

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





Mastering SD-Access Fabric Enabled Wireless

Packet Walk and Deep Dive Troubleshooting – Like a
TAC Engineer

Lakshmi Ganesh Kondaveeti
Senior Technical Leader, SDA/DNAC

BRKEWN-3322

CISCO *Live!*

#CiscoLiveAPJC



Cisco Webex App

Questions?

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

How

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

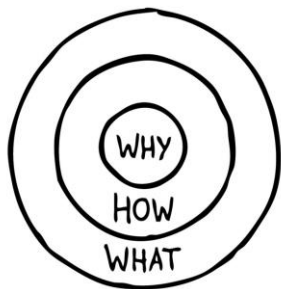
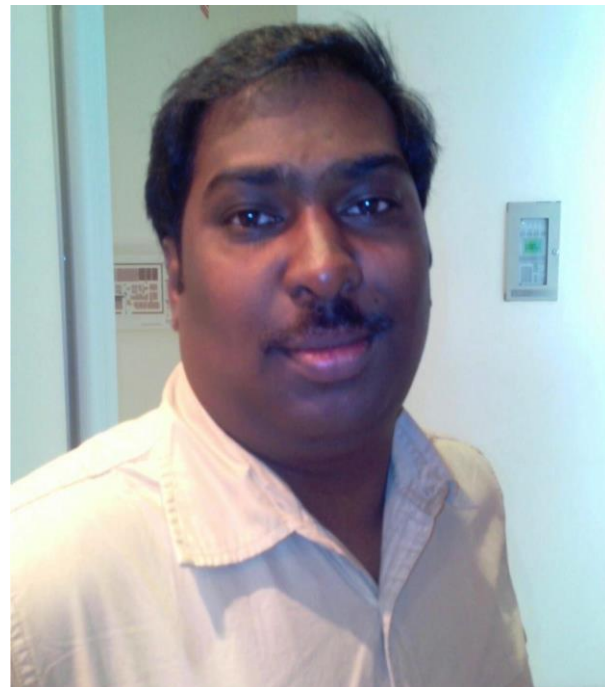
Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-3322>

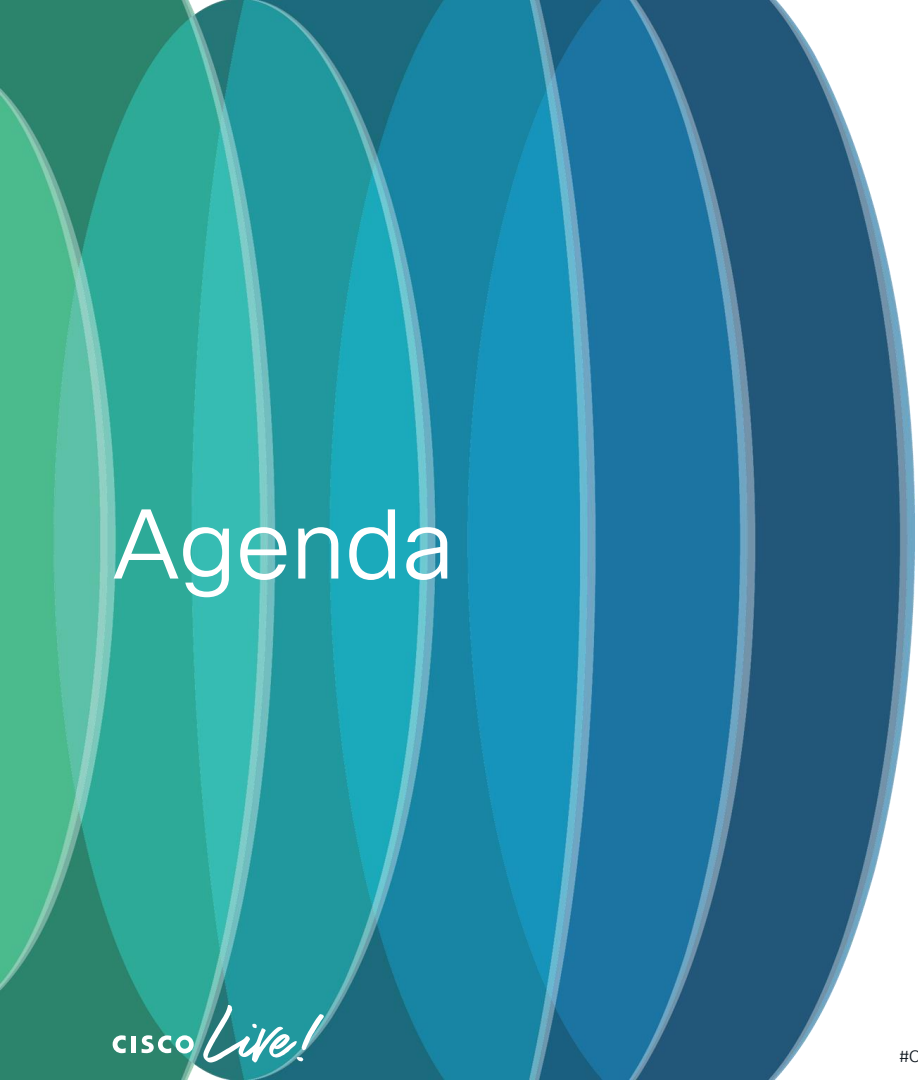


Lakshmi Ganesh Kondaveeti (LG)



Please download the slides

cisco *Live!*

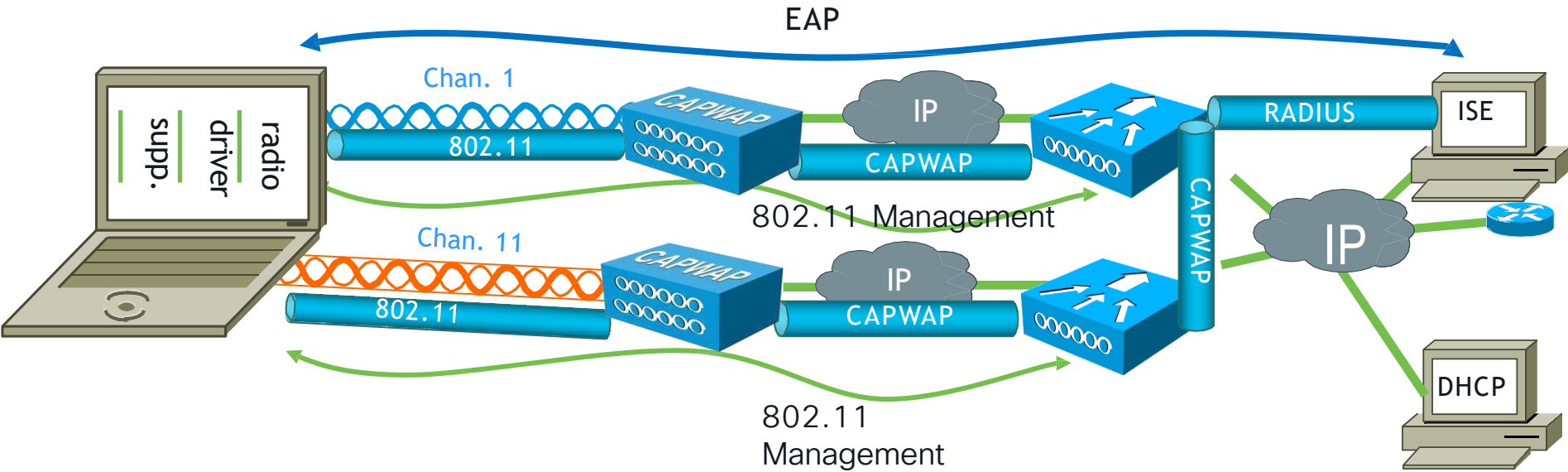


Agenda

- Architecture Overview
- Basic Workflows and Troubleshooting
 - AP Join
 - Client Onboarding
 - Client Roaming
- Some common scenarios
- Best practices

Where do we start?

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

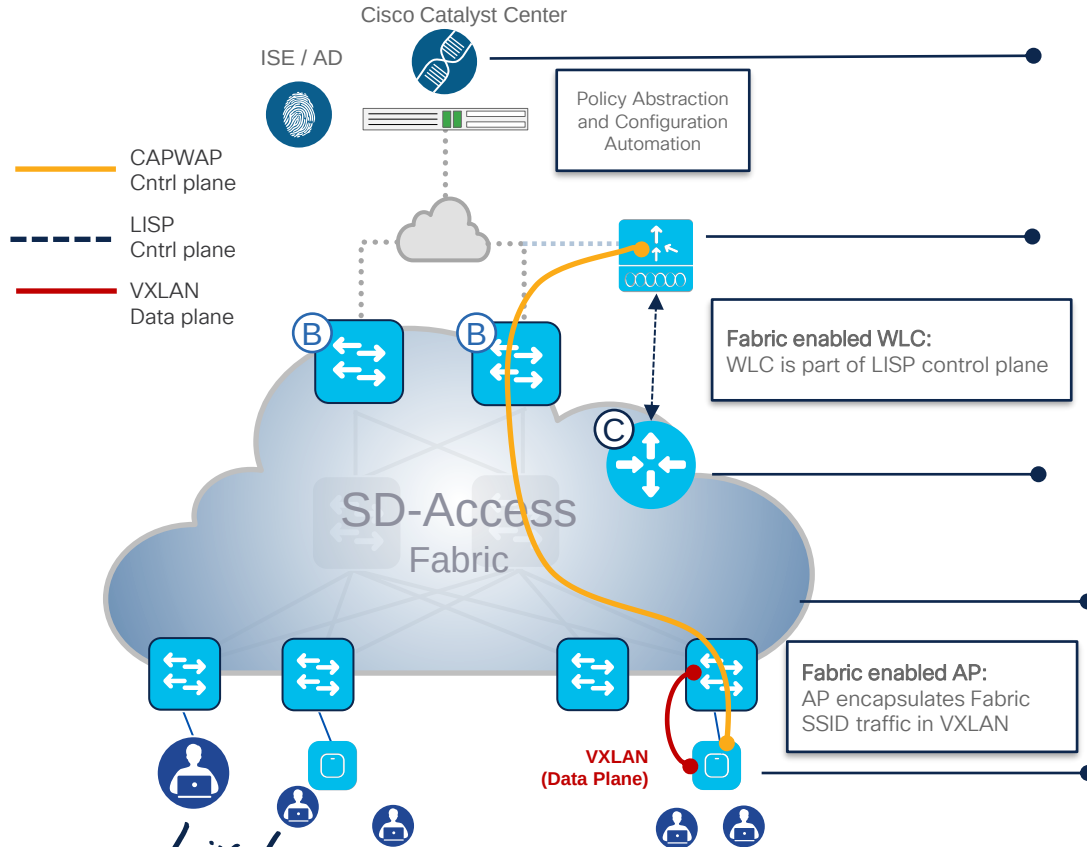
If we could “**break the dependence**” between IP addressing and policy, we could **greatly simplify** networks – and make networks **much more functional**.



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

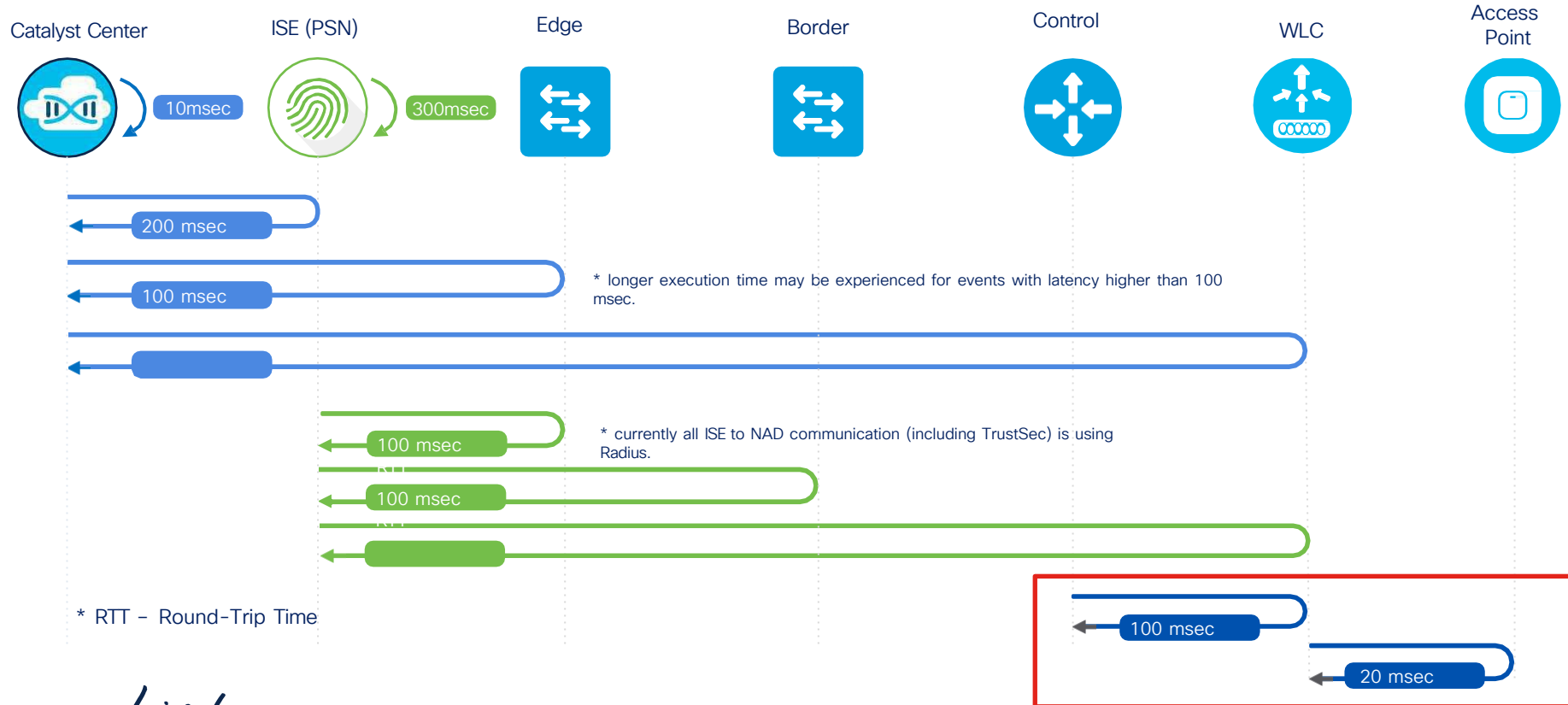
VXLAN from the AP

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

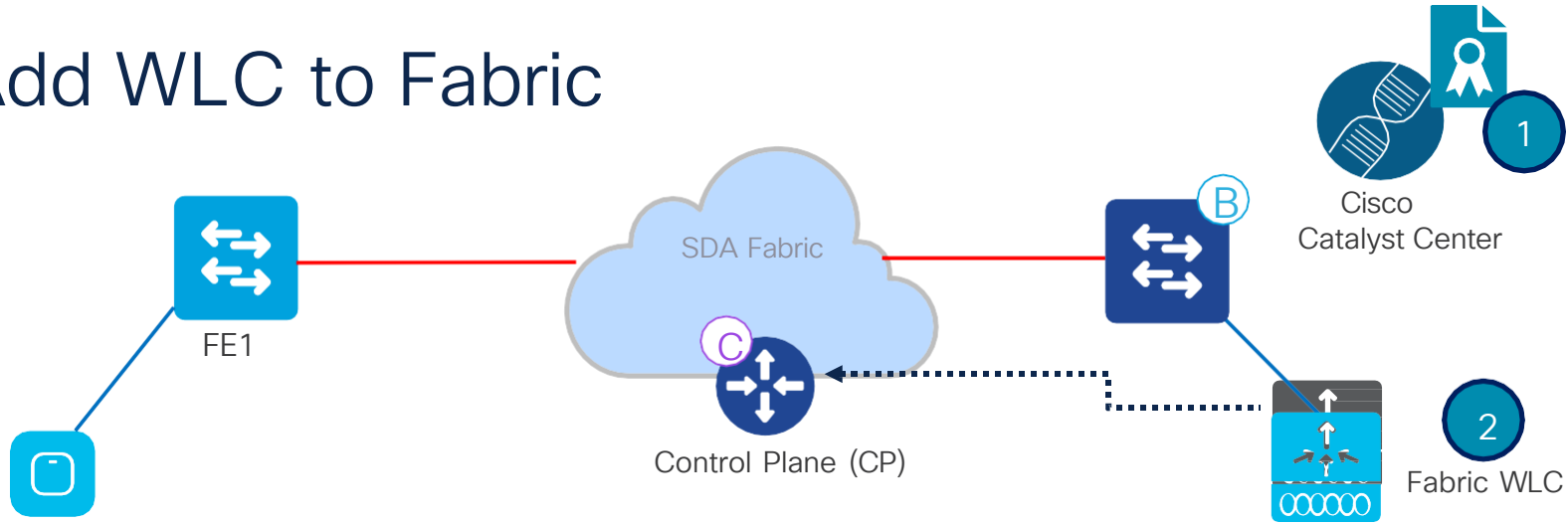
Quick overview of the design and deployment

Cisco SD-Access Network Requirements

Latency Requirements (RTT)



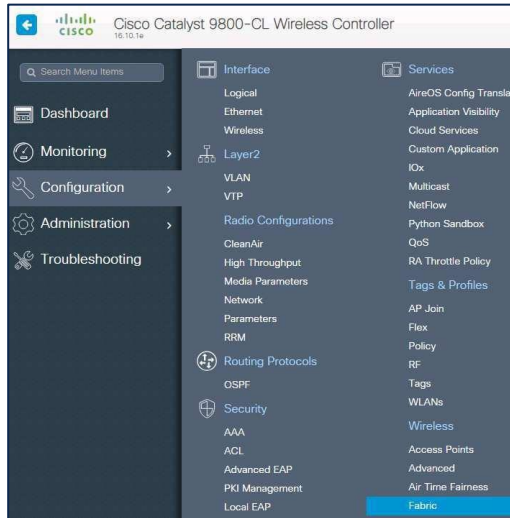
Add WLC to Fabric



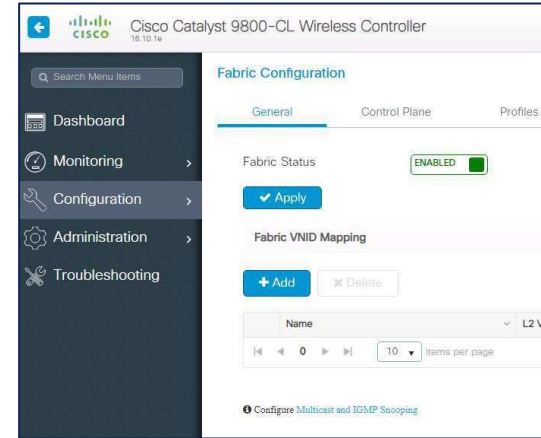
- 1 In Cisco Catalyst Center, first create the design, network settings, Wireless settings, discover, provision the WLC and then add it to the Fabric site
- 2 Fabric configuration is pushed to WLC. WLC becomes Fabric aware. Most importantly WLC is configured with credentials to establish a secure connection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

Add WLC to Fabric – verify settings

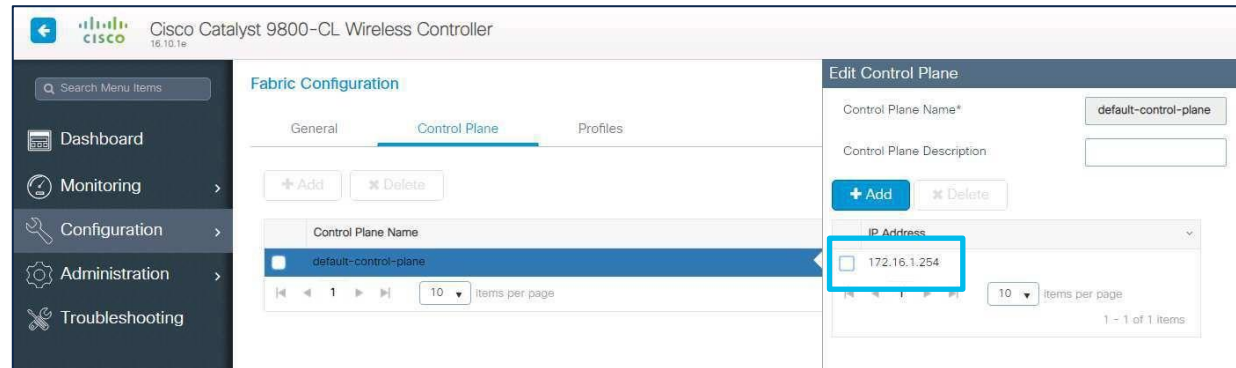
Configuration > Wireless > Fabric



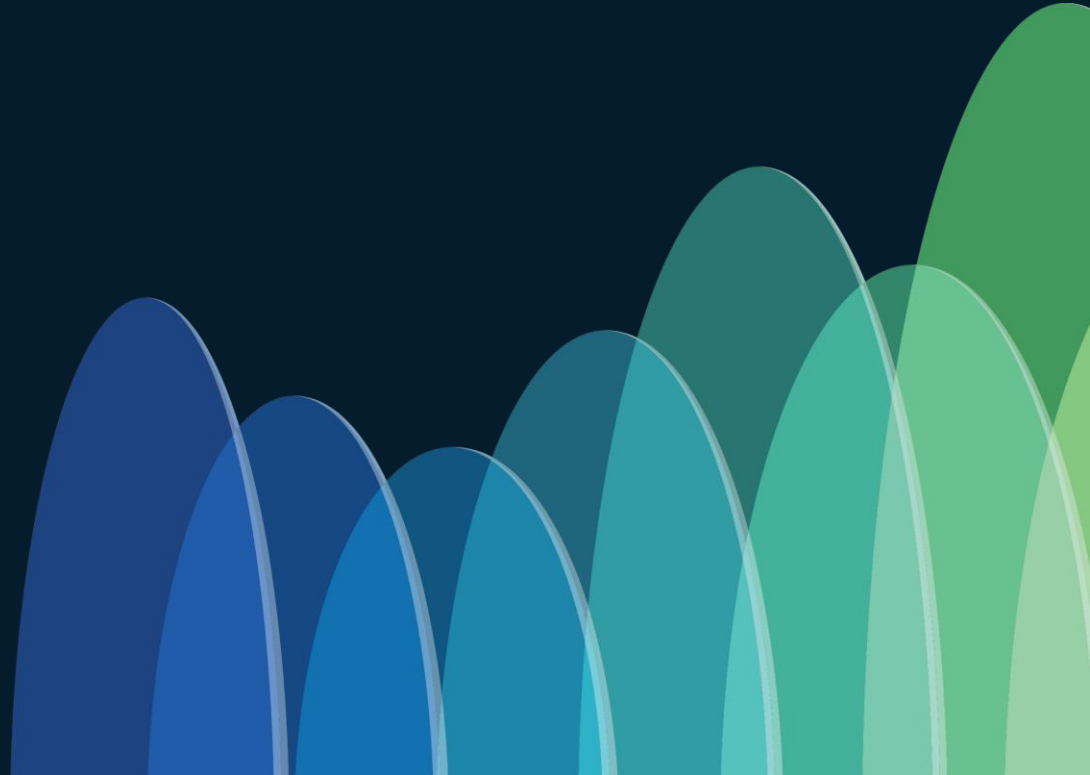
Fabric status is enabled



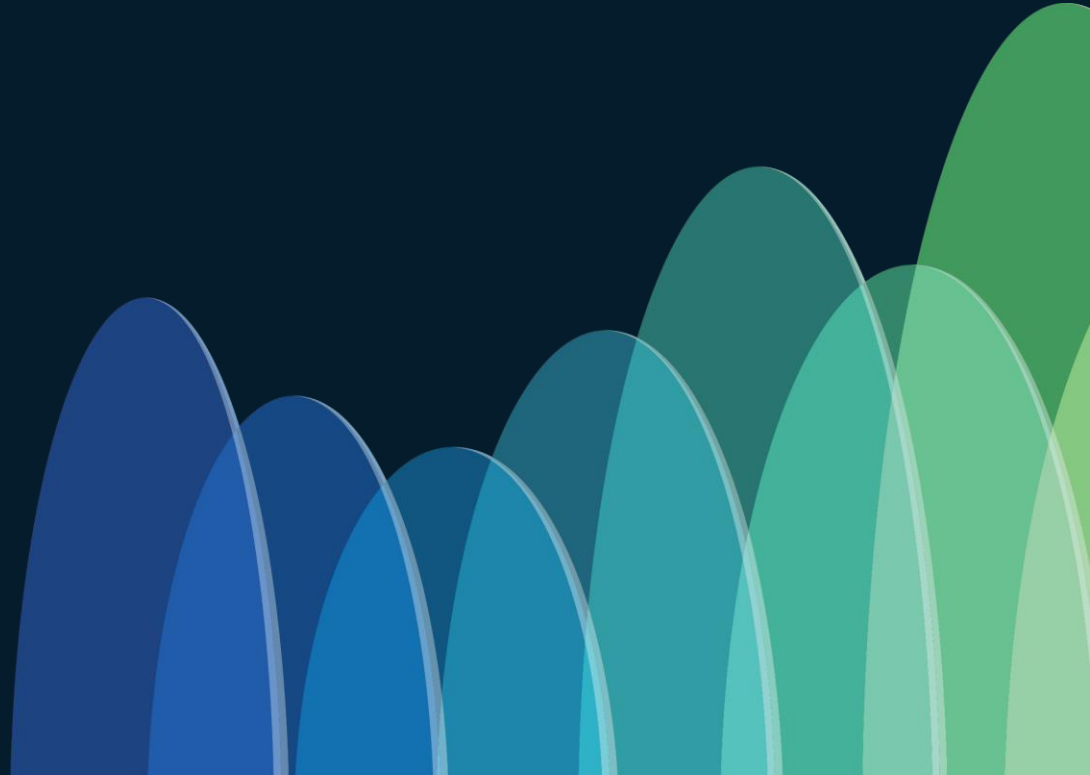
CP is correctly configured



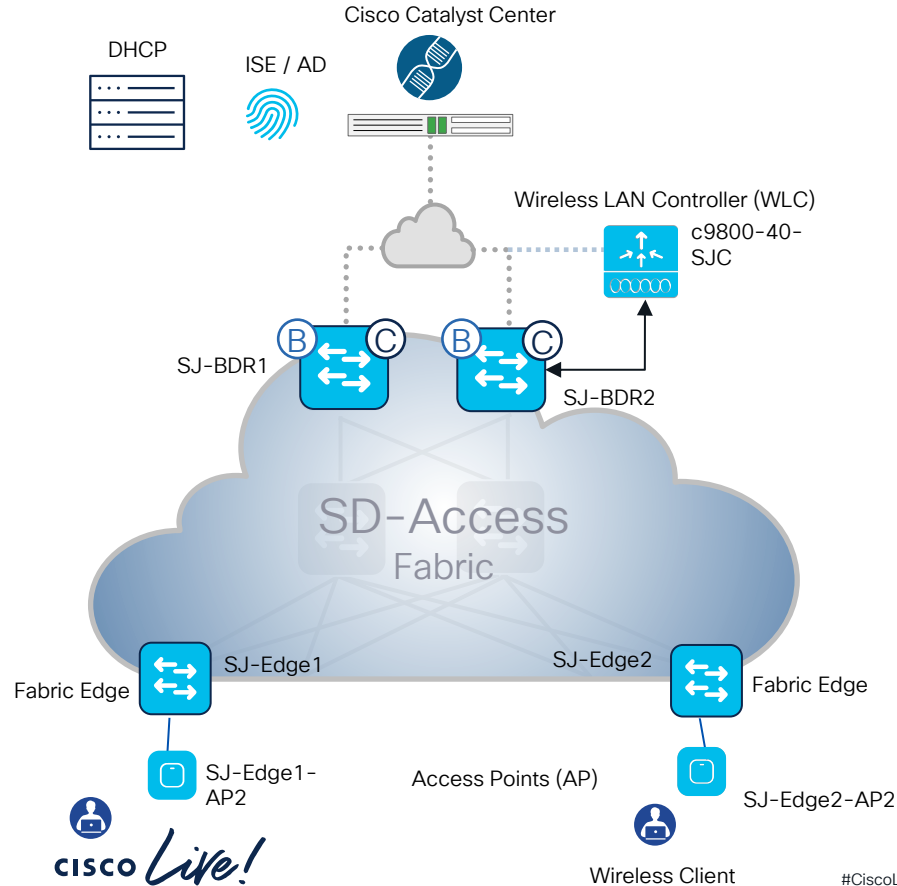
SD-Access Wireless Basic Workflows



AP Join/Onboarding Flow

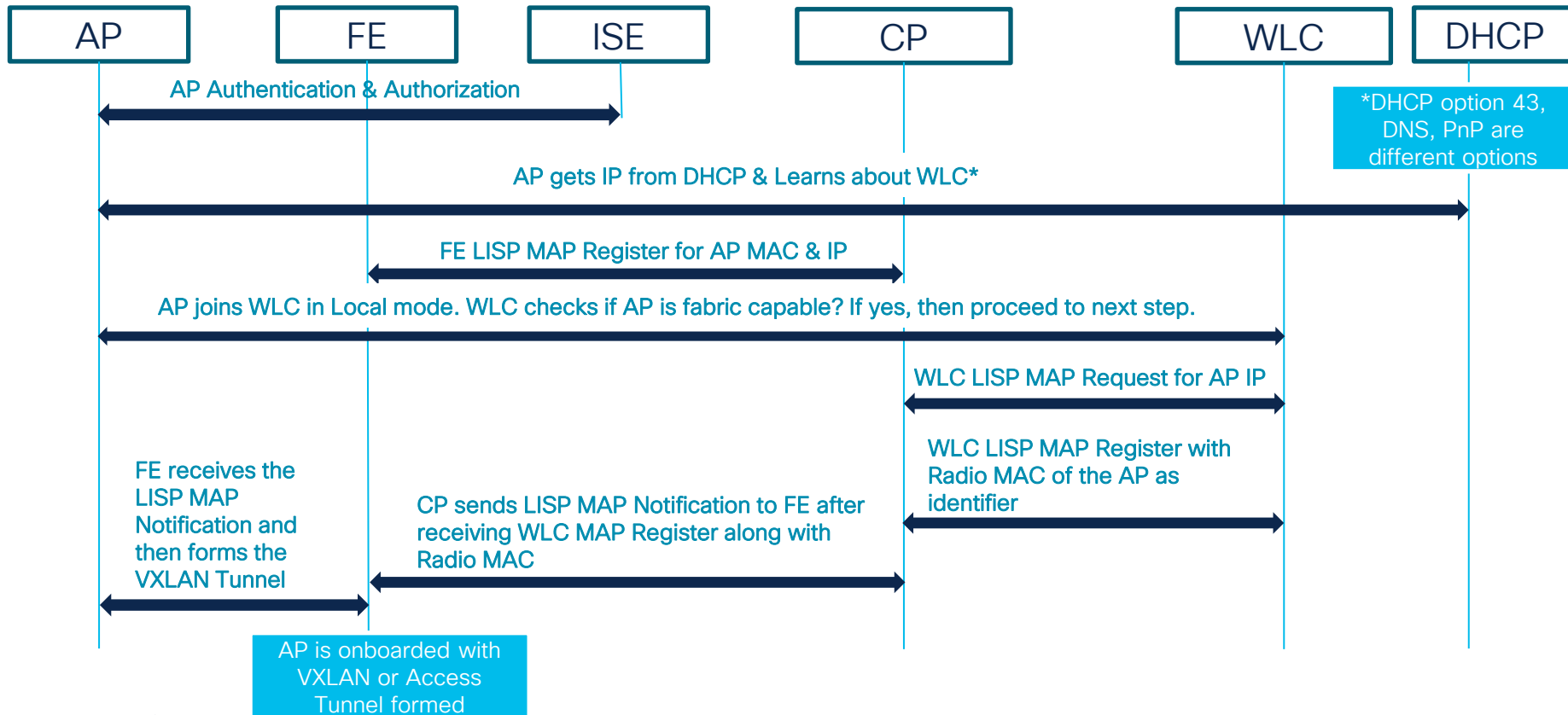


SD-Access Wireless Topology



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	
	IP: 10.127.85.85 Ethernet MAC: 1006.edfc.2cdc Radio MAC: 889c.ade7.9880 (Used for AP Join)
SJ-Edge2-AP2 (Connected to SJ-Edge2)	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



AP DHCP Flow - FE Uplink Captures

dhcphw.mac_addr == 10:06:ed:fc:2c:dc

	Destination	Header Checksum	VXLAN	Protocol	Length	Info
DHCP Discover - Transaction ID 0x330e2afd	10.127.84.2	0xab1e		DHCP	361	DHCP Discover - Transaction ID 0x330e2afd
DHCP Discover - Transaction ID 0x330e2afd	10.127.84.8	0xab17		DHCP	361	DHCP Discover - Transaction ID 0x330e2afd
DHCP Discover - Transaction ID 0x330e2afd	10.127.84.9	0xab15		DHCP	361	DHCP Discover - Transaction ID 0x330e2afd
DHCP Offer - Transaction ID 0x330e2afd	10.127.85.81	0x7e93,0x3429	4097	DHCP	412	DHCP Offer - Transaction ID 0x330e2afd
DHCP Request - Transaction ID 0x330e2afd	10.127.84.2	0xab0e		DHCP	373	DHCP Request - Transaction ID 0x330e2afd
DHCP Request - Transaction ID 0x330e2afd	10.127.84.8	0xab07		DHCP	373	DHCP Request - Transaction ID 0x330e2afd
DHCP Request - Transaction ID 0x330e2afd	10.127.84.9	0xab05		DHCP	373	DHCP Request - Transaction ID 0x330e2afd
DHCP ACK - Transaction ID 0x330e2afd	10.127.85.81	0x7e93,0x3428	4097	DHCP	412	DHCP ACK - Transaction ID 0x330e2afd

Client IP address: 0.0.0.0
Your (client) IP address: 10.127.85.85
Next server IP address: 10.127.84.8
Relay agent IP address: 10.127.85.81
Client MAC address: 10:06:ed:fc:2c:dc (10:06:ed:fc:2c:dc)

Option: (43) Vendor-Specific Information
Length: 6
Value: f1040a7f5415

Agent Remote ID
Sub-option: 3
Length of option: 8
LISP Instance ID: 4097
IP Locator : IPv4
Remote Locator: 10.127.84.105

Option 82 Suboption: (1) Agent Circuit ID
Length: 6
Agent Circuit ID: 000404030101
Option 82 Suboption: (2) Agent Remote ID
Length: 10
Agent Remote ID: 0308001001010a7f5469

f1040a7f5415=10.127.84.21

Agent Circuit ID = VLAN 1027

Second capture: 2

> Bootp flags: 0x0000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 10.127.85.85
Next server IP address: 10.127.84.8
Relay agent IP address: 10.127.85.81
Client MAC address: 10:06:ed:fc:2c:dc (10:06:ed:fc:2c:dc)
Client hardware address padding: 000000000000000000000000
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: (6) Domain Name Server
Option: (43) Vendor-Specific Information
Length: 6
Value: f1040a7f5415
Option: (82) Agent Information Option
Length: 20
Option 82 Suboption: (1) Agent Circuit ID
Length: 6
Agent Circuit ID: 000404030101
Option 82 Suboption: (2) Agent Remote ID
Length: 10
Agent Remote ID: 0308001001010a7f5469
> Option: (255) End

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 (retransmission?)]
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 (retransmission?)]
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
14395	2024-10-02 16:19:34.585968	0.000000s	10.127.84.21	10.127.85.85	0xb412	DTLSv1.2	125	Change Cipher Spec,Encrypted Handshake Message
14418	2024-10-02 16:19:35.804951	0.003993s	10.127.84.21	10.127.85.85	0x5cea	DTLSv1.2	1483	Application Data
14419	2024-10-02 16:19:35.804951	0.000000s	10.127.84.21	10.127.85.85	0x5d13	CAPWA...	1442	CAPWAP-Control - Join Request[Malformed Packet]
					0xae72	DTLSv1.2	1460	Application Data
						DTLSv1.2	1484	Application Data

AP Joins in Local Mode

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

FE Uplink Captures

No.	Time	DeltaTime	Source	Destination	Header Checksum	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 – WLC Captures

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 MAP Register to CP - WLC Captures

No.	Time	DeltaTime	Source	Destination	Header Checksum	V	Protocol	Length	Info
14492	2024-10-02 16:19:36.2...	0.000992s	10.127.84.21	10.127.84.100	0xa2fd		LISP	182	Msg: 236,WLC Registration (client join),AP [4097] 10.127.85.85,Client SGT: 0
14494	2024-10-02 16:19:36.2...	0.000000s	10.127.84.21	10.127.84.101	0x9f6c		LISP	182	Msg: 239,WLC Registration (client join),AP [4097] 10.127.85.85,Client SGT: 0
14496	2024-10-02 16:19:36.2...	0.000000s	10.127.84.100	10.127.84.21	0xd2b7		LISP	87	Msg: 86,Registration ACK
14498	2024-10-02 16:19:36.2...	0.000000s	10.127.84.101	10.127.84.21	0x649f		LISP	87	Msg: 26,Registration ACK

- > Frame 14492: 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: 236,WLC Registration (client join) for [8193] 88:9c:ad:e7:98:80/48,AP [4097] 10.127.85.85,Client SGT: 0
 - Type: WLC Registration (31)
 - Length: 128
 - Message ID: 236
 - 1.....= AP Join (A-bit): Set
 - .000 0000 0000 0000 0000 0000 0000 0000 = Res
 - Key ID: 0x0002
 - Authentication Data Length: 32
 - Authentication Data: 295ba422a82874fa22cd4505f46792ef91ae7218d592e1b9...
 - > Mapping Record 1,EID Prefix: [8193] 88:9c:ad:e7:98:80/48,TTL: 1440,Action: No-Action,Authoritative
 - > WLC Opaque Data: AP [4097] 10.127.85.85; Client SGT: 0;
 - Message End Marker: 0x9facade9 (correct)

Note, AP Radio MAC, L2 VNID, L3 VNID, AP IP, Client SGT

Note, WLC Registration Message Type 31

Note, AP Join (A-bit) is set to 1

VxLAN Tunnel Formation

CP sends the MAP Notification to FE - Control Plane Captures

38404	2024-10-02 05:25:53.192894	0.015999s	10.127.84.105	10.127.84.100	0x431b	LISP	308	Msg: 333,Registration for [4097] 10.127.85.85/32; Msg: 334,Registration for [4097] 10.127.85.85/32
38405	2024-10-02 05:25:53.193776	0.000882s	10.127.84.100	10.127.84.105	0x84d7	LISP	192	Msg: 435,Registration ACK; Msg: 436,Registration ACK; Msg: 437,Mapping Notification
40995	2024-10-02 05:26:47.963286	0.000551s	10.127.84.21	10.127.84.100	0xa3fd	LISP	182	Msg: 236,WLC Registration (client join),AP [4097] 10.127.85.85,Client SGT: 0
40996	2024-10-02 05:26:47.963800	0.000514s	10.127.84.100	10.127.84.21	0xd1b7	LISP	87	Msg: 86,Registration ACK
40997	2024-10-02 05:26:47.963848	0.000048s	10.127.84.100	10.127.84.105	0x84ce	LISP	200	Msg: 438,Mapping Notification

> Frame 40997: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface [Device]NPF_{927CAF3D-9F87-45BA-8D82-3D0522506438}, id 0
> Ethernet II, Src: f4:ee:31:0c:c4:5f (f4:ee:31:0c:c4:5f), Dst: e4:1f:7b:c2:ab:7f (e4:1f:7b:c2:ab:7f)
> Internet Protocol Version 4, Src: 10.127.84.100, Dst: 10.127.84.105
> Transmission Control Protocol, Src Port: 4342, Dst Port: 15603, Seq: 294, Ack: 523, Len: 146

> Locator/ID Separation Protocol (Reliable Transport), Msg: 438 Mapping Notification for [8193] 88:9c:ad:e7:98:80/48

Type: Mapping Notification (21)

Length: 146

Message ID: 438

xTR-ID: 00000000000000000000000000000000

Site-ID: 0000000000000000

> Mapping Record 1, EID Prefix: [8193] 88:9c:ad:e7:98:80/48, TTL: 1440, Action: No-Action, Not Authoritative
Message End Marker: 0x9facade9 (correct)

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

9030	2024-10-02 05:26:47.976996	0.001700s	10.127.84.100	10.127.84.105	0x85ce	LISP	200	Msg: 438,Mapping Notification
9031	2024-10-02 05:26:47.977026	0.000030s	10.127.84.101	10.127.84.105	0x678c	LISP	200	Msg: 388,Mapping Notification

> Frame 9030: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface [Device]NPF_{40B3E30A-3F9F-4837-8EC3-2AE26715EDCA}, id 0
> Ethernet II, Src: e4:1f:7b:c2:ab:7f (e4:1f:7b:c2:ab:7f), Dst: Cisco_55:53:48 (4c:e1:75:55:53:48)
> Internet Protocol Version 4, Src: 10.127.84.100, Dst: 10.127.84.105
> Transmission Control Protocol, Src Port: 4342, Dst Port: 15603, Seq: 294, Ack: 523, Len: 146

> Locator/ID Separation Protocol (Reliable Transport), Msg: 438 Mapping Notification for [8193] 88:9c:ad:e7:98:80/48

Type: Mapping Notification (21)

Length: 146

Message ID: 438

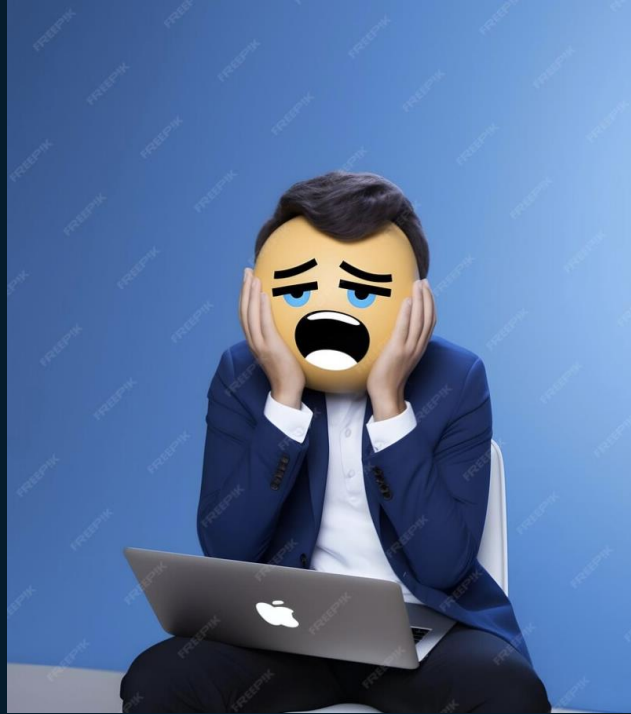
xTR-ID: 00000000000000000000000000000000

Site-ID: 0000000000000000

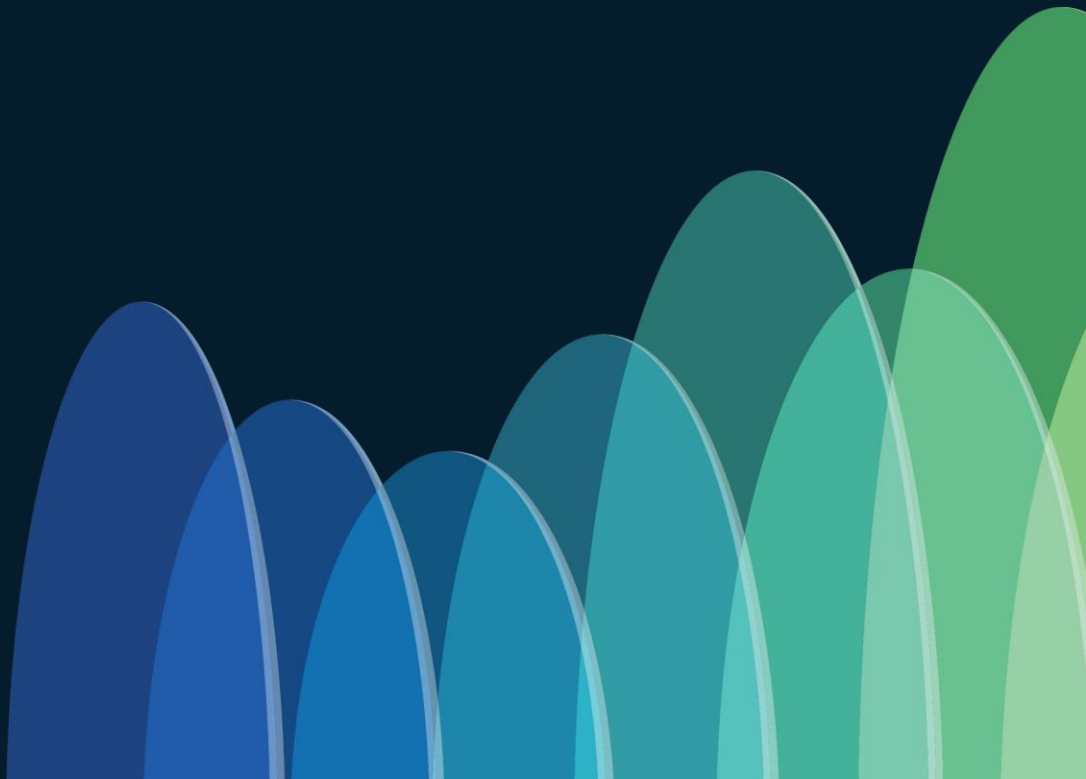
> Mapping Record 1, EID Prefix: [8193] 88:9c:ad:e7:98:80/48, TTL: 1440, Action: No-Action, Not Authoritative
Message End Marker: 0x9facade9 (correct)

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

When something breaks



AP Join Troubleshooting



Catalyst Center Checks

Cisco DNA Center

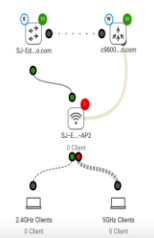
Network / Device 360

Tools

- Ping [Start](#)
- Trace Route [Start](#)
- AP Reboot [Reboot](#)
- Radio Reset [Reset](#)
- Flash LED Status: Off [Enable](#)
- Path Trace [Start](#)

Physical Neighbor Topology

Find by device ID, type, role, family & MAC



```
graph TD
    SJ-Edge1 --- SJ-Edge2
    SJ-Edge2 --- 2400_Clients
    SJ-Edge2 --- 5000_Clients
```

Provision > Inventory > Device > Run Commands

San Jose

Provision / Inventory

Router

Devices (13) Focus: Inventory

Filter devices

0 Selected [Add Device](#) [Tag](#)

Device Name	Family	Image Version	Site	Provision Status	Device Role	Last Sync Status	Platform	Serial Number	Series	Support Type
SJ-Edge2.cisco.com	Switches and Hubs	17.9.3	.../Corporate Office/Corporate Office-Floor2	Success	ACCESS	Managed (Updated: 6 hours ago)	C9300L-24P-4X	FOC2402LED8	Cisco Catalyst 9300 Series Switches	Supported
SJ-BDR2.cisco.com										
SJ-Edge1-AP1										
SJ-Edge1-AP2										
SJ-Edge1.cisco.com										
SJ-Edge2-AP1										
SJ-Edge2-AP2										
SJ-Edge2.cisco.com										
SJ-IN1.cisco.com										
SJ-IN2.cisco.com										

Run Commands

Reachable | IP Address 10.127.84.105 | Health 10 | Uptime 162 days 19 hrs

Family Switches and Hubs

Image Version 17.9.3

Site .../Corporate Office/Corporate Office-Floor2

Provision Status Success

Device Role ACCESS

Last Sync Status Managed (Updated: 6 hours ago)

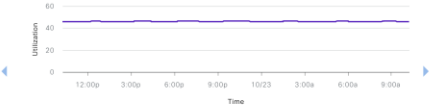
Platform C9300L-24P-4X

Serial Number FOC2402LED8

Series Cisco Catalyst 9300 Series Switches

Support Type Supported

Utilization (10) Memory 45.876% Time 10/23/2024 10:15



13 Records

Assurance > Dashboards > Health > Network > Device 360

Catalyst Center Checks

Cisco DNA Center

Fabric Sites

Find Hierarchy

- Global
- San Jose
- Corporate Office

Fabric Sites / San Jose

San Jose

Fabric Infrastructure

Authentication Ten

Select a Virtual Netw

Critical Pool: Not Sel

Corp

Edit Virtual Network: INFRA_VN

Filter | Delete Enable/Disable Supplicant-Based Extended Node Onboarding 0 Selected

	VLAN Name	Pool Type	Supplicant-Based Extended Node	IP Address Pool	VLAN ID	Layer 2 VNID	Layer-2 Flooding
☐	10_12...RA_VN	AP	Disabled	SI_Infra_VN 10.127.85.80/28	1027	8193	Disabled

Showing 1 of 1

10_127_85_80-INFRA_VN

10_12...RA_VN AP

Fabric Edge Checks

```
SJ-Edge2#show vlan
```

```
<snip>
```

```
1027 10_127_85_80-INFRA_VN          active  L2L10:8193, Gi1/0/1, Gi1/0/24
```

```
<snip ends>
```

 Identity Services Engine

Policy / Policy Elements

```
SJ-Edge2#show run int Vlan 1027
```

```
<snip>
```

```
interface Vlan1027
```

```
description Configured from Cisco DNA-Center
```

```
mac-address 0000.0c9f.ffd
```

```
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>
```

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

☐ ACL IPv6 (Filter-ID)

☐ Security Group ⓘ

☒ VLAN

Tag ID 1

Edit Tag

ID/Name 10_127_85_80-INFRA_VN ▼

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	lflid	Uptime
Ac1	0x000000046	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

Access-Tunnel
should be in "READY"
state

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

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

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

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
```

There should not
be any failures

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

WLC Checks

c9800-40-SJC#show wireless fabric summary

Fabric Status : Enabled

Fabric Status is Enabled

1) CP IPs.

2) LISP session is Up between WLC and CPs

Control-plane:

Name	IP-address	Key	Status
default-control-plane	10.127.84.100	91d46493aca049b7	Up
default-control-plane	10.127.84.101	91d46493aca049b7	Up

Fabric VNID Mapping:

Name	L2-VNID	L3-VNID	IP Address	Subnet	Control plane name
10_127_85_48-Corp	8194	0	0.0.0.0		default-control-plane
10_127_85_80-INFRA_VN	8193	4097	10.127.85.80	255.255.255.240	default-control-plane

IP Address Pool Name

L2VNID and L3VNID

IP Address and Subnet Mask

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 State	Slots	AP Model	Ethernet MAC	Radio MAC	Location	Country	IP Address

SJ-Edge1-AP1 Registered	3	C9130AXE-D	00df.1d9a.0e38	24d7.9c20.2d60	default location	US	10.127.85.83
SJ-Edge1-AP2 Registered	3	C9130AXI-D	6c71.0df2.4c04	2c57.4158.71a0	default location	US	10.127.85.84
SJ-Edge2-AP1 Registered	3	C9130AXI-D	1006.edfc.2c1c	889c.ade7.9280	default location	US	10.127.85.82
SJ-Edge2-AP2 Registered	3	C9130AXI-D	1006.edfc.2cdc	889c.ade7.9880	default location	US	10.127.85.85

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

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

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 Register	Up	Who Last Registered	Inst ID	EID Prefix
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 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

Note the wired0 interface of the AP

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

Note the IP, Hwaddr, "UP" status

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
1	10.127.84.105	00:00:0C:9F:FF:DD	Forward	VXLAN	25746	5325422	3077

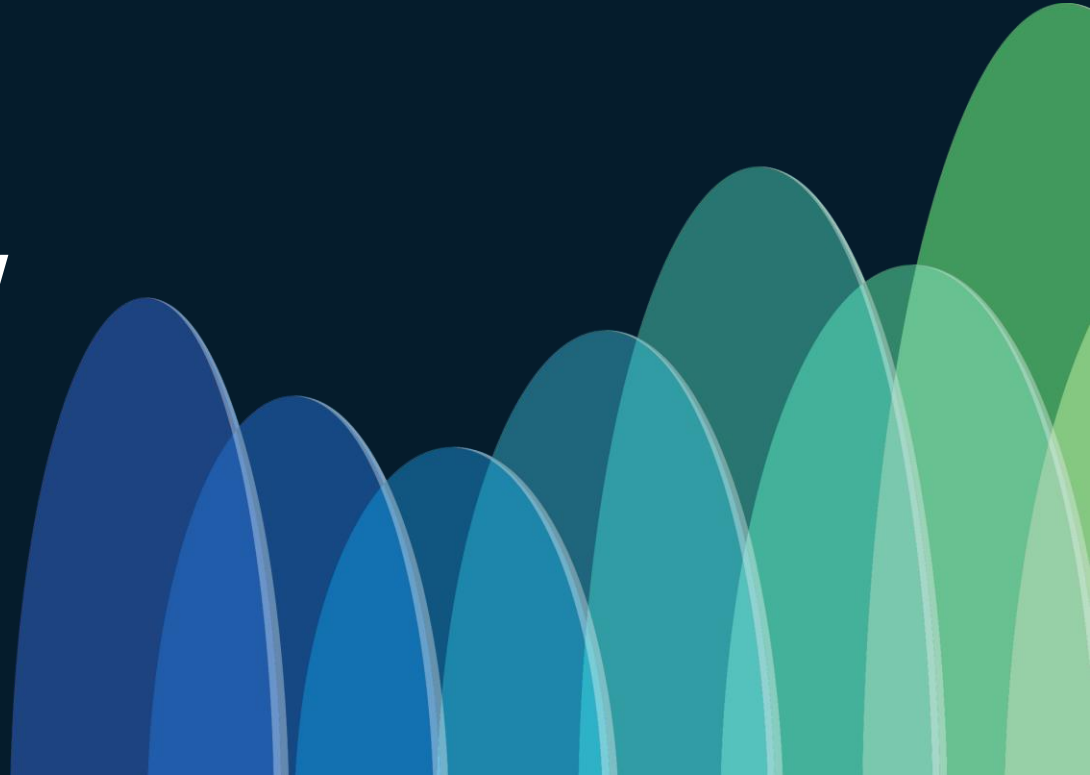
401508

AP APP Fabric Information:

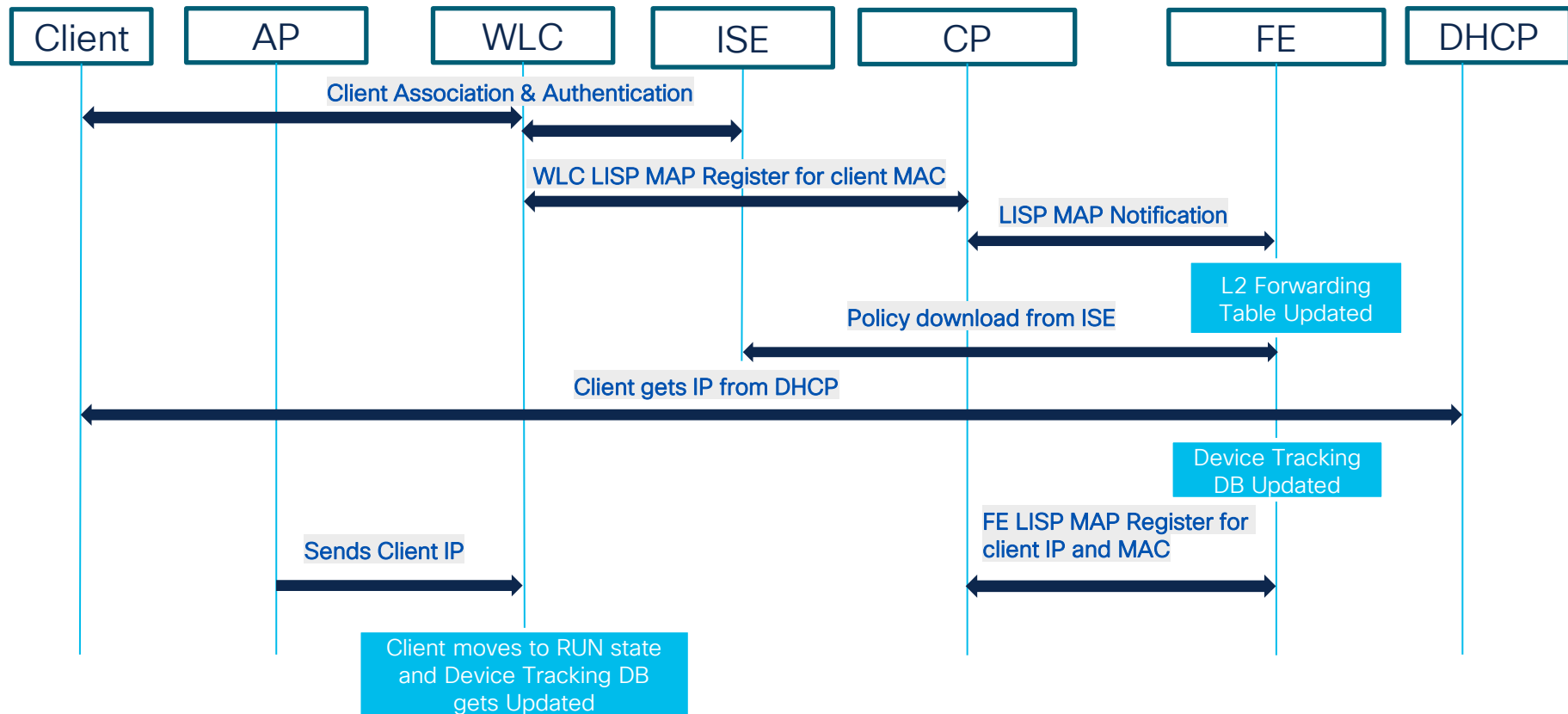
GW_ADDR	ENCAP_TYPE	VNID	SGT	FEATURE_FLAG	GW_SRC_MAC	GW_DST_MAC
SJ-Edge2-AP2#						

Note the 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



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_b7:50:27	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_b7:50:27	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_b7:50:27	0xe64c		EAP	91	Request,Identity
6930	2024-09-30 14:01:10.964946	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:27	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_b7:50:27	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_b7:50:27	0xe1ae		EAP	90	Success
7072	2024-09-30 14:01:13.819949	0.000000s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:27	0xe1ae		EAP	94	Success
7073	2024-09-30 14:01:13.822955	0.003006s	88:9c:ad:e7:98:81	Tp-LinkT_b7:50:27	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_b7:50:27	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_b7:50:27	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_b7:50:27	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

Client Onboarding Flow

LISP MAP Register for client MAC from WLC – WLC Captures

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 = Reserved: 0x00000000

Key ID: 0x0002

Authentication Data Length: 32

Authentication Data: 1044f3cf58b93585defd39975998bf32ca878ae8f5c4

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;

> 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)

Client Onboarding Flow – RA Traces from WLC

Client Association & Authentication

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

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_900000008] 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 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)
L3VNIID

Note, The SGT (2) and L3VNIID

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
1679	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

> Internet Protocol Version 4, Src: 10.127.84.8, Dst: 10.127.85.49

> User Datagram Protocol, Src Port: 67, Dst Port: 67

> 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

> Option: (82) Agent Information Option
Length: 20

> Option 82 Suboption: (1) Agent Circuit ID
Length: 6
Agent Circuit ID: 000404010d02

> Option 82 Suboption: (2) Agent Remote ID
Length: 10
Agent Remote ID: 0308001003010a7f5469

> Option: (255) End

Option: (82) Agent Information Option
Length: 20

Option 82 Suboption: (1) Agent Circuit ID
Length: 6
Agent Circuit ID: 000404010d02

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

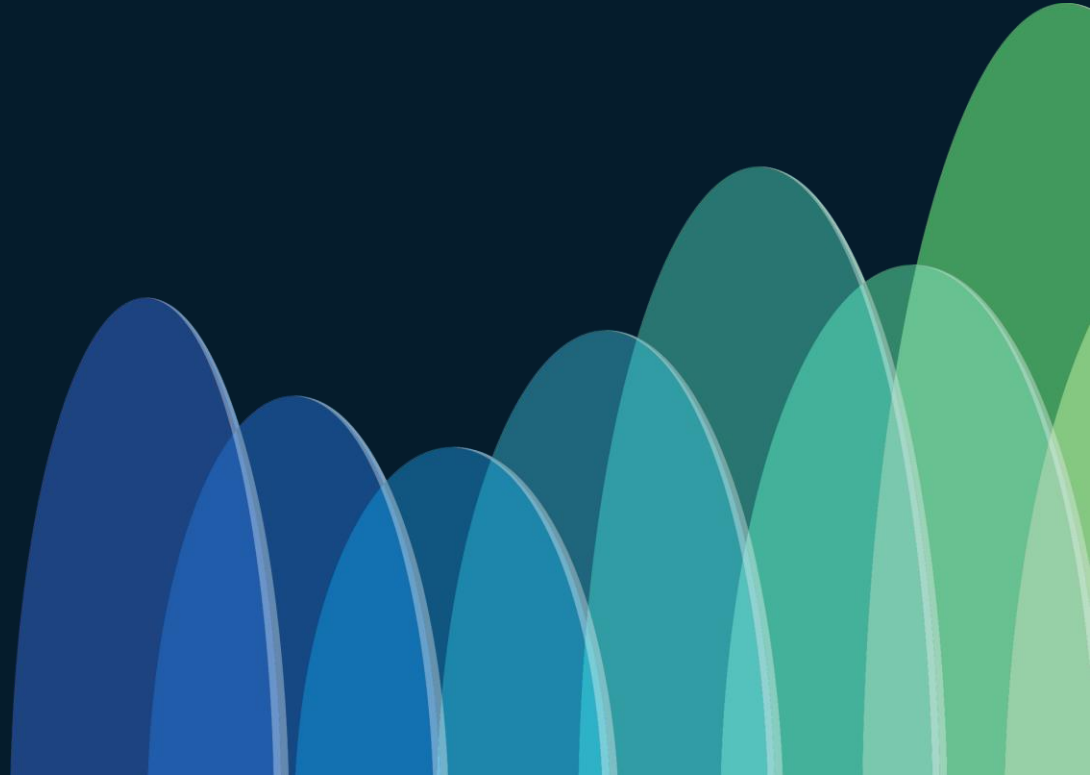
AP Sends Client IP

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 Override 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-switching vnid 8194

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

Client Onboarding Troubleshooting



Catalyst Center Checks

enter

in

Explore

Search: d037.45b7.5027

Hosts

D0:37:45:B7:50:27

no more results

D0:37:45:B7:50:27

MAC Address: D0:37:45:B7:50:27

Type: Microsoft-Workstation

Connection Type: WIRELESS

Endpoint Type: Wireless

Client 360

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

c9800-40-SJC#show wireless fabric summary

Fabric Status : Enabled

Fabric Status is Enabled

1) CP IPs.

2) LISP session is Up between WLC and CPs

Control-plane:
Name

IP-address

Key

Status

default-control-plane

10.127.84.100

91d46493aca049b7

Up

default-control-plane

10.127.84.101

91d46493aca049b7

Up

Fabric VNID Mapping:

Name

L2-VNID

L3-VNID

IP Address

Subnet

Control plane name

10_127_85_48-Corp

8194

0

0.0.0.0

default-control-plane

10_127_85_80-INFRA_VN

8193

4097

10.127.85.80 255.255.255.240

default-control-plane

IP Address Pool Name

L2-VNID

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)

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 6

AP Name	AP Model	Slots
OTT_9166	CW9166I-ROW	3
SJ-Edge1-AP1	C9130AXE-D	3
SJ-Edge1-AP2	C9130AXI-D	3
OTT_9164	CW9164I-B	3
SJ-Edge2-AP1	C9130AXI-D	3
SJ-Edge2-AP2	C9130AXI-D	3

Edit AP

General

Interfaces

High Availability

Inventory

ICap

Advanced

Support Bundle

General

Tags

AP Name*

SJ-Edge2-AP2

Location*

default location

Base Radio MAC

889c.ade7.9880

Ethernet MAC

1006.edfc.2cdc

Admin Status

ENABLED

AP Mode

Local

Operation Status

Registered

Fabric Status

Enabled

RLOC IP

10.127.84.105

Policy

PT_SanJo_Corpo...

Site

ST_SanJo_Corpo...

RF

HIGH

Write Tag Config to AP

Version

Primary Software Version

17.9.5.47

Predownload Status

N/A

Predownload Version

N/A

Next Retr Time

N/A

Cancel

Update & Apply to Device

Click to open it to see the details of the Policy tag.

You can also click the tags like Site and RF for more details.

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 Intf	Holdtme	Capability	Platform	Port ID
SJ-Edge2-AP2	Gig 1/0/1	122	R T	C9130AXI-	Gig 0

Note the AP in the CDP

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)

AP should be reachable

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	Ifld	Uptime
Ac0	0x0000003D	6 days, 23:36:15
Ac1	0x00000046	6 days, 23:36:13

Note the "Uptime" of the access-tunnel

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

Note the required permissions are present for the corresponding SGTs

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 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

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

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#

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
```

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

```
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 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

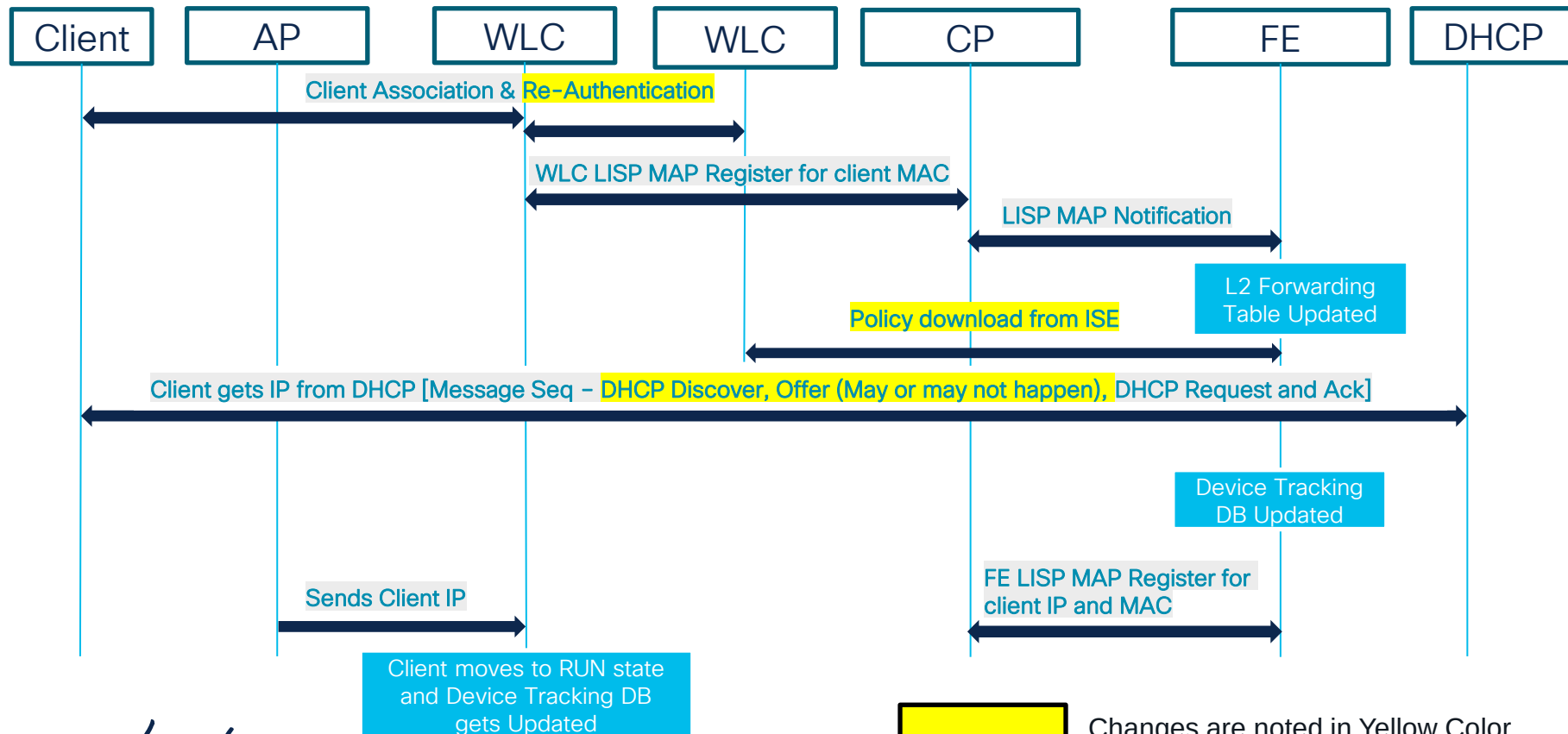
Note the LISP sessions being “Up” with the WLC and Edge.

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



Client Roaming Flow - RA Traces

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

Client Reassociation

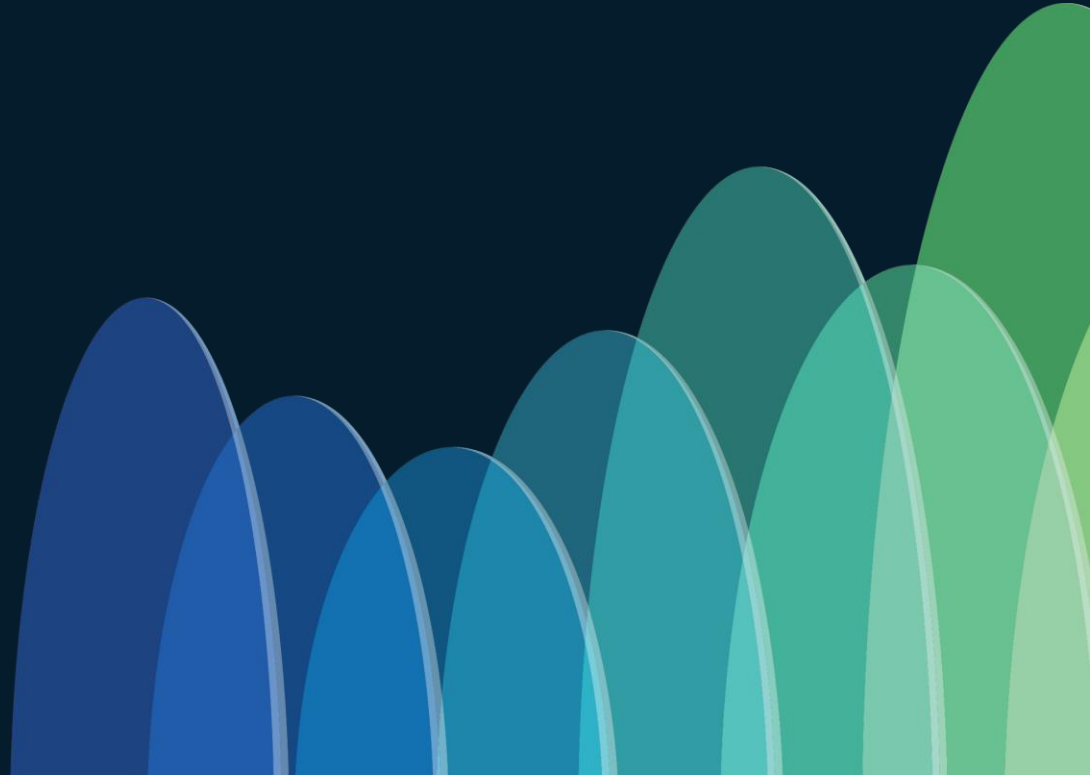
2024/09/30 15:17:58.739820062 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: d037.45b7.5027 **Re-Association received**. BSSID 2c57.4158.71a1, WLAN SJ_Corp_SSID_profile, Slot 0 AP 2c57.4158.71a0, SJ-Edge1-AP2, Site tag ST_SanJo_Corporat_9248f_0, Policy tag PT_SanJo_Corpo_Corporat_78519, Policy 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 Type	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Dot11 Roam

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?

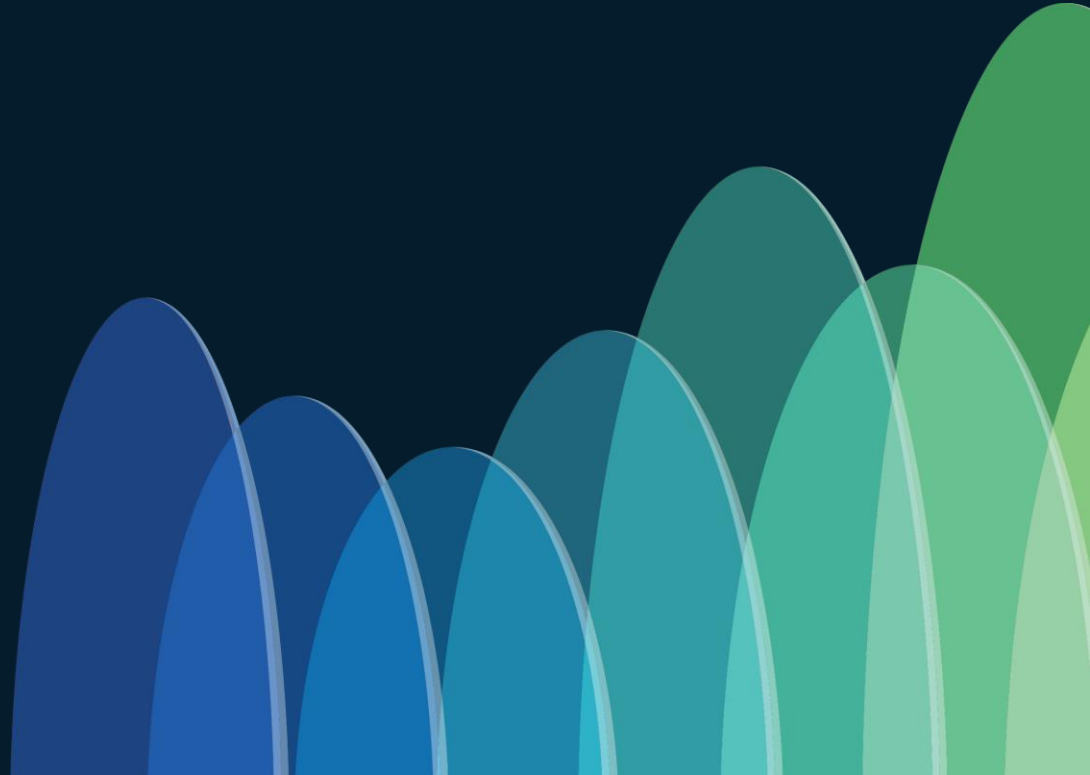
WLC = Did registration come from a Wireless Controller?

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 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
Q 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
<div> Search</div>						
	MAB	<div>OR</div> <div><div></div>Normalised Radius-RadiusFlowType EQUALS WiredMAB</div> <div><div></div>Normalised Radius-RadiusFlowType EQUALS WirelessMAB</div>	<div>Internal Users</div> <div></div> <div>> Options</div>	0		

Scenario – 1 – Contd

ISE Checks

▼ Authorization Policy(3)

				Results			
⊕	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search							
✓		Lab-APs-BGL	IdentityGroup-Name EQUALS Endpoint Identity Groups:BGL_AP	BGL-INFRA_VN	TrustSec_Devices	0	⚙
✓		Lab-APs-SJ	IdentityGroup-Name EQUALS Endpoint Identity Groups:SJ_AP	SJ-Infra_VN	TrustSec_Devices	0	⚙
✓		Default		DenyAccess	Select from list	0	⚙

Take note of Profiles

Security Group Tags can be created navigating to “Work Centers > TrustSec”

Scenario – 1 – Contd

ISE Checks

[Policy](#) > [Policy Elements](#) > [Results](#)

Go inside the noted “Authorization Profile”

[Authorization Profiles](#) > SJ-Infra_VN

Authorization Profile

* Name

SJ-Infra_VN

Description

SJ-Infra_VN

* Access Type

ACCESS_ACCEPT



Common Tasks

☒ VLAN

Tag ID **1**

[Edit Tag](#)

ID/Name

10_127_85_80-INFRA_VN

☐ Voice Domain Permission



```
SJ-Edge2#show vlan | i 1027
1027 10_127_85_80-INFRA_VN active L2Ll0:8193,
```

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

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)

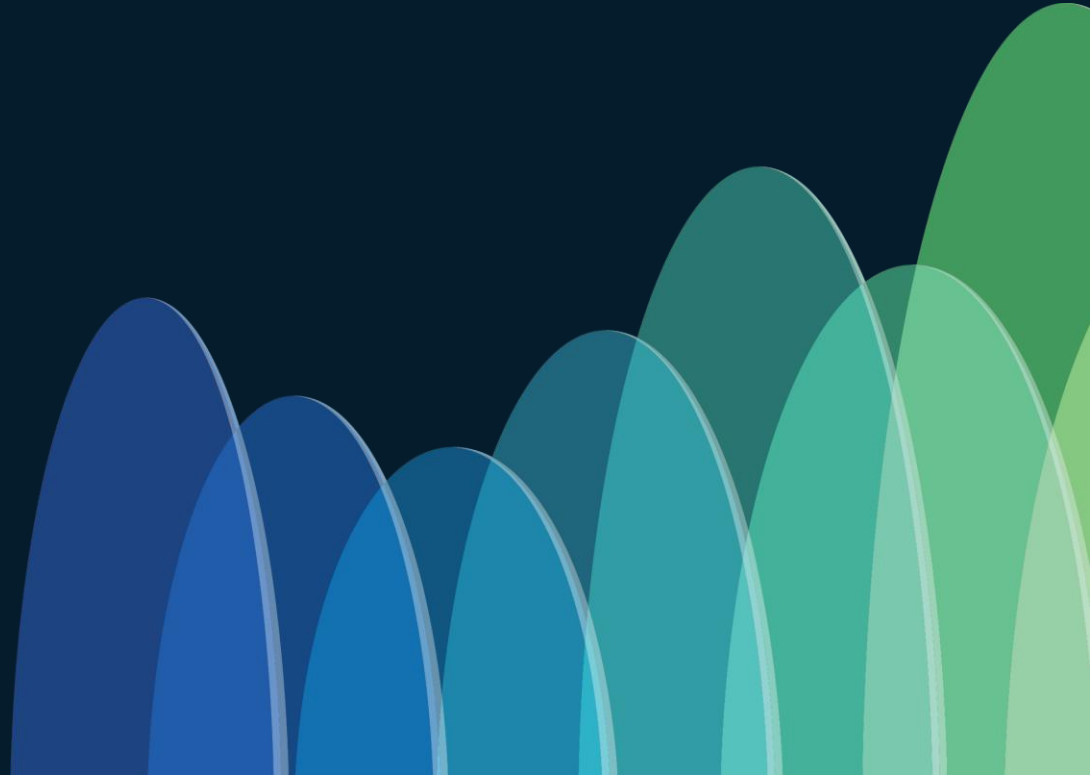
Debugs

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

Best practices and some troubleshooting tools



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.

Some Tools

Cisco Catalyst Center

Tools / Network Reasoner / Fabric Data Collection

1



Network Reasoner / Fabric Data Collection

Search Hierarchy



[Search Help](#)

Global

Unassigned Devices

Cisco Systems

Bangalore

San Jose

Sydney

2

Devices (7)



Filter devices



7 Selected

Tag

Troubleshoot

4

As of: Oct 10, 2024 1:03 PM



		Device Name	IP Address	Device Type	Site
3	☒	c9800-40-SJC.cisco.com	10.127.84.21	Wireless Controller	.../Corporate Office/Corporate Office-Server-room
	☒	SJ-BDR1.cisco.com	10.127.84.100	Switches and Hubs	.../Corporate Office/Corporate Office-Server-room
	☒	SJ-BDR2.cisco.com	10.127.84.101	Switches and Hubs	.../Corporate Office/Corporate Office-Server-room
	☒	SJ-Edge1.cisco.com	10.127.84.104	Switches and Hubs	.../Corporate Office/Corporate Office-Floor1

Some Tools

Cisco WLC – Troubleshooting Tools

 Dashboard

 Monitoring >

 Configuration >

 Administration >

 Licensing

 **Troubleshooting**

[Walk Me Through >](#)

Troubleshooting

 [Need help on what logs to collect for various scenarios?](#)



Logs

Manage Syslog, Webserver Log, License Log



Core Dump and System Report

View the list of core files and System Reports captured in the device



Debug Bundle

Capture require info like CLI outputs, logs as a single bundle for error reporting and debugging



Packet Capture

Capture packets with different filter options to feed into Wireshark for debugging



Ping and Trace Route

Check Ping-ability and Trace route info of a target destination through different sources



Radioactive Trace

Collect conditional trace logs using MAC address of a Client, AP etc.

Some Tools

Cisco WLC – Radioactive Traces Generation and Collection

The screenshot shows the Cisco WLC Troubleshooting > Radioactive Trace interface. The interface includes a sidebar with navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area displays the 'Radioactive Trace' section with a 'Conditional Debug Global State: Stopped' indicator. A table lists three trace entries with their MAC/IP addresses and trace file names. The entry for MAC/IP Address d037.45b7.5027 is selected. A 'Generate' button is visible next to each entry. A 'Last Run Result' section shows the state as 'Successful' and provides details for the selected trace file. An 'Enter time interval' dialog box is open, showing options to enable internal logs and generate logs for a specific time interval (10 minutes, 30 minutes, 1 hour, since last boot, or a custom interval). A blue box with text is overlaid on the bottom right of the dialog box.

1 Troubleshooting > Radioactive Trace

2 Dashboard

3 Conditional Debug Global State: Stopped

4 + Add - Delete ✓ Start ■ Stop

5 Generate

6 Enter time interval

7

Need help on what logs to collect for various scenarios?

Wireless Debug Analyzer

Last Run Result

✓ State Successful
[See Details](#)

MAC/IP Address d037.45b7.5027

Start Time 09/30/2024 15:20:13

End Time 09/30/2024 15:20:16

Trace file debugTrace_d037.45b7.5027.txt

MAC/IP Address Trace file

24d7.9c20.2d60 debugTrace_24d7.9c20.2d60.txt Generate

d037.45b7.5027 debugTrace_d037.45b7.5027.txt Generate

ec63.d7fc.f729 debugTrace_ec63.d7fc.f729.txt Generate

1 - 3 of 3 items

Enable Internal Logs ☒

Generate logs for last ☒ 10 minutes

☐ 30 minutes

☐ 1 hour

☐ since last boot

☐ 0-4294967295 seconds

Cancel Apply to Device

It is advisable to "Enable Internal Logs" to get more details in the RA Traces

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

Recap



- Architecture Overview
- Basic Workflows and Troubleshooting
 - AP Join
 - Client Onboarding
 - Client Roaming
- Some problem scenarios and list of useful commands
- Best practices and some troubleshooting tools

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



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



Continue your education



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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC