Informazioni sulla creazione di tunnel di accesso in SD-Access

Sommario

Introduzione

In questo documento viene descritto cos'è un tunnel di accesso in SD-Access, il suo scopo e come misurare la formazione del tunnel di accesso.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Locator ID Separation Protocol (LISP)
- Wireless

Componenti usati

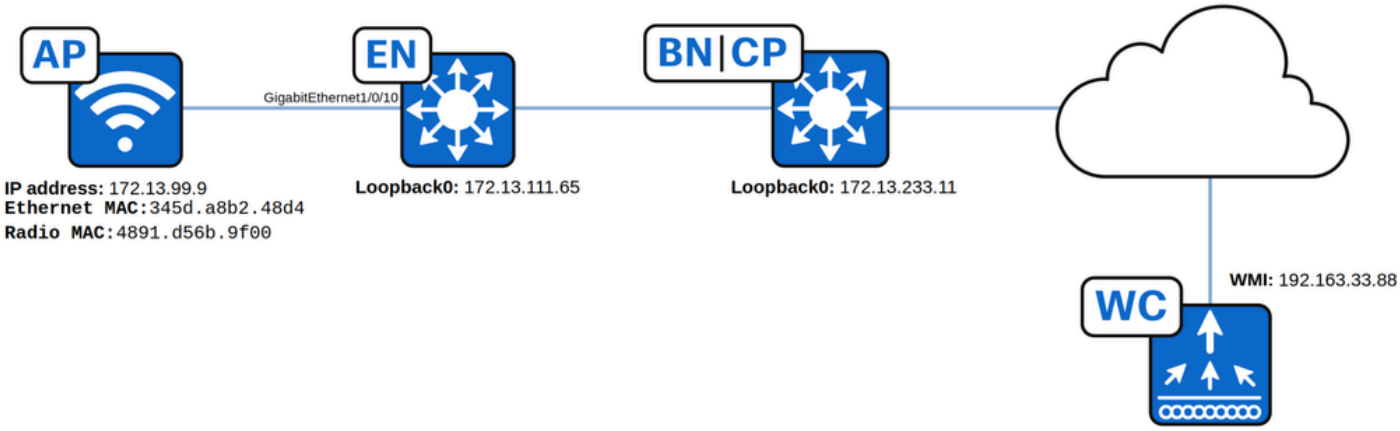
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Wireless LAN Controller (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- Border Node/Control Plane SDA - C9500-48P, Cisco IOS® XE 17.12.05

- Cisco Access Point - C9130AXI-A, versione 17.9.5.47

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.

Topologia



Topologia utilizzata in questo articolo

Panoramica

Un tunnel di accesso in Cisco SD-Access è un tunnel VXLAN (Virtual Extensible LAN) stabilito tra i nodi periferici del fabric e i punti di accesso (AP). Questo tunnel incapsula il traffico dei client nella VXLAN, consentendo una comunicazione perfetta all'interno del fabric SD-Access. Il tunnel di accesso funge da overlay del piano dati che trasferisce il traffico proveniente dai client wireless collegati al punto di accesso al perimetro della struttura, garantendo l'applicazione coerente delle policy e la segmentazione attraverso la rete.

Processo di formazione del tunnel di accesso

1. L'access point è collegato alla rete elettrica e si accende tramite Power over Ethernet (PoE).
2. L'access point ottiene un indirizzo IP tramite DHCP nella sovrapposizione. Durante questo processo, l'access point riceve anche l'opzione 43 dal server DHCP per il controller LAN wireless.
3. Fabric Edge registra l'indirizzo IP e l'indirizzo MAC Ethernet dell'access point e aggiorna il Control Plane LISP.
4. Il WLC interroga il provider di servizi LISP per sapere se l'access point è collegato a un dispositivo fabric.
5. Il Control Plane LISP risponde al WLC con l'indicatore di posizione (Loopback 0 IP) del dispositivo fabric a cui è collegato l'AP. In caso di risposta, l'access point è collegato all'infrastruttura e contrassegnato come abilitato per l'infrastruttura.
6. WLC esegue una registrazione LISP L2 per l'AP Radio MAC nel LISP Control Plane insieme

alle informazioni metada dal WLC al FE.
7. Il Control Plane LISP notifica il perimetro della struttura e invia i metadati ricevuti dal WLC. I metadati contengono un flag che indica che si tratta di un punto di accesso e dell'indirizzo IP del punto di accesso.
8. Fabric Edge elabora le informazioni. Viene a sapere che si tratta di un access point e crea un tunnel VXLAN noto anche come tunnel di accesso tra l'access point e il bordo della struttura.

Leggere attentamente questi passaggi per garantire la corretta formazione del tunnel di accesso per l'onboarding dei punti di accesso in SD-Access. Qualsiasi errore in questi controlli può impedire la creazione del tunnel. Se un passaggio non produce i risultati previsti, concentrare gli sforzi di risoluzione dei problemi sul componente correlato a tale passaggio.

Verifica del processo

Verificare se l'access point ottiene un indirizzo IP

Per verificare che l'access point riceva un indirizzo IP, eseguire questo comando sul nodo perimetrale:

<#root>

Edge#show device-tracking database interface gigabitEthernet 1/0/10

```
...
     Network Layer Address   Link Layer Address  Interface  vlan prlvl age state     Time left
DH4
```

172.13.99.9

345d.a8b2.48d4

Gi1/0/10

99

0024 15s REACHABLE 237 s try 0(47302 s)

Dall'output precedente, è possibile confermare che l'access point connesso all'interfaccia Gigabit Ethernet 1/0/10 abbia l'indirizzo IP 172.13.99.9 sulla VLAN 99, con indirizzo MAC Ethernet 345d.a8b2.48d4.
Se l'output è vuoto, l'access point non è riuscito a ottenere un indirizzo IP o l'interfaccia Power over Ethernet (PoE) non funziona. Per verificare che il PoE sia operativo, verificare che l'indirizzo MAC del punto di accesso sia visualizzato nella tabella degli indirizzi MAC eseguendo questo comando:

<#root>

Edge#show mac address-table interface gigabitEthernet 1/0/10

```
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
```

99

345d.a8b2.48d4

DYNAMIC

Gi1/0/10

Per verificare che l'alimentazione in linea per PoE sia operativa, eseguire questo comando:

<#root>

Edge#show power inline gigabitEthernet 1/0/10

```
Interface  Admin
```

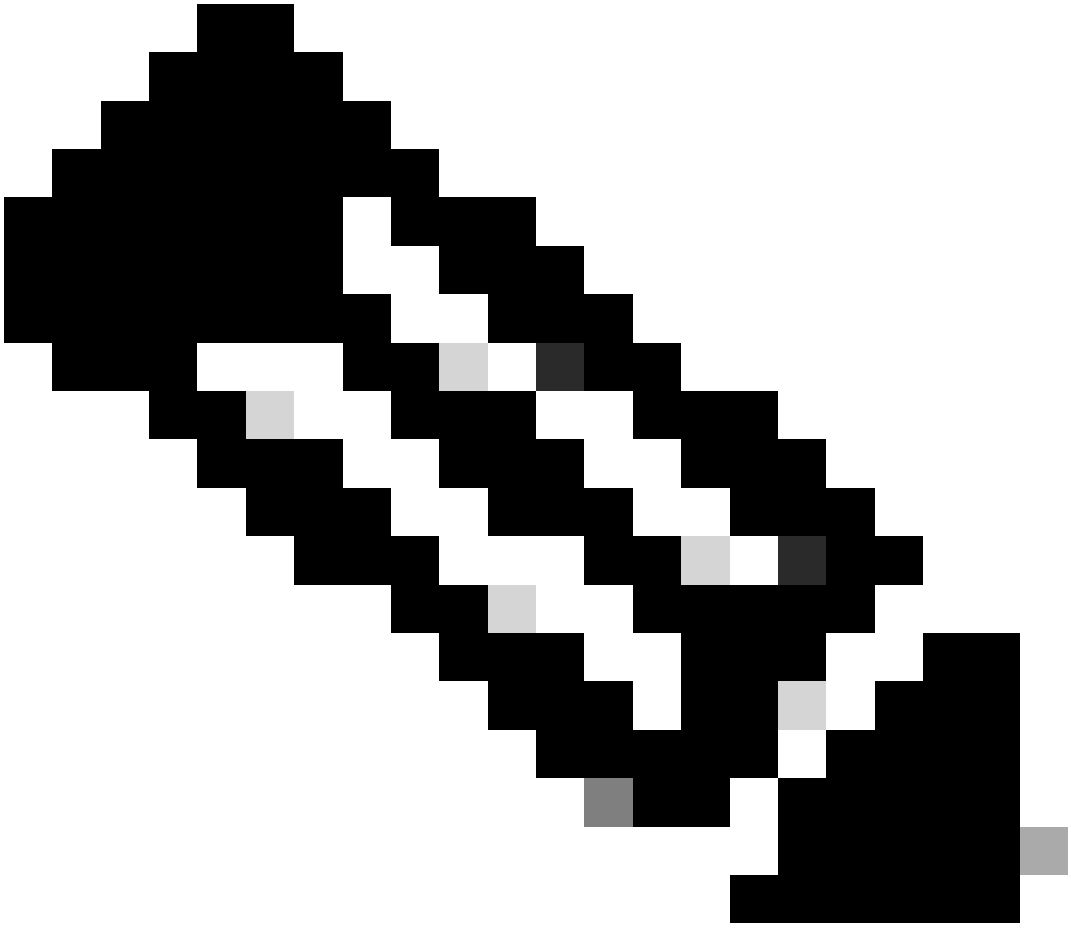
Oper

```
   Power   Device      Class  Max
                         (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Gi1/0/10    auto
```

on

```
     30.0   C9130AXI-A   4    30.0
```

La PoE funziona a 30,0 watt.



Nota: Dopo aver ottenuto un indirizzo IP, il punto di accesso tenta di collegarsi al controller WLC (Wireless LAN Controller), in modo simile alle reti tradizionali. Se l'access point non è presente nell'elenco quando si esegue il comando show ap summary, risolvere i problemi relativi al join dell'access point.

Verifica della registrazione di indirizzi MAC IP ed Ethernet dell'access point sul Control Plane LISP

Per identificare il control plane, noto anche come server di mappe, per il lato dell'infrastruttura, eseguire il comando:

<#root>

Edge#show lisp session

```
Sessions for VRF default, total: 1, established: 1
Peer State Up/Down In/Out Users
```

```
172.13.233.11

:4342 Up 1d02h 326/324 12
```

Il piano di controllo è 172.13.233.11 che sarebbe il loopback0 per quel dispositivo.

Un altro modo per identificare il control plane per il sito di infrastruttura è eseguire questo comando:

<#root>

```
Edge#show running-config | section map-server


etr map-server

172.13.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.13.233.11

 proxy-reply
etr map-server

172.13.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.13.233.11

 proxy-reply
```

Sul WLC, è possibile anche verificare che la sessione LISP con il control plane sia nello stato UP:

<#root>

```
WLC#show wireless fabric summary


Fabric Status :

Enabled



Control-plane:
Name                    IP-address       Key                Status
------------------------------------------------------------------------------------------
default-control-plane

172.13.233.11

    ddc2df8446e2479d

Up
```

Utilizzare questo comando per trovare l'indirizzo IP dell'access point registrato sul control plane:

<#root>

Border#show lisp instance-id 4097 ipv4 server 172.13.99.9

LISP Site Registration Information
...

EID-prefix: 172.13.99.9/32 instance-id 4097

First registered: 22:14:34
Last registered: 22:14:34
Routing table tag: 0
Origin: Dynamic, more specific of 172.13.99.0/24
...
TTL: 1d00h

State: complete

Extranet IID: Unspecified
Registration errors:

Authentication failures: 0

Allowed locators mismatch: 0

ETR 172.13.111.65:21839, last registered 22:14:34, proxy-reply, map-notify <-- Last registration

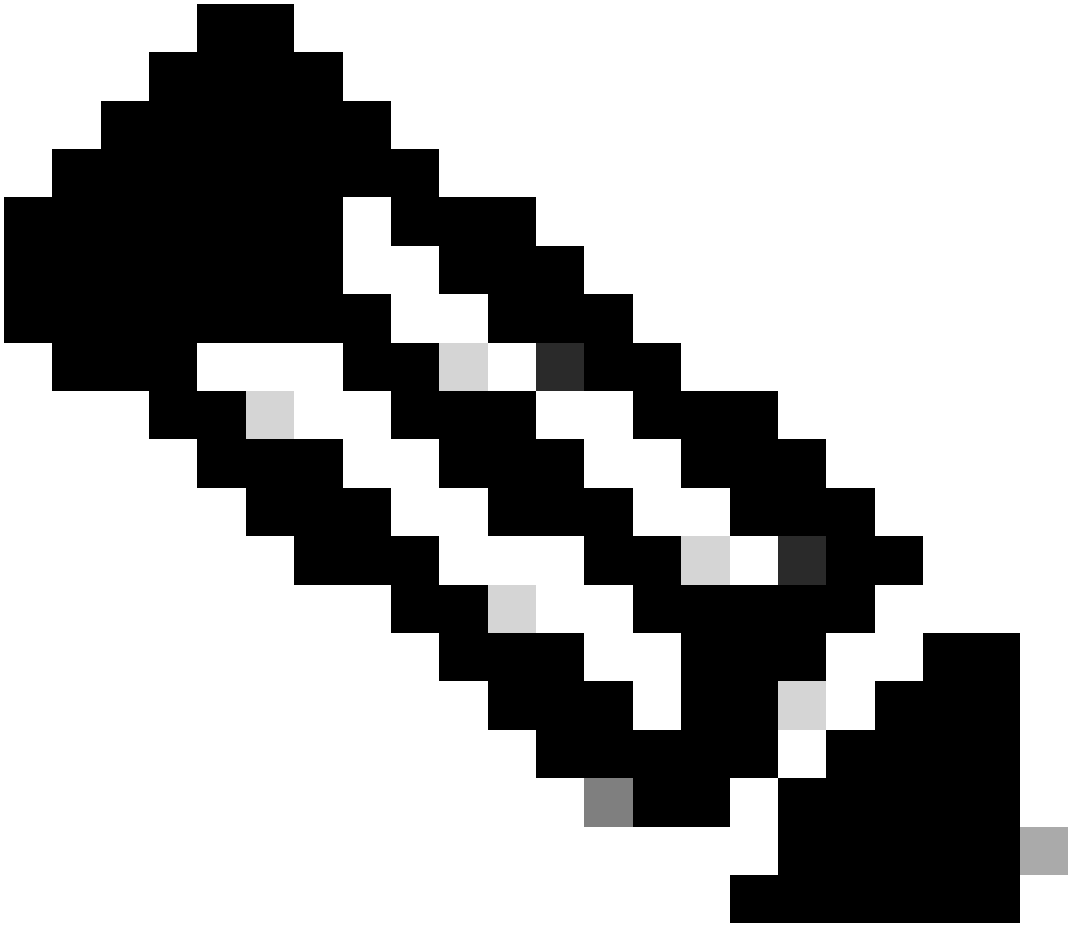
TTL 1d00h, no merge, hash-function sha1
state complete, no security-capability
...
Domain-ID 1559520338
Multihoming-ID unspecified
sourced by reliable transport

Locator

Local State Pri/Wgt Scope

172.13.111.65

yes up 10/10 IPv4 none



Nota: I punti di accesso utilizzano sempre INFRA_VN per il layer 3 e questo INFRA_VN è sempre mappato all'istanza con ID 4097.

La registrazione è stata completata per l'access point con indirizzo IP 172.13.99.9. Non ci sono errori di autenticazione ed è connesso al nodo perimetrale 172.13.111.65 (localizzatore).

Per verificare se l'indirizzo MAC è registrato sul piano di controllo, identificare innanzitutto l'ID istanza di layer 2 della VLAN a cui è connesso l'access point. Utilizzare i seguenti comandi:

<#root>

Edge#show vlan id 99

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
```

99

```
 AP_VLAN active
```

L2LI0:8188

, Gi1/0/10, Ac0
...

La VLAN 99 è mappata all'istanza con ID 8188. Utilizzando questo ID istanza, eseguire questo comando per verificare se l'indirizzo MAC Ethernet è registrato sul piano di controllo:

<#root>

Border#show lisp instance-id 8188 ethernet server 345d.a8b2.48d4

LISP Site Registration Information
...

EID-prefix: 345d.a8b2.48d4/48 instance-id 8188

First registered: 22:57:39
Last registered: 22:57:39
Routing table tag: 0
Origin: Dynamic, more specific of any-mac
...

State: complete

Extranet IID: Unspecified
Registration errors:

Authentication failures: 0

Allowed locators mismatch: 0

ETR 172.13.111.65:21839, last registered 22:57:39, proxy-reply, map-notify

   TTL 1d00h, no merge, hash-function sha1
   state complete, no security-capability
   ...
   Domain-ID 1559520338
   Multihoming-ID unspecified
   sourced by reliable transport

Locator

      Local State Pri/Wgt Scope

172.13.111.65

 yes   up   10/10   IPv4 none

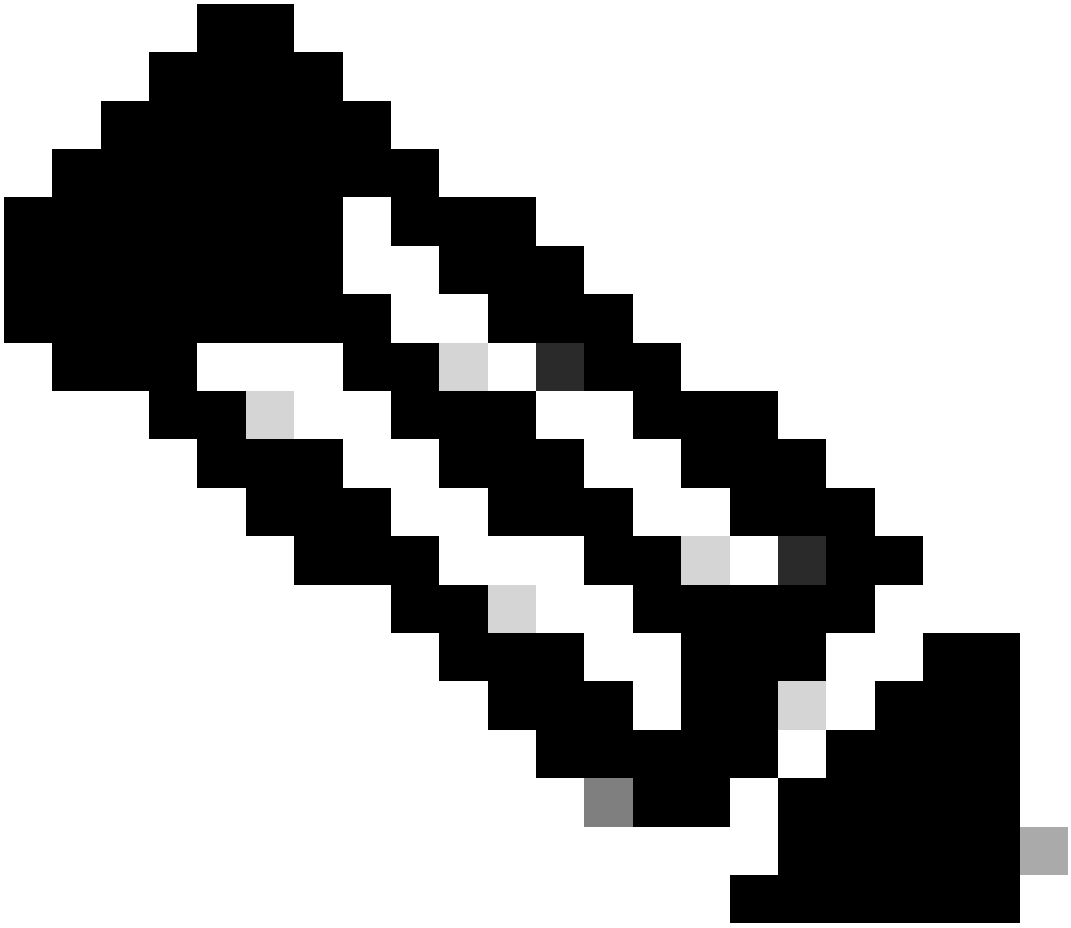
La registrazione dell'access point per l'indirizzo MAC ethernet 345d.a8b2.48d4 è completata senza errori di autenticazione ed è connessa al nodo perimetrale 172.13.11.65 (Locator).

Verificare che il WLC contrassegni il dispositivo come abilitato per la struttura

<#root>

```
WLC#show fabric ap summary

Number of Fabric AP : 1

AP Name           Slots  AP Model
Ethernet MAC


Radio MAC

        Location Country
IP Address

  State
-----------------------------------------------------------------------------------------------------------
AP345D.A8B2.48D4  3      C9130AXI-A
345d.a8b2.48d4


4891.d56b.9f00

   default location MX
172.13.99.9

 Registered
```

L'access point con indirizzo IP 172.13.99.9 è contrassegnato correttamente come Fabric AP. Se l'access point non è presente nell'elenco, il WLC non è riuscito a ricevere una risposta dal control plane dell'LISP. In questo output, l'indirizzo MAC della radio per l'access point è 4891.d56b.9f00.



Nota: Se l'access point è registrato sul control plane ma non è contrassegnato come abilitato per la struttura, verificare che nessun firewall blocchi il traffico LISP sulla porta UDP 4342.

Verificare la registrazione di Radio MAC sul control plane LISP

Utilizzare lo stesso comando utilizzato per verificare la registrazione dell'indirizzo MAC Ethernet, ma sostituire l'indirizzo MAC Ethernet con l'indirizzo MAC della radio:

<#root>

```
Border#show lisp instance-id 8188 ethernet server 4891.d56b.9f00

LISP Site Registration Information
...
EID-prefix: 4891.d56b.9f00/48 instance-id 8188
```

```
First registered: 22:49:43
Last registered: 22:49:43
Routing table tag: 0
Origin: Dynamic, more specific of any-mac
...
State: complete
Extranet IID: Unspecified
Registration errors:
```

Authentication failures: 0

```
Allowed locators mismatch: 0
ETR 192.163.33.88:59019, last registered 22:49:43, no proxy-reply, no map-notify
   TTL 1d00h, no merge, hash-function sha2
   state complete, no security-capability
   ...
   sourced by reliable transport
   Affinity-id: 0 , 0
```

WLC AP bit: Set

Locator

```
       Local State Pri/Wgt Scope
```

172.13.111.65

```
 yes   up    0/0     IPv4 none
```

L'indirizzo MAC radio è stato registrato completamente senza errori di autenticazione ed è connesso al nodo edge 172.13.111.65 (Locator). L'output mostra anche il bit AP WLC: Imposta, un flag utilizzato dal piano di controllo LISP per indicare al nodo del bordo che questa registrazione appartiene a un punto di accesso sulla relativa RLOC 172.13.111.65.

Verificare la creazione del tunnel di accesso

Il passaggio finale è verificare la creazione del tunnel di accesso sul lato del fabric. Come accennato in precedenza, questo è l'obiettivo ultimo di AP onboarding in SD-Access. Per verificare che il tunnel di accesso sia stato creato, eseguire questo comando:

<#root>

Edge#show access-tunnel summary

```
Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels = 1
Name   RLOC IP(Source)   AP IP(Destination) VRF ID Source Port Destination Port
------ --------------- ------------------ ------ ----------- ----------------
```

Ac0

172.13.111.65

172.13.99.9

0 N/A 4789

Name IfId Uptime
------ ---------- --------------------

Ac0 0x00000058 0 day, 00:00:51

Il tunnel di accesso 0 connette l'access point 172.13.99.9 a Edge Node Locator 172.13.111.65 ed è rimasto attivo per 51 secondi. Il timer è impostato su 0 dopo ogni reset.

È inoltre possibile verificare che il tunnel sia programmato al livello di astrazione del driver del motore di inoltro (FED), che si interfaccia direttamente con l'hardware dello switch:

<#root>

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

Interface IF_ID State

Ac0

0x00000058

READY

Utilizzando l'if_ID, è possibile trovare ulteriori informazioni su questo tunnel:

<#root>

Edge#show platform software fed switch active ifm if-id 0x00000058

Interface IF_ID : 0x0000000000000058
Interface Name : Ac0
Interface Block Pointer : 0x73d6c83dc6f8

Interface Block State : READY

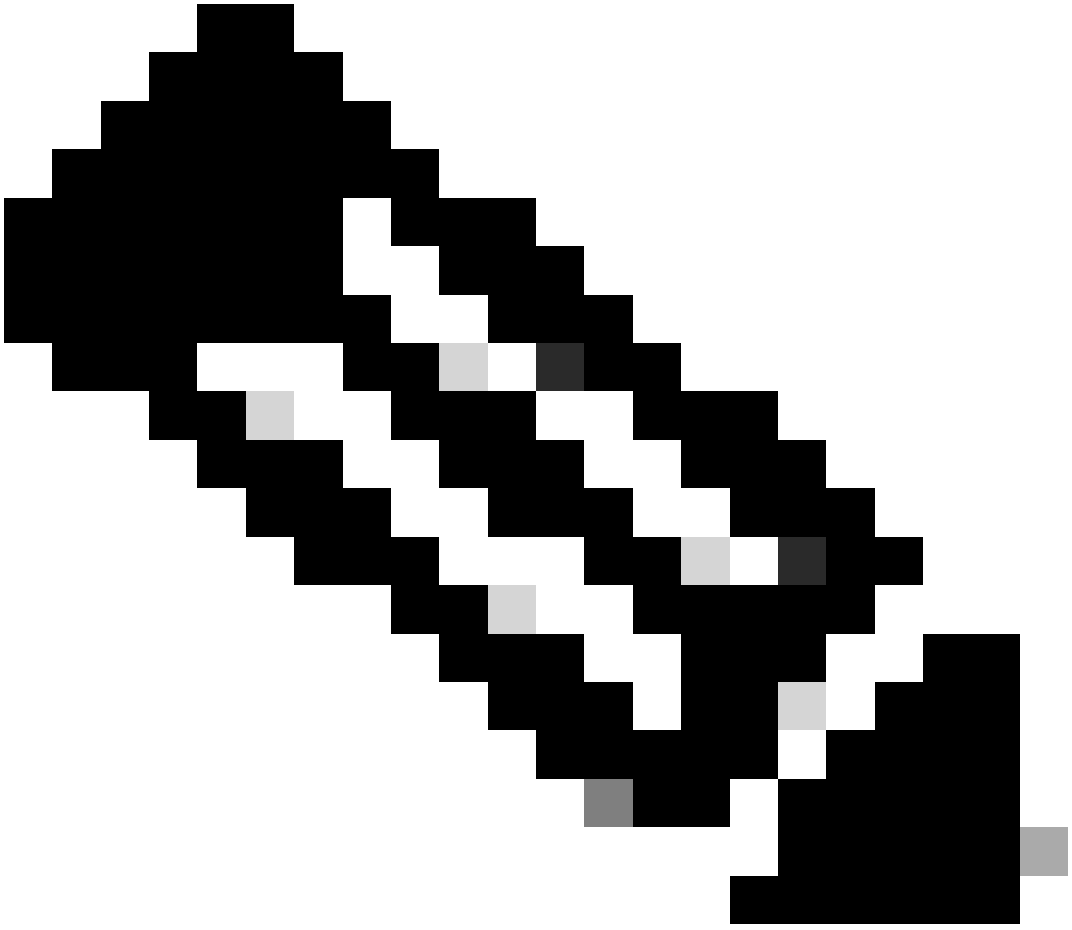
Interface State : Enabled

...

Interface Type : ACCESS_TUNNEL

```
...
Tunnel Type : L2Lisp
Encap Type : VxLan
...
```

Questo è un tunnel L2 lisp con incapsulamento VXLAN e l'interfaccia è di tipo access-tunnel.



> Nota: È importante che il numero di tunnel di accesso corrisponda all'output del comando show access-tunnel summary e del comando FED. Una mancata corrispondenza può indicare una programmazione errata.

Sull'access point, è possibile verificare la creazione del tunnel di accesso con questo comando:

<#root>

AP#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
```

172.13.111.65

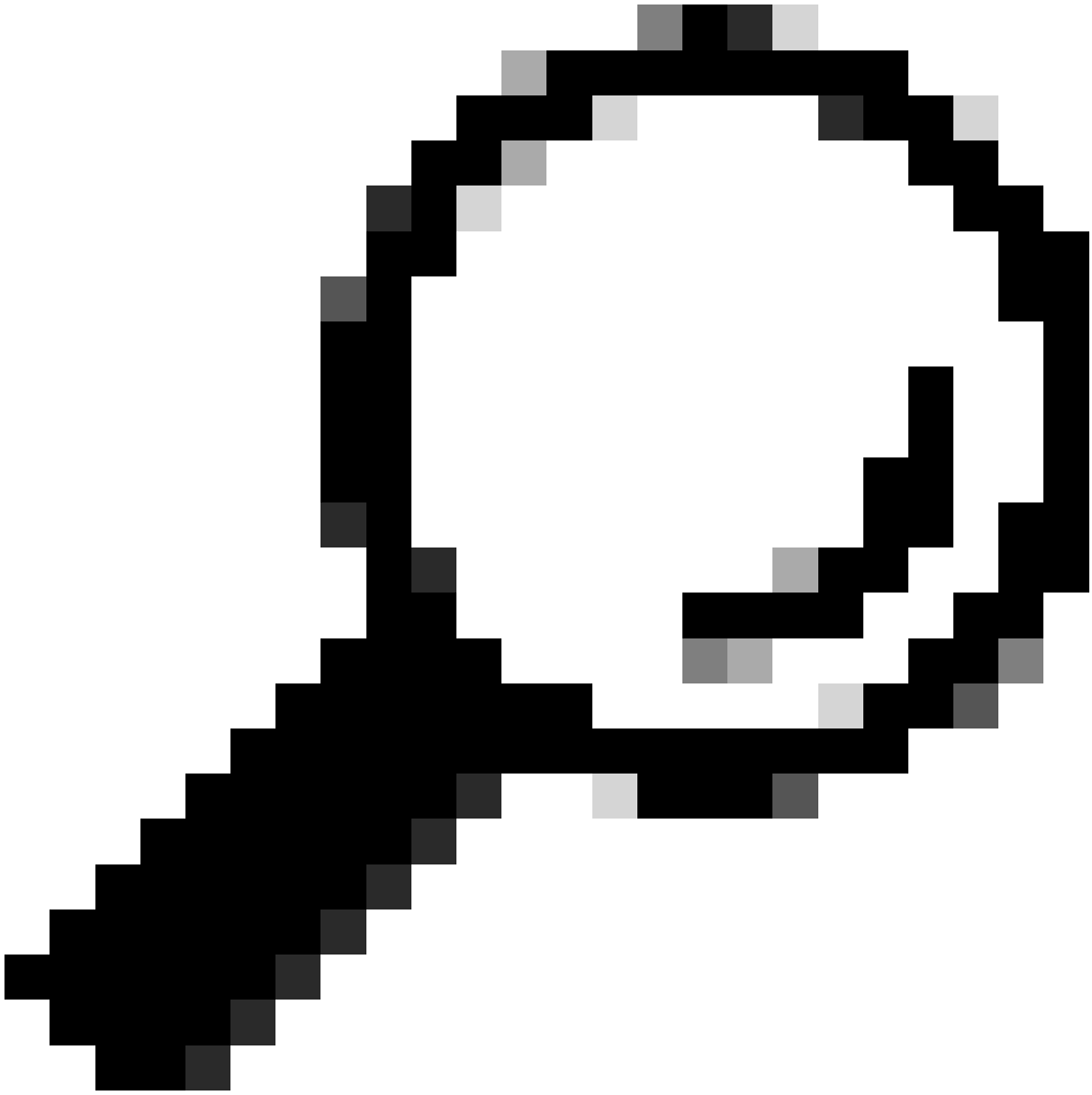
00:00:0C:9F:F2:80

Forward

VXLAN

```
      121
   17096    239       35041
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC
```

L'access point ha un tunnel di accesso che punta al localizzatore del nodo perimetrale 172.13.111.65. L'indirizzo MAC 00:00:0C:9F:F2:80 appartiene all'interfaccia virtuale dello switch (SVI) 99, che è la VLAN a cui è connesso l'access point. Il tipo di incapsulamento è VXLAN.



Suggerimento: Il tunnel viene visualizzato nell'access point solo quando è connesso un client attivo. In caso contrario, restituisce un output vuoto.

Debug e tracce

Per il debug più avanzato della creazione del tunnel di accesso, abilitare le seguenti tracce sul perimetro dell'infrastruttura:

```
set platformsoftware trace forwarding-manager switch active R0 access-tunnel debug
set platform software trace forwarding-manager switch active F0 access-tunnel debug
set platform software trace forwarding-manager switch active access-tunnel noise
request plat sof trace rotate all
show pla sof trace message forwarding-manager switch active R0 reverse
show pla sof trace message forwarding-manager switch active F0 reverse
```

```
show pla sof trace message fed sw active reverse
```

Comandi dipendenti dalla piattaforma del tunnel di accesso Catalyst 9000 per verificare la programmazione del tunnel di accesso sul lato fabric:

```
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 fed switch active ifm if-id <if-id>
```

Per eseguire il debug del processo per il tunnel di accesso sul WLC, abilitare questi comandi:

```
set platform software trace wncd chassis active r0 lisp-agent-api
set platform software trace wncd chassis active r0 lisp-agent-db
set platform software trace wncd chassis active r0 lisp-agent-fsm
set platform software trace wncd chassis active r0 lisp-agent-ha
set platform software trace wncd chassis active r0 lisp-agent-internal g
set platform software trace wncd chassis active r0 lisp-agent-lib
set platform software trace wncd chassis active r0 lisp-agent-lispmsg
set platform software trace wncd chassis active r0 lisp-agent-shim
set platform software trace wncd chassis active r0 lisp-agent-transport
```

Debug per il processo di registrazione. Questi comandi possono essere eseguiti sul nodo perimetrale per verificare se sta tentando di registrare l'indirizzo IP dell'access point e l'indirizzo MAC Ethernet, e sul control plane per confermare se la registrazione è stata eseguita correttamente.

```
debug lisp filter eid <mac-or-ip>
debug lisp control-plane all
```

Riepilogo

- I tunnel di accesso in SD-Access sono tunnel VXLAN tra i nodi periferici della struttura e punti di accesso che trasportano il traffico client all'interno della struttura incapsulata nella VXLAN.
- Consentono l'utilizzo di piani dati wireless unificati e l'applicazione coerente dei criteri perché il tag del gruppo di sicurezza (SGT) è contrassegnato a livello di punto di accesso per gli endpoint wireless.
- La verifica e la selezione implicano la verifica della registrazione sul control plane del fabric, la conferma della creazione sui nodi periferici del fabric e la verifica dello stato del fabric per l'access point sul WLC utilizzando comandi show specifici.
- La risoluzione dei problemi ha lo scopo di garantire la corretta creazione dei tunnel e la loro stabilità dopo le modifiche alla configurazione.

- Il tunnel di accesso è l'obiettivo finale quando si imbarca un nuovo access point in SD-Access.

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).