

Troubleshoot and verify SD-Access wireless initial setup

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components used](#)

[Topology](#)

[Troubleshoot and isolate](#)

[Quick verifications](#)

[scenario 1. Verify WLC registration with the LISP/MAP server control plane](#)

[scenario 2. Access points are not getting an ip address](#)

[scenario 3. Access points do not have a vxlan tunnel built towards their Fabric Edge node](#)

[scenario 4. access tunnel entries missing after a while](#)

[scenario 5. wireless clients not able to obtain an IP Address](#)

[scenario 6. Guest fabric / web authentication not working/not redirecting clients](#)

[Understand](#)

[How does a wireless client get an IP address in Fabric Architecture](#)

[Understand the web redirection flow in a fabric scenario](#)

[Logs of the AP joining the WLC in fabric-enabled state](#)

Introduction

This article describes the basic troubleshooting steps to identify basic connectivity issues in SD-Access wireless setups. It will describe the items and commands to check to isolate problems in the solution pertaining to wireless.

Prerequisites

Requirements

Knowledge of the SD-Access solution

An already set up SD-access topology

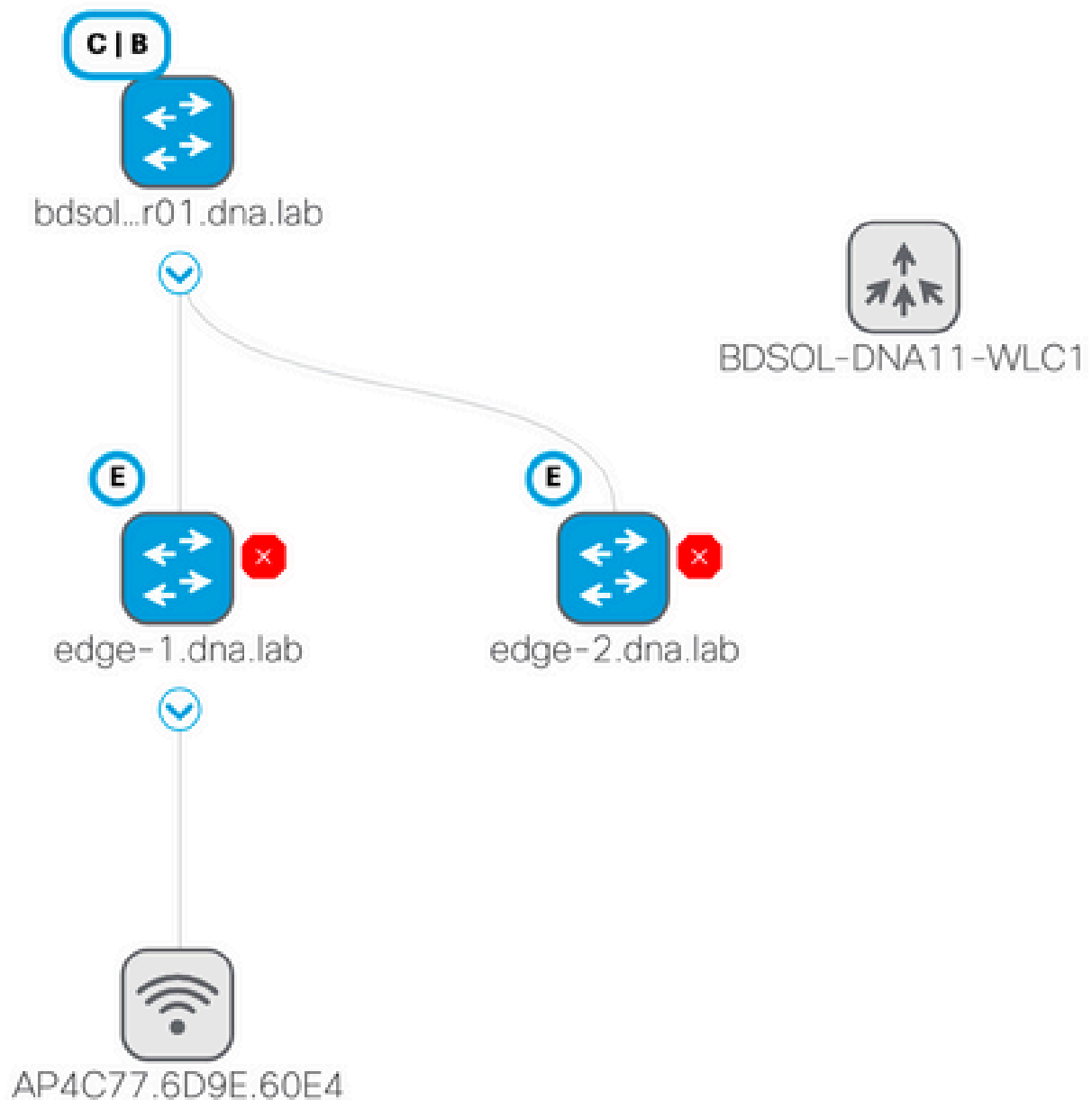
Components used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command. There are other types of devices supported for SD-access wireless, but this article focuses on the devices described in this section. Commands may vary depending on the platform and software version.

8.5.151 Wireless Controller

16.9.3 9300 switch as edge node

Topology



Troubleshoot and isolate

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 :

- Make sure that you have a specific route (and not using the default one) pointing to the WLC on the LISP control plane node

- Make sure that your APs are in the Infra VN, using the global routing table
- Make sure that APs have connectivity to the WLC by pinging the WLC from the AP itself
- Make sure that the fabric status of the control plane on the WLC is up
- Make sure that the APs are in fabric-enabled state

scenario 1. Verify WLC registration with the LISP/MAP server control plane

When you add the WLC to the fabric in DNA Center, commands are pushed to the controller to establish a connection to the node defined as control plane in DNA-C. The first step is to ensure this registration is successful. If the LISP configuration on the control plane got corrupted in some way, this registration could fail.

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes tabs for MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, and MANAGEMENT. On the left, a sidebar lists various configuration options under the 'Controller' heading, with 'Fabric Configuration' highlighted. The main content area is titled 'Fabric Control Plane Configuration'. It features a 'Fabric' toggle switch set to 'Enabled'. Below this, the 'Enterprise' section is expanded, showing configuration for a primary IP (172.16.2.254) and a secondary IP (empty). The 'Pre Shared Key' fields are masked with dots. The 'Connection Status' for the primary IP is shown as 'Up' in green text.

If this status shows as down, it may be interesting to run debugs or a packet capture between the WLC and the control plane. The registration involves both TCP and UDP on 4342. If the control plane didn't get the proper configuration, it might reply with a TCP RST to the TCP SYN sent by the WLC.

The same status can be verified with **show fabric map-server summary** on the command line. The process is debugged with **debug fabric lisp map-server all** on the WLC CLI. To provoke a reconnection attempt, you can go to DNA Center and chose to remove the WLC from the fabric and add it again.

Possible reasons are missing config lines in the control plane. Here's an example working config (the most important part only) :

```
rtr-cp-mer-172_16_200_4#show run | s WLC
locator-set WLC
  10.241.0.41
exit-locator-set
map-server session passive-open WLC
```

If the WLC ip is missing (10.241.0.41 here) or if the passive-open command is missing, the CP will refuse the WLC connection.

The debugs to run are :

- 'debug capwap events enable'
- 'debug capwap errors enable'
- 'debug fabric ap-join events enable'
- 'debug fabric ap-join detail enable'
- 'debug fabric lisp map-server all enable'

Here is an example of the control plane not answering the WLC

<#root>

```
*msfMsgQueueTask: May 07 14:08:10.080: Sent map-request to MS 10.32.47.128 for AP 10.32.58.36 VNID 4097
*msfMsgQueueTask: May 07 14:08:10.080: No messages are present in the Client list for Local UDP socket
*msfMsgQueueTask: May 07 14:08:10.080: msfSendLocalUDPSocketMessage:637 Message get for UDP file socket

*osapiBsnTimer: May 07 14:08:15.179: Map-reply timer for MS IP 10.32.47.128 expired for AP IP 10.32.58.36

*msfMsgQueueTask: May 07 14:08:15.179: msfQueue: recieved LISP_MAP_SERVER_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097

*msfMsgQueueTask: May 07 14:08:15.179: Added AP 10.32.58.36 VNID 4097 for long retry map-request

*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097
*msfMsgQueueTask: May 07 14:08:15.179: No messages are present in the Client list for Local UDP socket
*msfMsgQueueTask: May 07 14:08:15.179: msfSendLocalUDPSocketMessage:637 Message get for UDP file socket
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Request from 10.32.58.36:5248 epoch 1525
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Response sent to 10.32.58.36:5248
*osapiBsnTimer: May 07 14:08:17.839: NAK Timer expiry callback
*msfMsgQueueTask: May 07 14:08:17.839: msfQueue: recieved LISP_MAP_SERVER_NAK_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:17.839: Started periodic NAK processing timer

*msfMsgQueueTask: May 07 14:08:17.839: Process list of AP (1) for which RLOC is not received
```

Here is an example of the WLC debugs of an AP joining in fabric disabled state because the fabric control plane was missing a specific route to the WLC

```
(POD3-WLC1) >*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:55:26.295: ip c0a82700,subnet fffffff0,12vnid 8191,13vnid 1001
*emWeb: Oct 16 08:55:26.295: Vnid Mapping added at index 2 with entries 192_168_39_0-INFRA_VN,8191,4097

*emWeb: Oct 16 08:55:26.295:
    Log to TACACS server(if online): fabric vnid create name 192_168_39_0-INFRA_VN

*spamReceiveTask: Oct 16 08:55:26.295: Fabric is supported for AP f4:db:e6:61:24:a0 (Pod3-AP4800). apType 54

*spamReceiveTask: Oct 16 08:55:26.295: spamProcessFabricVnidMappingAddRequest: Fabric Adding vnid mapping
*spamReceiveTask: Oct 16 08:55:26.295: Vnid Mapping return from index 2 with entries name 192_168_39_0-INFRA_VN

*spamReceiveTask: Oct 16 08:55:26.295: spamSendFabricMapServerRequest: MS request from AP Pod3-AP4800 for 10.32.47.128
*emWeb: Oct 16 08:55:29.944:
```

Log to TACACS server(if online): save

```
(POD3-WLC1) >*spamApTask6: Oct 16 08:56:49.243: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 5
*spamApTask6: Oct 16 08:56:51.949: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 5
*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 5
*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 5
*spamApTask6: Oct 16 08:56:51.953: spamSendFabricMapServerRequest: MS request from AP Pod3-AP3800 f4:db:e6:64:02:a0
```

It is interesting to note that if there are two control planes in your fabric network, the WLC will always reach out to both for registration or queries. It is expected that both control plane give positive replies on registrations, so the WLC will fail to register APs in the fabric if one of the two control plane rejects it for any reason. One control plane not answering is acceptable however and the remaining control plane will be used.

APs reach out to the WLC through the global routing table, but LISP is still used to resolve the WLC. The traffic sent by APs to the WLC is pure CAPWAP control (no vxlan involved), but the return traffic sent by the WLC to the AP will be carried over Vxlan on the overlay. You will be unable to test connectivity from the AP gateway SVI on the edge towards the WLC because as it is an Anycast gateway, the same IP exists also on the border node. In order to test connectivity, the best is to ping from the AP itself.

scenario 2. Access points are not getting an ip address

Access points are expected to get an ip address from the AP Poo, in the Infra VNI defined in DNA Center. If this does not happen, it typically means that the switchport where the AP is connected didn't move to the right vlan. The switch, when detecting (through CDP) an access point being connected, will apply a switchport macro that will set the switchport in the vlan defined by DNA-C for the AP pool. If the problematic switchport is indeed not configured with the macro, you can either set the configuration manually (so that the AP gets an ip, joins the WLC and probably upgrades its code and possibly resolve any CDP bug) or troubleshoot the CDP connection process. You can optionally configure host onboarding to statically define the port on DNA-Center to host an AP so that it is provisioned with the right configuration.

Smartport macros do not kick in automatically if the switch was not provisioned with one AP at least, you can verify if the AP macro was provisioned with the right vlan (instead of the default vlan 1)

```
Pod3-Edge1#show macro auto device
Device:lightweight-ap
Default Macro:CISCO_LWAP_AUTO_SMARTPORT
Current Macro:CISCO_LWAP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=2045
```

The commands that Cisco DNA-C pushes to set this are

```
macro auto execute CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT builtin CISCO_LWAP_AUTO_SMARTPORT ACCESS_VLAN=2045
macro auto global processing
```

scenario 3. Access points do not have a vxlan tunnel built towards their Fabric Edge node

Once an AP joins the WLC, the WLC (if the AP is fabric capable) will register the AP on the control plane as a special type of client. The control plane will then request the Fabric Edge node where the AP is plugged to build a vxlan tunnel towards the AP.

The AP will only use vxlan encapsulation to send client traffic (and only for clients in RUN state), therefore it is normal to not see any vxlan information on the AP until a fabric client connects.

On the AP, the command **show ip tunnel fabric** will show the vxlan tunnel information once a client has connected.

```
AP4001.7A03.5736#show ip tunnel fabric
```

```
Fabric GWs Information:
```

Tunnel-Id	GW-IP	GW-MAC	Adj-Status	Encap-Type	Packet-In	Bytes-In	Packet-Out
1	172.16.2.253	00:00:0C:9F:F4:5E	Forward	VXLAN	39731	4209554	16345

```
AP4001.7A03.5736#
```

On the Fabric Edge node, the command **show access-tunnel summary** will show the vxlan tunnels built towards the access points. The tunnels will show as soon as the control plane ordered their creation when the AP joins.

```
edge01#show access-tunnel summ
```

```
Access Tunnels General Statistics:
```

```
Number of AccessTunnel Data Tunnels = 2
```

Name	SrcIP	SrcPort	DestIP	DstPort	VrfId
Ac1	172.16.2.253	N/A	192.168.102.130	4789	2
Ac0	172.16.2.253	N/A	192.168.102.131	4789	2

Name	IfId	Uptime
Ac1	0x0000003B	1 days, 22:53:48
Ac0	0x0000003A	0 days, 22:47:06

You can check on the WLC, on the access point page, the L2 LISP instance id corresponding to that AP and then check the statistics of that instance on the Fabric Edge where it is connected.

CAPWAP Preferred Mode	Ipv4 (Global Config)
DHCP Ipv4 Address	192.168.102.131
Static IP (Ipv4/Ipv6)	<input type="checkbox"/>

3490635A224C

Fabric

Fabric Status	Enabled
Fabric L2 Instance ID	8190
Fabric L3 Instance ID	4098
Fabric RlocIp	172.16.2.253

Time Statistics

UP Time	0 d, 00 h 29 m 57 s
Controller Associated Time	0 d, 00 h 26 m 46 s
Controller Association Latency	0 d, 00 h 03 m 10 s

SDA-D-6880-1#show lisp instance-id 8188 ethernet statistics
 LISP EID Statistics for instance ID 8188 - last cleared: never
 Control Packets:

Map-Requests in/out:	0/0
Encapsulated Map-Requests in/out:	0/0
RLOC-probe Map-Requests in/out:	0/0
SMR-based Map-Requests in/out:	0/0
Map-Requests expired on-queue/no-reply	0/0
Map-Resolver Map-Requests forwarded:	0
Map-Server Map-Requests forwarded:	0
Map-Reply records in/out:	0/0
Authoritative records in/out:	0/0
Non-authoritative records in/out:	0/0
Negative records in/out:	0/0
RLOC-probe records in/out:	0/0
Map-Server Proxy-Reply records out:	0
Map-Register records in/out:	24/0
Map-Server AF disabled:	0
Authentication failures:	0
Map-Notify records in/out:	0/0
Authentication failures:	0
Deferred packet transmission:	0/0
DDT referral deferred/dropped:	0/0
DDT request deferred/dropped:	0/0

scenario 4. access tunnel entries missing after a while

It is possible that the access tunnels are successfully created the first time when WLC is provisioned through Cisco DNA-C and added to the fabric but when re-provisioning wireless configuration (like the WLAN configuration) it is observed that access tunnel entries for APs are missing resulting wireless clients are unable to successfully get IP.

The topology is 9500(CP) --> 9300 (Edge) --> AP --> Wireless Client.

Entries are correctly observed in **show access-tunnel summary** on the edge node:

```
edge_2#show access-tunnel summary
```

```
Access Tunnels General Statistics:  
Number of AccessTunnel Data Tunnels = 1
```

```
Name SrcIP SrcPort DestIP DstPort VrfId  
-----  
Ac0 172.16.3.98 N/A 172.16.3.131 4789 0
```

```
Name IfId Uptime  
-----  
Ac0 0x0000003C 5 days, 18:19:37
```

But when checking **show platform software fed switch active ifm interfaces access-tunnel**, the entry for the AP is missing or failed to be programmed in the hardware in this example.

```
edge_2#show platform software fed switch active ifm interfaces access-tunnel  
Interface IF_ID State  
-----  
Ac0 0x0000003c FAILED
```

For more outputs :

```
edge_2#sh platform software access-tunnel switch active F0  
Name SrcIp DstIp DstPort VrfId Iif_id Obj_id Status  
-----  
Ac0 98.3.16.172 131.3.16.172 0x12b5 0x000 0x00003c 0x00585f Done
```

```
edge_2#sh platform software access-tunnel switch active R0  
Name SrcIp DstIp DstPort VrfId Iif_id  
-----  
Ac0 172.16.3.98 172.16.3.131 0x12b5 0x0000 0x00003c
```


You need to compare the different outputs and every tunnel showed by the **show access-tunnel summary** must be present in each of them.

scenario 5. wireless clients not able to obtain an IP Address

If the vxlan tunnel is present and all looks good but the wireless clients are systematically unable to obtain an IP address you are maybe facing an option 82 problem. Since the DHCP DISCOVER of the client is forwarded by the Anycast gateway on the edge node, there would be trouble for the DHCP server OFFER to be sent to the right edge node by the border on the way back. This is why the fabric edge that forwards the DHCP DISCOVER appends an option 82 field to the DHCP DISCOVER that contains the actual fabric RLOC (loopback ip) of the edge node encoded along with other informations. This means that your DHCP server must support option 82.

To troubleshoot the DHCP process, take captures on the fabric nodes (especially the client edge node) to verify that the fabric edge is appending the option 82 field.

scenario 6. Guest fabric / web authentication not working/not redirecting clients

The guest fabric scenario is extremely similar to Central Web Authentication (CWA) on Flexconnect access points and work exactly the same way (even if fabric APs are not in flexconnect mode).

The redirection ACL and URL must be returned by ISE in the first mac authentication result. Verify those in the ISE logs as well as the client detail page on the WLC.

The redirect ACL must be present as a Flex ACL on the WLC and must contain "permit" statements towards the ISE IP address on port 8443 (at least).

The client should be in "CENTRAL_WEBAUTH_REQ" state in the client details page on the WLC. The client will not be able to ping his default gateway and this is expected. If you are not redirected you can try to type manually an ip address in the client web browser (to rule out DNS, but ISE hostname will have to be resolved anyway). You should be able to enter the ISE IP on port 8443 in the client browser and see the portal page as this flow will not be redirected. If this does not happen, you are either facing an ACL issue or a routing issue towards. Collect packet captures along the way to see where the HTTP packets are stopped.

Understand

How does a wireless client get an IP address in Fabric Architecture

Packet capture is taken between the Fabric AP and the Fabric Edge. Packet are duplicated because two DHCP Discover packets were sent. The traffic was only ingress and captured on the Fabric Edge.

There are always two DHCP packets. One sent by CAPWAP directly to the controller to keep it updated. The other one sent by VXLAN to the Control Node. When the AP receive for example a DHCP Offer with VXLAN by the DHCP server, it sends a copy to the controller with CAPWAP.

No.	Time	Source	Destination	Protocol	Length	Info
81	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
82	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
83	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
84	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
85	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
86	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
87	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
88	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
89	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001
90	0.000000	10.10.10.10	255.255.255.255	DHCP	100	DHCP Discover - Transaction ID: 0x00000001

85	0.000252	0.0.0.0	255.255.255.255	DHCP	414 DHCP Request
86	0.000255	192.168.103.1	192.168.103.7	DHCP	418 DHCP ACK
87	0.000258	192.168.103.1	192.168.103.7	DHCP	418 DHCP ACK

```

> Frame 85: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits) on interface 0
> Ethernet II, Src: Cisco_70:60:04 (40:01:7a:70:60:04), Dst: Cisco_9f:f4:5c (00:00:0c:9f:f4:5c)
> Internet Protocol Version 4, Src: 172.16.3.131, Dst: 172.16.3.98
> User Datagram Protocol, Src Port: 49361, Dst Port: 4789
> Virtual eXtensible Local Area Network
> Ethernet II, Src: EdimaxTe_d3:80:b5 (74:da:38:d3:80:b5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Bootstrap Protocol (Request)

```

To see where the packet was sent, you need to click on it on Wireshark. Here we can see the source is our AP 172.16.3.131 and the packet was sent to the Fabric Edge 172.16.3.98. The Fabric Edge forwarded it to the Control Node.

Understand the web redirection flow in a fabric scenario

The redirect ACL on the WLC defines what traffic is redirected/intercepted on matching deny statements (there is an implicit deny at the end). That traffic to be redirected will be sent to the WLC inside CAPWAP encapsulation for the WLC to redirect. When matching a permit statement, it does not redirect that traffic and lets it through and forwards it on the fabric (traffic towards ISE enters this category).

Logs of the AP joining the WLC in fabric-enabled state

As soon as Access-Point register to WLC, controller will register its IP and MAC address in SDA Control Node (LISP Map Server).

The AP joins the WLC in fabric-enabled mode only if the WLC receive the LISP RLOC packet. This packet is sent to be sure that the AP is connected to a Fabric Edge.

The debugs used on the WLC for this example are :

- 'debug capwap events enable'
- 'debug capwap errors enable'
- 'debug fabric ap-join events enable'
- 'debug fabric ap-join detail enable'
- 'debug fabric lisp map-server all enable'

For the test, the AP is rebooted :

```
<#root>
```

```

*spamApTask0: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for Aggregated Payload
*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: Cleaned up AP RLOC NAK entry for AP 172.16.3.131 vnid 4097 for B
*msfMsgQueueTask: May 07 13:00:18.804: Inserted entry for AP IP 172.16.3.131 and VNID 4097, db idx 12
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply timer started for AP IP 172.16.3.131 and VNid 4097
*msfMsgQueueTask: May 07 13:00:18.804: Creating new timer for AP IP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply Timer Started Successfully for AP IP 172.16.3.131 and V
*msfMsgQueueTask: May 07 13:00:18.804: Not able to find nonce 0x3cd13556-0x81864b7b avl entry

```

```

*msfMsgQueueTask: May 07 13:00:18.804: FAIL: not able to find avl entry
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b inserted into nonce avl tree for AP
*msfMsgQueueTask: May 07 13:00:18.804: Set nonce 0x3cd13556-0x81864b7b for AP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b is updated for AP IP 172.16.3.131, VN
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for PHY payload s
*msfMsgQueueTask: May 07 13:00:18.804: Build and send map-request for AP IP 172.16.3.131 and VNID 4097
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferen
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferen
*msfMsgQueueTask: May 07 13:00:18.804: nonce = 3cd13556-81864b7b lisp_map_request_build allocating nonc
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmNeighbourC
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for CcxRmMeas pay

*msfMsgQueueTask: May 07 13:00:18.804: Sending map-request for AP 172.16.3.131 VNID 4097 to MS 172.16.3.

*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for AP ext-logging
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update for Delba sent to 172.16.

*msfMsgQueueTask: May 07 13:00:18.804: Map-request for AP IP 172.16.3.131 VNID 4097 to MS 172.16.3.254 i

*msfMsgQueueTask: May 07 13:00:18.804: Sent map-request to MS 172.16.3.254 for AP 172.16.3.131 VNID 4097

*msfMsgQueueTask: May 07 13:00:18.804: Invalid secondary MS IP 0.0.0.0 for map-request for AP IP 172.16
*msfMsgQueueTask: May 07 13:00:18.804: No messages are present in the Client list for Local UDP socket
*msfTcpTask: May 07 13:00:18.807: Sending the UDP control packet to queue task
*msfMsgQueueTask: May 07 13:00:18.807: msfQueue: recieved LISP_MAP_SERVER_UDP_PACKET_QUEUE_MSG
*msfMsgQueueTask: May 07 13:00:18.807: Mapping Record has locators and actions
*msfMsgQueueTask: May 07 13:00:18.807: Mapping record address 172.16.3.98 EID address 172.16.3.98
*msfMsgQueueTask: May 07 13:00:18.807: Got AVL entry for nonce 0x3cd13556-0x81864b7b in map-reply for A

*msfMsgQueueTask: May 07 13:00:18.807: Sent received RLOC IP 172.16.3.98 for AP 172.16.3.131 and VNID 40

*msfMsgQueueTask: May 07 13:00:18.807: Added RLOC 172.16.3.98 for AP IP 172.16.3.131

*spamReceiveTask: May 07 13:00:18.807: Recieved Fabric rloc response from msip 172.16.3.254 with apvnid

```