Resolución de problemas y verificación de la configuración inicial inalámbrica de SD-Access

Contenido

Introducción

En este artículo se describen los pasos básicos de resolución de problemas para identificar los problemas básicos de conectividad en las configuraciones inalámbricas de SD-Access. Describirá los elementos y comandos que se deben comprobar para aislar los problemas de la solución relacionados con la tecnología inalámbrica.

Prerequisites

Requirements

Conocimiento de la solución SD-Access

Una topología de acceso SD ya configurada

Componentes Utilizados

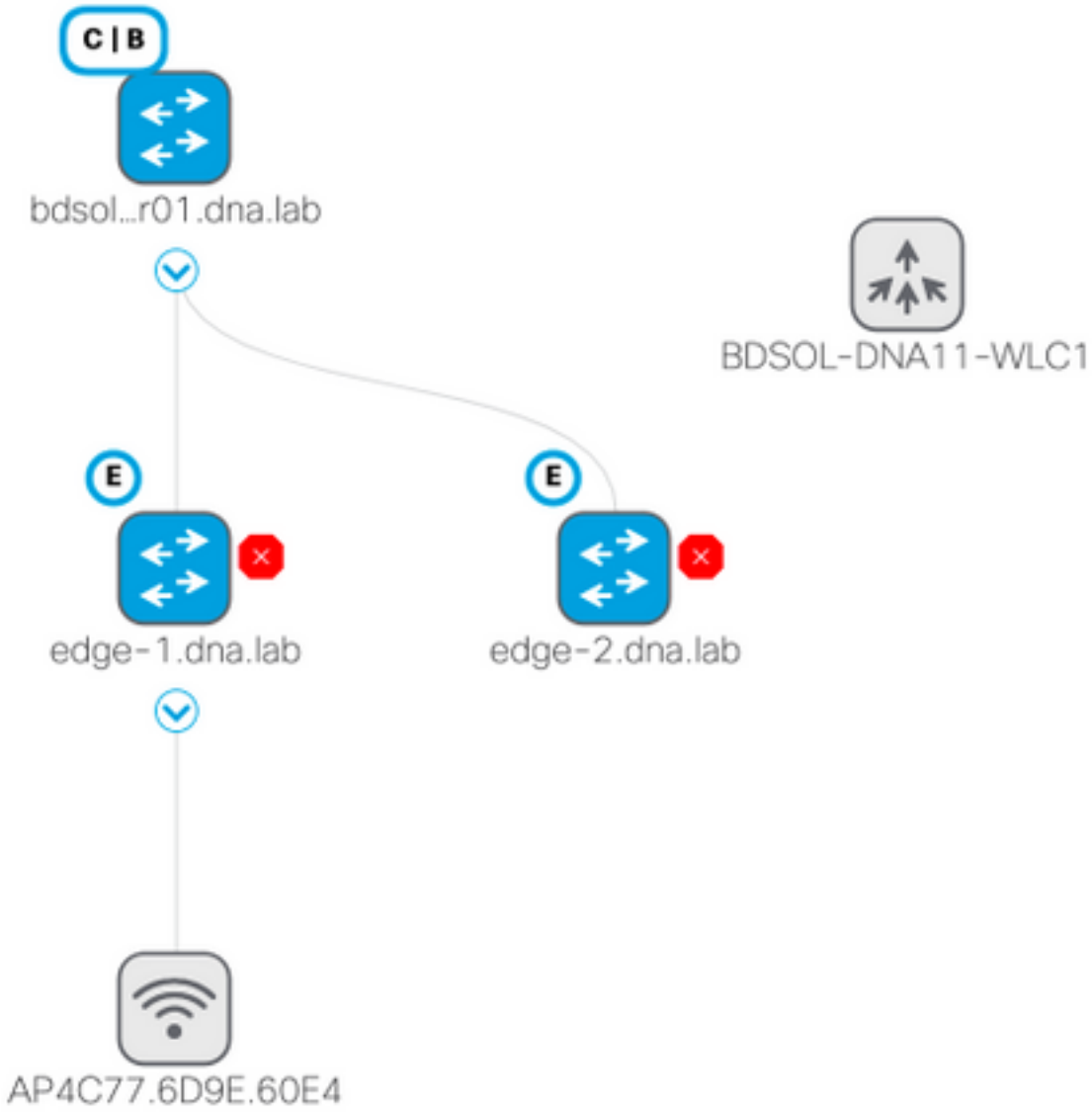
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando. Existen otros tipos de dispositivos compatibles con la tecnología inalámbrica de acceso SD, pero este artículo se centra en los dispositivos descritos en esta sección. Los comandos pueden variar según la plataforma y la versión del software.

8.5.151 Controlador inalámbrico

16.9.3 Switch 9300 como nodo de borde

Topología



Solucionar problemas y aislar

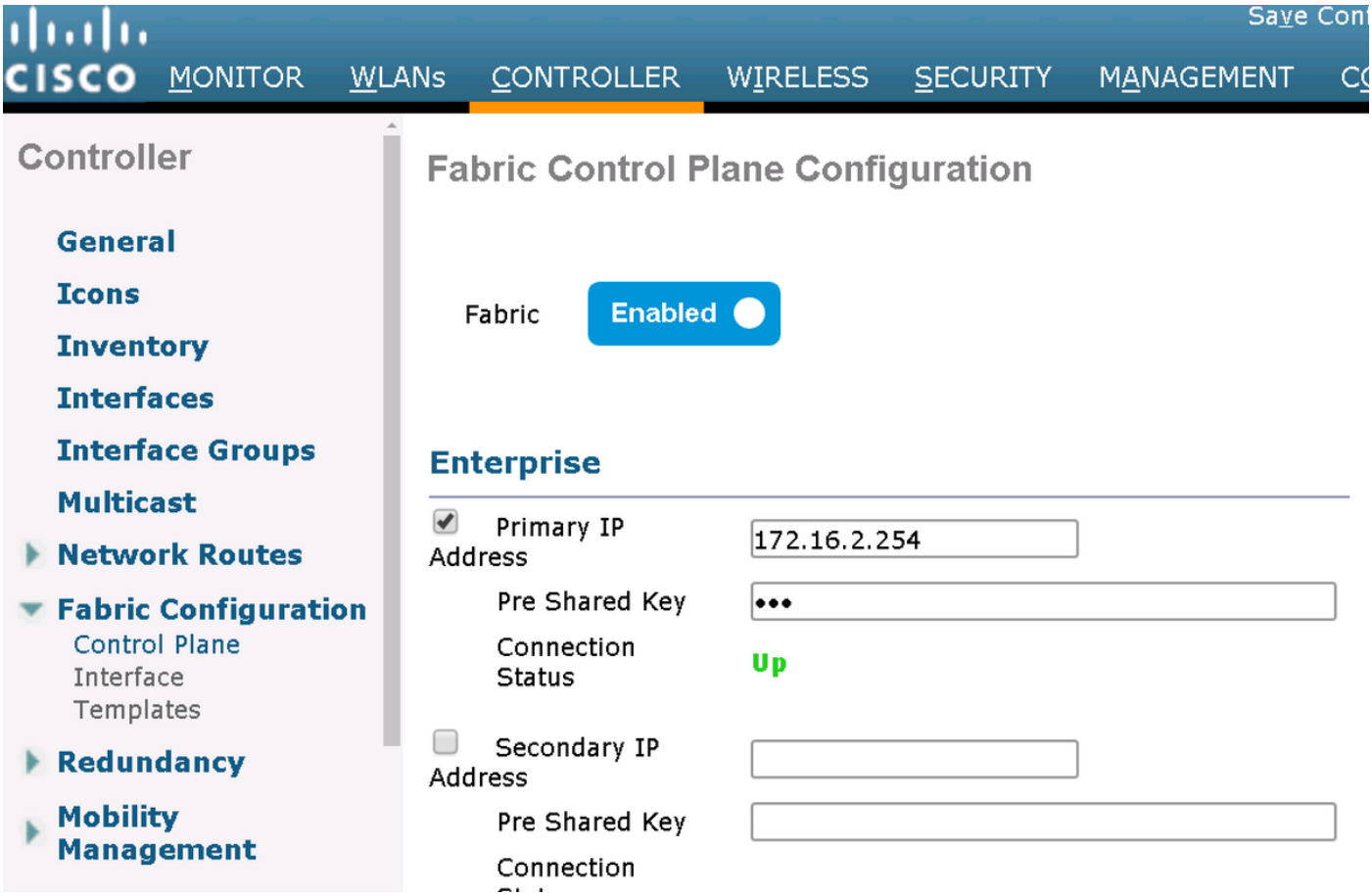
Verificaciones rápidas

Hay una serie de requisitos en los escenarios de acceso SD que a menudo son una fuente de errores, así que verifique primero que se cumplan estos requisitos :

- Asegúrese de que tiene una ruta específica (y que no utiliza la predeterminada) que apunta al WLC en el nodo del plano de control LISP
- Asegúrese de que sus AP estén en la VPN Infra, utilizando la tabla de ruteo global
- Asegúrese de que los AP tengan conectividad con el WLC haciendo ping al WLC desde el AP mismo
- Asegúrese de que el estado del entramado del plano de control en el WLC esté encendido
- Asegúrese de que los AP estén en estado habilitado para el entramado

escenario 1. Verifique el registro del WLC con el plano de control del servidor LISP/MAP

Cuando agrega el WLC al entramado en DNA Center, los comandos se envían al controlador para establecer una conexión con el nodo definido como plano de control en DNA-C. El primer paso es asegurar que este registro sea exitoso. Si la configuración LISP en el plano de control se dañó de alguna manera, este registro podría fallar.



Si este estado se muestra como inactivo, puede ser interesante ejecutar depuraciones o una captura de paquetes entre el WLC y el plano de control. El registro implica tanto TCP como UDP en 4342. Si el plano de control no obtuvo la configuración adecuada, podría responder con un TCP RST al TCP SYN enviado por el WLC.

El mismo estado se puede verificar con **show fabric map-server summary** en la línea de comandos. El proceso se depura con **debug fabric lisp map-server all** en la CLI del WLC. Para provocar un intento de reconexión, puede ir a DNA Center y elegir quitar el WLC del entramado y agregarlo otra vez.

Posibles razones son la falta de líneas de configuración en el plano de control. He aquí un

ejemplo de configuración en funcionamiento (la parte más importante solamente) :

```
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
```

Si falta el IP del WLC (10.241.0.41 aquí) o si falta el comando passive-open, el CP rechazará la conexión del WLC.

Los debugs a ejecutar son:

- **'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'**

Aquí hay un ejemplo del plano de control que no responde al WLC

```
*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 list with path /tmp/msif_local_udp_socket_file failed
*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 and VNID 4097
*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 list with path /tmp/msif_local_udp_socket_file failed
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Request from 10.32.58.36:5248
epoch 1525694896
*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
```

Este es un ejemplo de las depuraciones del WLC de un AP que se une en el estado inhabilitado del entramado porque al plano de control del entramado le faltaba una ruta específica al 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 ffffff00,l2vnid 8191,l3vnid 1001
*emWeb: Oct 16 08:55:26.295: Vnid Mapping added at index 2 with entries 192_168_39_0-
INFRA_VN,8191,4097,c0a82700,ffffff00.Count 3

*emWeb: Oct 16 08:55:26.295:
                              Log to TACACS server(if online): fabric vnid create name
192_168_39_0-INFRA_VN l2-vnid 8191 ip 192.168.39.0 subnet 255.255.255.0 l3-vnid 4097
```

```
*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 for AP Pod3-AP4800 f4:db:e6:61:24:a0,lradIp 192.168.39.100,AP l2_vnid 0, AP l3_vnid
0
*spamReceiveTask: Oct 16 08:55:26.295: Vnid Mapping return from index 2 with entries name
192_168_39_0-INFRA_VN,l2vnid 8191,l3vnid 4097,ip c0a82700,mask ffffff00.Count 3

*spamReceiveTask: Oct 16 08:55:26.295: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP4800 f4:db:e6:61:24:a0,l3vnid 4097,PMS 192.168.30.55,SMS 0.0.0.0,mwarIp 192.168.31.59,lradIp
192.168.39.100
*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 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.949: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP3800 f4:db:e6:64:02:a0 can not be sent ,AP vnid mapping does not exist
```

Es interesante notar que si hay dos planos de control en su red de la tela, el WLC siempre alcanzará a ambos para el registro o las consultas. Se espera que ambos planos de control den respuestas positivas en los registros, por lo que el WLC no podrá registrar los AP en el entramado si uno de los dos planos de control lo rechaza por cualquier razón. Sin embargo, se acepta un plano de control que no responde y se utilizará el plano de control restante.

Los AP llegan al WLC a través de la tabla de ruteo global, pero el LISP se sigue utilizando para resolver el WLC. El tráfico enviado por los AP al WLC es control CAPWAP puro (no vxlan implicado), pero el tráfico de retorno enviado por el WLC al AP se transportará sobre Vxlan en la superposición. No podrá probar la conectividad de la SVI de la gateway AP en el borde hacia el WLC porque como es una gateway Anycast, la misma IP existe también en el nodo de borde. Para probar la conectividad, lo mejor es hacer ping desde el propio AP.

situación hipotética 2. Los puntos de acceso no obtienen una dirección IP

Se espera que los puntos de acceso obtengan una dirección IP del grupo de puntos de acceso, en la VLAN de infrarrojos definida en el centro de ADN. Si esto no sucede, significa típicamente que el switchport donde el AP está conectado no se movió a la vlan derecha. El switch, cuando detecta (a través de CDP) un punto de acceso que se está conectando, aplicará una macro de puerto de switch que establecerá el puerto de switch en la vlan definida por DNA-C para el conjunto de AP. Si el puerto de switch problemático no está realmente configurado con la macro, puede establecer la configuración manualmente (de modo que el AP obtenga una ip, se una al WLC y probablemente actualice su código y posiblemente resuelva cualquier error CDP) o resolver problemas del proceso de conexión CDP. Opcionalmente, puede configurar la onboarding del host para definir estáticamente el puerto en DNA-Center para hospedar un AP de modo que se le suministre con la configuración correcta.

Las macros de Smartport no se activan automáticamente si el switch no se aprovisionó con un AP como mínimo, puede verificar si la macro de AP se aprovisionó con la vlan correcta (en lugar de la vlan predeterminada 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
```

Los comandos que Cisco DNA-C empuja para establecer esto son

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

situación hipotética 3. Los puntos de acceso no tienen un túnel vxlan construido hacia su nodo de Fabric Edge

Una vez que un AP se une al WLC, el WLC (si el AP es apto para el entramado) registrará el AP en el plano de control como un tipo especial de cliente. El plano de control solicitará entonces el nodo de borde del entramado donde el AP está conectado para construir un túnel vxlan hacia el AP.

El AP sólo utilizará la encapsulación vxlan para enviar el tráfico del cliente (y sólo para los clientes en estado RUN), por lo tanto, es normal no ver ninguna información vxlan en el AP hasta que un cliente de entramado se conecte.

En el AP, el comando **show ip tunnel fabric** mostrará la información del túnel vxlan una vez que un cliente se haya conectado.

```
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 Bytes-out
        1    172.16.2.253 00:00:0C:9F:F4:5E           Forward      VXLAN     39731  4209554
16345   2087073
AP4001.7A03.5736#
```

En el nodo de borde del fabric, el comando **show access-tunnel summary** mostrará los túneles vxlan construidos hacia los puntos de acceso. Los túneles se mostrarán tan pronto como el plano de control ordene su creación cuando el AP se una.

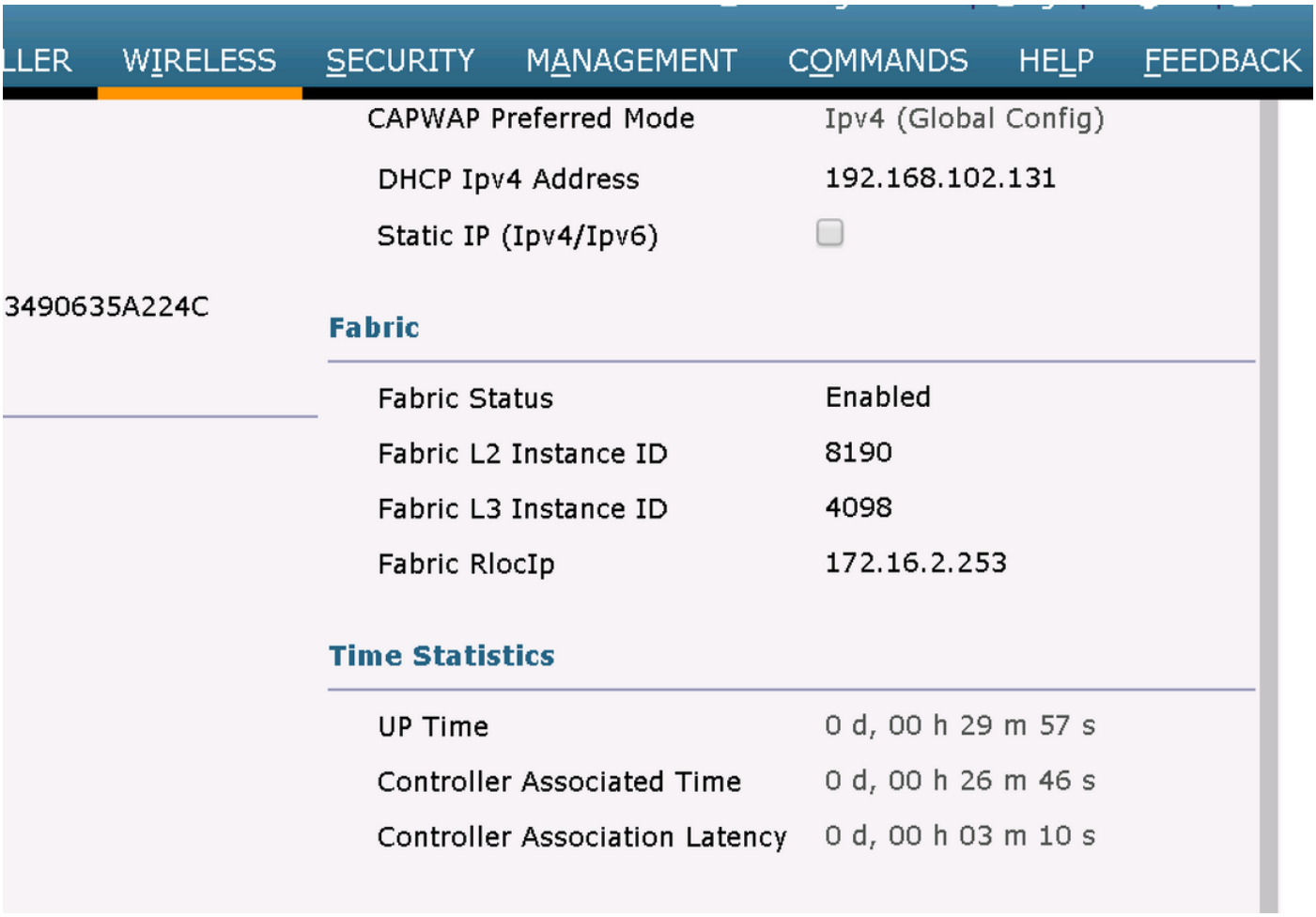
```
edge01#show access-tunnel summ

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
```

Puede verificar en el WLC, en la página del punto de acceso, el ID de instancia de LISP de L2 correspondiente a ese AP y luego verificar las estadísticas de esa instancia en el Fabric Edge donde está conectado.




```
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
```

escenario 4. faltan entradas de túnel de acceso después de un tiempo

Es posible que los túneles de acceso se creen con éxito la primera vez que el WLC se aprovisiona a través de Cisco DNA-C y se agrega al entramado, pero cuando se reaprovisiona la configuración inalámbrica (como la configuración WLAN) se observa que faltan entradas de túnel de acceso para los AP y los clientes inalámbricos resultantes no pueden obtener IP con éxito.

La topología es 9500(CP) —> 9300 (Edge) —> AP —> Wireless Client.

Las entradas se observan correctamente en **show access-tunnel summary** en el nodo de borde:

```
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
```

Pero cuando se verifica **show platform software fed switch active ifm interfaces access-tunnel,** la entrada para el AP falta o no se pudo programar en el hardware en este ejemplo.

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

Para obtener más salidas:

```
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
```

Debe comparar las diferentes salidas y cada túnel mostrado por el **show access-tunnel summary** debe estar presente en cada una de ellas.

situación 5. los clientes inalámbricos no pueden obtener una dirección IP

Si el túnel vxlan está presente y todo se ve bien pero los clientes inalámbricos son sistemáticamente incapaces de obtener una dirección IP, tal vez esté enfrentando un problema de la opción 82. Dado que el gateway Anycast reenvía el DHCP DISCOVER del cliente en el nodo de borde, podría haber problemas para que el servidor DHCP OFFER se envíe al nodo de borde derecho por el borde en el camino de regreso. Esta es la razón por la que el borde del entramado que reenvía el DHCP DISCOVER agrega un campo de opción 82 al DHCP DISCOVER que contiene el RLOC del entramado real (IP de loopback) del nodo del borde codificado junto con otra información. Esto significa que el servidor DHCP debe admitir la opción 82.

Para solucionar problemas del proceso DHCP, realice capturas en los nodos de fabric (especialmente en el nodo de borde del cliente) para verificar que el borde del fabric está agregando el campo de opción 82.

situación hipotética 6. El fabric de invitado/autenticación web no funciona/no redirige a los clientes

El escenario de fabric de invitado es extremadamente similar a la autenticación web central (CWA) en los puntos de acceso Flexconnect y funciona exactamente de la misma manera (incluso si los puntos de acceso de fabric no están en modo Flexconnect).

ISE debe devolver la ACL y la URL de redirección en el primer resultado de la autenticación MAC. Verifique los registros de ISE, así como la página de detalles del cliente en el WLC.

La ACL de redirección debe estar presente como una ACL Flex en el WLC y debe contener sentencias "permit" hacia la dirección IP de ISE en el puerto 8443 (al menos).

El cliente debe estar en el estado "CENTRAL_WEBAUTH_REQ" en la página de detalles del cliente en el WLC. El cliente no podrá hacer ping a su gateway predeterminado y se espera que así sea. Si no se le redirige, puede intentar escribir manualmente una dirección IP en el navegador web del cliente (para descartar DNS, pero el nombre de host de ISE deberá resolverse de todos modos). Debería poder introducir la IP de ISE en el puerto 8443 en el navegador del cliente y ver la página del portal, ya que este flujo no se redirigirá. Si esto no sucede, se enfrenta a un problema de ACL o a un problema de ruteo hacia. Recopile capturas de paquetes en el camino para ver dónde se detienen los paquetes HTTP.

Comprender

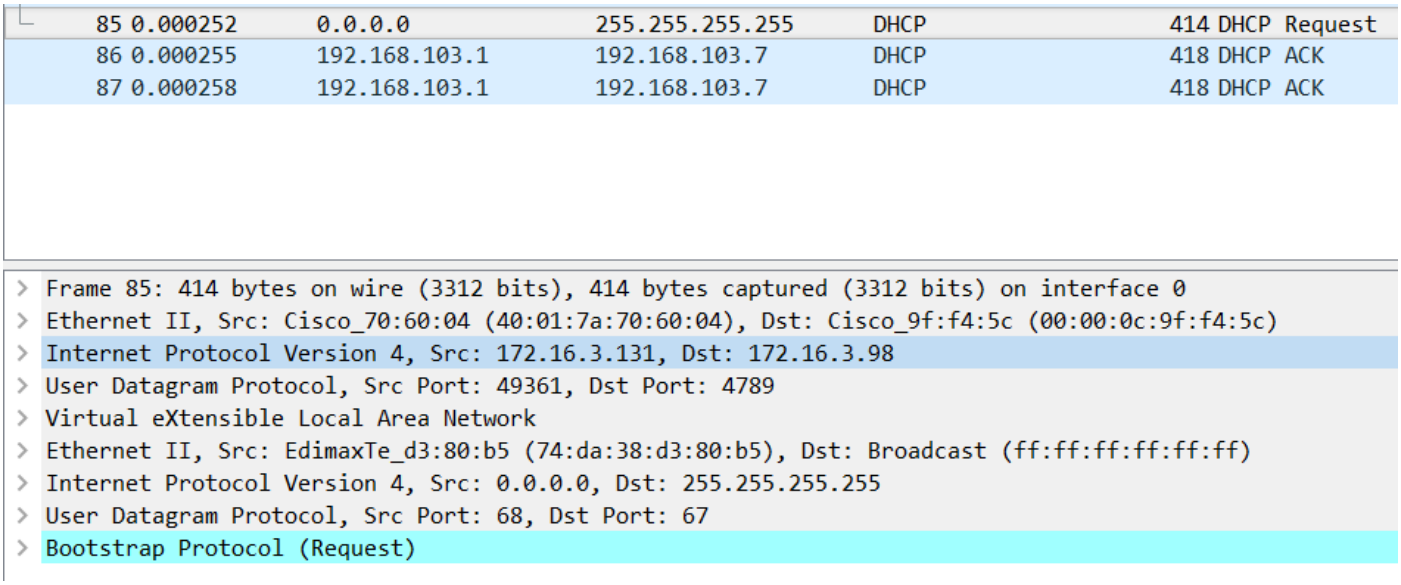
Cómo obtiene un cliente inalámbrico una dirección IP en la arquitectura de fabric

65	0.000191	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0x5fd8da22
66	0.000194	0.0.0.0	255.255.255.255	DHCP	418	DHCP Discover - Transaction ID 0x5fd8da22
80	0.000234	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0x5fd8da22
81	0.000238	0.0.0.0	255.255.255.255	DHCP	418	DHCP Discover - Transaction ID 0x5fd8da22
82	0.000241	192.168.103.1	192.168.103.7	DHCP	418	DHCP Offer - Transaction ID 0x5fd8da22
83	0.000245	192.168.103.1	192.168.103.7	DHCP	418	DHCP Offer - Transaction ID 0x5fd8da22
84	0.000248	0.0.0.0	255.255.255.255	DHCP	440	DHCP Request - Transaction ID 0x5fd8da22
85	0.000252	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request - Transaction ID 0x5fd8da22
86	0.000255	192.168.103.1	192.168.103.7	DHCP	418	DHCP ACK - Transaction ID 0x5fd8da22
87	0.000258	192.168.103.1	192.168.103.7	DHCP	418	DHCP ACK - Transaction ID 0x5fd8da22

La captura de paquetes se realiza entre el PA de fabric y el extremo de fabric. Los paquetes están duplicados porque se enviaron dos paquetes de detección DHCP. El tráfico solo era de entrada y

se capturaba en el fabric perimetral.

Siempre hay dos paquetes DHCP. Uno enviado por CAPWAP directamente al controlador para mantenerlo actualizado. El otro enviado por VXLAN al nodo de control. Cuando el AP recibe por ejemplo una oferta DHCP con VXLAN por el servidor DHCP, envía una copia al controlador con CAPWAP.



Para ver dónde se envió el paquete, debe hacer clic en él en Wireshark. Aquí podemos ver que el origen es nuestro AP 172.16.3.131 y el paquete fue enviado al Fabric Edge 172.16.3.98. El Fabric Edge lo reenvió al nodo de control.

Comprender el flujo de redirección web en una situación de fabric

La ACL de redirección en el WLC define qué tráfico se redirige/intercepta en las sentencias de negación coincidentes (hay una negación implícita al final). Ese tráfico que se redirigirá se enviará al WLC dentro de la encapsulación CAPWAP para que el WLC redirija. Al hacer coincidir una sentencia de permiso, no redirige ese tráfico y lo deja pasar y lo reenvía en el fabric (el tráfico hacia ISE entra en esta categoría).

Registros del AP que se une al WLC en el estado habilitado para el entramado

Tan pronto como Access-Point se registre en el WLC, el controlador registrará su dirección IP y MAC en el nodo de control SDA (servidor de mapa LISP).

El AP se une al WLC en el modo habilitado para el entramado solamente si el WLC recibe el paquete LISP RLOC. Este paquete se envía para asegurarse de que el AP esté conectado a un borde del entramado.

Las depuraciones utilizadas en el WLC para este ejemplo son:

- **'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'**

Para la prueba, el AP se reinicia :

*spamApTask0: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for Aggregated Payload 3 sent to 172.16.3.131:5256
*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 BOTH MS
*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 VNID 4097
*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 IP 172.16.3.131 VNID 4097 for MS 172.16.3.254
*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, VNID 4097 and MS IP 172.16.3.254, db idx 12
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for PHY payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: Build and send map-request for AP IP 172.16.3.131 and VNID 4097 to MS IP 172.16.3.254
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferenceCtrl payload sent to 172:16:3:131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferenceCtrl payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: nonce = 3cd13556-81864b7b lisp_map_request_build allocating nonce
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmNeighbourCtrl payload sent to 172.16.3.131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for CcxRmMeas payload sent to 172.16.3.131
***msfMsgQueueTask: May 07 13:00:18.804: Sending map-request for AP 172.16.3.131 VNID 4097 to MS 172.16.3.254**
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for AP ext-logging AP ext-logging message sent to 172.16.3.131:5256
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update for Delba sent to 172.16.3.131:5256
***msfMsgQueueTask: May 07 13:00:18.804: Map-request for AP IP 172.16.3.131 VNID 4097 to MS 172.16.3.254 is sent**
***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 172.16.3.131
*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 AP IP 172.16.3.131
***msfMsgQueueTask: May 07 13:00:18.807: Sent received RLOC IP 172.16.3.98 for AP 172.16.3.131 and VNID 4097 in map-reply to spam task**
***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 4097,fabricRLoc 172.16.3.98 apip 172.16.3.131 apRadMac 70:70:8b:20:29:00**

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).