

Entender a criação de túnel de acesso no SD-Access

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia](#)

[Overview](#)

[Processo de formação do túnel de acesso](#)

[Verificar o processo](#)

[Verifique se o AP obtém um endereço IP](#)

[Verificar o registro IP e MAC Ethernet do AP no plano de controle LISP](#)

[Verifique se a WLC está marcando o dispositivo como habilitado para estrutura](#)

[Verifique o registro MAC do rádio no plano de controle do LISP](#)

[Verifique a criação do túnel de acesso](#)

[Depurações e Rastreamentos](#)

[Summary](#)

Introdução

Este documento descreve o que é um túnel de acesso no SD-Access, sua finalidade e como você pode fazer a triagem da formação do túnel de acesso.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo de separação de ID de localizador (LISP)
- Tecnologia Wireless

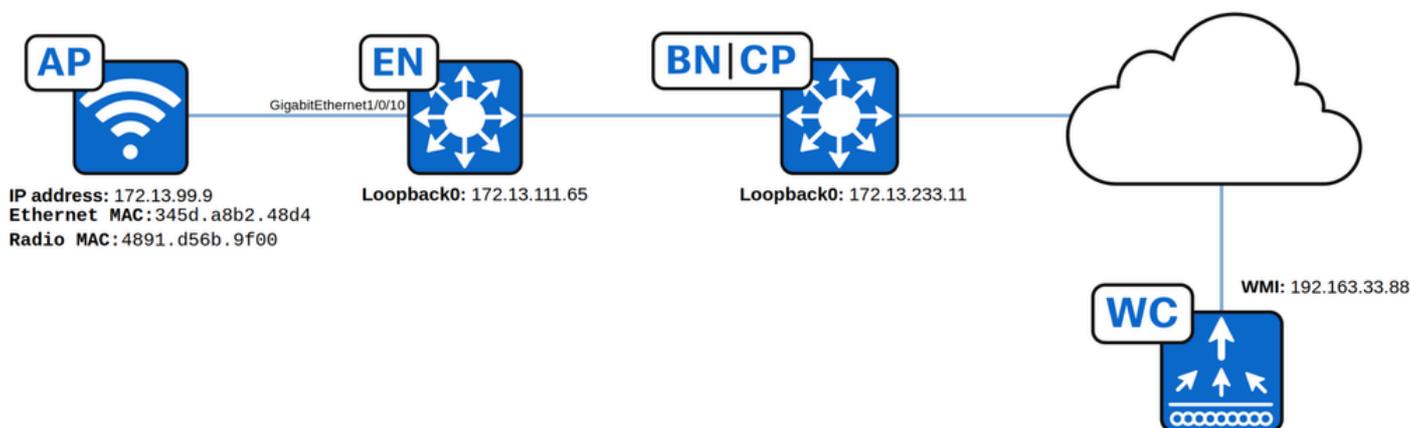
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controladora de LAN sem fio (WLC) da Cisco - C9800-CL, Cisco IOS® XE 17.12.04
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- Nó de borda SDA/Plano de controle - C9500-48P, Cisco IOS® XE 17.12.05
- Cisco Access Point - C9130AXI-A, versão 17.9.5.47

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia



Topologia usada neste artigo

Overview

Um túnel de acesso no Cisco SD-Access é um túnel Virtual Extensible LAN (VXLAN) estabelecido entre nós de borda de estrutura e Pontos de Acesso (APs). Esse túnel encapsula o tráfego do cliente em VXLAN, permitindo comunicação transparente dentro da estrutura SD-Access. O túnel de acesso serve como uma sobreposição de plano de dados que transporta o tráfego de clientes sem fio conectados ao ponto de acesso até a borda da malha, garantindo a aplicação consistente de políticas e a segmentação em toda a rede.

Processo de formação do túnel de acesso

1. O AP está conectado e é ligado via Power over Ethernet (PoE).
2. O AP obtém um endereço IP via DHCP na sobreposição. Durante esse processo, o AP também recebe a opção 43 do servidor DHCP para o Wireless LAN Controller.
3. A borda da estrutura registra o endereço IP e o MAC Ethernet do AP e atualiza o plano de controle do LISP.
4. A WLC consulta o PC LISP para saber se o AP está conectado a um dispositivo de estrutura.
5. O plano de controle LISP responde à WLC com o localizador (Loopback 0 IP) do dispositivo de estrutura que tem o AP conectado. Se houver uma resposta, significa que o AP está conectado à estrutura e marcado como Fabric enabled.
6. A WLC faz um registro L2 LISP para o MAC de rádio AP no plano de controle LISP junto com informações de metadados da WLC para o FE.
7. O plano de controle LISP notifica a borda da malha e envia os metadados recebidos da WLC. Esses metadados contêm um sinalizador que indica que é um AP e o endereço IP do

AP.

8. A borda da malha processa as informações. Ele aprende que é um AP e cria um túnel VXLAN também conhecido como túnel de acesso entre o AP e a borda da estrutura.

Leia essas etapas para garantir a formação bem-sucedida do túnel de acesso para integração de AP no SD-Access. Qualquer falha nessas verificações pode impedir a criação do túnel. Se uma etapa não produzir os resultados esperados, concentre os esforços de identificação e solução de problemas no componente relacionado a essa etapa.

Verificar o processo

Verifique se o AP obtém um endereço IP

Para verificar se o AP recebe um endereço IP, execute este comando no nó de borda:

```
<#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)
```

A partir da saída anterior, pode-se confirmar que o AP conectado à interface GigabitEthernet 1/0/10 tem o endereço IP 172.13.99.9 na VLAN 99, com o endereço MAC Ethernet 345d.a8b2.48d4.

Se a saída estiver vazia, o AP não conseguiu obter um endereço IP ou o Power over Ethernet (PoE) não está funcionando. Para confirmar se o PoE está operacional, verifique se o endereço MAC do ponto de acesso é exibido na tabela de endereços MAC, executando este 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
```

Para confirmar que a alimentação em linha para PoE está operacional, execute este 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

O PoE está operacional e funcionando a 30,0 watts.



Note: Depois de obter um endereço IP, o access point tenta se unir à controladora Wireless LAN (WLC), semelhante à rede tradicional. Se o AP não estiver listado ao executar o comando `show ap summary`, solucione os problemas de junção de AP.

Verificar o registro IP e MAC Ethernet do AP no plano de controle LISP

Para identificar o plano de controle, também conhecido como servidor de mapa, para a borda da malha, execute o 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
```

O plano de controle é 172.13.233.11, que seria o loopback0 para esse dispositivo.

Outra maneira de identificar o plano de controle para o site de estrutura é executar este 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
```

Na WLC, você também pode verificar se a sessão LISP com o plano de controle está no estado 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
```

Use este comando para encontrar o IP do AP registrado no plano de controle:

```
<#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

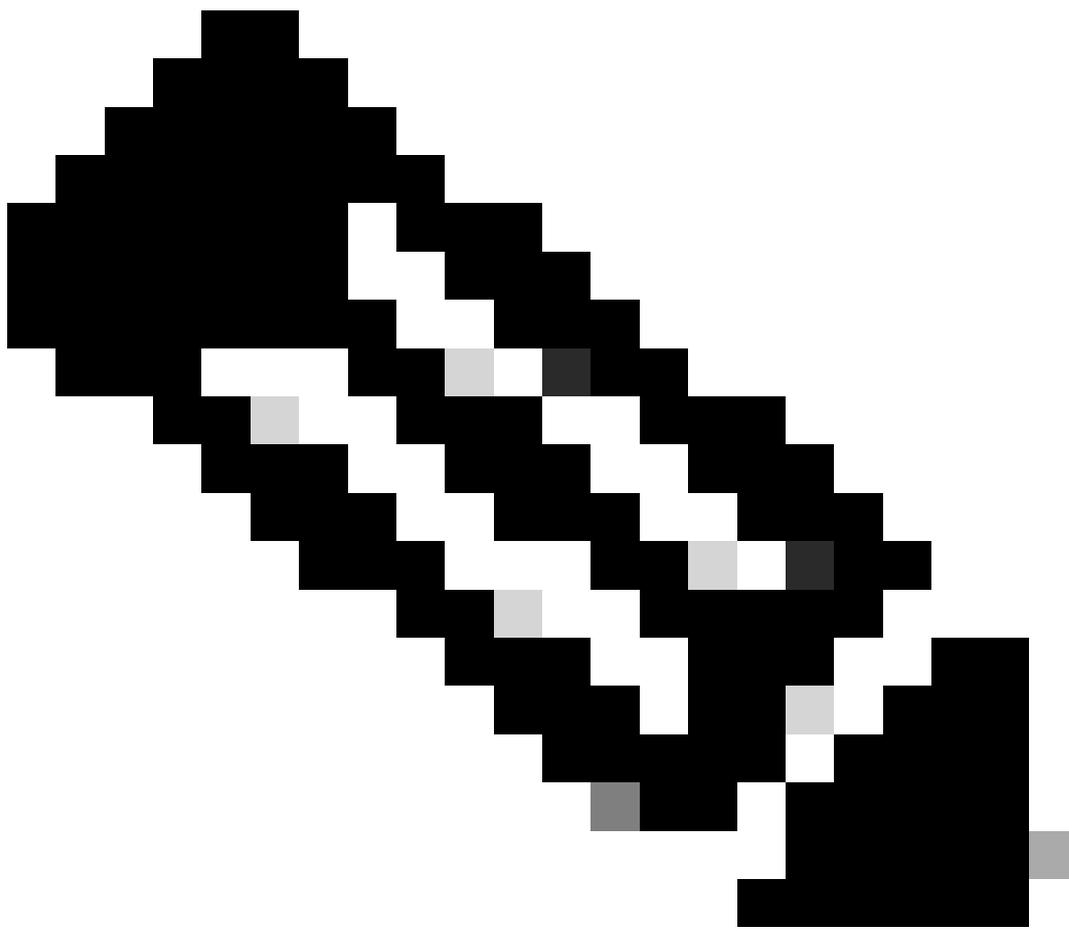
sourced by reliable transport

Locator

Local State Pri/Wgt Scope

172.13.111.65

yes up 10/10 IPv4 none



Note: Os APs sempre usam o INFRA_VN para a Camada 3, e este INFRA_VN é sempre mapeado para a ID de instância 4097.

O registro foi concluído para o AP com endereço IP 172.13.99.9. Não há falhas de autenticação e ele está conectado ao nó de borda 172.13.111.65 (Localizador).

Para verificar se o endereço MAC está registrado no plano de controle, primeiro, identifique o ID de instância da Camada 2 para a VLAN à qual o AP está conectado. Use estes comandos:

```
<#root>
```

```
Edge#show vlan id 99
```

```
VLAN Name Status Ports
```

```
-----
```

```
99
```

```
AP_VLAN active
```

```
L2LI0:8188
```

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

```
...
```

A VLAN 99 está mapeada para a ID de instância 8188. Usando esse ID de instância, execute este comando para confirmar se o endereço MAC Ethernet está registrado no plano de controle:

```
<#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
```

O registro para o MAC Ethernet 345d.a8b2.48d4 do AP é concluído sem falhas de autenticação e é conectado no nó de borda 172.13.111.65 (Localizador).

Verifique se a WLC está marcando o dispositivo como habilitado para estrutura

```
<#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
```

O AP com endereço IP 172.13.99.9 está marcado corretamente como um AP de estrutura. Se o AP não estiver listado, indica que a WLC falhou ao receber uma resposta do plano de controle LISP. Nesta saída, o endereço MAC de rádio para o AP é 4891.d56b.9f00.



Note: Se o AP estiver registrado no plano de controle, mas não estiver marcado como habilitado para estrutura, certifique-se de que nenhum firewall esteja bloqueando o tráfego LISP na porta UDP 4342.

Verifique o registro MAC do rádio no plano de controle do LISP

Use o mesmo comando que foi usado para verificar o registro do endereço MAC Ethernet, mas substitua o endereço MAC Ethernet pelo endereço MAC de rádio:

```
<#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
```

O endereço MAC do rádio é totalmente registrado sem nenhuma falha de autenticação e é conectado ao nó de borda 172.13.111.65 (Localizador). A saída também mostra o bit AP de WLC: Set, uma flag usada pelo plano de controle LISP para indicar ao nó de borda que esse registro pertence a um AP em seu RLOC 172.13.111.65.

Verifique a criação do túnel de acesso

A etapa final é verificar a criação do túnel de acesso na borda da estrutura. Como dito anteriormente, esse é o objetivo final da integração do AP no SD-Access. Para verificar a criação do túnel de acesso, execute este 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

O túnel de acesso 0 conecta o AP 172.13.99.9 ao localizador de nó de borda 172.13.111.65 e permanece ativo por 51 segundos. O temporizador é definido como 0 após cada reinicialização.

Você também pode confirmar se o túnel está programado na camada de abstração do Forwarding Engine Driver (FED), que faz a interface diretamente com o hardware do switch:

<#root>

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

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

```
Ac0  
0x00000058  
    READY
```

Usando o IF_ID, você pode encontrar mais informações sobre este túnel:

<#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
```

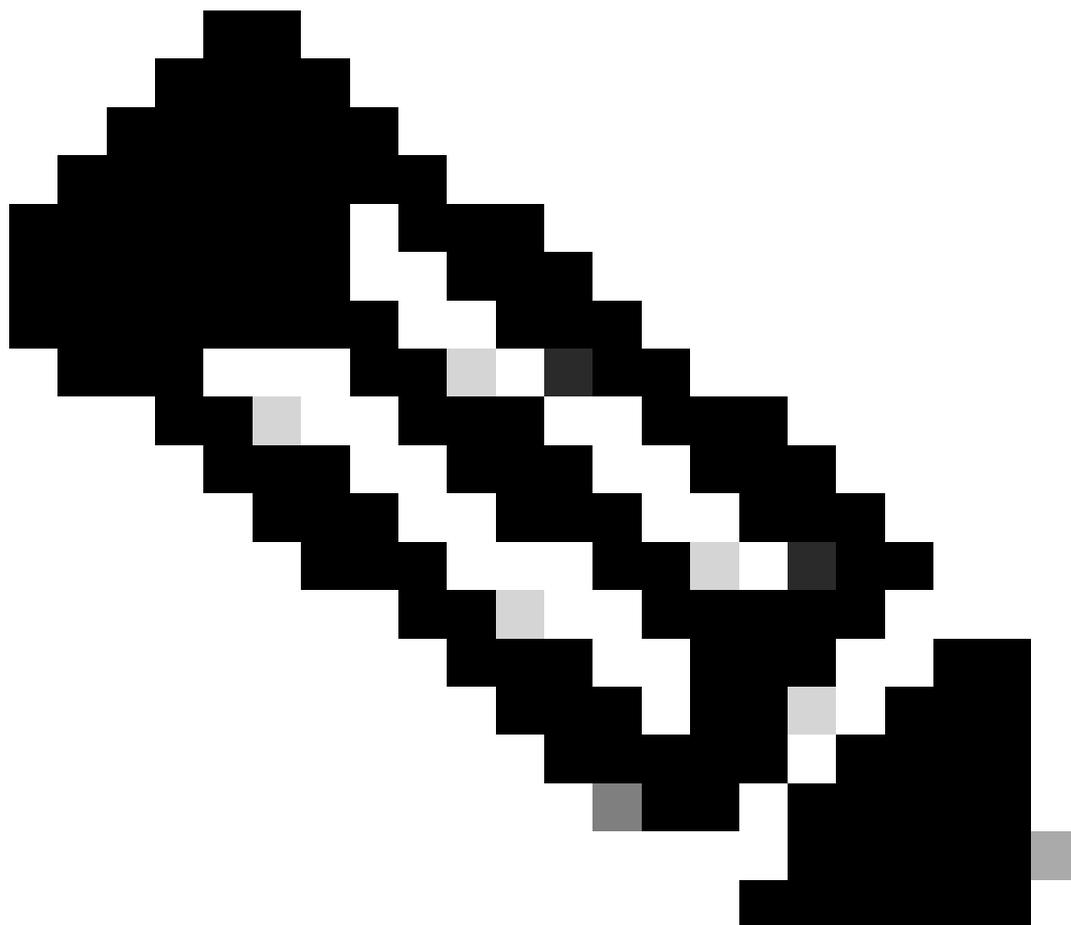
```
Interface State : Enabled
```

...

```
Interface Type : ACCESS_TUNNEL
```

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

Esse é um túnel L2 lisp usando encapsulamento VXLAN e o tipo de interface é access-tunnel.



Note: É importante que o número de túneis de acesso corresponda à saída do comando `show access-tunnel summary` e do comando FED. Uma incompatibilidade pode indicar uma programação incorreta.

No AP, você pode verificar a criação do túnel de acesso com este 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
```

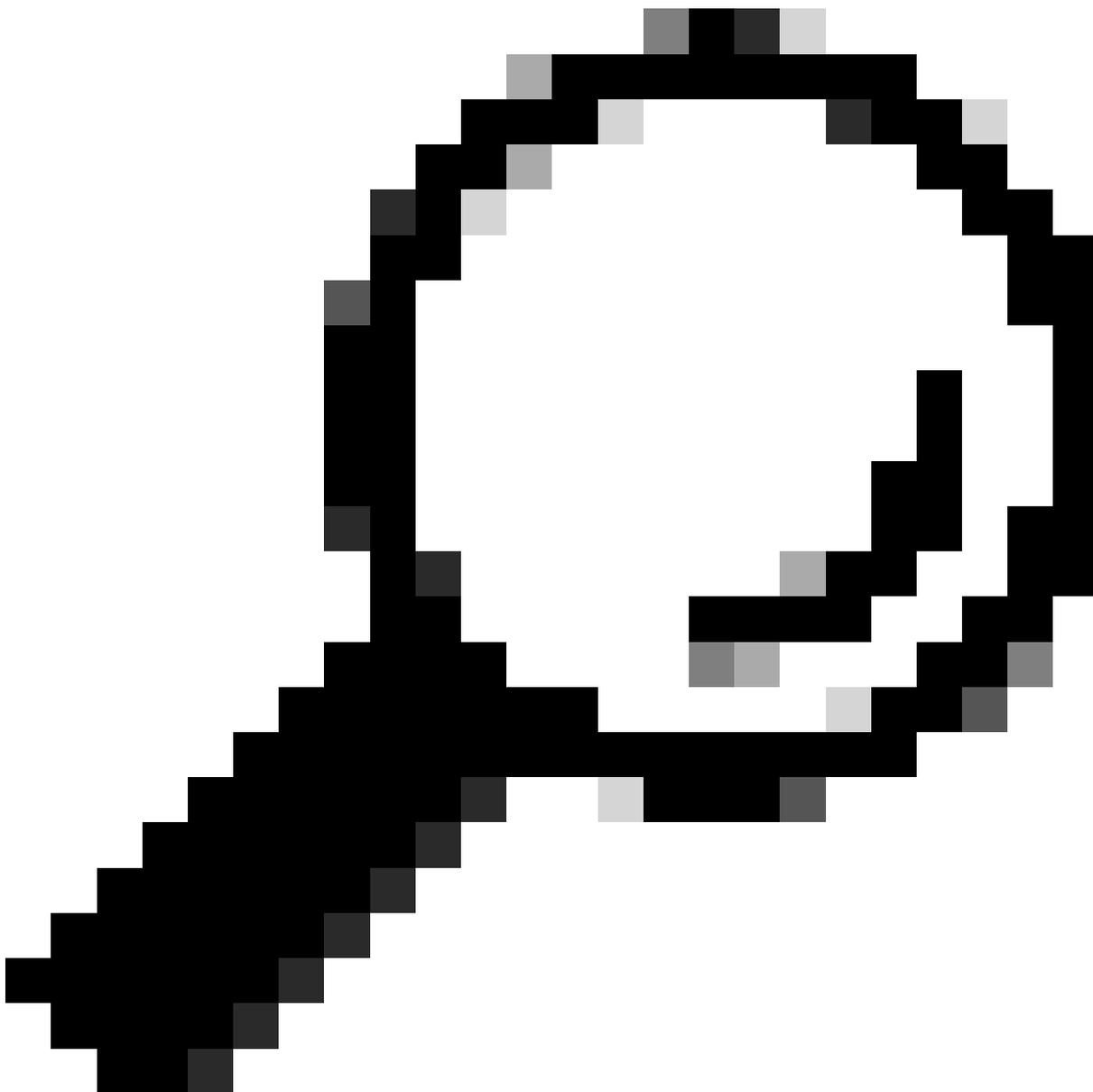
```
121
```

```
17096 239 35041
```

```
AP APP Fabric Information:
```

```
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC
```

O AP tem um túnel de acesso que aponta para o localizador 172.13.111.65 do nó de borda. O endereço MAC 00:00:0C:9F:F2:80 pertence à interface virtual do Switch (SVI) 99, que é a VLAN onde o AP está conectado. O tipo de encapsulamento é VXLAN.



Tip: O túnel aparece no AP somente quando um cliente ativo está conectado. Caso contrário, o comando retornará uma saída vazia.

Depurações e Rastreamentos

Para uma depuração mais avançada da criação do túnel de acesso, habilite estes rastreamentos na borda da estrutura:

```
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
```

Comandos dependentes da plataforma do túnel de acesso do Catalyst 9000 para verificar a programação do túnel de acesso na borda da estrutura:

```
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>
```

Para depurar o processo para o túnel de acesso na WLC, habilite estes comandos:

```
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
```

Depurações para o processo de registro. Esses comandos podem ser executados no nó de borda para verificar se ele está tentando registrar o endereço IP do AP e o MAC Ethernet, e no plano de controle para confirmar se o registro está ocorrendo com êxito.

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

Summary

- Túneis de acesso em SD-Access são túneis VXLAN entre nós de borda de estrutura e pontos de acesso que transportam o tráfego de cliente dentro da estrutura encapsulada em VXLAN.
- Eles permitem planos de dados sem fio unificados e aplicação consistente de políticas, pois a marcação de grupo de segurança (SGT) é marcada no nível do ponto de acesso para terminais sem fio.
- A verificação e a triagem envolvem a verificação do registro no plano de controle da estrutura, a confirmação da criação nos nós de borda da estrutura e a verificação do status da estrutura para o AP na WLC usando comandos show específicos.
- A solução de problemas se concentra em garantir que os túneis sejam criados corretamente e permaneçam estáveis após as alterações de configuração.
- O túnel de acesso é o objetivo final ao integrar um novo AP ao SD-Access.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.