Solución de problemas de acceso definido por software inalámbrico en Cisco DNA Center

Contenido

Introducción

Este documento describe las preguntas frecuentes sobre tecnología inalámbrica y cómo resolver problemas de acceso definido por software en Cisco DNA Center.

Hoja de referencia de comandos para fabric

Esta es la hoja de referencia de comandos para el fabric en el nodo de control, el nodo perimetral, el controlador de LAN inalámbrica (WLC) y el punto de acceso (AP).

Nodo de control:

- 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 para un ID de instancia específico
- show lisp site
- show tech-support
- show tech-support lisp

Nodo perimetral:

- 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 commands
- 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 (If Fabric in a box or Embedded wireless running on 9300/9400/9500)
- show tech-support (si el fabric está en una caja o la tecnología inalámbrica incorporada se ejecuta en 9300/9400/9500)

Punto de Acceso:

- show ip tunnel fabric
- show tech-support

Transferencia de configuración WLC de AireOS desde Cisco DNA Center

Aquí se muestra el empuje de configuración WLC de AireOS de Cisco DNA Center después del aprovisionamiento (Nota: Utilizando la referencia como 3504 (WLC).

show radius summary after WLC Provisioning:

```
(sdawlc3504) >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
```

La inserción de configuración WLAN se ve en show wlan summary.

```
(sdawlc3504) >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
```

Inserción de configuración WLC desde Cisco DNA Center

Aquí muestra el empuje de la configuración del WLC de Cisco DNA Center después de que el WLC se agrega a la tela.

¿Cómo comprobar si Map-Server es alcanzable?

show fabric map-server summary after WLC is added to Fabric.

```
(sdawlc3504) >show fabric map-server summary

MS-IP     Connection status

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

192.168.4.45    UP

192.168.4.66    UP
```

Debug Fabric Map-Server Connectivity

La conectividad del plano de control (CP) puede interrumpirse o permanecer inactiva por diversos motivos.

- Si el PC se apagó. (que no es en este caso)
- Los nodos intermedios que se desactivan que están conectando el WLC al CP, por ejemplo, el router de fusión.
- Si la conectividad CP al WLC se apagó debido al link inactivo. Esto puede ser WLC a un vecino inmediato o CP a un vecino inmediato hacia WLC.

show fabric map-server detailed

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

Depuraciones que pueden proporcionar más información

debug fabric lisp map-server tcp enable

debug fabric lisp map-server all enable

¿Cómo se comprueba que el fabric está habilitado y cuál es el resultado esperado?

show fabric summary después de agregar el WLC al entramado.

```
(sdawlc3504) >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 reguested ...................... 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 Nam
-------  -------------------------------  ----  ----------  ------  ---------------  -------  --------
 19      dnac_wpa2_206                    WLAN  8189        0       0.0.0.0          0         182_11_
 20      dnac_open_206                    WLAN  8189        0       0.0.0.0          0         182_11_
```

Transferencia de configuración WLAN desde Cisco DNA Center

La inserción de configuración WLAN de Cisco DNA Center se observa en show fabric wlan summary después de agregar el WLC al Fabric y de asignar el pool IP del cliente al Fabric

Wireless LAN (WLAN) en Provisioning > Fabric > Host Onboarding.

show fabric wlan summary after Fabric provisioning.

```
(sdawlc3504) >show fabric wlan summary

WLAN ID  SSID                             Type  L2 Vnid     SGT     RLOC IP          Clients  VNID Nam
-------  -------------------------------  ----  ----------  ------  ---------------  -------  --------
 19      dnac_wpa2_206                    WLAN  8189        0       0.0.0.0          0         182_11_
 20      dnac_open_206                    WLAN  8189        0       0.0.0.0          0         182_11_
```

Depurar problemas inalámbricos

Depuración de unión a PA/Depuración de formación de túnel de acceso

1. Verifique si el AP tiene la dirección IP.

show ip dhcp snooping binding → On Fabric Edge

Si no muestra una IP para la interfaz AP conectada, habilite estos debugs en Switch y verifique si AP está obteniendo IP o no.

debug ip dhcp snooping packet

debug ip dhcp snooping event

Archivo de registro de ejemplo adjunto a continuación →

Ejemplo:

```
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. Verifique si el AP se une al WLC.

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

Si el AP nunca se ha unido al WLC, habilite estos debugs en el WLC.

- debug capwap events enable
- debug capwap errors enable

3. Si el AP forma CAPWAP pero no se forman túneles de acceso entre el AP y el Switch, realice estas comprobaciones

Paso 1. ¿Los AP en WLC tienen IP RLOC o no, si no por favor verifique el punto 1 aquí.

1. Para hacer que el protocolo del plano de control del entramado sea más resistente, es importante que una ruta específica al WLC esté presente en la tabla de ruteo global de cada nodo de entramado. La ruta a la dirección IP del WLC debe ser redistribuida en el protocolo IGP subyacente en el borde o configurada estáticamente en cada nodo. En otras palabras, el WLC no debe ser alcanzable a través de la ruta predeterminada.

Paso 2. Si los AP en el WLC muestran los RLOC correctos y debajo de show fabric summary muestra el RLOC solicitado con el RLOC recibido todo bien, verifique estos pasos

2. Verifique el nodo del plano de control, show lisp instance-id <L2 ap instance id> ethernet server→ Debe contener Base Radio MAC para AP.

Verifique en el nodo de borde del entramado, show lisp instance-id <L2 ap instance id> ethernet database wlc → Debe contener Base Radio MAC para AP y no la Ethernet MAC de AP.

Si los 2 comandos anteriores no muestran Radio Base MAC de AP y los túneles de acceso no se están formando. Habilite debug lisp control-plane all en el plano de control y busque Base Radio MAC en el registro.

Nota: debug lisp control-plane all on Control plane is very chatty, desactive el registro de la consola antes de activar las depuraciones.

Si ve la falla de autenticación como se muestra aquí, verifique la clave de autenticación entre el WLC y el nodo CP.

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

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

Cómo verificar la clave de autenticación en la configuración del entramado entre el WLC y el CP.

En el WLC, verifique en la GUI en Controlador > Configuración de Fabric > Plano de control > (Clave precompartida)

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)

Nota: Por lo general, Cisco DNA Center introduce esta clave, así que no la cambie a menos que sea necesario y sepa qué está configurado en CP/WLC]

4. Verificaciones generales y comandos show para túneles de acceso.

- 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#
```

Si los túneles de acceso bajo el comando b) son más altos que a), eso es un problema. En este caso, las entradas de la fuente no se borraron correctamente en Fabric Edge y, por lo tanto, hay varias entradas de túnel de acceso en la fuente en comparación con IOS. Compare Dest IP después de ejecutar el comando que se muestra aquí. Si varios túneles de acceso comparten la misma IP de destino, ese es el problema con la programación.

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

Nota: Cada IF-ID se puede obtener del comando anterior.

```
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. Seguimientos y depuraciones que deben recopilarse.

Paso 1. Recopilar Archive logs antes de activar seguimientos/depuraciones

request platform software trace archive target flash:<Filename>

```
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]
```

Paso 2. Aumente el búfer de registro y desactive la consola.

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

Paso 3. Establecer seguimientos.

- 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

Paso 4. Habilitar depuraciones.

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

Paso 5. shut/no shut interface port where AP is connected.

Paso 6. Recopile los archive logs del mismo modo que el Paso 1. con un nombre de archivo diferente.

Paso 7. Redireccione el archivo de registro a la memoria flash.

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

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

Depuración del cliente

Debug Wireless Client's issues on SDA FEW can be tricky.

Siga este flujo de trabajo para eliminar un dispositivo cada vez.

1. WLC

2. Borde del fabric

3. Punto de acceso (si la depuración en Fabric Edge apunta a AP)

4. Nodo intermedio/de borde. (Si hay un problema con la ruta de datos)

5. Nodo del plano de control. (Si se produce un problema con la ruta de control)

Depuración de WLC

Para los problemas de conectividad del cliente, comience la depuración recolectando la información en el WLC que incluye los comandos show y los debugs.

Comandos show de AireOS WLC:

- show run-config
- show tech
- show wlan summary
- show wlan <id> —> Recopile esta salida para todos los SSID, al menos 1 para los que funcionan y los que no
- show fabric summary
- show fabric map-server summary
- show client summary
- show client detail <mac_id>

Comandos de depuración WLC de AireOS:

- debug client <mac1> —> Client assoc, roaming, debugs.
- debug fabric client detail enable —> Esto proporciona información sobre los mensajes de registro del fabric

Depuración de fabric perimetral

Una vez depurado en el WLC y observado no hay problemas relacionados con la trayectoria del plano de control para el cliente. El cliente se mueve desde Assoc, Authentication, y ejecuta el estado con etiquetado SGT o parámetros AAA correctos, y se desplaza a este paso para aislar aún más el problema.

Otra cosa que se debe verificar es que la programación del túnel de acceso es correcta, como se describe en la sección de depuración de AP anterior.

Comandos show para verificar:

Buscar ID de instancia de L2 lisp de (mostrar detalle de cliente <mac_id> de arriba)

<#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 sh
```

```
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 addre

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 swit

show platform software matm switch active F0 mac

Comandos de depuración en Fabric Edge

Es necesario recopilar seguimientos de la fuente si hay algún problema en la programación de la entrada del cliente en Fabric Edge. Hay 2 maneras de hacer lo mismo después de habilitar estas depuraciones.

Los comandos debug y set deben estar habilitados independientemente del método.

- 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 (Asegúrese de deshabilitar el registro de la consola y aumentar el búfer de registro)

- debug device-tracking
- debug lisp control-plane all
- debug platform fhs all
- debug platform software l2lisp events
- debug matm all

Método 1. Recopilar registros de seguimiento de radio activa para un cliente específico después de habilitar las depuraciones.

 Nota: si se produce un problema con DHCP, no utilice este método]

Espere a que el problema se reproduzca

- 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>

Redirija los registros de la consola a la memoria flash después de que se reproduzca el problema.

Método 2. Recopilar registros de seguimiento de archivos después de habilitar las depuraciones.

Espere a que el problema se reproduzca

request platform software trace archive

Recopile el archivo, decodifique los registros y analice los registros fed, ios y fman para el mac del cliente.

Redirija los registros de la consola a la memoria flash después de que se reproduzca el problema.

Depuración del punto de acceso

Depuraciones en los modelos 2800/3800/1562 AP:

Para los problemas del lado AP, asegúrese de recolectar todos los comandos show del WLC y los registros antes de recolectar los registros del lado AP y adjuntar a SR.

Siga estos pasos para depurar los problemas relacionados con los datos en el lado del cliente.

1. Recopile los comandos show de AP: (2-3 veces, antes y después de completar los ensayos)

- show clock
- term len 0
- term mon
- show tech
- show logging
- show controllers nss stats show controllers nss status
- show ip tunnel fabric

Si el problema de CWA, por favor, recopile los siguientes registros, además de los comandos principales. Los siguientes comandos deben recopilarse una vez antes y después de completar la prueba.

- show client access-lists pre-auth all <client mac>
- 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. Depuraciones de AP (filtro por dirección MAC)

Problemas de trayecto de datos del cliente:

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

Seguimientos de AP de cliente:

- 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
- term mon
- exec-timeout 0 0

Problemas de CWA:

- 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

Depuración de casos prácticos

Depuración de CWA del cliente

Aspectos a destacar:

- Al implementar CWA en SDA, utilice siempre DNAC para implementar la configuración.
- Una vez implementadas mediante DNAC, DNAC también implementaría en ISE la política de autorización, la política de autenticación y el perfil de autorización.
- Las identidades para la autenticación deben configurarse manualmente tal como se hace para Dot1x

Averigüe en qué etapa se observa el problema.

Paso 1. ¿Está el cliente recibiendo una dirección IP y pasando a Webauth pendiente?

1. Si la respuesta es sí, vaya al paso siguiente.
2. Si la respuesta es no, el problema se encuentra en la fase de incorporación inicial.
3. Verifique la configuración en WLC y AP.
4. Verifique que la ACL se está empujando en el AP y coincida con lo que está en el WLC
5. Si la ACL no se inserta correctamente, recargue el AP y asegúrese de que sea un estado interino en el que la configuración no se presione. Una vez confirmado en 1 AP, asegúrese de que el aprovisionamiento de los AP se realiza a través de DNAC.

Paso 2. ¿El cliente puede cargar la página de redireccionamiento?

1. Si la respuesta es sí, vaya al paso siguiente.
2. Si la respuesta es no, el problema puede estar en varios lugares.
3. Verifique la configuración en WLC y AP.
4. Verifique que la ACL se está empujando en el AP y coincida con lo que está en el WLC
5. Si la ACL no se inserta correctamente, recargue el AP y asegúrese de que sea un estado interino en el que la configuración no se presione. Una vez confirmado en 1 AP, asegúrese

de que el aprovisionamiento de los AP se realiza a través de DNAC.
6. Compruebe la disponibilidad desde el WLC al ISE y el switch donde el AP está conectado al ISE. Asegúrese de que no hay firewall entre
7. Compruebe que DNS está configurado correctamente.

Paso 3. ¿El cliente puede ver la página web pero el problema es con el inicio de sesión y el avance hacia el éxito?

1. Asegúrese de volver a comprobar las configuraciones de los pasos 1 y 2.
2. Asegúrese de que el perfil de autorización, la directiva de autenticación y la directiva de autorización son correctos.
3. Comprobar los registros de ISE Live
4. Asegúrese de que el nombre de usuario/contraseña esté configurado correctamente en las identidades de ISE.
5. Recopile los debugs en el WLC y el AP como abajo si todo se ve bien.

1. Depuraciones en WLC:

- Recopile los siguientes comandos show para AireOS y Polaris respectivamente:

AireOS:

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

Polaris:

- 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>

- Habilite estas depuraciones en AireOS y Polaris.

AireOS:

- debug client <client_mac>
- debug aaa all enable

- Reproduzca el problema
- Recopilar registros de consola/ssh/telnet

Polaris (9300/9400/9500):

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

Reproduzca el problema

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

request platform software trace archive

Recopile ambos archivos de flash

2. Depuraciones en AP:

Recopilar información de ACL:

show ip access-lists

Recopile las siguientes depuraciones de AP:

- 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

Depuración DHCP del cliente

Algunos problemas se pueden depurar mediante estos depuradores.

1. No ver los mensajes de detección de DHCP en el switch.

2. El cliente inalámbrico no recibe la oferta de DHCP. La detección de DHCP se observa en los registros de debug ip dhcp snooping packet.

3. Recopile la captura de paquetes en el puerto conectado al AP, el puerto de link ascendente y el puerto conectado al servidor DHCP en el lado de fusión.

Los comandos Debugs/Show pueden ser:

1. Compruebe en Cisco DNA Center si SSID está asignado a IP Pool.

2. Verifique si la WLAN está habilitada en el WLC.

3. Compruebe si las radios están activadas y si las redes 802.11a y 802.11b están activadas.

Depuración del rendimiento del cliente en AP

1. Reduzca el problema a redes por cable o inalámbricas, o a ambas afectadas. Pruebe el mismo tráfico en un cliente conectado a la red inalámbrica en el mismo VNID y pruebe el mismo tráfico en la red por cable en el mismo VNID.

2. Si los clientes cableados en Fabric en la misma VPN no experimentan problemas pero los clientes inalámbricos sí, el problema está en el lado del AP.

3. Para depurar en el lado del AP para cualquier problema relacionado con el rendimiento o el tráfico del cliente, asegúrese de que la conectividad del cliente no sea el problema, para empezar.

4. Asegúrese de utilizar el cliente de depuración en el WLC que el cliente está observando la degradación durante el roaming, el tiempo de espera de la sesión o la conexión estable al mismo AP.

5. Una vez que se haya reducido que el problema está en el mismo AP, siga estos pasos para recopilar depuraciones en los AP 3800/2800/4800 junto con la captura de paquetes en el switch conectado a AP y las capturas de paquetes por aire.

Paso 1. Asegúrese de que el tráfico utilizado para reproducir el problema esté imitando el problema.

Paso 2. La captura de paquetes por aire debe configurarse en el lado del cliente en el que se ha realizado la prueba.

```
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 mach
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wirele

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 S

Nexus switches:
https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/113038-span-nexus-config
IOS switches:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/network_management/
```

Paso 3. Depure el cliente desde el WLC y la captura de paquetes desde el switch donde AP está

conectado. Las capturas EPC de switches se pueden aprovechar para capturar estos registros.

Paso 4. Depuraciones de la sesión 3800 AP ssh/telnet

```
Logs to be collected from 3800 AP:

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

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
```

Nota: necesita ejecutar este último conjunto de comandos en el combo radio vap correcto. Por ejemplo, si el cliente está en radio 1, vap 1: cat /click/client_ip_table/list = En la salida, verifique el puerto conectado al cliente/interfaz aprXvY, utilice el mismo para obtener la siguiente salida. cd /click/fromdev_ apr1v3/ cat icounts accounts calls cd /click/todev_ apr1v3/ cat icounts calls Steps B - E B) Start OTA between AP. Cliente. Y Start Wired PCAP(puerto de punto de acceso de extensión donde está conectado el cliente). (Se necesita pcap por cable e inalámbrico para el análisis.) C) Use Open-Auth WLAN(no hay seguridad para analizar pcap de OTA). Inicie la prueba de iperf y manténgala en funcionamiento durante 10-15 minutos, de forma continua. D) Repita el paso A cada dos minutos con el comando date. Realice 5 o más iteraciones. E) Después de completar la prueba - Recopile show tech del AP.

Incorporación de PA

Método/pasos tradicionales:

Se considera que el alcance de la VLAN AP tiene la opción 43 o la opción 60 que señala al WLC.

1. Seleccione Autenticación como Sin Autenticación.

2. Configure Infra_VN con el pool IP del AP y Default_VN con el pool IP del cliente inalámbrico.

3. Configure los puertos de la interfaz de borde donde los AP están conectados con Infra_VN.

4. Una vez que el AP consigue la IP y se une al WLC, se descubre en el inventario del dispositivo.

5. Seleccione el punto de acceso y asígnelo a un sitio específico y aprovisione el punto de acceso.

6. Una vez aprovisionado, el AP se asigna al grupo AP creado durante la adición del WLC al entramado.

Plug and Play/aprovisionamiento de puntos de acceso sin intervención

Se considera que AP Vlan Scope tiene la opción 43 que apunta a Cisco DNA Center. Siga la guía de DNAC para configurar AP PNP

Lado del borde del fabric:

Habilite estas depuraciones.

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

Información Relacionada

- Guías de configuración inalámbrica para cada versión
- Guía de implementación inalámbrica de SD
- Guía de prácticas recomendadas sobre tecnología inalámbrica
- Documentos de referencia técnica para redes inalámbricas
- Matriz de compatibilidad para SDA
- Guías del usuario de Cisco DNA Center para cada versión

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).