Inzicht in het maken van toegangstunnels in SD-Access

Inhoud

Inleiding

Dit document beschrijft wat een toegangstunnel is in SD-Access, het doel ervan en hoe u de vorming van de toegangstunnel kunt triageren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Locator ID Separation Protocol (LISP)
- Draadloos

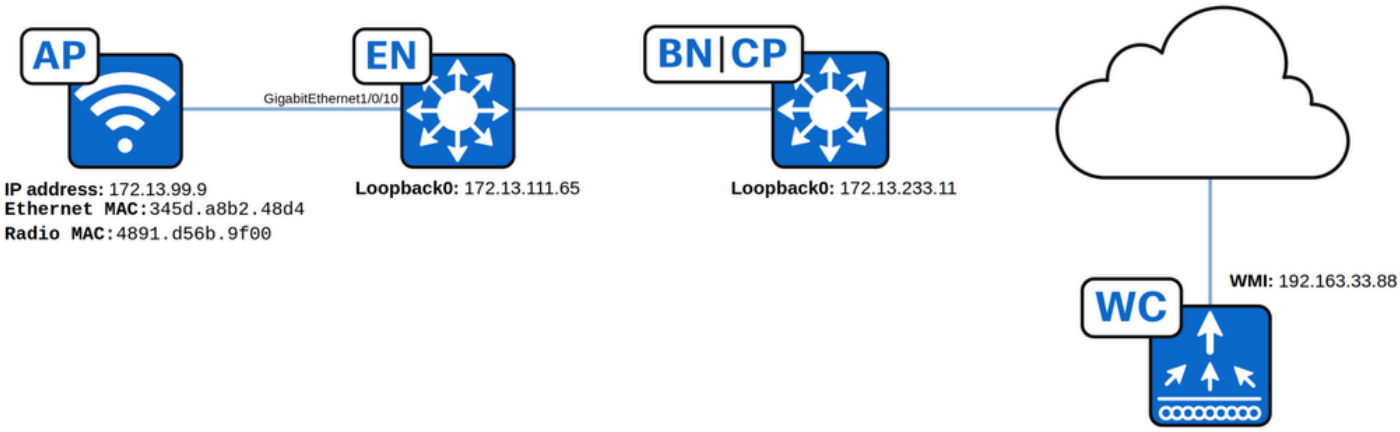
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Wireless LAN Controller (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- SDA Border Node/Control Plane - C9500-48P, Cisco IOS® XE 17.12.05
- Cisco Access Point - C9130AXI-A, versie 17.9.5.47

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie



Topologie gebruikt in dit artikel

Overzicht

Een toegangstunnel in Cisco SD-Access is een Virtual Extensible LAN (VXLAN)-tunnel die is ingesteld tussen fabric edge nodes en toegangspunten (AP's). Deze tunnel omvat clientverkeer in VXLAN, waardoor naadloze communicatie binnen de SD-Access-fabric mogelijk is. De toegangstunnel dient als een overlay van een gegevensvliegtuig die verkeer van draadloze clients die zijn verbonden met het toegangspunt naar de fabric-rand transporteert, waardoor consistente beleidshandhaving en segmentatie in het hele netwerk wordt gewaarborgd.

proces voor het vormen van toegangstunnels

1. Het toegangspunt is aangesloten en kan worden ingeschakeld via Power over Ethernet (PoE).
2. AP krijgt een IP-adres via DHCP in de overlay. Tijdens dit proces ontvangt het toegangspunt ook optie 43 van de DHCP-server voor de draadloze LAN-controller.
3. Fabric edge registreert het IP-adres van AP en Ethernet MAC en werkt het LISP-controlevlak bij.
4. WLC vraagt de LISP CP om te weten of het toegangspunt is verbonden met een fabric-apparaat.
5. LISP Control plane reageert op de WLC met locator (Loopback 0 IP) van het fabric-apparaat waarop het toegangspunt is aangesloten. Als er een antwoord is, betekent dit dat het toegangspunt is aangesloten op Fabric en is gemarkeerd als Fabric ingeschakeld.
6. WLC doet een L2 LISP-registratie voor de AP Radio MAC in het LISP Control-vliegtuig, samen met metagegevens van de WLC naar de FE.
7. LISP Control plane meldt fabric edge en verzendt de metagegevens die zijn ontvangen van

WLC. Deze metagegevens bevatten een markering die aangeeft dat het om een toegangspunt en het IP-adres van het toegangspunt gaat.
8. Fabric Edge verwerkt de informatie. Het leert dat het een toegangspunt is en maakt een VXLAN-tunnel, ook bekend als Access-tunnel tussen het toegangspunt en de rand van de stof.

Lees deze stappen door om te zorgen voor een succesvolle vorming van toegangstunnels voor AP-onboarding binnen SD-Access. Elke fout in deze controles kan voorkomen dat er een tunnel wordt gemaakt. Als een stap niet de verwachte resultaten oplevert, richt u de inspanningen voor probleemoplossing op het onderdeel dat aan die stap is gerelateerd.

Verifieer het proces

Controleer of het toegangspunt een IP-adres krijgt

Voer deze opdracht uit op de edge node om te controleren of het toegangspunt een IP-adres ontvangt:

<#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)
```

Op basis van de vorige uitvoer kan worden bevestigd dat het toegangspunt dat is aangesloten op de Gigabit Ethernet 1/0/10-interface het IP-adres 172.13.99.9 heeft op VLAN 99, met Ethernet MAC-adres 345d.a8b2.48d4.
Als de uitvoer leeg is, kan het toegangspunt geen IP-adres verkrijgen of werkt Power over Ethernet (PoE) niet. Controleer of het MAC-adres van het toegangspunt wordt weergegeven in de MAC-adrestabel door deze opdracht uit te voeren om te bevestigen dat PoE operationeel is:

<#root>

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

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

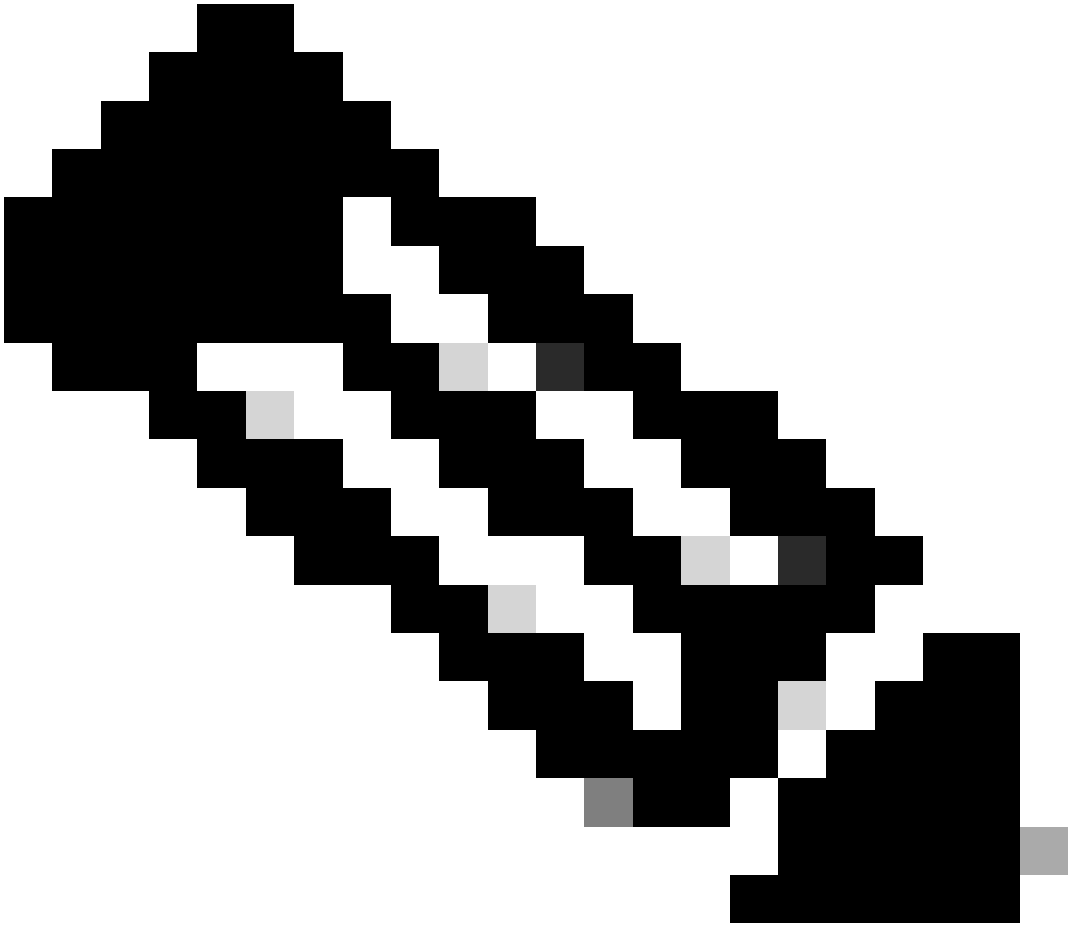
```
---- ----------- -------- -----
99


345d.a8b2.48d4
 DYNAMIC
Gi1/0/10
```

Voer deze opdracht uit om te bevestigen dat de inline power voor PoE operationeel is:

<#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
```

PoE is operationeel en werkt op 30,0 watt.



Opmerking: na het verkrijgen van een IP-adres probeert het toegangspunt zich aan te sluiten bij de draadloze LAN-controller (WLC), vergelijkbaar met traditionele netwerken. Als het toegangspunt niet wordt vermeld tijdens het uitvoeren van de opdracht Overzicht toegangspunt weergeven, moet u het probleem oplossen door het toegangspunt aan te sluiten.

Verifieer de IP- en Ethernet MAC-registratie van AP op LISP Control Plane

Voer de opdracht uit om het controlevlak, ook wel de kaartserver genoemd, voor de fabric-rand te identificeren:

<#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
```

Het controlevlak is 172.13.233.11, wat de loopback0 voor dat apparaat zou zijn.

Een andere manier om het controlevlak voor de fabriekssite te identificeren, is door deze opdracht uit te voeren:

<#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
```

Op de WLC kunt u ook controleren of de LISP-sessie met het controlevlak zich in de UP-status bevindt:

<#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
```

Gebruik deze opdracht om het IP-adres van het toegangspunt te vinden dat is geregistreerd in het controlevlak:

<#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

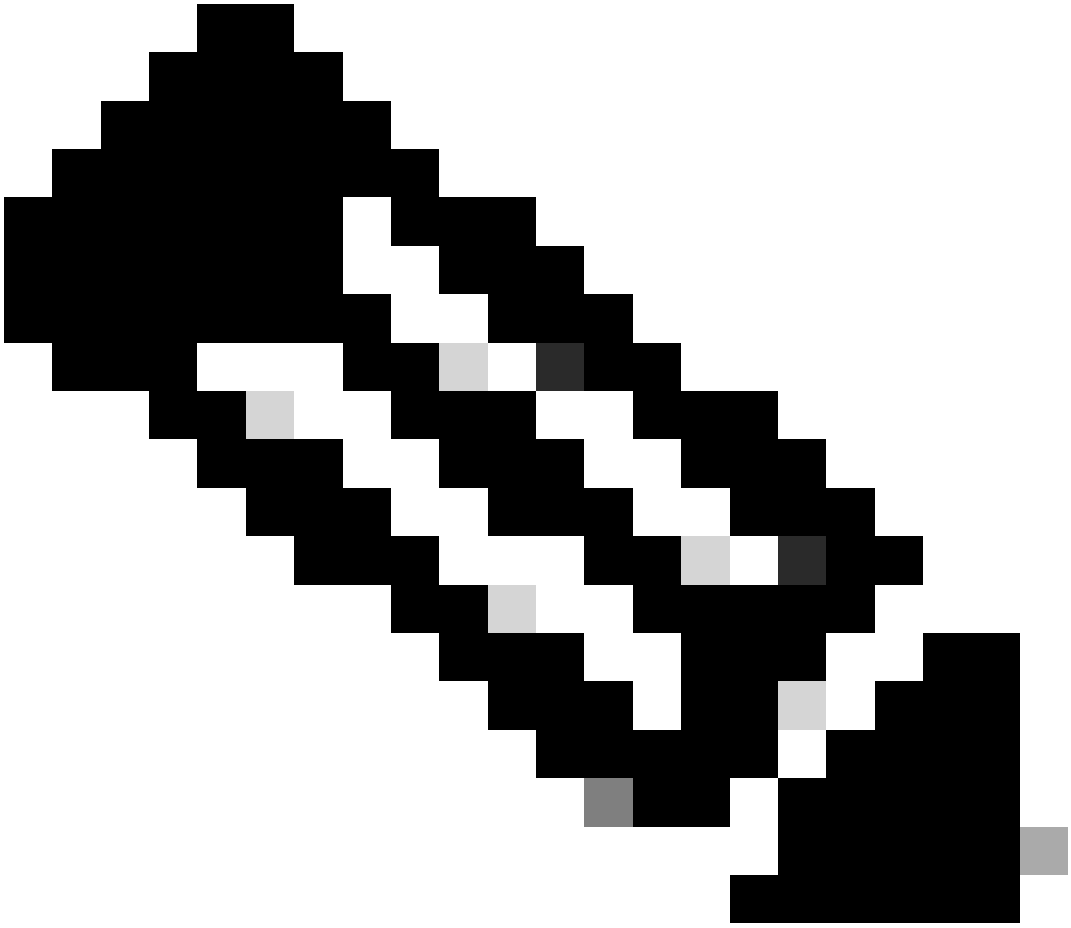
TTL 1d00h, no merge, hash-function sha1
state complete, no security-capability
...
Domain-ID 1559520338
Multihoming-ID unspecified
sourced by reliable transport

Locator

Local State Pri/Wgt Scope

172.13.111.65

yes up 10/10 IPv4 none



Opmerking: AP's gebruiken altijd de INFRA_VN voor Layer 3 en deze INFRA_VN wordt altijd toegewezen aan instantie-ID 4097.

De registratie is voltooid voor het toegangspunt met IP-adres 172.13.99.9. Er zijn geen verificatiefouten en deze is verbonden met de edge node 172.13.111.65 (Locator).

Om te controleren of het MAC-adres is geregistreerd in het controlevlak, moet u eerst de Layer 2-instantie-ID identificeren voor het VLAN waarmee het toegangspunt is verbonden. Gebruik deze commando's:

<#root>

Edge#show vlan id 99

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

99

```
 AP_VLAN active
```

```
L2LI0:8188

, Gi1/0/10, Ac0
...
```

VLAN 99 is toegewezen aan instantie-ID 8188. Voer met deze instantie-ID deze opdracht uit om te bevestigen of het Ethernet-MAC-adres is geregistreerd in het besturingsvlak:

<#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
```

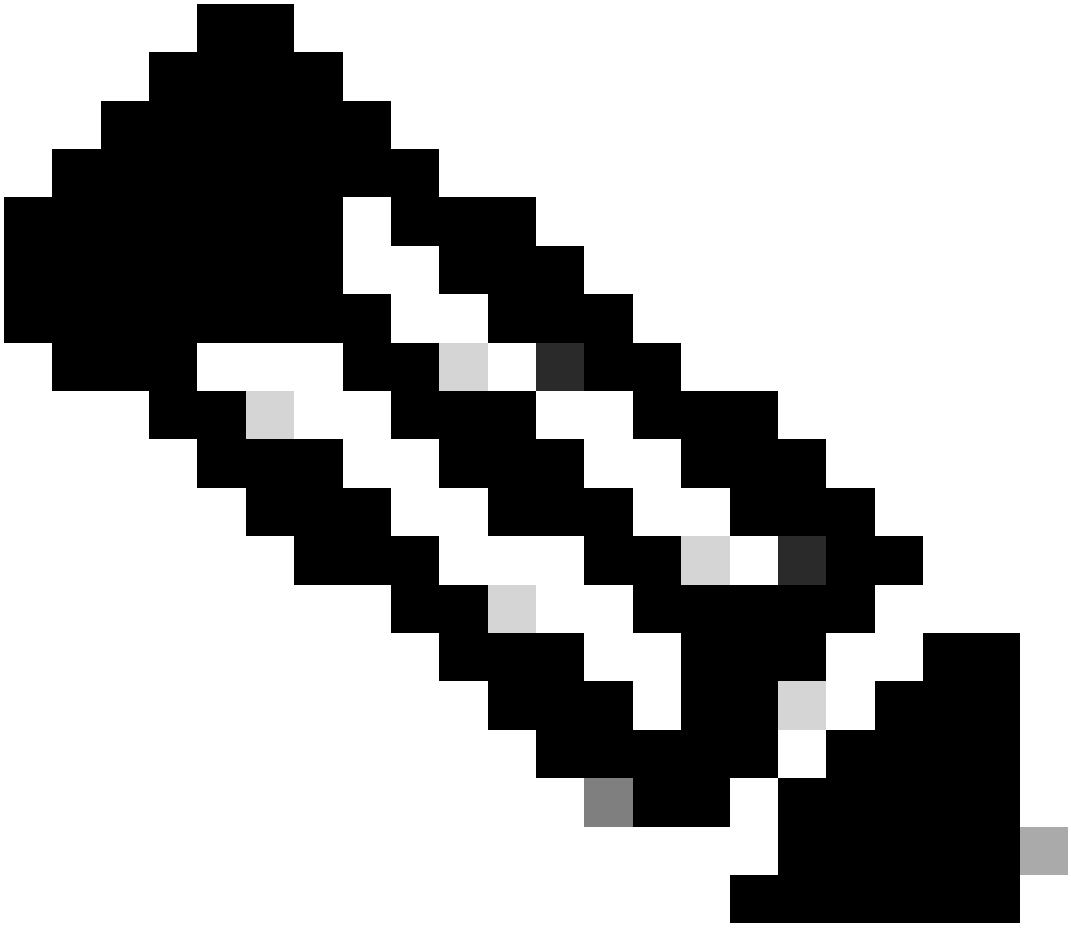
De registratie voor AP's ethernet MAC 345d.a8b2.48d4 is voltooid zonder verificatiefouten en is aangesloten op edge node 172.13.111.65 (Locator).

Controleer of de WLC het apparaat markeert als Fabric-enabled

<#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
```

Het toegangspunt met IP-adres 172.13.99.9 is correct gemarkeerd als een verbindingspunt. Als het toegangspunt niet wordt vermeld, geeft dit aan dat de WLC geen antwoord heeft ontvangen van het LISP-controlevlak. In deze uitvoer is het MAC-adres van de radio voor het toegangspunt 4891.d56b.9f00.



Opmerking: Als het toegangspunt is geregistreerd in het controlevlak maar niet is gemarkeerd als geschikt voor de verbinding, moet u controleren of er geen firewall is die LISP-verkeer blokkeert op UDP-poort 4342.

Verifieer de Radio MAC-registratie op het LISP-besturingsvlak

Gebruik dezelfde opdracht die werd gebruikt om de registratie van het Ethernet-MAC-adres te verifiëren, maar vervang het Ethernet-MAC-adres door het radio-MAC-adres:

<#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
```

Het MAC-adres voor de radio is volledig geregistreerd zonder verificatiefouten en is verbonden met edge node 172.13.111.65 (Locator). De uitvoer toont ook WLC AP bit: Set, een vlag die door het LISP-besturingsvlak wordt gebruikt om aan de randnode aan te geven dat deze registratie behoort tot een AP op zijn RLOC 172.13.111.65.

Verifieer de aanmaak van de toegangstunnel

De laatste stap is om de creatie van de toegangstunnel aan de rand van de stof te verifiëren. Zoals eerder vermeld, is dit het ultieme doel van AP-onboarding in SD-Access. Voer deze opdracht uit om te controleren of de toegangstunnel is gemaakt:

<#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

Toegangstunnel 0 verbindt AP 172.13.99.9 met edge node locator 172.13.111.65 en is 51 seconden lang geopend. De timer is ingesteld op 0 na elke reset.

U kunt ook bevestigen dat de tunnel is geprogrammeerd op de abstractielaag Forwarding Engine Driver (FED), die rechtstreeks met de tunnelhardware is verbonden:

<#root>

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

Interface IF_ID State

Ac0

0x00000058

READY

Met behulp van de IF_ID kunt u meer informatie vinden over deze 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

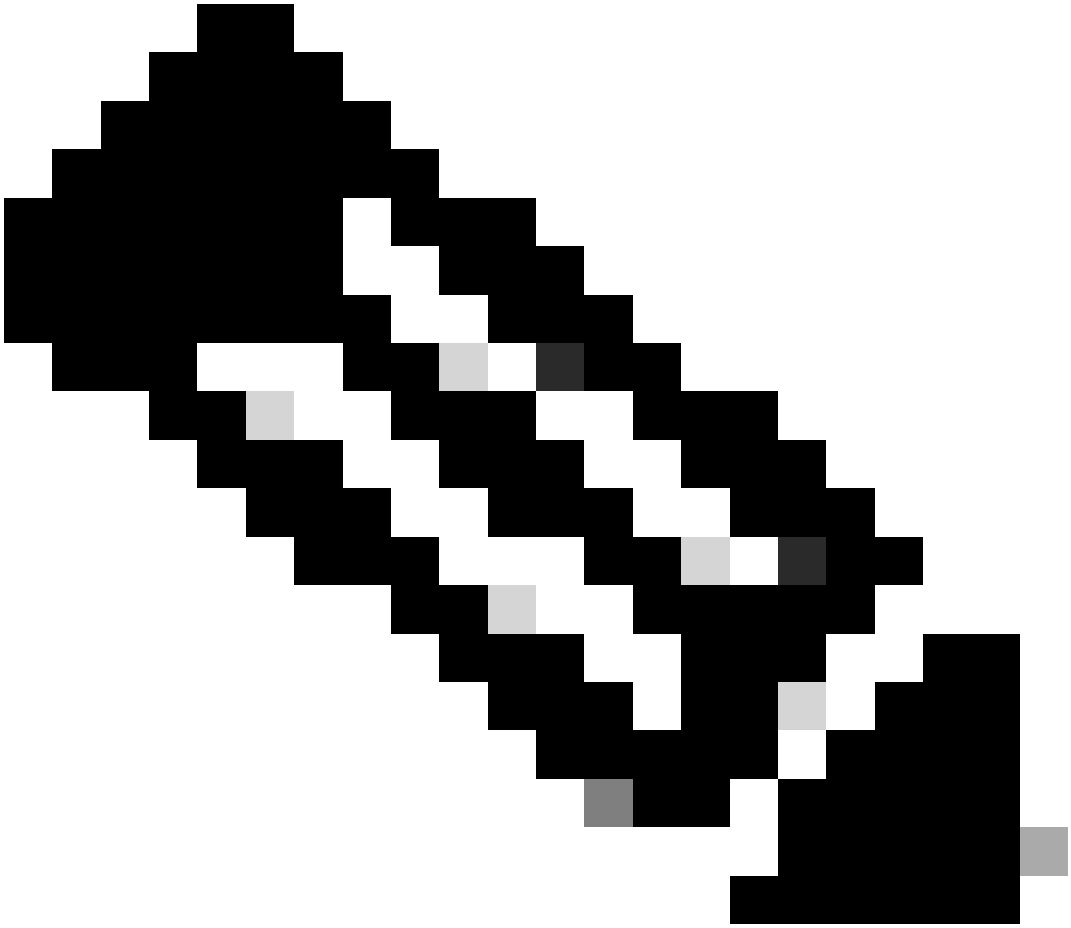
Interface State : Enabled

...

Interface Type : ACCESS_TUNNEL

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

Dit is een L2 lisp-tunnel met behulp van VXLAN-inkapseling en het interfacetype is access-tunnel.



> Opmerking: Het is belangrijk dat het aantal toegangstunnels overeenkomt met de uitvoer van zowel de opdracht show access-tunnel summary als de opdracht FED. Een mismatch kan wijzen op een verkeerde programmering.

Op het toegangspunt kunt u de creatie voor de toegangstunnel controleren met deze opdracht:

<#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

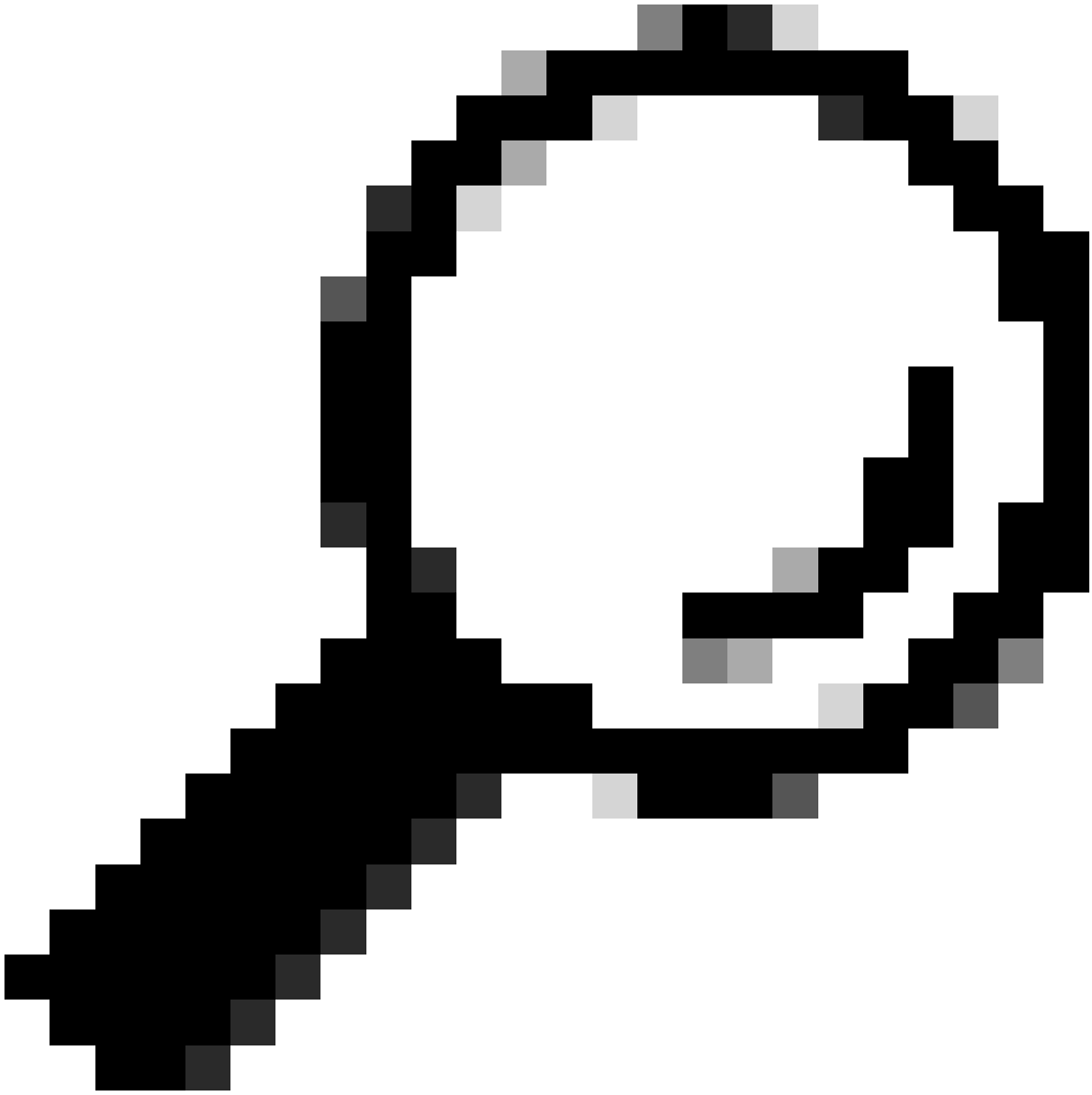
00:00:0C:9F:F2:80

```
 Forward
```

VXLAN

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

Het toegangspunt heeft een toegangstunnel die wijst naar de locator van de edge node 172.13.111.65. Het MAC-adres 00:00:0C:9F:F2:80 behoort tot Switch virtual interface (SVI) 99, het VLAN waarop het toegangspunt is aangesloten. Het inkapselingstype is VXLAN.



Tip: De tunnel wordt alleen op het toegangspunt weergegeven als er een actieve client is aangesloten. Anders geeft de opdracht een lege uitvoer terug.

Debugs en sporen

Voor geavanceerdere foutopsporing bij het maken van toegangstunnels kunt u deze sporen inschakelen op de rand van de stof:

```
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
```

Catalyst 9000 access-tunnel platform-afhankelijke opdrachten om de programmatie van de access-tunnel op fabric edge te verifiëren:

```
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>
```

Voor het debuggen van het proces voor de toegangstunnel op de WLC schakelt u de volgende opdrachten in:

```
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
```

Debugs voor het registratieproces. Deze opdrachten kunnen worden uitgevoerd op de edge node om te controleren of deze probeert het IP-adres en de Ethernet MAC van het toegangspunt te registreren, en op het controlevlak om te bevestigen of de registratie succesvol verloopt.

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

Samenvatting

- Access-tunnels in SD-Access zijn VXLAN-tunnels tussen fabric edge-nodes en toegangspunten die clientverkeer binnen de fabric vervoeren die is ingekapseld in VXLAN.
- Ze maken uniforme draadloze gegevensvlakken en consistente beleidshandhaving mogelijk omdat de tag voor de beveiligingsgroep (SGT) op het niveau van het toegangspunt is gecodeerd voor draadloze eindpunten.
- Verificatie en triage omvatten het controleren van de registratie op het fabric control-vlak, het bevestigen van de creatie op fabric edge-nodes en het verifiëren van de fabric-status voor het toegangspunt op de WLC met behulp van specifieke show-opdrachten.
- Problemen oplossen is erop gericht ervoor te zorgen dat tunnels correct worden gemaakt en stabiel blijven na configuratiewijzigingen.
- De toegangstunnel is het uiteindelijke doel bij het onboarden van een nieuw toegangspunt

tot SD-Access.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.