# Dynamische SGT/L2VNID-toewijzing op draadloze SDA begrijpen

## Inhoud



## Inleiding

Dit document beschrijft het proces van Dynamic SGT en L2VDI-toewijzing op Fabric Enabled Wireless 802.1x SID's.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Remote Verificatie-inbelgebruikersservice (RADIUS)
- Draadloze LAN-controller (WLC)
- Identity Services Engine (ISE)
- Security Group Tag (SGT)
- L2VNID (Layer 2 Virtual Network Identifier)
- SD-Access fabric enabled draadloos (SDA LITTLE)
- Locator/ID-scheidingsprotocol (LISP)
- Virtual eXtensible Local Area Network (VXLAN)
- Fabric Control Plane (CP) en Edge Node (EN)
- Catalyst Center (CatC, voorheen bekend als Cisco DNA Center)

### Gebruikte componenten

WLC 9800 Cisco IOS® XE versie 17.6.4

Cisco IOS® XE

ISE-versie 2.7

CatC versie 2.3.5.6

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.

# Achtergrondinformatie

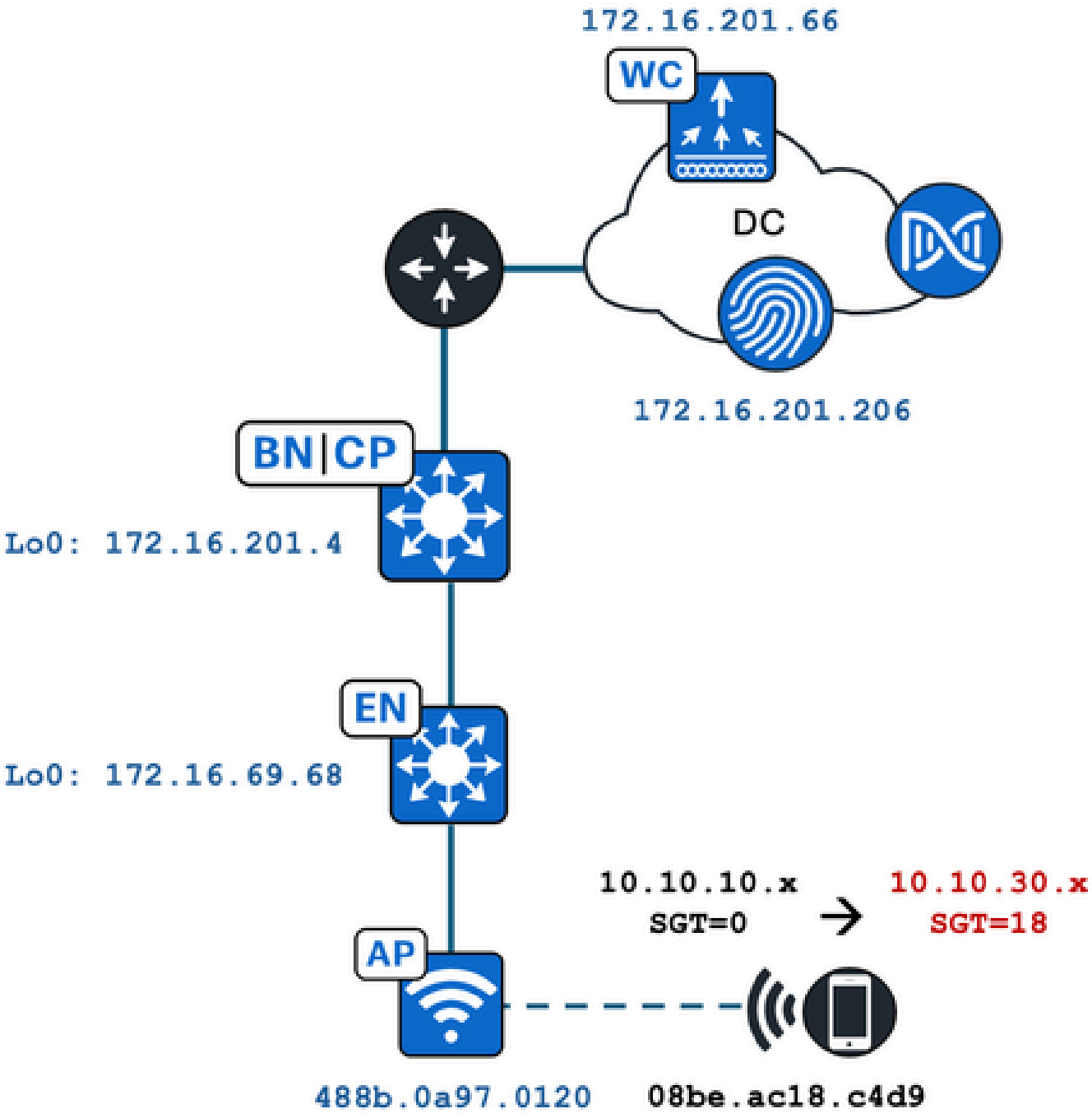
Een van de belangrijkste aspecten van SD-Access is de micro-segmentatie binnen een VN die via de schaalbare groepen wordt bereikt.

De SGT kan statisch per fabric enabled WLAN of SSID worden toegewezen (hoewel ze niet hetzelfde zijn, heeft hun verschil geen invloed op het hoofddoel van dit document, dus gebruiken we onderling verwisselbaar de twee termen voor dezelfde betekenis om de leesbaarheid te vergroten). In veel echte implementaties zijn er echter vaak gebruikers die verbinding maken met hetzelfde WLAN die een andere reeks beleid of netwerkinstellingen vereisen. Bovendien is het in sommige scenario's nodig om verschillende IP-adressen toe te wijzen aan specifieke clients binnen dezelfde Fabric WLAN om specifieke IP-gebaseerde beleidslijnen op deze clients toe te passen of aan de IP-adresseringsvereisten van het bedrijf te voldoen. L2VNID (Layer 2 Virtual Network Identifier) is de parameter die de WEINIGE infrastructuur gebruikt om draadloze gebruikers in verschillende subnetbereiken te plaatsen. De Access points verzenden de L2VNID in de VxLAN-header naar het Fabric Edge Node (EN), die deze vervolgens correleert met het corresponderende L2 VLAN.

Om deze granulariteit te bereiken binnen hetzelfde WLAN, wordt Dynamic SGT en/of L2VID-toewijzing gebruikt. De WLC verzamelt de identiteitsinformatie van het eindpunt, stuurt het naar ISE voor authenticatie, die het gebruikt om het juiste beleid te matchen dat op deze client moet worden toegepast en retourneert de SGT en/of L2VNID informatie na succesvolle authenticatie.

# Topologie

Om te begrijpen hoe dit proces werkt, hebben we een voorbeeld ontwikkeld met behulp van deze laboratoriumtopologie:




In dit voorbeeld is het WLAN statisch geconfigureerd met:

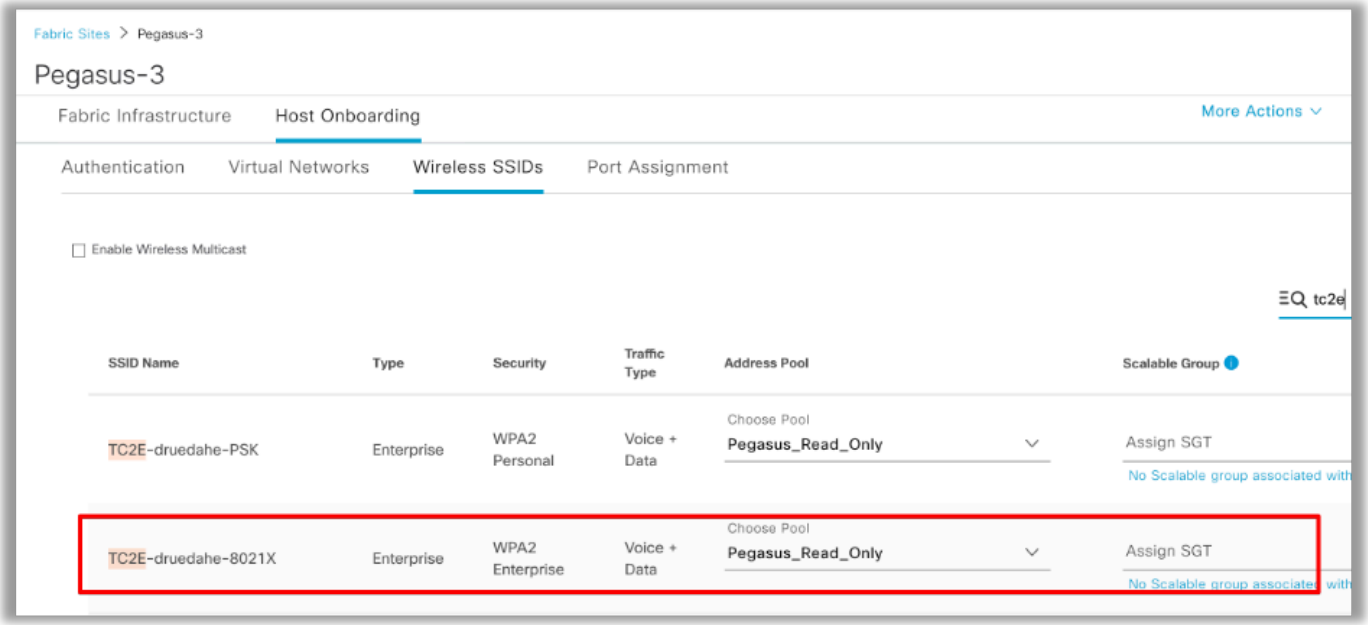
- L2VNID = 8198 / IP-poolnaam = Pegasus_Read_Only —> VLAN 1030 (10.10.10.x)
- Geen SGT

De draadloze client die er verbinding mee maakt, krijgt dynamisch deze parameters:

- L2VNID = 8199 / IP-poolnaam = 10_10_30_0-READONLY_VN —> VLAN 1031 (10.10.30.x)
- SGT = 18

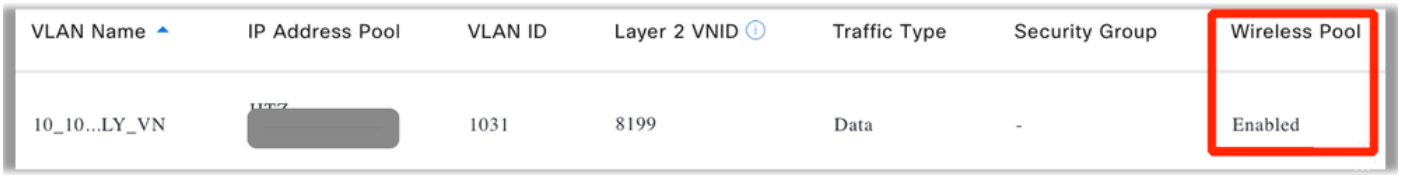
## Configuratie

Eerst moeten we het betrokken WLAN identificeren en controleren hoe het is geconfigureerd. In dit voorbeeld wordt de "TC2E-duredahe-802.1x" SSID gebruikt. Op het moment van dit document redactie, SDA wordt alleen ondersteund via CatC, dus we moeten controleren wat er is geconfigureerd. Onder Provision/SD-Access/Fabric Sites/<specifieke Fabric-site>/Host Onboarding/draadloze SSID's:




De SSID heeft de IP Pool genoemd "Pegasus_Read_Only" in kaart gebracht en heeft geen SGT statisch toegewezen wat SGT=0 betekent. Dit betekent dat, als een draadloze client verbinding maakt en met succes wordt geverifieerd zonder dat ISE attributen terugstuurt voor dynamische toewijzing, dit de draadloze clientinstellingen zijn.

De pool die dynamisch wordt toegewezen moet voorafgaand in de configuratie aanwezig zijn WLC. En dit wordt gedaan door de IP-pool toe te voegen als "Draadloze Pool" in het Virtuele Netwerk op de CatC:




In de WLC GUI onder Configuration/Wireless/Fabric geeft deze instelling op deze manier weer:


De "Pegasus_Read_Only"-pool komt overeen met de 8198 L2VNID en we willen dat onze klant op de 8199 L2VNID staat, wat betekent dat ISE de WLC moet vertellen om de "10_10_30_0-READONLY_VN"-pool voor deze client te gebruiken. Het is de moeite waard om te onthouden dat de WLC geen configuratie bevat voor de Fabric VLAN's. Zij is alleen bekend met de L2VNID's. Elke wordt vervolgens toegewezen aan een specifiek VLAN in de SDA Fabric ENs.

## Verificatie

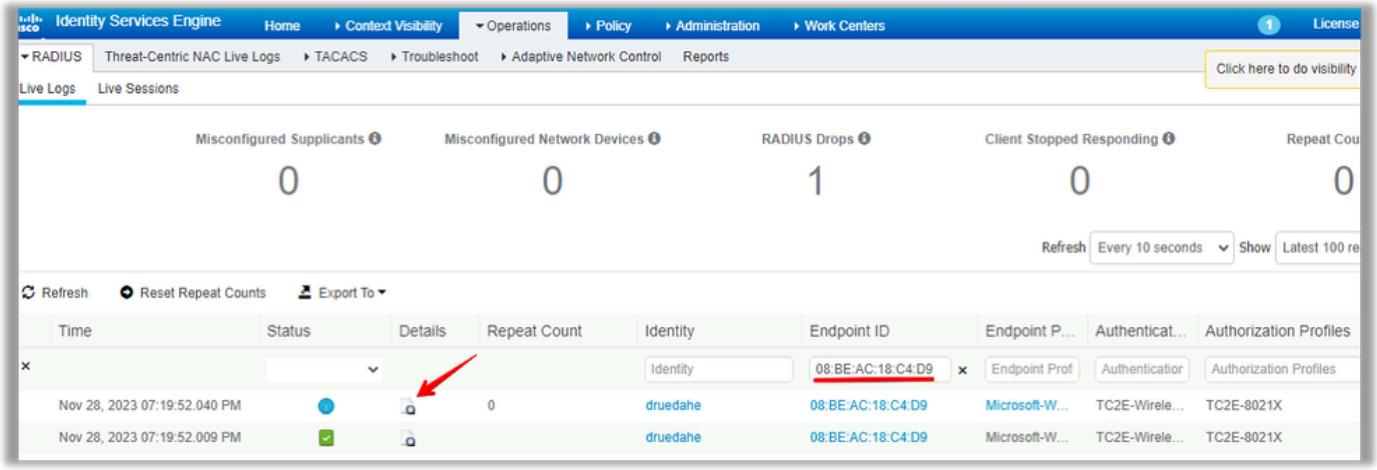
De gemelde symptomen voor problemen met betrekking tot de dynamische toewijzing van SGT/L2VNID zijn:

1. SG-beleid wordt niet afgedwongen op draadloze clients die verbinding maken met een specifiek WLAN. (probleem met dynamische SGT-toewijzing).
2. Draadloze clients verkrijgen geen IP-adres via DHCP, of ze verkrijgen geen IP-adres uit het gewenste subnetbereik bij een specifiek WLAN. (Dynamisch L2VID-toekenningsprobleem).

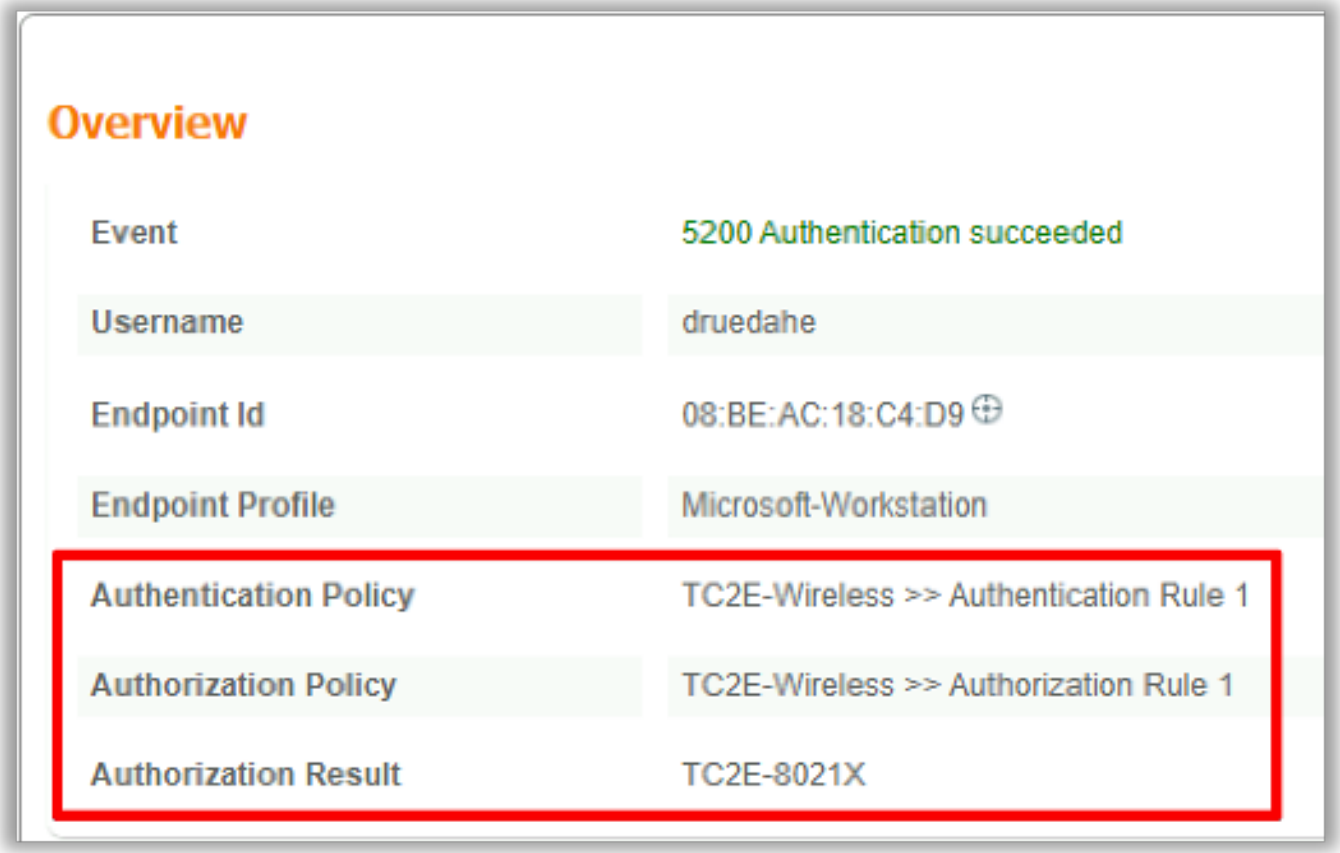
Nu wordt de verificatie van elk relevant knooppunt in dit proces beschreven.

## ISE-verificatie

Het uitgangspunt is ISE. Ga naar de ISE GUI onder Operation/RADIUS/Live Logs/ en gebruik het mac-adres van de draadloze client als filter in het veld Endpoint ID en klik vervolgens op het pictogram Details:




Vervolgens wordt een ander tabblad geopend met de verificatiedetails. We zijn vooral geïnteresseerd in twee secties, Overzicht en Resultaat:




Het overzicht toont aan of het voorgenomen of gewenste beleid voor deze draadloze cliëntauthentificatie werd gebruikt. Zo niet, dan moet de ISE-beleidsconfiguratie worden herzien, maar dit valt buiten de reikwijdte van dit document.

Het resultaat toont wat door ISE aan de WLC werd teruggegeven. Het doel is om de SGT en de L2VNID dynamisch toe te wijzen, dus deze gegevens moeten hier worden opgenomen, en dat is het. Let op twee dingen:

1. De naam L2VNID wordt verzonden als attribuut "Tunnel-Private-Group-ID". ISE moet de naam teruggeven (10_10_30_0-READONLY_VN) en niet de id (8199).

2. Het SGT wordt verzonden als een "cisco-av-paar". In het kenmerk cts:security-group-tag wordt opgemerkt dat de SGT-waarde niet in ascii (18) in hex (12) staat, maar dat ze hetzelfde zijn. TC2E_Learners is de SGT-naam in ISE intern.

## WLC-verificatie

In de WLC kunnen we de show wireless fabric client overview opdracht gebruiken om de clientstatus en de show wireless fabric overview te controleren om de fabric-configuratie en de aanwezigheid van de dynamisch toegewezen L2VNID te bevestigen:

```
<#root>

eWLC#

show wireless fabric client summary

Number of Fabric Clients : 1

MAC Address    AP Name                          WLAN State              Protocol Method     L2 VNID    I
-------------------------------------------------------------------------------------------------------
08be.ac18.c4d9 DNA12-AP-01                       19   Run                 11ac     Dot1x

8199

       172.16.69.68
```

```
<#root>

eWLC4#

show wireless fabric summary


Fabric Status      : Enabled


Control-plane:
Name                              IP-address        Key                                Status
-------------------------------------------------------------------------------------------
default-control-plane             172.16.201.4      f9afa1                             Up

Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address             Subnet        Control plane n
-------------------------------------------------------------------------------------------------------
  Pegasus_APs         8196           4097           10.10.99.0          255.255.255.0      default-cont
  Pegasus_Extended     8207           0                                   0.0.0.0            default-con
  Pegasus_Read_Only     8198           0                                   0.0.0.0            default-co
```

```
10_10_30_0-READONLY_VN


8199

          0                                   0.0.0.0           default-control-plane
```

Als de verwachte informatie niet wordt weergegeven, kunnen we RA Traces voor het draadloze client mac-adres in de WLC in staat stellen om precies de gegevens te zien die van ISE worden ontvangen. In dit document vindt u informatie over het verkrijgen van de RA Traces-uitvoer voor een specifieke client:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_debug_ra_ewlc.html?bookSearch=true

In de RA Trace-uitvoer voor de client worden de door ISE verzonden kenmerken meegeleverd in het RADIUS-access-pakket:

<#root>

```
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS: Received from id 1812/14 172.16.201.206:0,

Access-Accept

, len 425
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  authenticator c6 ac 95 5c 95 22 ea b6 - 21 7d 8a f
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  User-Name           [1]     10  "druedahe"
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Class               [25]    53  ...
{wncd_x_R0-0}{1}: [radius] [21860]: (info): 01:
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Tunnel-Type         [64]     6  VLAN
{wncd_x_R0-0}{1}: [radius] [21860]: (info): 01:
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Tunnel-Medium-Type  [65]     6  ALL_802
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  EAP-Message         [79]     6  ...
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Message-Authenticator[80]    18  ...
{wncd_x_R0-0}{1}: [radius] [21860]: (info): 01:
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:

Tunnel-Private-Group-Id[81]    25  "10_10_30_0-READONLY_VN"

{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  EAP-Key-Name        [102]   67  *
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Cisco       [26]    38
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:

Cisco AVpair       [1]     32  "cts:security-group-tag=0012-01"

{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Cisco       [26]    34
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:

Cisco AVpair       [1]     28  "cts:sgt-name=TC2E_Learners"

{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Cisco       [26]    26
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:   Cisco AVpair       [1]     20  "cts:vn=READONLY_V
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Microsoft   [26]    58
…
{wncd_x_R0-0}{1}: [epm-misc] [21860]: (info): [08be.ac18.c4d9:capwap_9000000a] Username druedahe receiv
{wncd_x_R0-0}{1}: [epm-misc] [21860]: (info): [08be.ac18.c4d9:capwap_9000000a] VN READONLY_VN received
…
{wncd_x_R0-0}{1}: [auth-mgr] [21860]: (info): [08be.ac18.c4d9:capwap_9000000a] User Profile applied suc
```

```
{wncd_x_R0-0}{1}: [client-auth] [21860]: (note): MAC: 08be.ac18.c4d9  ADD MOBILE sent. Client state fla
```

De WLC stuurt de informatie over SGT en L2VNID naar:

1. Het access point (AP) via CAPWAP (Control and Provisioning of Wireless Access points).

2. De Fabric CP via LISP.

De Fabric CP verstuurt vervolgens de SGT-waarde via LISP naar de Fabric EN waar het toegangspunt is aangesloten.

## Fabric EN-verificatie

De volgende stap is te valideren als de Fabric EN de dynamisch ontvangen informatie weergeeft. Het opdracht show VLAN bevestigt het VLAN dat aan L2VNID 8199 is gekoppeld:

```
<#root>

EDGE-01#

show vlan | i 819

1028 Pegasus_APs                      active    Tu0:8196, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/10, Gi1/0/18
1030 Pegasus_Read_Only                active    Tu0:8198, Gi1/0/15

1031 10_10_30_0-READONLY_VN

           active

Tu0:8199

, Gi1/0/1, Gi1/0/2, Gi1/0/9
```

We zien dat de L2VNID 8199 is toegewezen aan VLAN 1031.

En de show device-tracking database mac <mac address>geeft weer als de draadloze client zich op het gewenste VLAN bevindt:

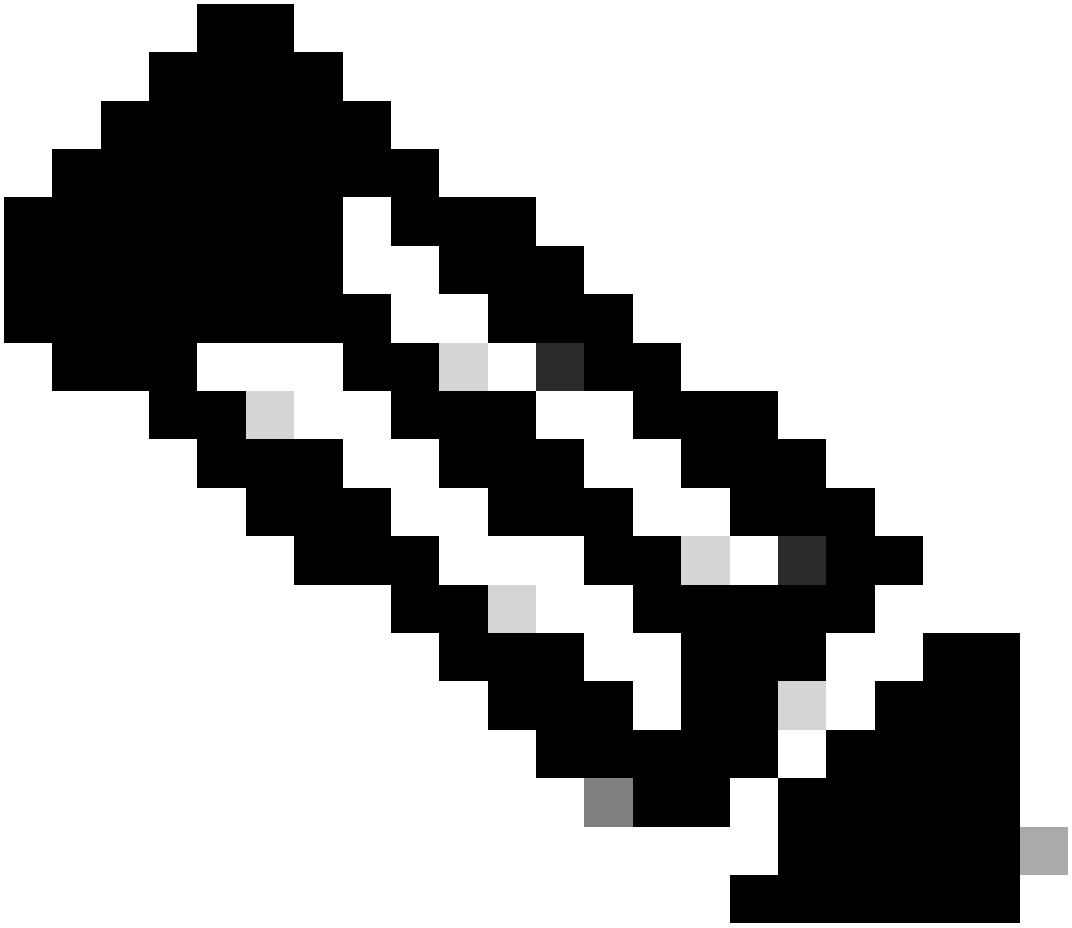
```
<#root>

EDGE-01#

show device-tracking database mac 08be.ac18.c4d9

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 15:16:09.219 UTC Thu Nov 23 2023
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
```

```
    Network Layer Address                  Link Layer Address Interface  vlan  prlvl age    state
macDB has 0 entries for mac 08be.ac18.c4d9,vlan 1028, 0 dynamic
macDB has 2 entries for mac 08be.ac18.c4d9,vlan 1030, 0 dynamic
DH4

10.10.30.12                            08be.ac18.c4d9

     Ac1

1031

  0025  96s    REACHABLE 147 s try 0(691033 s)
```

Ten slotte biedt de op rollen gebaseerde sgt-map vrf <vrf name> all opdracht de SGT-waarde die aan de client is toegewezen. In dit voorbeeld maakt VLAN 1031 deel uit van VRF "READONLY_VN":

<#root>

```
EDGE-01#

show cts role-based sgt-map vrf READONLY_VN all

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 10:54:01.496 UTC Fri Dec 1 2023

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================

10.10.30.12



18

      LOCAL
10.10.30.14             4       LOCAL
```



Opmerking: de beleidshandhaving Cisco TrustSec (CTS) in een SDA Fabric for Wireless Clients (zoals voor bekabelde clients) wordt uitgevoerd door de EN's, niet door de AP's of de WLC.

Hiermee kan het EN de beleidsregels toepassen die zijn geconfigureerd voor het gespecificeerde SGT.

Als deze uitgangen niet goed bevolken, kunnen we het debug lisp control-plane all-commando in het EN gebruiken om te controleren of het de LISP-melding ontvangt die van de WLC komt:

<#root>

```
378879: Nov 28 18:49:51.376: [MS]  LISP: Session VRF default, Local 172.16.69.68, Peer 172.16.201.4:434
```

**wlc mapping-notification**

```
 for IID 8199  EID 08be.ac18.c4d9/48  (state: Up, RX 0, TX 0).
378880: Nov 28 18:49:51.376: [XTR] LISP-0 IID 8199 MAC: Map Server 172.16.201.4,
```

**WLC Map-Notify for EID 08be.ac18.c4d9**

```
 has 0 Host IP records, TTL=1440.
378881: Nov 28 18:49:51.376: [XTR] LISP-0 IID 8199: WLC entry prefix 08be.ac18.c4d9/48 client, Created.
378888: Nov 28 18:49:51.377: [XTR] LISP-0 IID 8199 MAC:
```

**SISF event**

```
 scheduled Add of client MAC 08be.ac18.c4d9.
378889: Nov 28 18:49:51.377: [XTR] LISP: MAC,
```

**SISF L2 table event CREATED for 08be.ac18.c4d9 in Vlan 1031**

```
, IfNum 92, old IfNum 0, tunnel ifNum 89.
```

De LISP notificatie wordt eerst ontvangen door de CP, die het vervolgens doorgeeft aan de EN. De SISF of Device-tracking vermelding wordt aangemaakt bij ontvangst van dit LISP-bericht, dat een belangrijk onderdeel van het proces is. Deze melding is ook te zien bij:

<#root>

```
EDGE-01#
```

**show lisp instance-id 8199 ethernet database wlc clients detail**

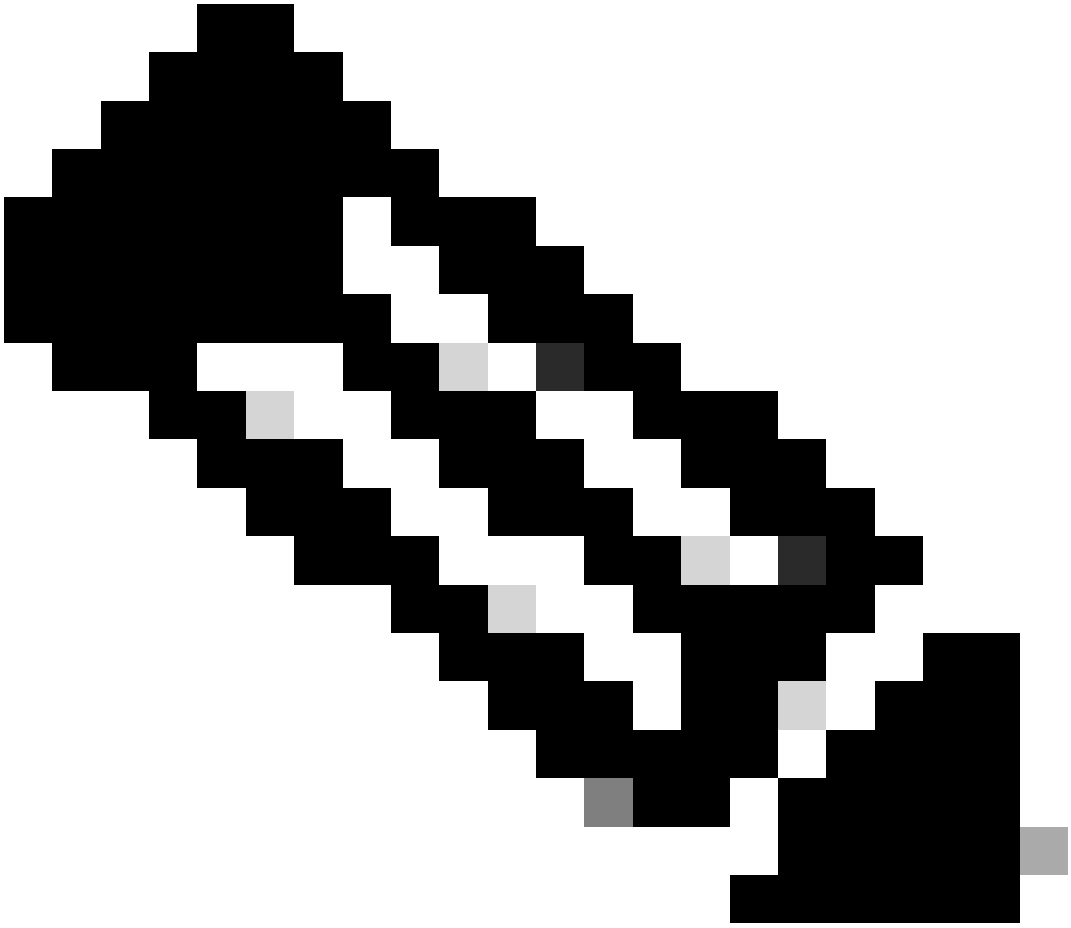
```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 21:23:31.737 UTC Wed Nov 29 2023


WLC clients/access-points information for router lisp 0 IID
```

**8199**

```
Hardware Address: 08be.ac18.c4d9
Type:             client
Sources:          1
Tunnel Update:    Signalled
Source MS:        172.16.201.4
RLOC:             172.16.69.68
Up time:          00:01:09
Metadata length:  34
Metadata (hex):   00 01 00 22   00 01 00 0C   0A 0A 63 0B   00 00 10 01
                  00 02 00 06   00
```

**12**

```
 00 03   00 0C 00 00   00 00 65 67
                  AB 7B
```



Opmerking: De gemarkeerde waarde 12 in de sectie Metadata is de hexadecimale versie van de SGT 18 die we oorspronkelijk wilden toewijzen. En dit bevestigt dat het hele proces op de juiste manier is afgerond.

## Packets verificatie

Als laatste bevestigingsstap kunnen we ook de Embedded Packet Capture (EPC) tool gebruiken in de EN switch en zien hoe de pakketten van deze client worden verzonden door de AP. Zie voor meer informatie over het verkrijgen van een opnamebestand met EPC:

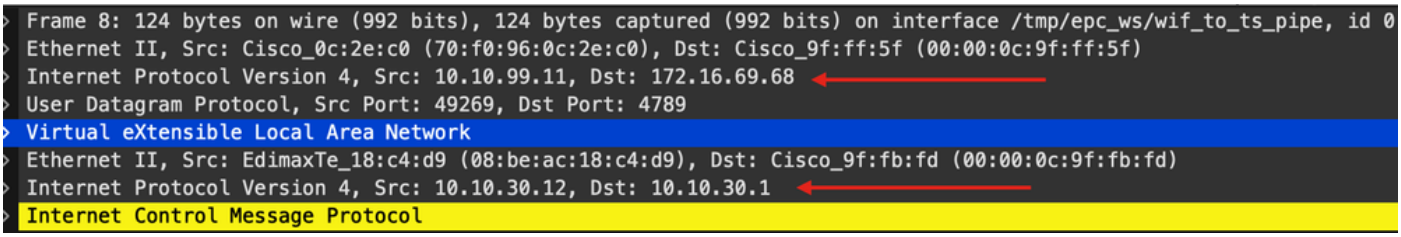
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_packet_capture.html

Bij dit voorbeeld is een ping naar de gateway gestart in de draadloze client zelf:

icmp

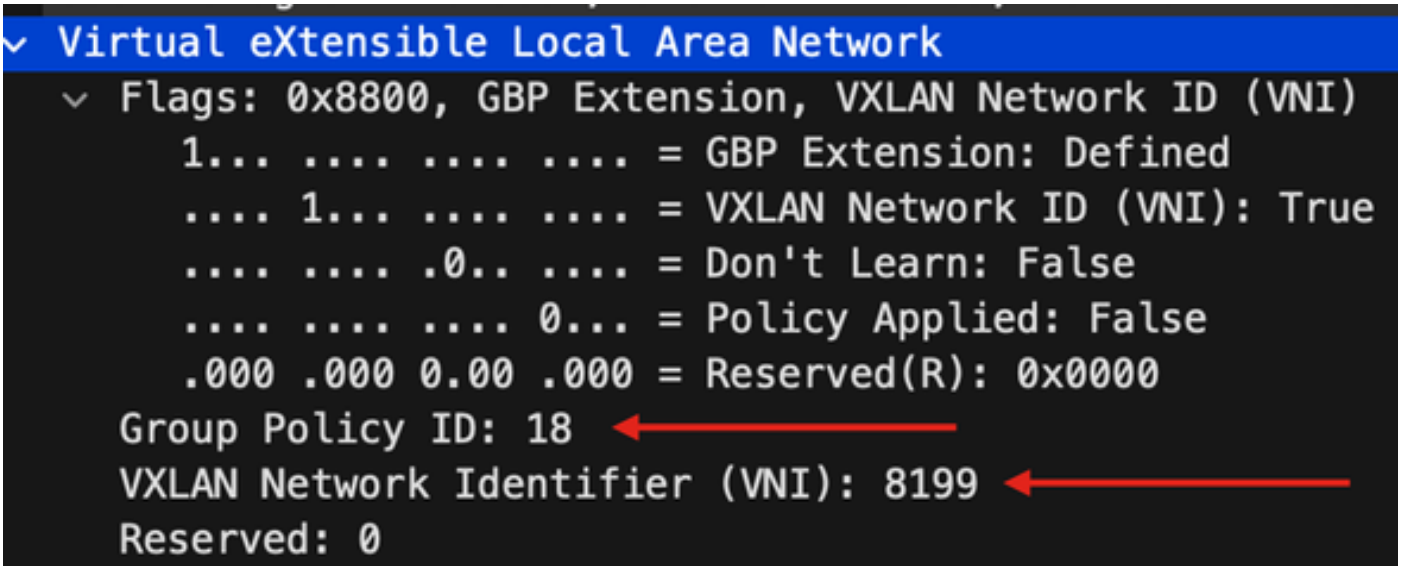
| No. | Time | Arrival Time | Source | Destination | VXLAN N | Protocol | Identification | Length | Info |
|---|---|---|---|---|---|---|---|---|---|
| 8 | 0.082365 | 2023-12-01 18:47:34.384734 | 10.10.30.12 | 10.10.30.1 | 8199 | ICMP | 0x01e1 (481),0x… | 124 | Echo (ping) request |
| 18 | 0.000028 | 2023-12-01 18:47:39.277504 | 10.10.30.12 | 10.10.30.1 | 8199 | ICMP | 0x01e3 (483),0x… | 124 | Echo (ping) request |

Merk op dat het pakket al voorzien is van een VXLAN header van het toegangspunt, aangezien het toegangspunt en het toegangspunt een VXLAN-tunnel vormen tussen de twee voor de Fabric draadloze clients:




De bron van de tunnel is het AP ip-adres (10.10.99.11) en de bestemming is het EN Loopback0 ip-adres (172.16.69.68). In de VXLAN-header kunnen we de feitelijke gegevens van de draadloze client zien, in dit geval het ICMP-pakket.

Controleer tot slot de VXLAN-header:




Let op de SGT-waarde als Group Policy ID — in dit geval in ASCII-formaat en de L2VNID-waarde als VXLAN Network Identifier (VNI).

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.