Analyse der Erstellung von Zugriffstunnels in SD-Access

Inhalt

Einleitung

Dieses Dokument beschreibt, was ein Zugriffstunnel in SD-Access ist, seinen Zweck und wie Sie die Bildung des Zugriffstunnels einschätzen können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Locator ID Separation Protocol (LISP)
- Wireless

Verwendete Komponenten

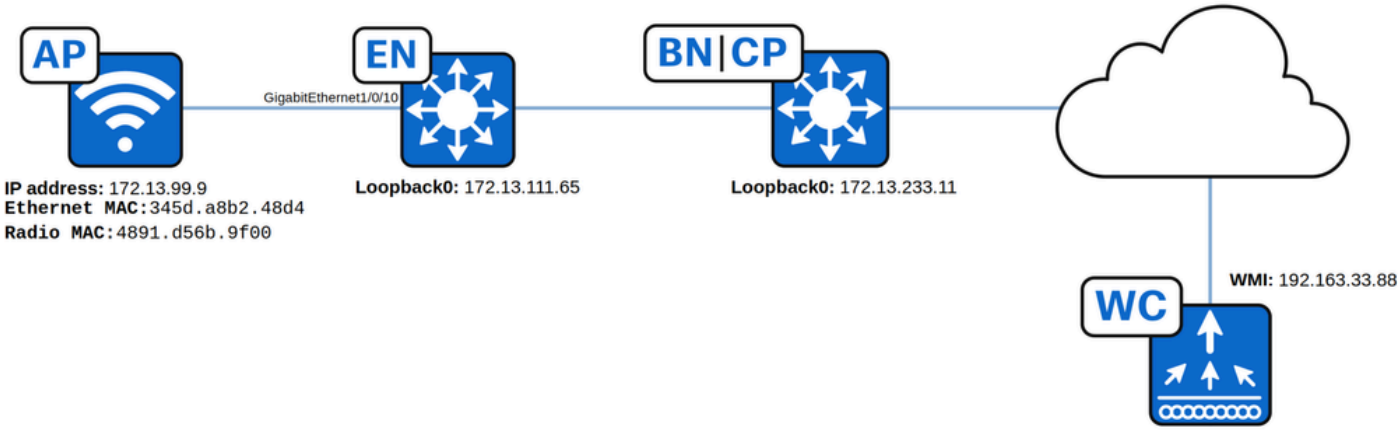
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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-Grenzknoten/Kontrollebene - C9500-48P, Cisco IOS® XE 17.12.05

- Cisco Access Point - C9130AXI-A, Version 17.9.5.47

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



Topologie in diesem Artikel

Überblick

Ein Zugriffstunnel in Cisco SD-Access ist ein Virtual Extensible LAN (VXLAN)-Tunnel, der zwischen Fabric Edge-Knoten und Access Points (APs) eingerichtet wird. Dieser Tunnel kapselt den Client-Datenverkehr in VXLAN und ermöglicht so die nahtlose Kommunikation innerhalb der SD-Access-Fabric. Der Zugriffstunnel dient als Überlagerung der Datenebene, die den Datenverkehr von mit dem Access Point verbundenen Wireless-Clients zum Fabric-Edge überträgt und so eine konsistente Richtliniendurchsetzung und -segmentierung im gesamten Netzwerk sicherstellt.

Entstehungsprozess eines Zugangstunnels

1. Der AP ist angeschlossen und wird über Power over Ethernet (PoE) hochgefahren.
2. AP bekommt über DHCP im Overlay eine IP-Adresse. Während dieses Vorgangs erhält der WAP auch die Option 43 vom DHCP-Server für den WLAN-Controller.
3. Fabric Edge registriert die IP-Adresse und Ethernet-MAC des AP und aktualisiert die LISP-Kontrollebene.
4. Der WLC fragt den LISP-CP ab, um zu erfahren, ob der AP mit einem Fabric-Gerät verbunden ist.
5. Die LISP-Kontrollebene antwortet dem WLC mit Locator (Loopback 0 IP) des Fabric-Geräts, an das der WAP angeschlossen ist. Wenn die Antwort "Ja" lautet, bedeutet dies, dass der Access Point mit dem Fabric verbunden und als Fabric aktiviert gekennzeichnet ist.
6. Der WLC führt eine L2-LISP-Registrierung für die AP-Radio-MAC auf der LISP-

Kontrollebene durch, zusammen mit Metadateninformationen vom WLC an die FE.
7. Die LISP-Kontrollebene benachrichtigt Fabric Edge und sendet die vom WLC empfangenen Metadaten. Diese Metadaten enthalten ein Flag, das angibt, dass es sich um einen Access Point und die IP-Adresse des Access Points handelt.
8. Fabric Edge verarbeitet die Informationen. Er erkennt, dass es sich um einen Access Point handelt, und erstellt einen VXLAN-Tunnel, der auch als Access Tunnel zwischen dem Access Point und dem Fabric Edge bezeichnet wird.

Lesen Sie diese Schritte durch, um sicherzustellen, dass der Zugriffstunnel für das AP-Onboarding in SD-Access erfolgreich erstellt wird. Wenn diese Prüfungen fehlschlagen, kann die Tunnelerstellung verhindert werden. Wenn ein Schritt nicht zu den erwarteten Ergebnissen führt, konzentrieren Sie die Fehlerbehebungsmaßnahmen auf die Komponente, die zu diesem Schritt gehört.

Überprüfen des Prozesses

Überprüfen Sie, ob der AP eine IP-Adresse erhält.

Führen Sie folgenden Befehl auf dem Edge-Knoten aus, um zu überprüfen, ob der Access Point eine IP-Adresse empfängt:

<#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)

Aus der vorherigen Ausgabe kann bestätigt werden, dass der mit der Schnittstelle GigabitEthernet 1/0/10 verbundene AP die IP-Adresse 172.13.99.9 im VLAN 99 hat, mit der Ethernet MAC-Adresse 345d.a8b2.48d4.
Wenn die Ausgabe leer ist, konnte der Access Point entweder keine IP-Adresse abrufen, oder Power over Ethernet (PoE) funktioniert nicht. Mit dem folgenden Befehl können Sie überprüfen, ob die MAC-Adresse des Access Points in der MAC-Adresstabelle angezeigt wird, um sicherzustellen, dass PoE betriebsbereit ist:

<#root>

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

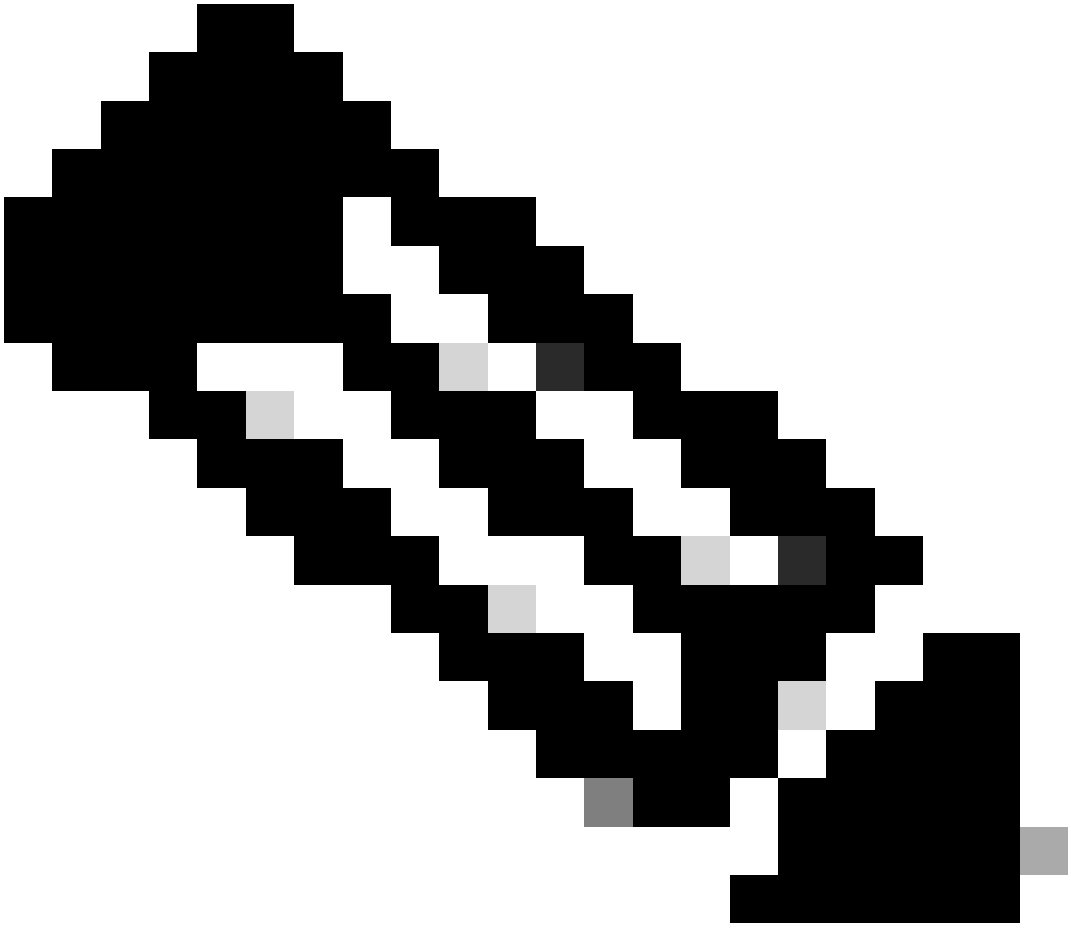
```
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----

99


345d.a8b2.48d4

 DYNAMIC

Gi1/0/10
```

Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Inline-Stromversorgung für PoE funktioniert:

<#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 ist betriebsbereit und arbeitet mit 30,0 Watt.



Anmerkung: Nach Erhalt einer IP-Adresse versucht der Access Point, dem Wireless LAN Controller (WLC) beizutreten, ähnlich wie bei herkömmlichen Netzwerken. Wenn der Access Point bei der Ausführung des Befehls show ap summary nicht aufgeführt ist, beheben Sie die Fehlerbehebung beim AP-Beitritt.

Überprüfen der IP- und Ethernet-MAC-Registrierung des AP auf der LISP-Kontrollebene

Führen Sie den folgenden Befehl aus, um die Steuerungsebene für das Fabric Edge zu identifizieren, die auch als Map Server bezeichnet wird:

<#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

Die Kontrollebene ist 172.13.233.11, was der Loopback0 für dieses Gerät wäre.

Eine weitere Möglichkeit zur Identifizierung der Kontrollebene für den Fabric-Standort besteht in der Ausführung des folgenden Befehls:

<#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

Auf dem WLC können Sie auch überprüfen, ob sich die LISP-Sitzung mit der Kontrollebene im UP-Status befindet:

<#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

Verwenden Sie diesen Befehl, um die auf der Kontrollebene registrierte IP-Adresse des AP zu finden:

<#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

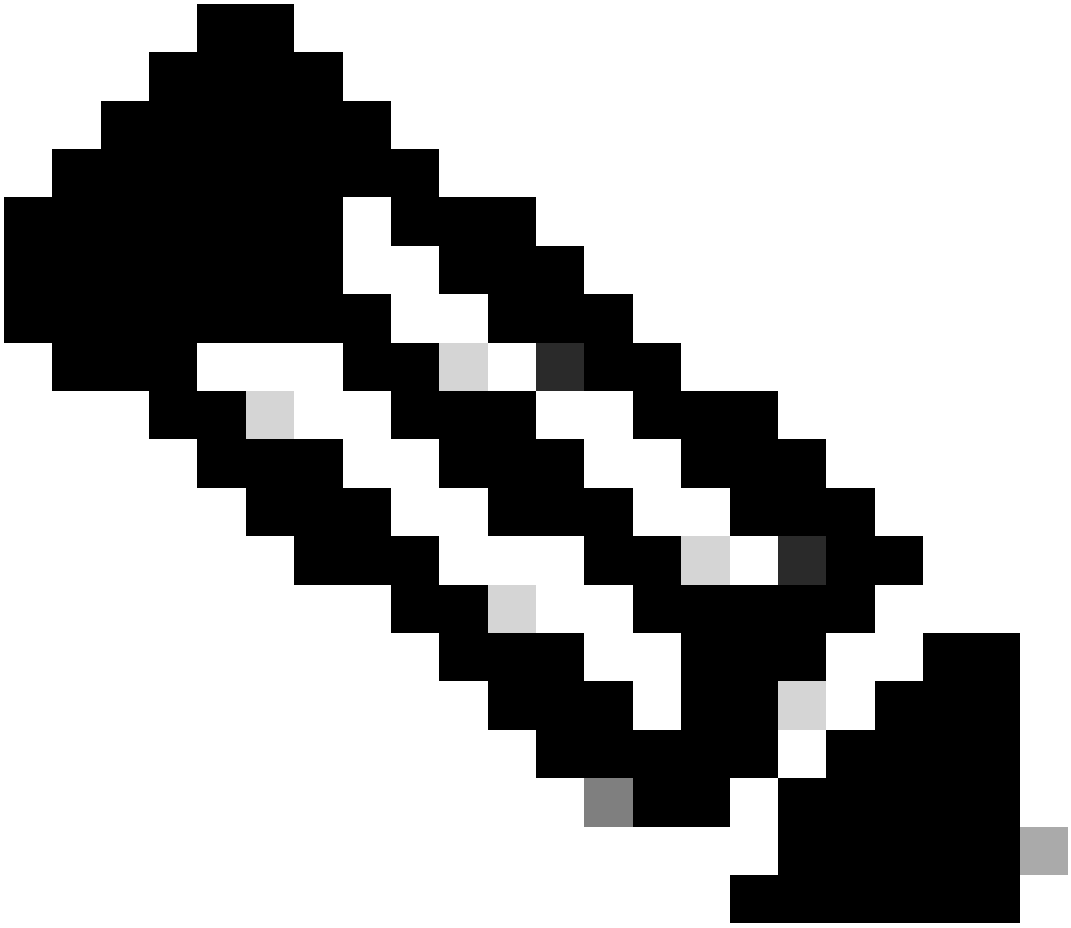
TTL 1d00h, no merge, hash-function sha1
state complete, no security-capability
...
Domain-ID 1559520338
Multihoming-ID unspecified
sourced by reliable transport

Locator

Local State Pri/Wgt Scope

172.13.111.65

yes up 10/10 IPv4 none



Anmerkung: APs verwenden immer INFRA_VN für Layer 3, und diese INFRA_VN ist immer der Instanz-ID 4097 zugeordnet.

Die Registrierung für den Access Point mit der IP-Adresse 172.13.99.9 ist abgeschlossen. Es treten keine Authentifizierungsfehler auf, und er ist mit dem Edge-Knoten 172.13.111.65 (Locator) verbunden.

Um zu überprüfen, ob die MAC-Adresse auf der Steuerungsebene registriert ist, geben Sie zunächst die Layer-2-Instanz-ID für das VLAN an, mit dem der WAP verbunden ist. Verwenden Sie folgende Befehle:

<#root>

Edge#show vlan id 99

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

99

```
 AP_VLAN active
L2LI0:8188
, Gi1/0/10, Ac0
...
```

VLAN 99 ist der Instanz-ID 8188 zugeordnet. Führen Sie unter Verwendung dieser Instanz-ID den folgenden Befehl aus, um zu überprüfen, ob die Ethernet-MAC-Adresse auf der Steuerungsebene registriert ist:

<#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
```

Die Registrierung für die Ethernet-MAC 345d.a8b2.48d4 des AP ist ohne Authentifizierungsfehler abgeschlossen und wird am Edge-Knoten 172.13.111.65 (Locator) angeschlossen.

Stellen Sie sicher, dass der WLC das Gerät als Fabric-fähig markiert.

<#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

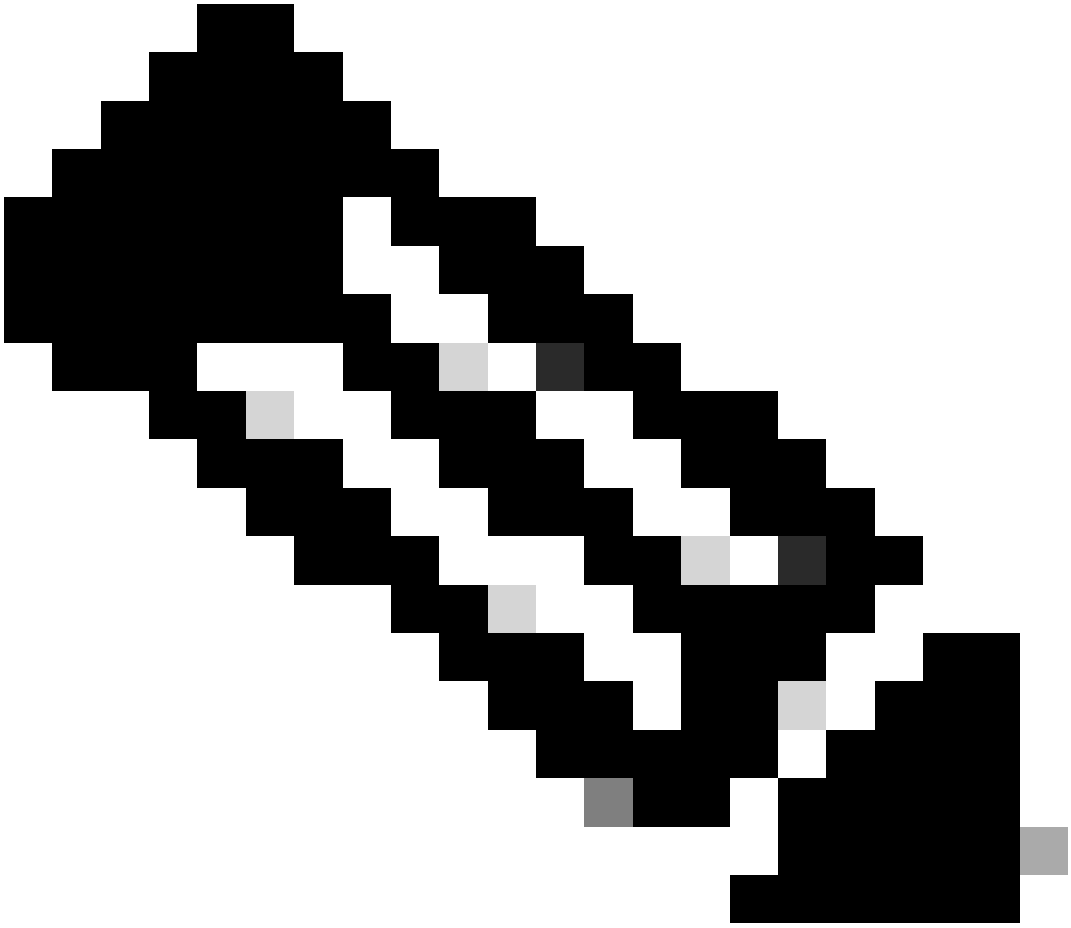
4891.d56b.9f00

default location MX

172.13.99.9

Registered

Der AP mit der IP-Adresse 172.13.99.9 ist korrekt als Fabric AP markiert. Wenn der WAP nicht aufgeführt ist, bedeutet dies, dass der WLC keine Antwort von der LISP-Kontrollebene erhalten hat. In dieser Ausgabe lautet die MAC-Adresse des WAP 4891.d56b.9f00.



Anmerkung: Wenn der Access Point auf der Steuerungsebene registriert, aber nicht als Fabric-aktiviert markiert ist, stellen Sie sicher, dass keine Firewall den LISP-Datenverkehr auf dem UDP-Port 4342 blockiert.

Überprüfen Sie die Radio MAC-Registrierung auf der LISP-Kontrollebene.

Verwenden Sie denselben Befehl, der zur Verifizierung der Registrierung der Ethernet-MAC-Adresse verwendet wurde, ersetzen Sie jedoch die Ethernet-MAC-Adresse durch die Funk-MAC-Adresse:

<#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
```

Die MAC-Adresse der Funkeinheit ist vollständig registriert, ohne dass Authentifizierungsfehler auftreten, und sie ist mit dem Edge-Knoten 172.13.111.65 (Locator) verbunden. Die Ausgabe zeigt auch das WLC-AP-Bit an: Set: Ein Flag, das von der LISP-Kontrollebene verwendet wird, um dem Edge-Knoten anzuzeigen, dass diese Registrierung zu einem AP im RLOC 172.13.111.65 gehört.

Überprüfen der Erstellung des Zugriffstunnels

Der letzte Schritt besteht darin, die Erstellung des Zugriffstunnels am Fabric-Edge zu überprüfen. Wie bereits erwähnt, ist dies das eigentliche Ziel der Integration von APs in SD-Access. Führen Sie den folgenden Befehl aus, um die Erstellung des Zugriffstunnels zu überprüfen:

<#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
```

Zugangstunnel 0 verbindet AP 172.13.99.9 mit Edge Node Locator 172.13.111.65 und ist seit 51 Sekunden aktiv. Der Timer wird nach jedem Zurücksetzen auf 0 gesetzt.

Sie können auch bestätigen, dass der Tunnel auf der Abstraktionsebene des Forwarding Engine Driver (FED) programmiert ist, die direkt mit der Switch-Hardware verbunden ist:

<#root>

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


Interface    IF_ID        State
----------------------------------------------------------------------

Ac0

0x00000058

  READY
```

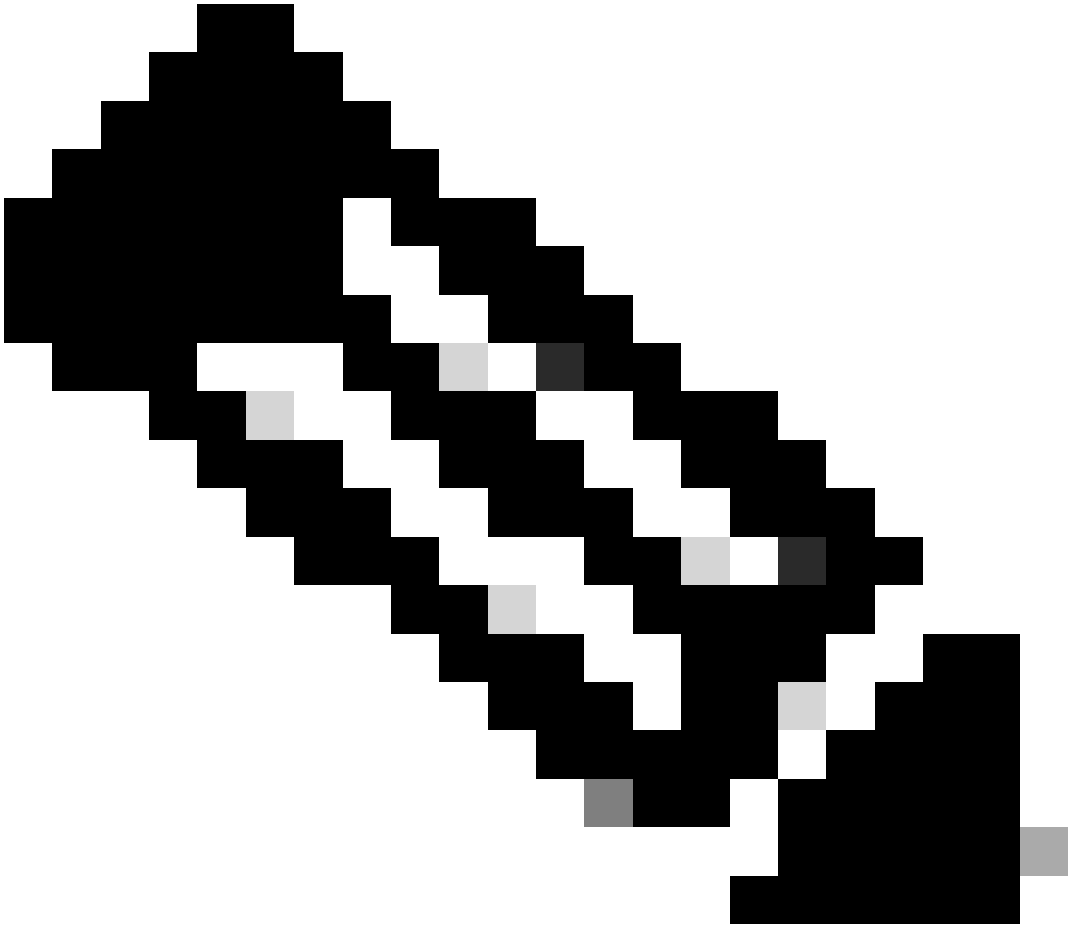
Weitere Informationen zu diesem Tunnel finden Sie unter IF_ID:

<#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
...
```

Hierbei handelt es sich um einen L2-lisp-Tunnel mit VXLAN-Kapselung. Der Schnittstellentyp lautet access-tunnel.



> Anmerkung: Es ist wichtig, dass die Anzahl der Zugriffstunnel in der Ausgabe des Befehls show access-tunnel summary und des Befehls FED übereinstimmt. Eine Nichtübereinstimmung kann auf eine Fehlprogrammierung hinweisen.

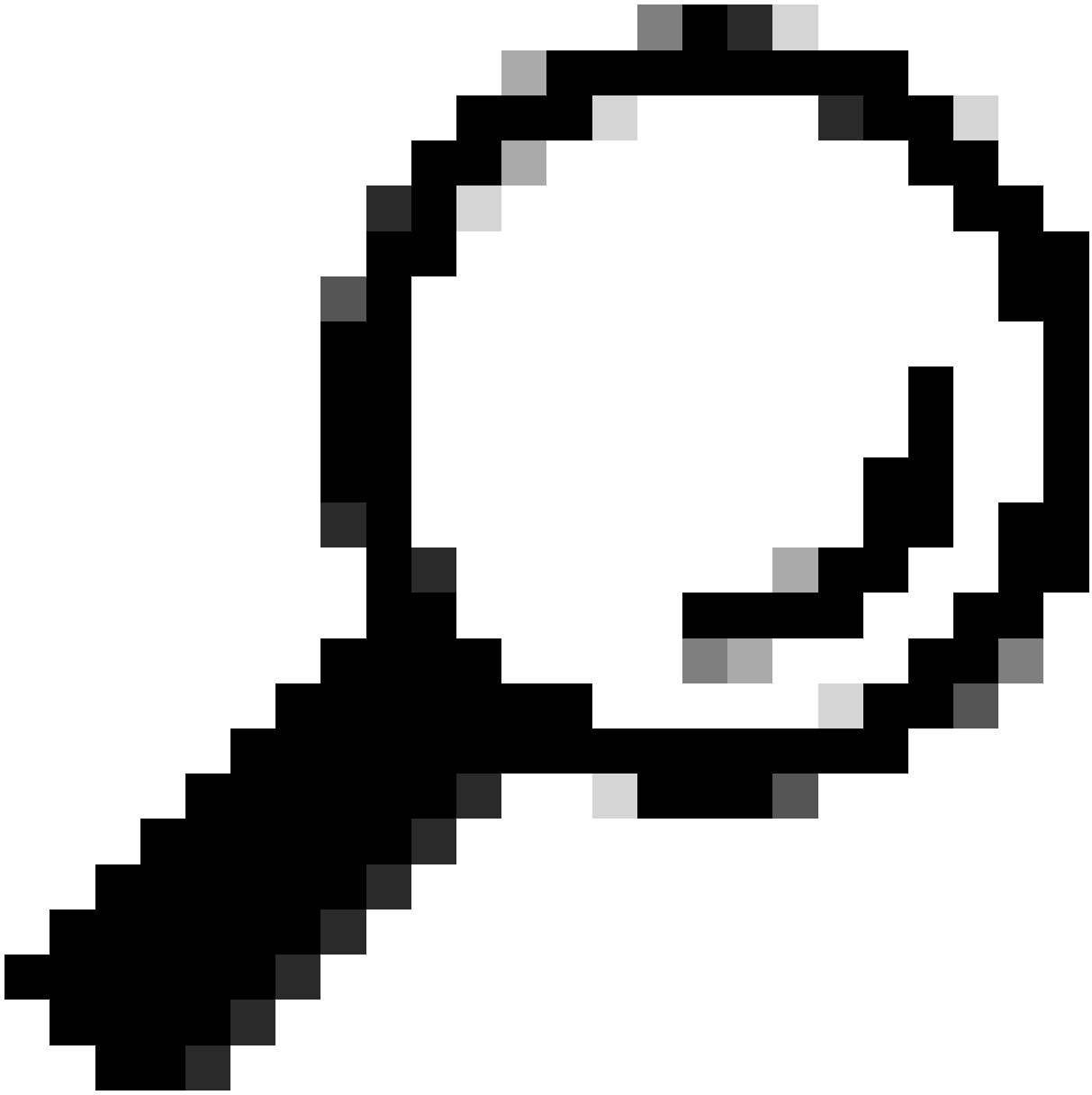
Auf dem Access Point können Sie die Erstellung des Zugriffstunnels mit dem folgenden Befehl

überprüfen:

<#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
```

Der Access Point verfügt über einen Zugriffstunnel, der auf den Locator 172.13.111.65 des Edge-Knotens verweist. Die MAC-Adresse 00:00:0C:9F:F2:80 gehört zu Switch Virtual Interface (SVI) 99, dem VLAN, mit dem der Access Point verbunden ist. Der Kapselungstyp ist VXLAN.



Tipp: Der Tunnel wird nur dann auf dem Access Point angezeigt, wenn ein aktiver Client angeschlossen ist. Andernfalls gibt der Befehl eine leere Ausgabe zurück.

Debuggen und Ablaufverfolgungen

Um das Debugging bei der Erstellung von Zugriffstunneln weiter zu verfeinern, aktivieren Sie die folgenden Ablaufverfolgungen am Fabric-Edge:

```
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
```

Plattformabhängige Befehle für Catalyst 9000 Access-Tunnel zur Verifizierung der Access-Tunnel-Programmierung am Fabric-Edge:

```
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>
```

Um den Prozess für den Zugriffstunnel auf dem WLC zu debuggen, aktivieren Sie folgende Befehle:

```
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
```

Debuggen für den Registrierungsprozess. Diese Befehle können auf dem Edge-Knoten ausgeführt werden, um zu überprüfen, ob versucht wird, die IP-Adresse und die Ethernet-MAC des Access Points zu registrieren. Auf der Kontrollebene kann überprüft werden, ob die Registrierung erfolgreich durchgeführt wurde.

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

Zusammenfassung

- Zugriffstunnel in SD-Access sind VXLAN-Tunnel zwischen Fabric Edge-Knoten und Access Points, die Client-Datenverkehr innerhalb der in VXLAN gekapselten Fabric übertragen.
- Sie ermöglichen einheitliche Wireless-Datenebenen und die konsistente Durchsetzung von Richtlinien, da das Security Group Tag (SGT) auf Access Point-Ebene für Wireless-Endgeräte gekennzeichnet ist.
- Verifizierung und Triage umfassen die Überprüfung der Registrierung auf der Fabric-Kontrollebene, die Bestätigung der Erstellung an den Fabric-Edge-Knoten und die Verifizierung des Fabric-Status des AP auf dem WLC mithilfe spezifischer Befehle zum Anzeigen.
- Die Fehlerbehebung soll sicherstellen, dass Tunnel korrekt erstellt werden und auch nach

Konfigurationsänderungen stabil bleiben.

- Beim Einbinden eines neuen AP in SD-Access ist der Zugriffstunnel das letzte Ziel.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.