Risoluzione dei problemi e verifica della configurazione iniziale wireless di SD-Access

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Topologia](#)
[Risoluzione dei problemi e isolamento](#)
[Verifica rapida](#)
[scenario 1. Verificare la registrazione del WLC con il control plane del server LISP/MAP](#)
[scenario 2. I punti di accesso non ricevono un indirizzo IP](#)
[scenario 3. I punti di accesso non dispongono di un tunnel vxlan costruito verso il rispettivo nodo Fabric Edge](#)
[scenario 4. voci del tunnel di accesso mancanti dopo un breve periodo](#)
[scenario 5. i client wireless non sono in grado di ottenere un indirizzo IP](#)
[scenario 6. Infrastruttura guest/autenticazione Web non funzionante/client non reindirizzati](#)
[Comprendere](#)
[In che modo un client wireless ottiene un indirizzo IP nell'architettura fabric](#)
[Comprendere il flusso di reindirizzamento Web in uno scenario fabric](#)
[Registri dell'access point che si unisce al WLC nello stato abilitato per l'infrastruttura](#)

Introduzione

In questo articolo vengono descritte le procedure di base per la risoluzione dei problemi di connettività nelle impostazioni wireless di SD-Access. Descrive gli elementi e i comandi da controllare per isolare i problemi della soluzione relativi al wireless.

Prerequisiti

Requisiti

Conoscenza della soluzione SD-Access

Una topologia di accesso SD già configurata

Componenti usati

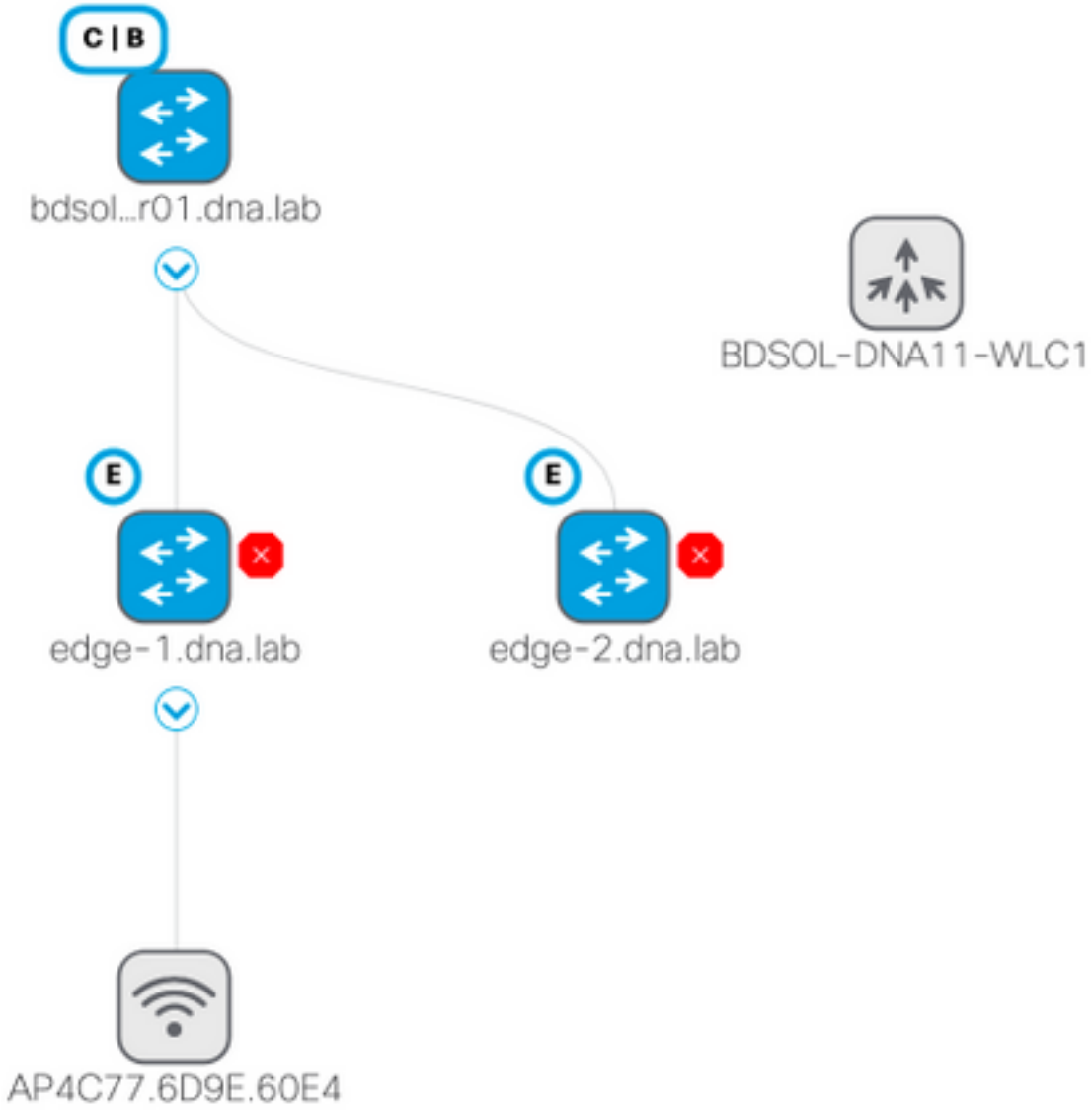
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi. Per l'accesso wireless SD sono supportati altri tipi di

dispositivi, ma in questo articolo vengono illustrati in modo specifico i dispositivi descritti in questa sezione. I comandi possono variare a seconda della piattaforma e della versione del software.

8.5.151 Controller wireless

16.9.3 9300 switch come nodo edge

Topologia



Risoluzione dei problemi e isolamento

Verifica rapida

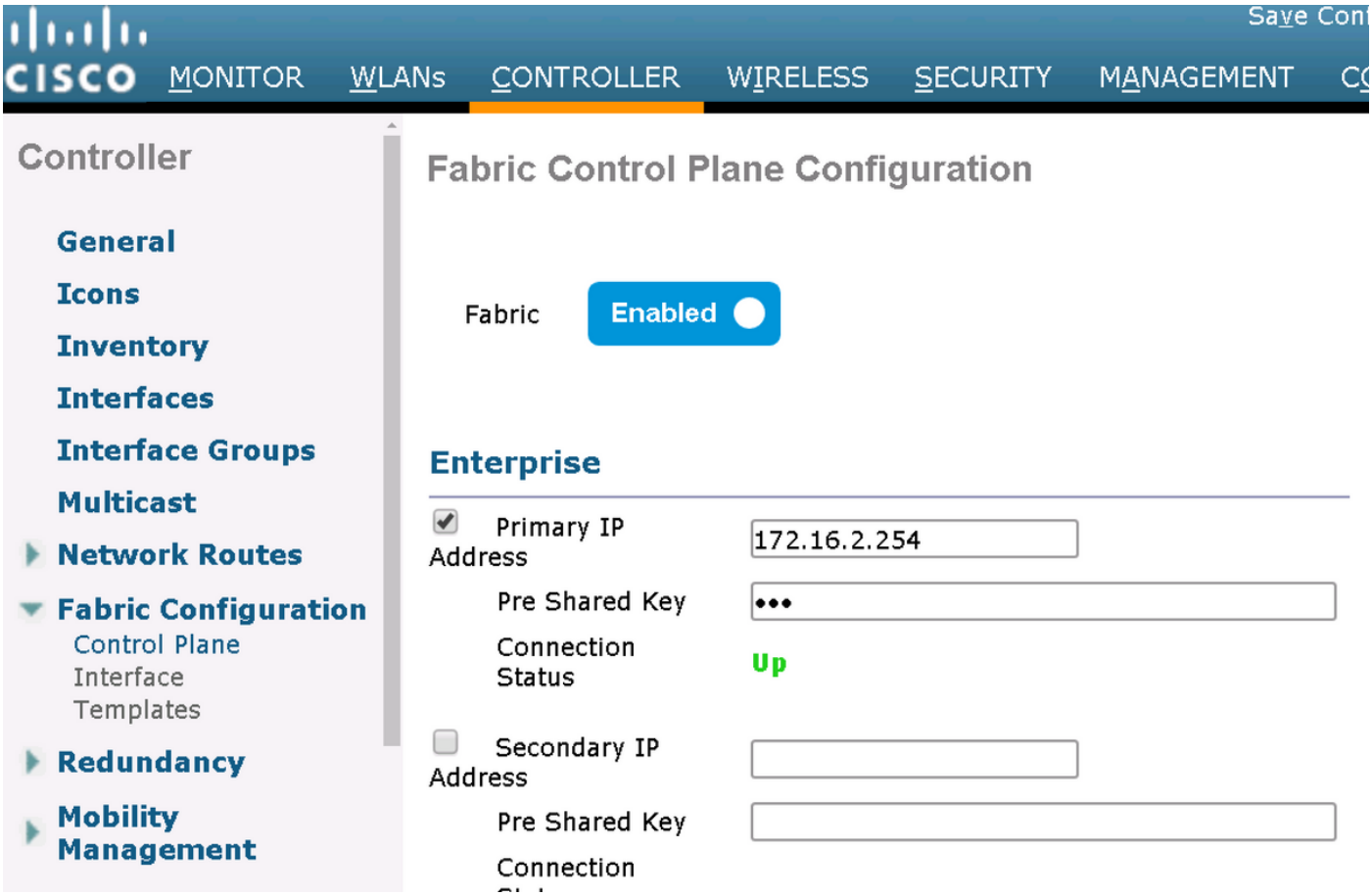
Negli scenari di accesso SD esiste una serie di requisiti che spesso sono causa di errori. Verificare prima che questi requisiti siano soddisfatti:

- Accertarsi di disporre di un percorso specifico (e non di quello predefinito) che punti al WLC sul nodo del control plane LISP

- Verificare che i punti di accesso si trovino nell'infrastruttura VN, utilizzando la tabella di routing globale
- Verificare che gli access point siano collegati al WLC eseguendo il ping del WLC dall'access point stesso
- Verificare che lo stato del fabric del control plane sul WLC sia attivo
- Verificare che gli access point siano nello stato abilitato per l'infrastruttura

scenario 1. Verificare la registrazione del WLC con il control plane del server LISP/MAP

Quando si aggiunge il WLC al fabric in DNA Center, i comandi vengono inviati al controller per stabilire una connessione al nodo definito come control plane in DNA-C. Il primo passaggio consiste nel garantire la riuscita della registrazione. Se la configurazione LISP sul control plane si danneggiasse in qualche modo, la registrazione potrebbe non riuscire.



Se lo stato è inattivo, potrebbe essere interessante eseguire il debug o acquisire un pacchetto tra il WLC e il control plane. La registrazione riguarda sia TCP che UDP sullo switch 4342. Se il control plane non ha ottenuto la configurazione corretta, potrebbe rispondere con una richiesta TCP RST alla richiesta TCP SYN inviata dal WLC.

Èpossibile verificare lo stesso stato con **show fabric map-server summary** sulla riga di comando. Il processo viene sottoposto a debug con **debug fabric lisp map-server all** sulla CLI del WLC. Per provocare un tentativo di riconnessione, è possibile andare al DNA Center e scegliere di rimuovere il WLC dal fabric e aggiungerlo di nuovo.

Possibili cause: linee di configurazione mancanti nel control plane. Di seguito è riportato un esempio di configurazione di lavoro (solo la parte più importante):

```
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
```

Se il comando WLC ip è mancante (10.241.0.41 qui) o se il comando passive-open è mancante, il CCP rifiuterà la connessione WLC.

I debug da eseguire sono:

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

Di seguito è riportato un esempio del control plane che non risponde 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
```

Di seguito è riportato un esempio di debug WLC di un access point in stato fabric disabilitato perché nel control plane del fabric manca un percorso specifico verso il 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
```

Èinteressante notare che se ci sono due control plane nella rete di fabric, il WLC si rivolgerà sempre a entrambi per la registrazione o le richieste. Si prevede che entrambi i control plane diano risposte positive sulle registrazioni, quindi il WLC non riuscirà a registrare gli access point nel fabric se uno dei due control plane lo rifiuta per qualsiasi motivo. Un piano di comando che non risponde è accettabile, ma verrà utilizzato il piano di comando rimanente.

I punti di accesso raggiungono il WLC tramite la tabella di routing globale, ma il protocollo LISP viene ancora utilizzato per risolvere il WLC. Il traffico inviato dagli access point al WLC è un controllo CAPWAP puro (non riguarda la vxlan), ma il traffico di ritorno inviato dal WLC all'access point verrà trasferito sulla Vxlan sul sovrimpressione. Non sarà possibile verificare la connettività dalla SVI del gateway AP sul perimetro del WLC perché, trattandosi di un gateway Anycast, lo stesso IP esiste anche sul nodo di confine. Per verificare la connettività, la cosa migliore è eseguire il ping dall'access point stesso.

scenario 2. I punti di accesso non ricevono un indirizzo IP

I punti di accesso devono ottenere un indirizzo IP dall'access point Poo, nell'infrastruttura VNI definita in DNA Center. Se l'operazione non riesce, in genere la porta dello switch a cui è connesso l'access point non è stata spostata sulla vlan corretta. Quando lo switch rileva (tramite CDP) un punto di accesso collegato, applica una macro switchport che imposta la porta dello switch nella vlan definita da DNA-C per il pool AP. Se la porta dello switch con il problema non è stata configurata con la macro, è possibile impostare la configurazione manualmente (in modo che l'access point ottenga un indirizzo IP, si unisca al WLC e probabilmente aggiorni il codice e risolva eventuali bug CDP) o risolvere i problemi relativi al processo di connessione CDP. Facoltativamente, è possibile configurare l'onboarding dell'host in modo che definisca in modo statico la porta di DNA-Center su cui ospitare un access point in modo che venga configurato correttamente.

Le macro Smartport non vengono eseguite automaticamente se allo switch non è stato assegnato almeno un access point. È possibile verificare se alla macro AP è stato assegnato il vlan corretto (anziché la vlan predefinita 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
```

I comandi utilizzati da Cisco DNA-C per impostare questa condizione sono

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

scenario 3. I punti di accesso non dispongono di un tunnel vxlan costruito verso il rispettivo nodo Fabric Edge

Quando un access point si unisce al WLC, il WLC (se l'access point è compatibile con la struttura) registra l'access point sul control plane come tipo speciale di client. Il control plane richiederà quindi al nodo Fabric Edge in cui l'access point è collegato di costruire un tunnel vxlan verso l'access point.

L'access point utilizzerà l'incapsulamento vxlan solo per inviare il traffico dei client (e solo per i client in stato RUN), quindi è normale non visualizzare alcuna informazione vxlan sull'access point finché un client fabric non si connette.

Sul punto di accesso, il comando **show ip tunnel fabric** visualizzerà le informazioni del tunnel vxlan una volta che un client si è connesso.

```
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#
```

Sul nodo Fabric Edge, il comando **show access-tunnel summary** mostrerà i tunnel vxlan costruiti verso i punti di accesso. I tunnel verranno visualizzati non appena il control plane ne ha ordinato la creazione quando l'access point si unisce.

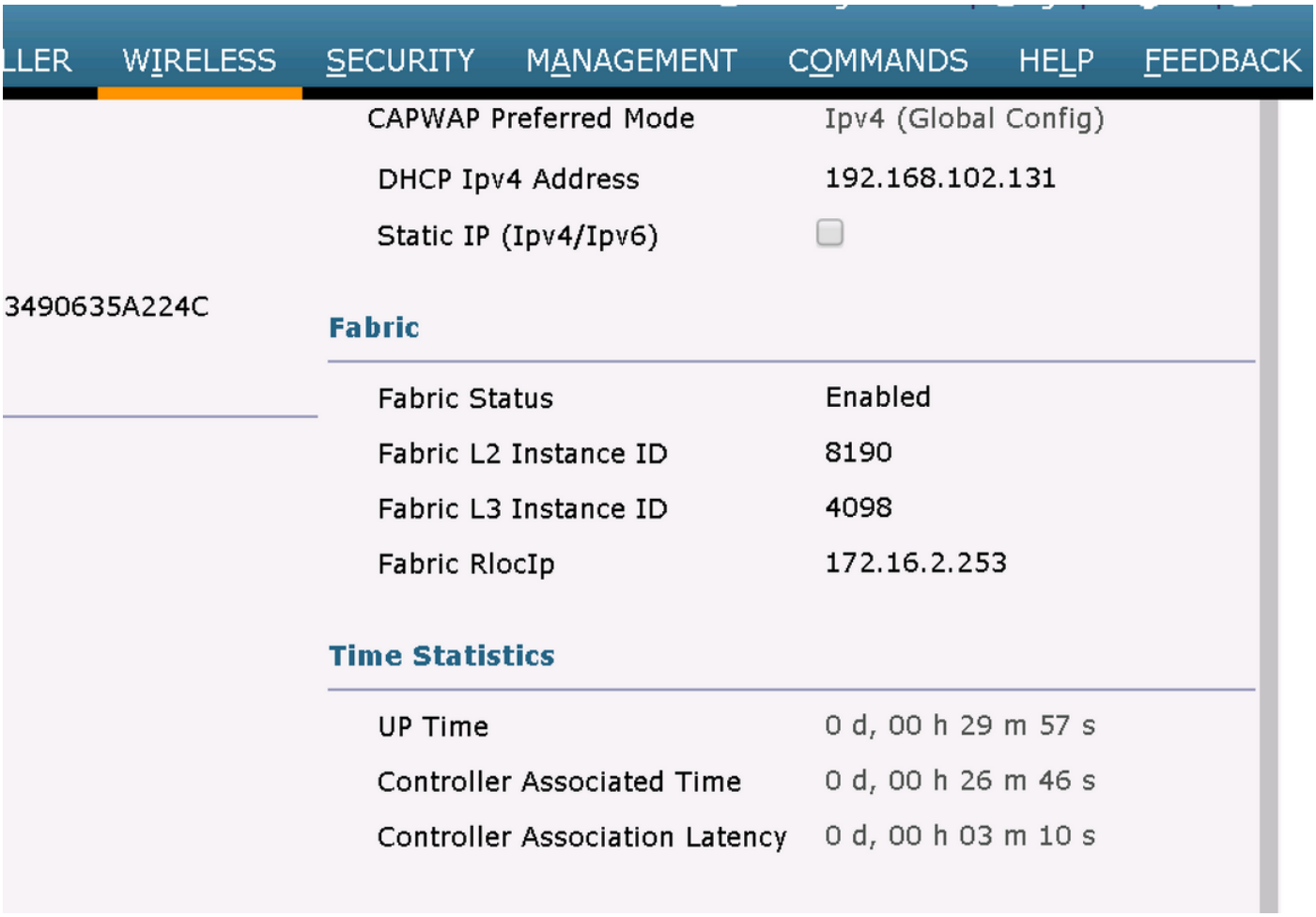
```
edge01#show access-tunnel summ

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
```

Èpossibile controllare sulla pagina del punto di accesso del WLC l'ID istanza L2 LISP corrispondente all'access point e quindi controllare le statistiche dell'istanza sul Fabric Edge a cui è connesso.




```
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. voci del tunnel di accesso mancanti dopo un breve periodo

Èpossibile che i tunnel di accesso vengano creati correttamente la prima volta che si esegue il provisioning WLC tramite Cisco DNA-C e si aggiungono alla struttura, ma quando si esegue di nuovo il provisioning della configurazione wireless (come la configurazione WLAN), si osserva che le voci del tunnel di accesso per gli AP non sono presenti e i client wireless non sono in grado di ottenere l'IP.

La topologia è 9500(CP) —> 9300 (Edge) —> AP —> Wireless Client.

Le voci vengono osservate correttamente in **show access-tunnel summary** sul nodo perimetrale:

```
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
```

Tuttavia, quando si seleziona **show platform software fed switch active ifm interfaces access-tunnel, la voce relativa all'access point risulta mancante o non può essere programmata nell'hardware in questo esempio.**

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

Per altri output:

```
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
```

Ènecessario confrontare i diversi output e ogni tunnel mostrato dal **riepilogo show access-tunnel** deve essere presente in ciascuno di essi.

scenario 5. i client wireless non sono in grado di ottenere un indirizzo IP

Se il tunnel vxlan è presente e tutto sembra funzionare correttamente ma i client wireless non sono sistematicamente in grado di ottenere un indirizzo IP, è possibile che si stia verificando un problema relativo all'opzione 82. Poiché il comando DHCP DISCOVER del client viene inoltrato dal gateway Anycast sul nodo periferico, potrebbero verificarsi dei problemi per l'invio del server DHCP OFFERTO al nodo laterale destro dal bordo posteriore. Per questo motivo, il lato fabric che inoltra il comando DHCP DISCOVER aggiunge un campo opzione 82 al comando DHCP DISCOVER che contiene l'RLOC (loopback ip) effettivo del nodo edge codificato insieme ad altre informazioni. Ciò significa che il server DHCP deve supportare l'opzione 82.

Per risolvere i problemi relativi al processo DHCP, acquisire le clip sui nodi fabric (in particolare sul nodo edge del client) per verificare che il bordo dell'infrastruttura stia aggiungendo il campo dell'opzione 82.

scenario 6. Infrastruttura guest/autenticazione Web non funzionante/client non reindirizzati

Lo scenario della struttura guest è estremamente simile a CWA (Central Web Authentication) sui punti di accesso Flexconnect e funziona esattamente allo stesso modo (anche se gli access point della struttura non sono in modalità flexconnect).

L'ACL di reindirizzamento e l'URL devono essere restituiti da ISE nel primo risultato dell'autenticazione MAC. Verificare quanto riportato nei log ISE e nella pagina dei dettagli del client sul WLC.

L'ACL di reindirizzamento deve essere presente come ACL Flex sul WLC e deve contenere istruzioni "allow" (permesso) verso l'indirizzo IP di ISE sulla porta 8443 (almeno).

Il client deve essere nello stato "CENTRAL_WEBAUTH_REQ" nella pagina dei dettagli del client sul WLC. Il client non sarà in grado di eseguire il ping del gateway predefinito. Questa condizione è prevista. Se non si viene reindirizzati, è possibile provare a digitare manualmente un indirizzo IP nel browser Web del client (per escludere il DNS, ma il nome host ISE dovrà essere risolto comunque). Dovrebbe essere possibile immettere l'indirizzo IP ISE sulla porta 8443 nel browser del client e visualizzare la pagina del portale, in quanto questo flusso non verrà reindirizzato. Se il problema non si verifica, significa che si è verificato un problema con l'ACL o un problema di routing verso il router. Raccogliere le acquisizioni dei pacchetti lungo il percorso per individuare il punto in cui i pacchetti HTTP sono stati arrestati.

Comprendere

In che modo un client wireless ottiene un indirizzo IP nell'architettura 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
```

L'acquisizione dei pacchetti viene effettuata tra il Fabric AP e il Fabric Edge. I pacchetti sono duplicati perché sono stati inviati due pacchetti di individuazione DHCP. Il traffico era solo in entrata e acquisito sul perimetro della struttura.

Ci sono sempre due pacchetti DHCP. Uno inviato da CAPWAP direttamente al controller per mantenerlo aggiornato. L'altro viene inviato dalla VXLAN al Control Node. Quando l'access point riceve, ad esempio, un'offerta DHCP con VXLAN dal server DHCP, ne invia una copia al controller con CAPWAP.

```
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)
```

Per vedere dove il pacchetto è stato inviato, è necessario fare clic su di esso su Wireshark. Qui possiamo vedere che l'origine è il nostro AP 172.16.3.131 e il pacchetto è stato inviato al Fabric Edge 172.16.3.98. Il perimetro dell'infrastruttura lo ha inoltrato al nodo di controllo.

Comprendere il flusso di reindirizzamento Web in uno scenario fabric

L'ACL di reindirizzamento sul WLC definisce il traffico che viene reindirizzato/intercettato sulle istruzioni deny corrispondenti (alla fine, è presente un rifiuto implicito). Il traffico da reindirizzare verrà inviato al WLC all'interno dell'incapsulamento CAPWAP in modo che il WLC lo reindirizzi. Quando corrisponde a un'istruzione di autorizzazione, non reindirizza il traffico in questione, lo lascia passare e lo inoltra sul fabric (il traffico verso ISE entra in questa categoria).

Registri dell'access point che si unisce al WLC nello stato abilitato per l'infrastruttura

Non appena Access-Point si registra sul WLC, il controller registrerà il proprio indirizzo IP e MAC nel SDA Control Node (LISP Map Server).

L'access point si unisce al WLC in modalità abilitata per struttura solo se il WLC riceve il pacchetto LISP RLOC. Questo pacchetto viene inviato per verificare che l'access point sia collegato a un Fabric Edge.

In questo esempio, i debug utilizzati sul WLC sono:

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

Per il test, l'access point viene riavviato:

```
*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**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).