

排除Cisco DNA Center上的无线软件定义访问故障

目录

[简介](#)

[交换矩阵的命令备忘单](#)

[AireOS WLC从思科DNA中心推送配置](#)

[思科DNA中心的WLC配置推送](#)

[如何检查映射服务器是否可达？](#)

[调试交换矩阵映射服务器连接](#)

[如何检查交换矩阵是否已启用以及预期输出是什么？](#)

[思科DNA中心的WLAN配置推送](#)

[调试无线问题](#)

[AP加入调试/接入隧道形成调试](#)

[客户端调试](#)

[WLC调试](#)

[交换矩阵边缘调试](#)

[接入点调试](#)

[使用案例调试](#)

[客户端CWA调试](#)

[客户端DHCP调试](#)

[AP上的客户端性能调试](#)

[AP自注册](#)

[传统方法/步骤：](#)

[即插即用/零接触AP调配](#)

[相关信息](#)

简介

本文档介绍无线常见问题以及如何对Cisco DNA Center上的软件定义访问进行故障排除。

交换矩阵的命令备忘单

以下是控制节点、边缘节点、无线局域网控制器(WLC)和接入点(AP)上交换矩阵的命令备忘单。

控制节点：

- `show lisp instance-id <L2 ap instance id>`以太网服务器- MAC到终端标识(EID)映射
- `show lisp instance-id <L3 ap instance id> ipv4 server` - IP到EID映射
- `show lisp instance-id 8188 ethernet server address-resolution` — 特定实例ID的MAC到IP映射
- `show lisp site`
- `show tech-support`

- show tech-support lisp

边缘节点：

- 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
- 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

WLC(AireOS):

- show fabric ap summary
- show fabric summary
- show fabric map-server summary
- show run-config
- show run-config命令
- show tech

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 (如果9300/9400/9500上运行的是机箱中的交换矩阵或嵌入式无线)
- show tech-support (如果9300/9400/9500上运行的是机箱中的交换矩阵或嵌入式无线)

访问点:

- show ip tunnel fabric
- show tech-support

AireOS WLC从思科DNA中心推送配置

此处显示调配后从Cisco DNA Center推送的AireOS WLC配置(注意：使用参考作为3504 WLC)。

在WLC调配后显示radius摘要：

(sdawl3504) >show radius summary

```

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... Lower
Accounting Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
Keywrap..... Disabled
Fallback Test:
  Test Mode..... Passive
  Probe User Name..... cisco-probe
  Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen
RADIUS Authentication Framed-MTU..... 1300 Bytes

```

Authentication Servers

Idx	Type	Server Address	Port	State	Tout	MgmtTout	RFC3576	IPSec - state/Profile Name/Radi
1	* NM	192.168.2.193	1812	Enabled	2	5	Enabled	Disabled - /none
2	M	172.27.121.193	1812	Enabled	2	5	Enabled	Disabled - /none

WLAN配置推送在show wlan summary下显示。

(sdawl3504) >show wlan summary

Number of WLANs..... 7

WLAN ID	WLAN Profile Name / SSID	Status	Interface N
1	Test / Test	Enabled	management
17	dnac_guest_F_global_5dfbd_17 / dnac_guest_206	Disabled	management
18	dnac_psk_2_F_global_5dfbd_18 / dnac_psk_206	Disabled	management
19	dnac_wpa2__F_global_5dfbd_19 / dnac_wpa2_206	Enabled	management
20	dnac_open__F_global_5dfbd_20 / dnac_open_206	Enabled	management
21	Test!23_F_global_5dfbd_21 / Test!23	Disabled	management

思科DNA中心的WLC配置推送

此处显示了将WLC添加到交换矩阵后Cisco DNA Center的WLC配置推送。

如何检查映射服务器是否可达？

将WLC添加到交换矩阵后show fabric map-server summary。

```
(sdawl3504) >show fabric map-server summary
```

```
MS-IP      Connection status
```

```
-----
```

```
192.168.4.45    UP
```

```
192.168.4.66    UP
```

调试交换矩阵映射服务器连接

由于各种原因，控制平面(CP)连接可能会关闭或保持关闭。

- 如果CP发生故障。(本例并非如此)
- 连接WLC和CP的中间节点，例如融合路由器。
- 如果CP与WLC的连接因链路关闭而中断。这可以是WLC到直接邻居，或是CP到直接邻居到WLC。

```
show fabric map-server detail
```

```
show fabric TCP creation-history <Map-Server IP>
```

可以提供更多信息的调试

```
debug fabric lisp map-server tcp enable
```

```
debug fabric lisp map-server all enable
```

如何检查交换矩阵是否已启用以及预期输出是什么？

将WLC添加到交换矩阵后显示交换矩阵摘要。

```
(sdawl3504) >show fabric summary
```

```
Fabric Support..... enabled
```

```
Enterprise Control Plane MS config
```

```
-----
```

```
Primary Active MAP Server
```

```
IP Address..... 192.168.4.45
```

```
Secondary Active MAP Server
```

```
IP Address..... 192.168.4.66
```

```
Guest Control Plane MS config
```

```
-----
```

```
Fabric TCP keep alive config
```

```
-----
```

```
Fabric MS TCP retry count configured ..... 3
```

```

Fabric MS TCP timeout configured ..... 10
Fabric MS TCP keep alive interval configured .... 10
Fabric Interface name configured ..... management

Fabric Clients registered ..... 0

Fabric wlans enabled ..... 3

Fabric APs total Registration sent ..... 30

Fabric APs total DeRegistration sent ..... 9

Fabric AP RLOC requested ..... 15

Fabric AP RLOC response received ..... 30

Fabric AP RLOC send to standby ..... 0

Fabric APs registered by WLC ..... 6

```

VNID Mappings configured: 4

Name	L2-Vnid	L3-Vnid	IP Address/Subnet
182_10_50_0-INFRA_VN	8188	4097	182.10.50.0 / 255.255.255.128
10_10_10_0-Guest_Area	8190	0	0.0.0.0 / 0.0.0.0
182_10_100_0-DEFAULT_VN	8191	0	0.0.0.0 / 0.0.0.0
182_11_0_0-DEFAULT_VN	8189	0	0.0.0.0 / 0.0.0.0

Fabric Flex-Acl-tables	Status
DNAC_FABRIC_FLEX_ACL_TEMPLATE	Applied

Fabric Enabled Wlan summary

WLAN ID	SSID	Type	L2 Vnid	SGT	RLOC IP	Clients	VNID Name
19	dnac_wpa2_206	WLAN	8189	0	0.0.0.0	0	182_11_0_0-DEFAULT_VN
20	dnac_open_206	WLAN	8189	0	0.0.0.0	0	182_11_0_0-DEFAULT_VN

思科DNA中心的WLAN配置推送

将WLC添加到交换矩阵后，从Cisco DNA Center的show fabric wlan summary下可以看到来自WLAN的WLAN配置推送，并且客户端IP池在Provision > Fabric > Host Onboarding下分配给交换矩阵无线LAN(WLAN)。

在交换矩阵调配后显示交换矩阵wlan摘要。

```
(sdawl3504) >show fabric wlan summary
```

WLAN ID	SSID	Type	L2 Vnid	SGT	RLOC IP	Clients	VNID Name
19	dnac_wpa2_206	WLAN	8189	0	0.0.0.0	0	182_11_0_0-DEFAULT_VN
20	dnac_open_206	WLAN	8189	0	0.0.0.0	0	182_11_0_0-DEFAULT_VN

调试无线问题

AP加入调试/接入隧道形成调试

1.检查AP是否获得IP地址。

在交换矩阵边缘上显→ip dhcp snooping binding

如果未显示连接的AP接口的IP，请在交换机上启用这些调试，并检查AP是否获得IP。

```
debug ip dhcp snooping packet
```

```
debug ip dhcp snooping event
```

示例日志文件附加在下面→

示例：

```
Floor_Edge-6#sh ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
-----
0C:75:BD:0D:46:60 182.10.50.7 670544 dhcp-snooping 1021 GigabitEthernet1/0/7 → AP interface should be havi
```

2.检查AP是否加入WLC。

- show ap summary → On WLC
- show ap join stat summary → On WLC

如果AP从未加入WLC，请在WLC上启用这些调试。

- debug capwap events enable
- debug capwap errors enable

3.如果AP形成CAPWAP，但AP和交换机之间未形成访问隧道，请执行这些检查

步骤1.如果WLC中的AP没有RLOC IP，请在此处检查点1。


1.为了使交换矩阵控制平面协议具有更强的恢复力，每个交换矩阵节点的全局路由表中必须存在通向WLC的特定路由。通向WLC IP地址的路由应重新分发到边界处的基础IGP协议中，或在每个节点处静态配置。换句话说，WLC不应通过默认路由到达。

步骤2.如果WLC中的AP显示正确的RLOC，并在show fabric summary下显示请求了RLOC且接收的RLOC全部正常，请检查这些步骤

2.检查控制平面节点，show lisp instance-id <L2 ap instance id> ethernet server→它应包含AP的基本无线电MAC。

在交换矩阵边缘节点上选中，show lisp instance-id <L2 ap instance id> ethernet database wlc → 它应包含AP的基本无线电MAC，而不是AP的以太网MAC。

如果以上2个命令未显示AP的基本无线电MAC，且未形成接入隧道。在控制平面上启用debug lisp control-plane all，并在日志记录中搜索基本无线电MAC。

 注意：debug lisp control-plane all on Control plane is trally chatty，please disable console logging before turn on the debugs.

如果您看到此处所示的身份验证失败，请检查WLC和CP节点之间的身份验证密钥。

```
Dec 7 17:42:01.655: LISP-0: MS Site EID IID 8188 prefix any-mac SVC_VLAN_IAF_MAC site site_uci, Registr
```


```
Dec 7 17:42:01.659: LISP-0: Building reliable registration message registration-rejected for IID 8188
```

如何检查WLC和CP之间的交换矩阵配置上的身份验证密钥。

在WLC上，请在Controller > Fabric Configuration > Control Plane >(Pre Shared Key)

On CP, please check on switch using sh running-config | b map-server session CP#sh running-config | b map-server session map-server session passive-open WLC site site_uci description map-server configured from apic-em authentication-key

(Ensure that the Pre shared key on WLC should match with this authentication key on CP)

 注意：通常，Cisco DNA Center会推送此密钥，因此，除非需要并且知道CP/WLC上配置了什么，否则不要更改此密钥]

4.访问隧道的常规检查和show命令。

- show access-tunnel summary

```
Floor_Edge-6#sh access-tunnel summary
```

```
Access Tunnels General Statistics:  
Number of AccessTunnel Data Tunnels = 5
```

```
Name SrcIP SrcPort DestIP DstPort VrfId
```

```
-----  
Ac4 192.168.4.68 N/A 182.10.50.6 4789 0  
Ac24 192.168.4.68 N/A 182.10.50.5 4789 0  
Ac19 192.168.4.68 N/A 182.10.50.8 4789 0  
Ac15 192.168.4.68 N/A 182.10.50.7 4789 0  
Ac14 192.168.4.68 N/A 182.10.50.2 4789 0
```

```
Name IfId Uptime
-----
Ac4 0x00000037 2 days, 20:35:29
Ac24 0x0000004C 1 days, 21:23:16
Ac19 0x00000047 1 days, 21:20:08
Ac15 0x00000043 1 days, 21:09:53
Ac14 0x00000042 1 days, 21:03:20
```

- show platform software fed switch active ifm interfaces access-tunnel

```
Floor_Edge-6#show platform software fed switch active ifm interfaces access-tunnel
Interface          IF_ID          State
-----
Ac4                0x00000037    READY
Ac14               0x00000042    READY
Ac15               0x00000043    READY
Ac19               0x00000047    READY
Ac24               0x0000004c    READY
```

```
Floor_Edge-6#
```

如果命令b)下的Access-tunnels高于a)，则存在问题。此时，交换矩阵边缘未正确清除Fed条目，因此，与IOS相比，Fed上有多个访问隧道条目。执行此处所示的命令后，比较目的IP。如果多个接入隧道共享相同的目标IP，则编程会出现此问题。

- show platform software fed switch active if-id <Each AP IF-ID>

 注意：每个IF-ID都可以从上一个命令获取。

```
Floor_Edge-6#show platform software fed switch active ifm if-id 0x00000037
Interface IF_ID      : 0x0000000000000037
Interface Name      : Ac4
Interface Block Pointer : 0xffc0b04c58
Interface State     : READY
Interface Status    : ADD
Interface Ref-Cnt   : 2
Interface Type      : ACCESS_TUNNEL
  Tunnel Type      : L2Lisp
  Encap Type       : VxLan
  IF_ID            : 0x37

  Port Information
  Handle ..... [0x2e000094]
  Type ..... [Access-tunnel]
  Identifier ..... [0x37]
  Unit ..... [55]
  Access tunnel Port Logical Subblock
    Access Tunnel id : 0x37
    Switch Num       : 1
    Asic Num         : 0
```

```

PORT LE handle      : 0xffc0b03c58
L3IF LE handle     : 0xffc0e24608
DI handle          : 0xffc02cdf48
RCP service id     : 0x0
HTM handle decap   : 0xffc0e26428
RI handle decap    : 0xffc0afb1f8
SI handle decap    : 0xffc0e26aa8
RCP opq info       : 0x1
L2 Brdcast RI handle : 0xffc0e26808
GPN                : 3201
Encap type         : VXLAN
L3 protocol        : 17
Src IP             : 192.168.4.68
Dest IP            : 182.10.50.6
Dest Port          : 4789
Underlay VRF       : 0
XID cpp handle     : 0xffc03038f8
Port L2 Subblock
  Enabled ..... [No]
  Allow dot1q ..... [No]
  Allow native ..... [No]
  Default VLAN ..... [0]
  Allow priority tag ... [No]
  Allow unknown unicast [No]
  Allow unknown multicast[No]
  Allow unknown broadcast[No]
  Allow unknown multicast[Enabled]
  Allow unknown unicast [Enabled]
  IPv4 ARP snoop ..... [No]
  IPv6 ARP snoop ..... [No]
  Jumbo MTU ..... [0]
  Learning Mode ..... [0]
Port QoS Subblock
  Trust Type ..... [0x7]
  Default Value ..... [0]
  Ingress Table Map ..... [0x0]
  Egress Table Map ..... [0x0]
  Queue Map ..... [0x0]
Port Netflow Subblock
Port CTS Subblock
  Disable SGACL ..... [0x0]
  Trust ..... [0x0]
  Propagate ..... [0x1]
%Port SGT ..... [-180754391]

```

Ref Count : 2 (feature Ref Counts + 1)

IFM Feature Ref Counts

FID : 91, Ref Count : 1

No Sub Blocks Present

- show platform software access-tunnel switch active R0

Floor_Edge-6#show platform software access-tunnel switch active R0

Name	SrcIp	DstIp	DstPort	VrfId	Iif_id
Ac4	192.168.4.68	182.10.50.6	0x12b5	0x0000	0x000037
Ac14	192.168.4.68	182.10.50.2	0x12b5	0x0000	0x000042
Ac15	192.168.4.68	182.10.50.7	0x12b5	0x0000	0x000043
Ac19	192.168.4.68	182.10.50.8	0x12b5	0x0000	0x000047

Ac24 192.168.4.68 182.10.50.5 0x12b5 0x0000 0x00004c

- show platform software access-tunnel switch active R0 statistics

```
Floor_Edge-6#show platform software access-tunnel switch active R0 statistics
Access Tunnel Counters (Success/Failure)
-----
Create                6/0
Create Obj Download   6/0
Delete                3/0
Delete Obj Download   3/0
NACK                  0/0
```

- show platform software access-tunnel switch active F0

```
Floor_Edge-6#show platform software access-tunnel switch active F0
Name      SrcIp      DstIp      DstPort  VrfId     Iif_id     Obj_id     Status
-----
Ac4       192.168.4.68 182.10.50.6 0x12b5  0x000    0x000037  0x00d270  Done
Ac14      192.168.4.68 182.10.50.2 0x12b5  0x000    0x000042  0x03cbca  Done
Ac15      192.168.4.68 182.10.50.7 0x12b5  0x000    0x000043  0x03cb9b  Done
Ac19      192.168.4.68 182.10.50.8 0x12b5  0x000    0x000047  0x03cb6b  Done
Ac24      192.168.4.68 182.10.50.5 0x12b5  0x000    0x00004c  0x03caf4  Done
```

- show platform software access-tunnel switch active F0 statistics

```
Floor_Edge-6#show platform software access-tunnel switch active F0 statistics
Access Tunnel Counters (Success/Failure)
-----
Create                0/0
Delete                3/0
HW Create             6/0
HW Delete             3/0
Create Ack            6/0
Delete Ack            3/0
NACK Notify           0/0
```

- show platform software object-manager switch active f0 statistics

```
Floor_Edge-6#show platform software object-manager switch active f0 statistics
Forwarding Manager Asynchronous Object Manager Statistics

Object update: Pending-issue: 0, Pending-acknowledgement: 0
```

```
Batch begin: Pending-issue: 0, Pending-acknowledgement: 0
Batch end: Pending-issue: 0, Pending-acknowledgement: 0
Command: Pending-acknowledgement: 0
Total-objects: 987
Stale-objects: 0
Resolve-objects: 3
Error-objects: 1
Paused-types: 0
```

- 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

5.需要收集的跟踪和调试。

步骤1.在启用跟踪/调试之前收集存档日志

```
request platform software trace archive target flash:<文件名>
```

```
Floor_Edge-6#request platform software trace archive target flash:Floor_Edge-6_12_14_18
Waiting for trace files to get rotated.
Creating archive file [flash:Floor_Edge-6_12_14_18.tar.gz]
Done with creation of the archive file: [flash:Floor_Edge-6_12_14_18.tar.gz]
```

Step 2. 增加日志记录缓冲区并禁用控制台。

```
Floor_Edge-6(config)#logging buffered 214748364
Floor_Edge-6(config)#no logging console
```

步骤3.设置跟踪。

- set platform software trace forwarding switch active R0 access-tunnel verbose
- set platform software trace forwarding switch active F0 access-tunnel verbose
- set platform software trace fed switch active ifm_main debug
- set platform software trace fed switch active access_tunnel verbose
- set platform software trace forwarding-manager switch active F0 aom verbose

步骤4.启用调试。

- debug l2lisp all
- debug lisp control-plane all
- 调试平台软件l2lisp事件

第 5 步： 关闭/不关闭AP所连接的接口端口。

步骤6.使用不同的文件名收集与步骤1相同的存档日志。

第 7 步： 将日志文件重定向到闪存。

```
Floor_Edge-6#show logging | redirect flash:<Filename>
```

```
Floor_Edge-6#show logging | redirect flash:console_logs_Floor_Edge-6_12_14_18
```

客户端调试

在SDA FEW上调试无线客户端的问题可能会很棘手。

请按照此工作流程逐一消除一台设备。

1. WLC
- 2.交换矩阵边缘
- 3.接入点 (如果在交换矩阵边缘上调试指向AP)
- 4.中级/边界节点。(如果数据路径有问题)
- 5.控制平面节点。(如果出现控制路径问题)

WLC调试

对于客户端连接问题，请通过收集WLC上的信息 (包括show命令和调试) 开始调试。

AireOS WLC show命令：

- show run-config
- show tech
- show wlan summary
- show wlan <id> —>收集所有SSID的此输出，至少收集1个正常运行和非正常运行的输出
- show fabric summary
- show fabric map-server summary
- show client summary
- show client detail <mac_id>

AireOS WLC调试命令：

- debug client <mac1> —> Client assoc、roaming、debugs。
- debug fabric client detail enable —>这提供交换矩阵注册消息信息

交换矩阵边缘调试

在WLC上调试并观察到客户端没有与控制平面路径相关的问题。客户端从Assoc、Authentication移出，并使用正确的SGT标记或AAA参数运行状态，然后移至此步骤以进一步隔离问题。

要检验的另一件事是访问隧道编程是否正确，如上述AP调试部分所述。

用于验证的show命令：

从查找L2 lisp实例ID (从上面显示客户端详细信息<mac_id>)

```
<#root>
```

```
show lisp instance-id
```

```
ethernet database wlc
```

--> This lists all WLC associated clients for that specific L2 lisp instance ID. A number of sources s

```
show lisp instance-id
```

```
ethernet database wlc
```

--> This shows the detail for the specific client

```
show device-tracking database | i Vl
```

--> Find Specific SVI where the client is connected and needs to be present.

```
show device-tracking database | i
```

--> Find the client entry, should be against correct VLAN, Interface, State, and Age.

```
show mac address-table dynamic vlan
```

--> The entry for the mac should match the device-tracking database, if it does please check mac address

```
show ip dhcp snooping binding vlan
```

```
show ip arp vrf
```

```
show mac address-table vlan
```

```
show platform software fed switch active matm macTable vlan
```

```
--> If this is correct, programming for wireless client is happening correctly on local switch  
show platform software matm switch active F0 mac
```

交换矩阵边缘上的debug命令

如果交换矩阵边缘上的客户端条目的编程出现问题，则需要收集馈送跟踪。启用这些调试后，有两种方法可以完成相同操作。

无论使用何种方法，都需要启用debugs和set命令。

- set platform software trace fed switch active all-modules emergency
- set platform software trace fed switch active l2_fib_entry verbose
- set platform software trace fed switch active l2_fib_adj verbose
- set platform software trace fed switch active inject verbose
- set platform software trace fed switch active matm verbose

debug (确保禁用控制台日志记录并增加日志记录缓冲区)

- debug device-tracing
- debug lisp control-plane all
- debug platform fhs all
- 调试平台软件|2lisp事件
- debug matlab all

方法1.启用调试后收集特定客户端的无线活动跟踪日志。

 注意：如果DHCP问题，请勿使用此方法]

等待问题重新生成

- debug platform condition mac <mac-id> control-plane
- debug platform condition start
- debug platform condition stop
- request plat soft trace filter-binary wireless context mac <mac-id>

重现问题后，将控制台日志重定向到闪存。

方法2.启用调试后收集存档跟踪日志。

等待问题重新生成

request platform software trace archive

收集文件解码日志并分析客户端mac的fed、ios、fman日志。

重现问题后，将控制台日志重定向到闪存。

接入点调试

2800/3800/1562 AP型号上的调试：

对于AP端问题，请确保在收集AP端日志并附加到SR之前收集所有WLC show命令和日志。

请按照以下步骤在客户端调试与数据相关的问题。

1.收集AP show命令：（测试完成前后2-3次）

- show clock
- term len 0
- 学期星期一
- show tech
- show logging
- show controllers nss stats show controllers nss status
- show ip tunnel fabric

如果CWA出现问题，请收集以下日志以及主要命令。以下命令需要在测试完成前后收集一次。

- show client access-lists pre-auth all
- show client access-lists post-auth all <client mac>
- show ip access-lists
- show controller d [0/1] client
- show capwap cli detailrcb
- show tech support

2. AP调试 (按MAC地址过滤)

客户端数据路径问题：

- debug dot11 client datapath eapol addr <mac>
- debug dot11 client datapath dhcp addr <mac>
- debug dot11 client datapath arp addr <mac>

客户端AP跟踪：

- config ap client-trace address add <mac>
- config ap client-trace output console-log enable
- config ap client-trace filter all enable
- config ap client-trace filter probe disable
- config ap client-trace start
- 学期星期一
- exec-timeout 0 0

CWA问题：

- debug capwap client avc all
- debug capwap client acl
- debug client <client mac>
- debug dot11 client level info address <mac>
- debug dot11 client level events address <mac>
- debug flexconnect pmk

使用案例调试

客户端CWA调试

注意事项：

- 在SDA中部署CWA时，请始终使用DNAC部署配置。
- 使用DNAC部署后，授权策略、身份验证策略和授权配置文件也将由DNAC部署在ISE上。
- 身份验证的标识需要手动配置，就像对Dot1x所做的那样

找出问题出现的阶段。

步骤1.客户端是否获取IP地址并转到Webauth Pending?

1. 如果是，请继续下一步。

2. 如果否，则问题出在初始加入阶段。
3. 检查WLC和AP上的配置。
4. 检查AP上推送的ACL是否与WLC上的匹配
5. 如果未正确推送ACL，请重新加载AP，并确保它处于未推送配置的临时状态。在1个AP上确认后，确保通过DNAC完成AP调配。

步骤2.客户端能否加载重定向页面？

1. 如果是，请继续下一步。
2. 如果不是，则问题可能出现在多个地方。
3. 检查WLC和AP上的配置。
4. 检查AP上推送的ACL是否与WLC上的匹配
5. 如果未正确推送ACL，请重新加载AP，并确保它处于未推送配置的临时状态。在1个AP上确认后，确保通过DNAC完成AP调配。
6. 检查从WLC到ISE的可达性，并检查AP连接到ISE的交换机。确保中间没有防火墙
7. 检查DNS配置是否正确。

步骤3.客户端能否看到网页，但问题是登录后能否成功？

1. 确保仔细检查步骤1和步骤2配置。
2. 确保授权配置文件、身份验证策略和授权策略正确。
3. 检查ISE实时日志
4. 确保在ISE身份中正确配置用户名/密码。
5. 如果一切正常，请按如下所示收集WLC和AP上的调试。

1. WLC上的调试：

- 分别收集以下AireOS和Polaris的show命令：

AireOS:

- show run-config
- show wlan summary
- show wlan <id_for_Guest>
- show flexconnect acl summary
- show flexconnect acl detailed <ACL_from_previous_command>

北极星：

- show running
- show tech-support wireless
- show tech-support wireless fabric
- show wlan summary
- show wlan id <id_for_guest>
- show ap name <AP_name> config general
- show running-config | sec ACL
- show wireless profile flex summary
- show wireless profile flex detailed <profile_name_from_above>

- 在AireOS和Polaris上启用这些调试。

AireOS:

- debug client <client_mac>
- debug aaa all enable
- 重现问题
- 收集控制台/ssh/telnet日志

Polaris(9300/9400/9500):

```
set platform software trace wncd switch active r0 all-modules debug
```

重现问题

```
show platform software trace message wncd switch active R0 reverse | redirect flash:<filename>
```

```
request platform software trace archive
```

从闪存收集这两个文件

2. AP上的调试 :

收集ACL信息 :

```
show ip access-lists
```

从AP收集以下调试 :

- debug capwap client avc all
- debug capwap client acl
- debug client <client mac>
- debug dot11 client level info address <mac>
- debug dot11 client level events address <mac>
- debug flexconnect pmk

客户端DHCP调试

可以使用这些调试来调试某些问题。

1.在交换机上看不到DHCP发现消息。

2.无线客户端未获得DHCP提供。在debug ip dhcp snooping packet日志中观察到DHCP发现。

3.收集与AP连接的端口、上行链路端口以及与Fusion端的DHCP服务器连接的端口上的数据包捕获。

调试/显示命令，可以是：

- 1.检查Cisco DNA Center (思科DNA中心) 是否已将SSID分配给IP池。
- 2.检查WLC上是否启用了WLAN。
- 3.检查无线电是否已启用，802.11a和802.11b网络是否已启用。

AP上的客户端性能调试

- 1.将问题缩小到有线或无线，或同时影响两者。在同一VNID上测试连接到无线的客户端上的相同流量，并在同一VNID上测试有线上的相同流量。
- 2.如果相同VN上交换矩阵中的有线客户端没有遇到问题，但无线客户端遇到问题，则问题出在AP端。
。
- 3.要在AP端调试任何客户端性能或与流量相关的问题，首先确保客户端连接不是问题。
- 4.确保在WLC上使用debug client时，客户端在漫游期间、会话超时或到同一AP的稳定连接期间观察到性能下降。
- 5.一旦确定问题发生在同一个AP上，请按照以下步骤收集3800/2800/4800 AP上的调试以及连接到AP的交换机上的数据包捕获和无线数据包捕获。

步骤1.确保用于重现问题的流量实际模拟该问题。

步骤2.在执行测试的客户端需要设置无线数据包捕获。

Instructions for collecting over-the-air packet captures:

Here you find the guide how to set up an Over-The-Air packet capture, you can use a windows client machine
<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Mobility.html>

There are few things we need to consider:

- +Use an Open L2/L3 security SSID to avoid encryption on the packets through the air.
- +Set client-serving-AP and sniffer AP on the same channel.
- +Sniffer AP should be close enough to capture what serving-client-AP is receiving or sending.

SPAN session should be taken at the same time than OTA pcap for a proper analysis, how to configure a SPAN session on

Nexus switches:

<https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/113038-span-nexus-configuration.html>

IOS switches:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/network_management/15-0_2_EX_network_management_15-0_2_EX.html

步骤3.从WLC调试客户端，并从连接AP的交换机捕获数据包。可以利用交换机EPC捕获来捕获这些日志。

步骤4.从3800 AP ssh/telnet会话进行调试

Logs to be collected from 3800 AP:

A) Run following commands once before starting the test. [Once all commands are tested, copy all commands]

Step A

Devshell commands on AP - Use SSH.

1) To Get wired0 input packet count

```
date
cd /click/fromdev_wired0/
cat icounts ocounts calls
```

2) Fabric gateway and clients

```
cat /click/client_ip_table/cli_fabric_clients
cd /click/fabric_tunnel/
cat show_fabric_gw
```


3) Tunnel Decap stats

```
cd /click/tunnel_decap/
cat icounts ocounts tunnel_decap_stats tunnel_decap_no_match decap_vxlan_stats
cat tunnel_decap_list
```

4) Tunnel Encap stats

```
cd /click/tunnel_encap/
cat icounts ocounts tunnel_encap_stats encap_vxlan_stats tunnel_encap_discard
cat get_mtu eogre_encap_list
```

5) Wireless client stats

 注意：需要在正确的无线电vap组合上发出这些最后一组命令。例如，如果客户端在无线电1上，则vap 1:cat /click/client_ip_table/list =从输出中，检查客户端连接的端口/接口 aprXvY，使用相同的命令获取以下输出。cd /click/fromdev_ apr1v3/ cat igues ocounts calls cd /click/todev_ apr1v3/ cat igues ocounts calls

步骤B - E B)在AP之间启动OTA。客户端.和启动有线PCAP (客户端连接的生成接入点端口)。 (分析时需要有线和无线pcap。) C)使用开放式身份验证WLAN (没有安全性可分析OTA pcap)。启动iperf测试，并持续运行10-15分钟。D)使用date命令每隔两分钟重复步骤A。进行5次或更多次迭代。E)测试完成后 — 从AP收集show tech。

AP自注册

传统方法/步骤：

AP Vlan范围具有指向WLC的选项43或选项60。

1.选择Authentication作为No Authentication。

2.使用AP IP池配置Infra_VN，使用无线客户端IP池配置Default_VN。

3.配置AP与Infra_VN连接的边缘接口端口。

4.一旦AP获得IP并加入WLC，即会在设备资产中发现它。

5.选择AP并将其分配给特定站点并调配AP。

6.调配后，AP会分配到在将WLC添加到交换矩阵期间创建的AP组。

即插即用/零接触AP调配

AP Vlan范围具有指向Cisco DNA Center的选项43。按照DNAC指南配置AP PNP

交换矩阵边缘侧：

启用这些调试。

- debug ip dhcp snooping packet
- debug ip dhcp snooping event

相关信息

- [每个版本的无线配置指南](#)
- [SD无线部署指南](#)
- [无线最佳实践指南](#)
- [无线技术参考文档](#)
- [SDA的兼容性矩阵](#)
- [每个版本的Cisco DNA Center用户指南](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。