BSSID: MAC: 889c.ade7.9281 capwap IFID: 0x90000003, Add mobil
2025/06/20 18:28:15.079588340 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  L2 Authentication initiated. method DOT1X, Policy VLAN 1, AAA override = 1 , NAC = 0
2025/06/20 18:28:15.080450179 {wncd_x_R0-0}{1}: [site-manager-ap] [15082]: (ERR): Failed to get flex interface name vlan table root
2025/06/20 18:28:15.081349113 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (note): Authentication Success. Resolved Policy bitmap:11 for client ec63.d7fc.f729
2025/06/20 18:29:45.082253726 {wncd_x_R0-0}{1}: [errmsg] [15082]: (note): %DOT1X-5-FAIL: R0/0: wncd: Authentication failed for client (ec63.d7fc.f729) with reason (No Response from Client) on Interface ca
2025/06/20 18:29:45.082531498 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (ERR): SANET_AUTHC_FAILURE - No Response from Client, audit session id 15547F0A00000005A8D6B16A7
2025/06/20 18:29:45.082550762 {wncd_x_R0-0}{1}: [errmsg] [15082]: (note): %SESSION_MGR-5-FAIL: R0/0: wncd: Authorization failed or unapplied for client (ec63.d7fc.f729) on Interface capwap_90000003 AuditS
2025/06/20 18:29:55.083275604 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Co client reap timer callback. Co client reap timer triggering E_CO_CLIENT_CONNECT_TIMEOUT event, cli
2025/06/20 18:29:55.083342500 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (ERR): ec63.d7fc.f729CLIENT_STAGE_TIMEOUT State = AUTHENTICATING, WLAN profile = SJ_Corp_SSID_profile, Policy profile = SJ_Corp_SS
2025/06/20 18:29:55.083369294 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_L2AUTH_CONNECT_TIMEOUT, details: , fsm-state
2025/06/20 18:29:55.083519937 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Delete mobile payload sent for BSSID: 889c.ade7.9281 WTP mac: 889c.ade7.9280 slot id: 0
2025/06/20 18:29:55.083699299 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_DELETE_IN_PROGRESS
2025/06/20 18:29:55.084613832 {wncd_x_R0-0}{1}: [sanet-shim-translate] [15082]: (note): MAC: ec63.d7fc.f729  Session manager disconnect event called, session label: 0x34000050
2025/06/20 18:29:55.085742854 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_DELETE_IN_PROGRESS -> S_CO_DELETED
2025/06/23 06:41:02.209724436 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Association received. BSSID 889c.ade7.9280, WLAN EEC_Exp, Slot 0 AP 889c.ade7.9280, SJ-Edge2-AP1, Sit
2025/06/23 06:41:02.209964796 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
2025/06/23 06:41:02.210705345 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729  Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
2025/06/23 06:41:02.211068931 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
2025/06/23 06:41:02.211353370 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  L2 Authentication initiated. method PSK, Policy VLAN 352, AAA override = 0, NAC = 0
2025/06/23 06:41:02.213391451 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (note): Authentication Success. Resolved Policy bitmap:11 for client ec63.d7fc.f729
2025/06/23 06:41:02.213614721 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  ADD MOBILE sent. Client state flags: 0x71  BSSID: MAC: 889c.ade7.9280 capwap IFID: 0x90000003, Add mobil
2025/06/23 06:41:02.253665212 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (note): MAC: ec63.d7fc.f729  EAP Key management successful. AKM:PSK Cipher:CCMP WPA Version: WPA2
2025/06/23 06:41:02.253808853 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  L2 PSK Authentication Success. EAP type: NA, Resolved VLAN: 352, Audit Session id: 15547F0A000000A59A56B
2025/06/23 06:41:02.254249467 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Mobility discovery triggered. Client mode: Local
2025/06/23 06:41:02.254254623 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2025/06/23 06:41:02.255433129 {wncd_x_R0-0}{1}: [mm-client] [15082]: (note): MAC: ec63.d7fc.f729 Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IFID: 0xa0000003, Client R
2025/06/23 06:41:02.255590673 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  ADD MOBILE sent. Client state flags: 0x72  BSSID: MAC: 889c.ade7.9280 capwap IFID: 0x90000003, Add mobil
2025/06/23 06:41:02.255766465 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
2025/06/23 06:41:02.255888594 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729  Client datapath entry params - ssid:EEC_Exp,slot_id:0 bssid ifid: 0x0, radio_ifid: 0x9000000a, wlan_ifid: 0xf0
2025/06/23 06:41:02.256196660 {wncd_x_R0-0}{1}: [dpath_svc] [15082]: (note): MAC: ec63.d7fc.f729 Client datapath entry created for ifid 0xa0000003
2025/06/23 06:41:02.256476894 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2025/06/23 06:41:02.404022207 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (ERR): MAC: 0000.0000.0000  vlan_mode_api: fsm_ctxt not found
2025/06/23 06:41:05.778682535 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (ERR): MAC: 0000.0000.0000  vlan_mode_api: fsm_ctxt not found
2025/06/23 07:17:22.705798404 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Re-Association received. BSSID 889c.ade7.9880, WLAN EEC_Exp, Slot 0 AP 889c.ade7.9880, SJ-Edge2-AP2,
2025/06/23 07:17:22.705935348 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2025/06/23 07:17:22.706466185 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729  Association success. AID 2, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
2025/06/23 07:17:22.706695241 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Delete mobile payload sent for BSSID: 889c.ade7.9280 WTP mac: 889c.ade7.9280 slot id: 0
2025/06/23 07:17:22.707108086 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
2025/06/23 07:17:22.708088849 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  ADD MOBILE sent. Client state flags: 0x71  BSSID: MAC: 889c.ade7.9880 capwap IFID: 0x9000000c, Add mobil
2025/06/23 07:17:22.744876468 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (note): MAC: ec63.d7fc.f729  EAP Key management successful. AKM:PSK Cipher:CCMP WPA Version: WPA2
2025/06/23 07:17:22.745019080 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  L2 PSK Authentication Success. EAP type: NA, Resolved VLAN: 352, Audit Session id: 15547F0A000000A59A56B
2025/06/23 07:17:22.745433966 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Mobility discovery triggered. Client mode: Local
2025/06/23 07:17:22.745438686 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2025/06/23 07:17:22.745697077 {wncd_x_R0-0}{1}: [mm-client] [15082]: (note): MAC: ec63.d7fc.f729 Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 889
2025/06/23 07:17:22.745932349 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729  ADD MOBILE sent. Client state flags: 0x76  BSSID: MAC: 889c.ade7.9880 capwap IFID: 0x9000000c, Add mobil
2025/06/23 07:17:22.746104443 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
2025/06/23 07:17:22.746429588 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2025/06/23 07:17:39.142919647 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Re-Association received. BSSID 2c57.4158.71a0, WLAN EEC_Exp, Slot 0 AP 2c57.4158.71a0, SJ-Edge1-AP2,
2025/06/23 07:17:39.143042319 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2025/06/23 07:17:39.143657454 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729  Association success. AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
2025/06/23 07:17:39.143943419 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729  Delete mobile payload sent for BSSID: 889c.ade7.9880 WTP mac: 889c.ade7.9880 slot id: 0
2025/06/23 07:17:39.144396513 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729  Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
```



Debug Analyzer – Home Page

Show Advanced Debug Insights NEW!!

Select a client MAC Address and connection to see logs.

ec63.d7fc.f729

Download CSV

Connection 10 of 10 < 1 ... 9 10 >

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

Time	Task	Translated
2025/06/23 12:08:05.797	client-orch-sm	Client made a new Association to an AP/BSSID: BSSID 889c.ade7.9881, WLAN SJ_Corp_SSID_profile, Slot 0 AP 889c.ade7.9880, SJ-Edge2-AP2, Site tag ST_SanJo_Corporat_9248f_0, Policy tag PT_SanJo_Corpo_Corporat_78519, Policy profile SJ_Corp_SSID_profile, Switching Local, old BSSID 889c.ade7.9881, Socket delay 0ms
2025/06/23 12:08:05.798	dot11	Association success for client, assigned AID is: 2
2025/06/23 12:08:32.420	client-auth	Starting EAPOL 4-Way Handshake
2025/06/23 12:08:32.436	client-keymgmt	Negotiated the following encryption mechanism: AKM:DOT1X Cipher:CCMP WPA Version: WPA2
2025/06/23 12:08:32.436	client-orch-state	Starting Mobility Anchor discovery for client
2025/06/23 12:08:32.439	client-orch-state	Entering IP learn state
2025/06/23 12:08:32.493	client-iplearn	Client got IP: 10.127.85.54, discovered through: IP Snooping

Advanced Debug Insights

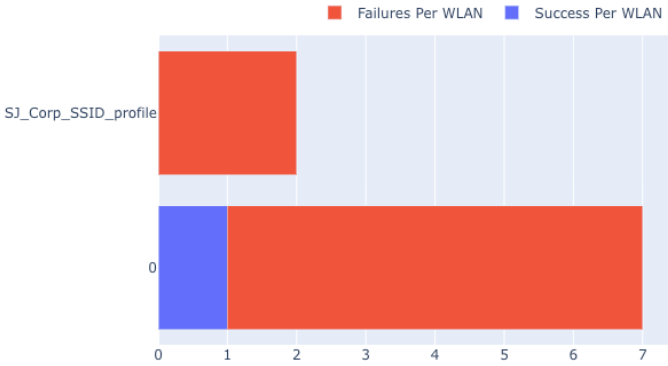
of success/failed sessions, start/end timestamp per client

Advanced Debug Insights

9800 WLC Advanced Debug Insights (Help)

Client MAC Address	Success Sessions	Failed Sessions	Start Time	End Time
ec63.d7fc.f729	1	8	June 23, 2025 11:50:4...	June 23, 2025 12:08:05...

Success/Failure stats per WLAN



Advanced Debug Insights

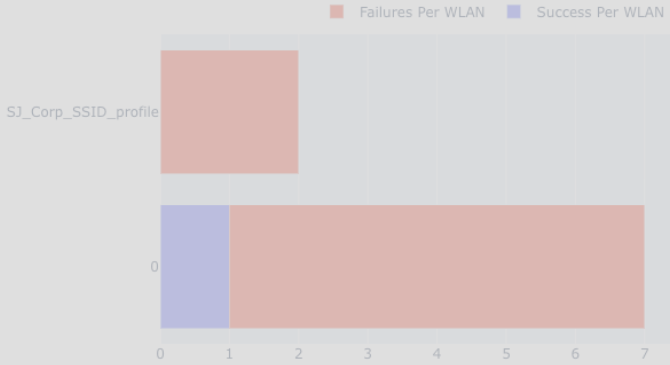
of success/failed sessions, start/end timestamp per client

Advanced Debug Insights

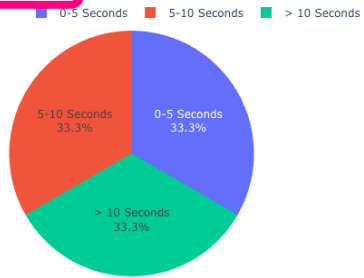
9800 WLC Advanced Debug Insights (Help)

Client MAC Address	Success Sessions	Failed Sessions	Start Time	End Time
ec63.d7fc.f729	1	8	June 23, 2025 11:50:4...	June 23, 2025 12:08:05...

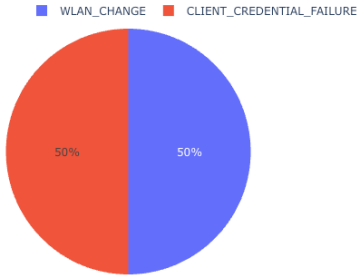
Success/Failure stats per WLAN



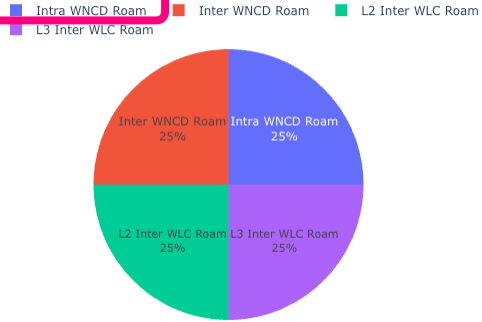
Client Onboarding Time



Delete Reasons



Client Roam Statistics



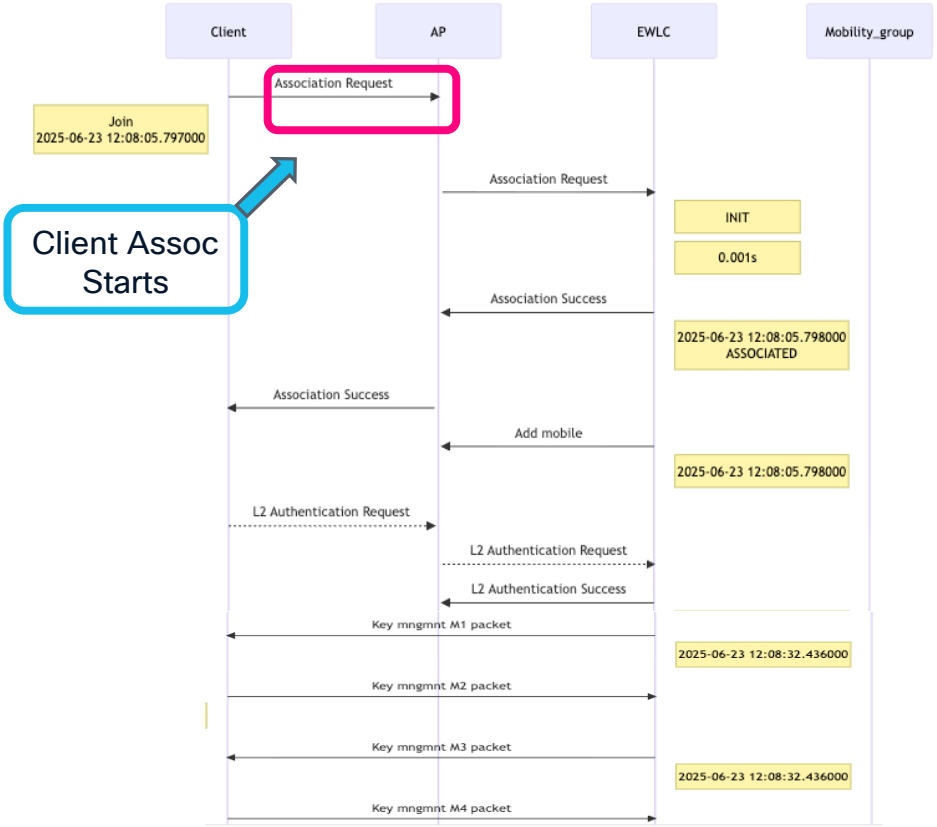
Client Onboarding time for 0-5/10 secs, Delete Reasons, Roam (Intra/inter WNCd/WLC stats

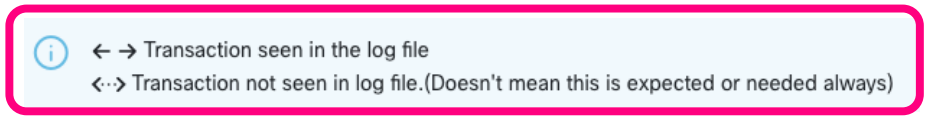
Client Session Table

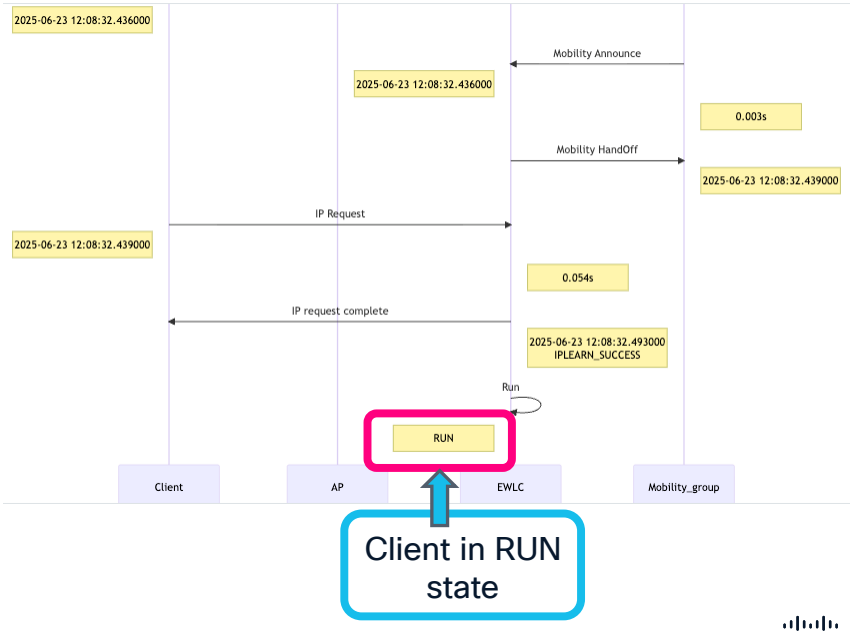
Client MAC: Ec63.D7fc.F729

Session	State	Auth Method	AP	WLAN	Mobility Role	IP Address	Onboarding Time	Start/Run Time	Delete Reason	Delete Time
1	IPLEARN	UNKNOWN	Site tag ST_SanJo_Corporat_9248f_0	0	Local-None		0 ms	11:50:47:555 /		
2	INIT	UNKNOWN	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:04:28:337 /	WLAN_CHANGE	12:04:28:000
3	L2AUTH	DOT1X	889c.ade7.9280	SJ_Corp_SSID_profile	NONE-NONE		0 ms	12:04:28:340 /		
4	L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:04:29:900 /	CLIENT_CREDENTIAL_FAILURE	12:04:43:000
5	L2AUTH	DOT1X	889c.ade7.9880	SJ_Corp_SSID_profile	NONE-NONE		0 ms	12:07:12:867 /		
6	L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:07:14:325 /		
7	L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:07:15:568 /		
8	L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:07:36:743 /		
9	RUN	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	Local-None	10.127.85.54	26698 ms	12:08:05:797 / 12:08:32:495		

Packet Flow Between Client, AP, WLC







WiFi-HAWK

- Over the air capture analyzer

WiFi-Hawk

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

WiFi Hawk

How to use?

- Upload file
- View Excel Analysis

▷▷▷▷▷▷	Auth request	Info	2727	FT BSS Transition
◁◁◁◁◁◁	Auth resp-fail	Error	2729	Failed, Status code:Invalid pairwise master key identifier
------	General Warning	Warning	2731	Deauth sent from client, not to current AP. Reason:1 (Unspecified
▷▷▷▷▷▷	Auth request	Info	3367	FT BSS Transition
◁◁◁◁◁◁	Auth resp-fail	Error	3370	Failed, Status code:Invalid pairwise master key identifier
------	General Warning	Warning	3372	Deauth sent from client, not to current AP. Reason:1 (Unspecified

Quick Index view

- List of BSSIDs (APs) and clients active during the capture
- Quick glance on who is having problems
- Last known state for each client (probing, auth, full traffic, etc)
- Click on each item for full details

Table of contents

Generated:	2022-03-11 10:28
Wireless Consultant Version:	0.7
Total Frames:	82685
File Type:	Radio Tap
Processing time:	131.21 seconds
Total BSSIDs seen:	76
Total Clients seen:175	175

Processing Errors:

Invalid Frames	0
Exceptions	75
Non Parsed Frames	0
Filtered Frames	0
FCS Errors	0

AP BSSIDs	SSID	Events	Errors	Warnings
e0:10:7f:65:61:53	SSID-island-256150	146	0	145
58:1d:91:6b:2d:10	SSID-AR5511_6B2D10	58	0	57
58:bf:ea:bb:c0:66	SSID-Rsecure	57	0	56
58:bf:ea:bb:c0:61	SSID-handheld	53	0	52
58:bf:ea:bb:c0:67	SSID-rjil-consultant	50	0	49
58:bf:ea:bb:c0:60	SSID-secure-impact	49	0	48
[illegible]	[illegible]	43	0	40

Clients	Last State	Events	Errors	Warnings
a8:9f:ba:51:f1:b9	EAPoL 4-WAY completed	555	0	0
34:a8:4e:50:06:00	Deauthenticated	476	0	476
2c:54:cf:fa:fc:52	Association failed	445	0	0
ac:22:0b:5b:e7:fa	Probing	441	0	0
80:6c:1b:20:39:de	Probing	402	0	0
7c:7a:91:b3:69:ba	Bidirectional Traffic	250	2	0
[illegible]	[illegible]	238	0	0

Event Flow

- Color coded events registered per device
- Summary of repeated items for a more concise view
- Quick location in capture of important issues (frame/time)
- Added information for better understanding
- Translation of reason codes, failures, EAP types, etc

Event Flow:

Direction	Type	Severity	BSSID	Frame	Time	Info
>>>>>>	Probe requests	Info	NA	28669	NA	Consecutive requests:48
<<<<<<	Probe responses	Info	NA	28617	NA	Consecutive responses:223
>>>>>>	Auth request	Info	64:f6:9d:55:5c:f4	28688	Thu, 12 May 2016 11:22:33 CEST	Auth Open System
<<<<<<	Auth resp success	Info	64:f6:9d:55:5c:f4	28690	Thu, 12 May 2016 11:22:33 CEST	Auth Open System
>>>>>>	Assoc request	Info	64:f6:9d:55:5c:f4	28693	Thu, 12 May 2016 11:22:33 CEST	Type: 802.1x . To SSID:Jio_AKA-Ahmedabad
<<<<<<	EAP ID request	Info	64:f6:9d:55:5c:f4	28701	Thu, 12 May 2016 11:22:33 CEST	Identy request
>>>>>>	EAP ID response	Info	64:f6:9d:55:5c:f4	28715	Thu, 12 May 2016 11:22:33 CEST	Identy response
<<<<<<	EAP request	Info	64:f6:9d:55:5c:f4	28802	Thu, 12 May 2016 11:22:33 CEST	EAP-AKA
>>>>>>	EAP response	Info	64:f6:9d:55:5c:f4	28880	Thu, 12 May 2016 11:22:33 CEST	EAP-AKA
>>>>>>	EAP response	Info	64:f6:9d:55:5c:f4	28883	Thu, 12 May 2016 11:22:33 CEST	EAP-AKA
<<<<<<	EAP Success	Info	64:f6:9d:55:5c:f4	29201	Thu, 12 May 2016 11:22:34 CEST	Dot1x Auth success
<<<<<<	EAP KEY RX	Info	64:f6:9d:55:5c:f4	29203	Thu, 12 May 2016 11:22:34 CEST	EAPoL M1
<<<<<<	EAP Start	Info	64:f6:9d:55:5c:f4	29214	Thu, 12 May 2016 11:22:34 CEST	EAP START
<<<<<<	EAP Start	Info	64:f6:9d:55:5c:f4	29219	Thu, 12 May 2016 11:22:34 CEST	EAP START
<<<<<<	EAP ID request	Info	64:f6:9d:55:5c:f4	29221	Thu, 12 May 2016 11:22:34 CEST	Identy request
<<<<<<	EAP ID request	Info	64:f6:9d:55:5c:f4	29223	Thu, 12 May 2016 11:22:34 CEST	Identy request
>>>>>>	Client going to sleep	Info	64:f6:9d:55:5c:f4	39809	Thu, 12 May 2016 11:22:53 CEST	Signaling AP that is going to sleep
>>>>>>	Sleep Time	Warning	NA	48017	NA	Client slept for more than 0:00:12 seconds
>>>>>>	Sleep Time	Warning	NA	49805	NA	Client slept for more than 0:00:03 seconds
>>>>>>	Sleep Cycles	Info	NA		NA	Consecutive sleep-awake cycles:2
>>>>>>	Client awake	Info	64:f6:9d:55:5c:f4	49805	Thu, 12 May 2016 11:23:08 CEST	Signaling AP that is going to sleep

Detecting easy to miss problems

Simplify finding issues across large captures

- Unencrypted traffic leak (client/AP)
- Beacon loss
- High co-channel
- 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	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	

Diagnostic Tools - Takeaways

Scenario : Troubleshooting Client Connectivity, AP Join, Best Practice miss etc

AP/WLC Debugs

- Correlating AP and WLC side of debugs, outputs
- Example : AP join issues

WCAE

- Gain insights on best practices, warnings, RF, performance issues
- Example : Checking WLC Performance

Debug Analyzer

- Analyze client RA traces in table, graphical format for quick and easy consumption with various statistics
- Example : Client connectivity

WiFi-Hawk (OTA)

- Get insights on over the air packet capture
- Example : Debugging an RF Issue/AP/Client issue


CISCO