# Dynamische SGT/L2VNID-Zuordnung bei SDA Wireless

## Inhalt



## Einleitung

In diesem Dokument wird der Prozess der dynamischen SGT- und L2VNID-Zuweisung für Fabric-fähige Wireless 802.1x-SSIDs beschrieben.

## Voraussetzungen

### Anforderungen

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

- RADIUS (Remote Authentication Dial-In User Service)
- Wireless LAN-Controller (WLC)
- Identity Services Engine (ISE)
- Security Group Tag (SGT)
- L2VNID (Layer 2 Virtual Network Identifier)
- SD-Access Fabric Enabled Wireless (SDA FEW)
- Locator/ID Separation Protocol (LISP)
- Virtual eXtensible Local Area Network (VXLAN)
- Fabric Control Plane (CP) und Edge Node (EN)
- Catalyst Center (CatC, ehemals Cisco DNA Center)

### Verwendete Komponenten

WLC 9800 Cisco IOS® XE Version 17.6.4

Cisco IOS® XE

ISE Version 2.7

CatC Version 2.3.5.6

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.

# Hintergrundinformationen

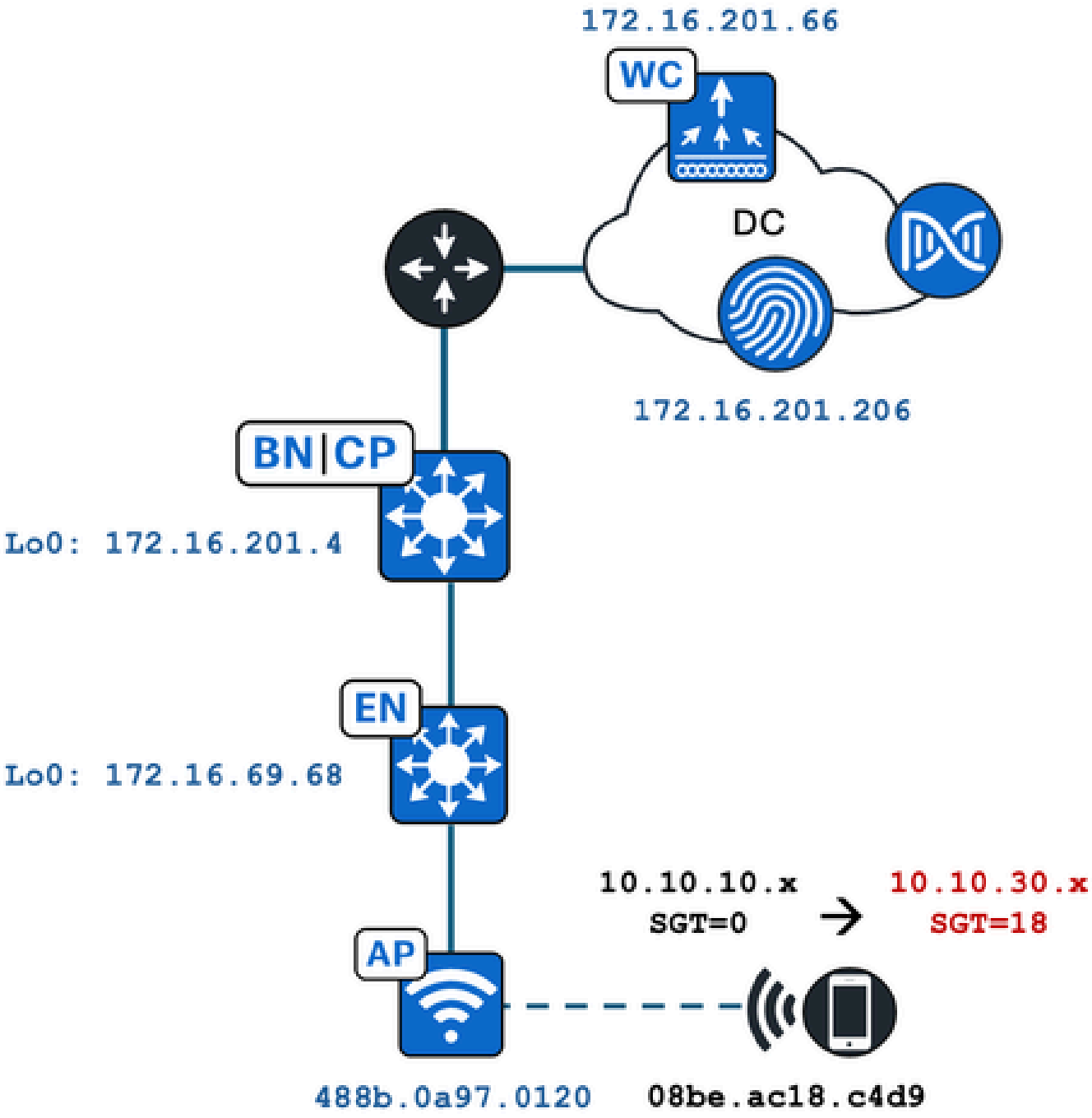
Einer der wichtigsten Aspekte von SD-Access ist die Mikrosegmentierung innerhalb eines VPN über die skalierbaren Gruppen.

Die SGTs können statisch über ein Fabric-fähiges WLAN oder eine SSID zugewiesen werden (obwohl sie nicht identisch sind, wirkt sich ihr Unterschied nicht auf das Hauptziel dieses Dokuments aus. Daher verwenden wir die beiden Begriffe für dieselbe Bedeutung, um die Lesbarkeit zu verbessern). In vielen echten Bereitstellungen gibt es jedoch Benutzer, die eine Verbindung mit demselben WLAN herstellen und andere Richtlinien oder Netzwerkeinstellungen benötigen. Darüber hinaus müssen in einigen Szenarien bestimmten Clients im selben Fabric-WLAN unterschiedliche IP-Adressen zugewiesen werden, um ihnen entweder spezifische IP-basierte Richtlinien zuweisen oder die IP-Adressierungsanforderungen des Unternehmens erfüllen zu können. Die L2VNID (Layer 2 Virtual Network Identifier) ist der Parameter, den die FEW-Infrastruktur verwendet, um Wireless-Benutzer in verschiedenen Subnetzbereichen zu platzieren. Die Access Points senden die L2VNID im VxLAN-Header an den Fabric Edge Node (EN), der sie dann mit dem entsprechenden L2-VLAN korreliert.

Um diese Genauigkeit innerhalb desselben WLAN zu erreichen, wird die dynamische SGT- und/oder L2VNID-Zuordnung verwendet. Der WLC sammelt die Identitätsinformationen des Endpunkts, sendet sie zur Authentifizierung an die ISE, die sie verwendet, um die richtige Richtlinie für diesen Client anzuwenden, und gibt die SGT- und/oder L2VNID-Informationen bei erfolgreicher Authentifizierung zurück.

# Topologie

Um zu verstehen, wie dieser Prozess abläuft, haben wir ein Beispiel mit dieser Labortopologie entwickelt:




In diesem Beispiel wird das WLAN statisch konfiguriert mit:

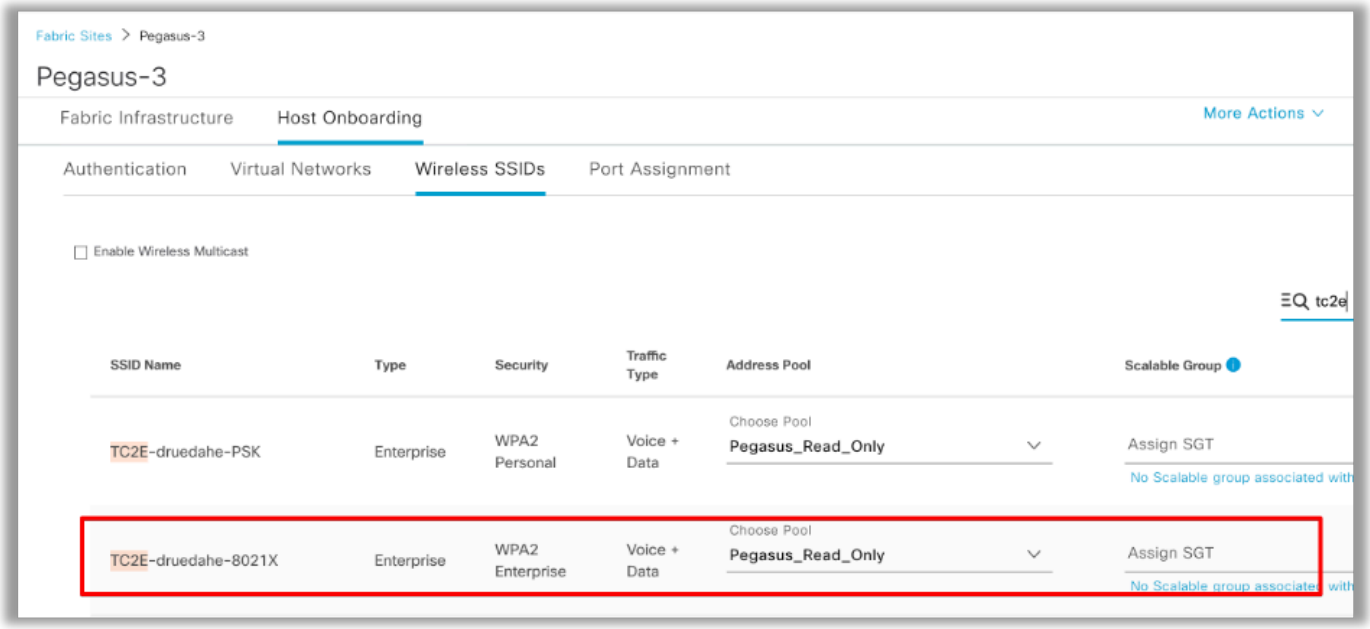
- L2VNID = 8198 / IP-Poolname = Pegasus_Read_Only —> VLAN 1030 (10.10.10.x)
- Kein SGT

Der Wireless-Client, der sich mit ihm verbindet, erhält dynamisch die folgenden Parameter:

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

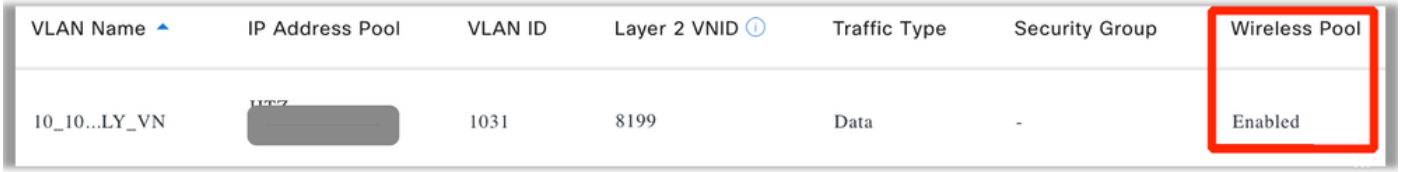
## Konfiguration

Zunächst müssen wir das WLAN identifizieren und seine Konfiguration überprüfen. In diesem Beispiel wird die SSID "TC2E-druedahe-802.1x" verwendet. Zum Zeitpunkt der Redaktion dieses Dokuments wird SDA nur über CatC unterstützt. Daher müssen wir überprüfen, welche Konfiguration hier vorhanden ist. Unter Bereitstellung/SD-Zugriff/Fabric-Standorte/<spezifischer Fabric-Standort>/Host-Integration/Wireless-SSIDs:




Dem SSID ist der IP-Pool mit dem Namen "Pegasus_Read_Only" zugeordnet, und es ist kein statisches SGT zugewiesen, d. h., es ist "SGT=0". Das heißt, wenn ein Wireless-Client erfolgreich eine Verbindung herstellt und sich authentifiziert, ohne dass die ISE Attribute für eine dynamische Zuweisung zurücksendet, sind dies die Wireless-Client-Einstellungen.

Der dynamisch zugewiesene Pool muss vor der WLC-Konfiguration vorhanden sein. Dazu wird der IP-Pool im virtuellen Netzwerk des CatC als "Wireless-Pool" hinzugefügt:




In der WLC-GUI unter "Configuration/Wireless/Fabric" spiegelt diese Einstellung Folgendes wider:


Der Pool "Pegasus_Read_Only" entspricht der 8198 L2VNID, und wir möchten, dass unser Client der 8199 L2VNID angehört. Das bedeutet, dass die ISE den WLC anweisen muss, den Pool "10_10_30_0-READONLY_VN" für diesen Client zu verwenden. Beachten Sie, dass der WLC keine Konfiguration für die Fabric-VLANs enthält. Er kennt nur die L2VNIDs. Jede einzelne wird dann einem bestimmten VLAN in den SDA Fabric ENs zugeordnet.

## Verifizierung

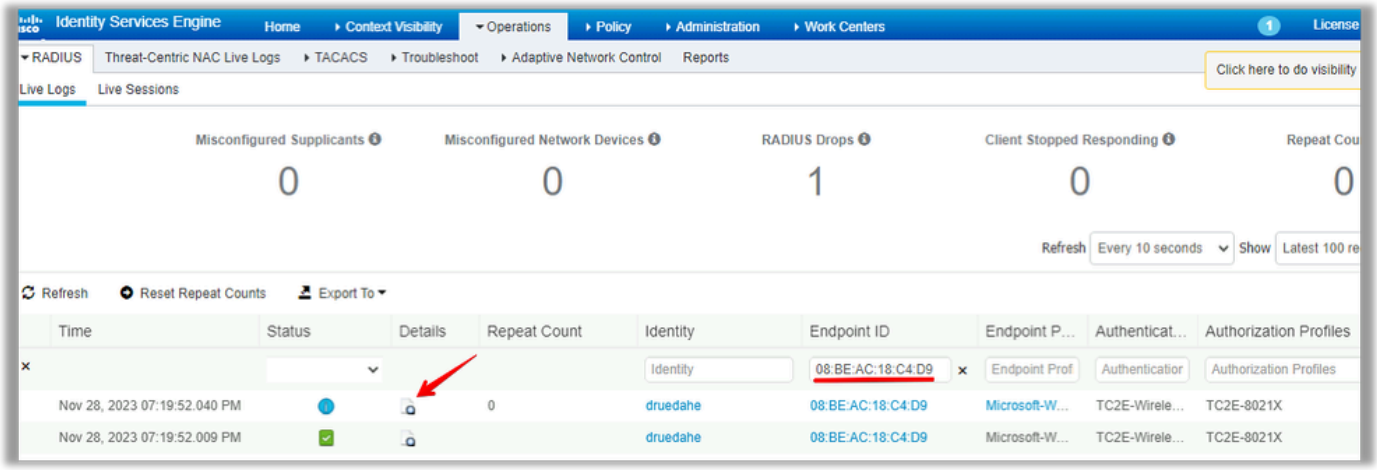
Bei Problemen mit der dynamischen Zuweisung von SGT/L2VNID werden die folgenden Symptome gemeldet:

1. Sicherheitsgruppen-Richtlinien werden nicht auf Wireless-Clients durchgesetzt, die eine Verbindung mit einem bestimmten WLAN herstellen (Problem mit dynamischer SGT-Zuweisung).
2. Wireless-Clients erhalten keine IP-Adresse über DHCP, oder sie beziehen keine IP-Adresse aus dem gewünschten Subnetzbereich in einem bestimmten WLAN. (Problem mit dynamischer L2VNID-Zuweisung).

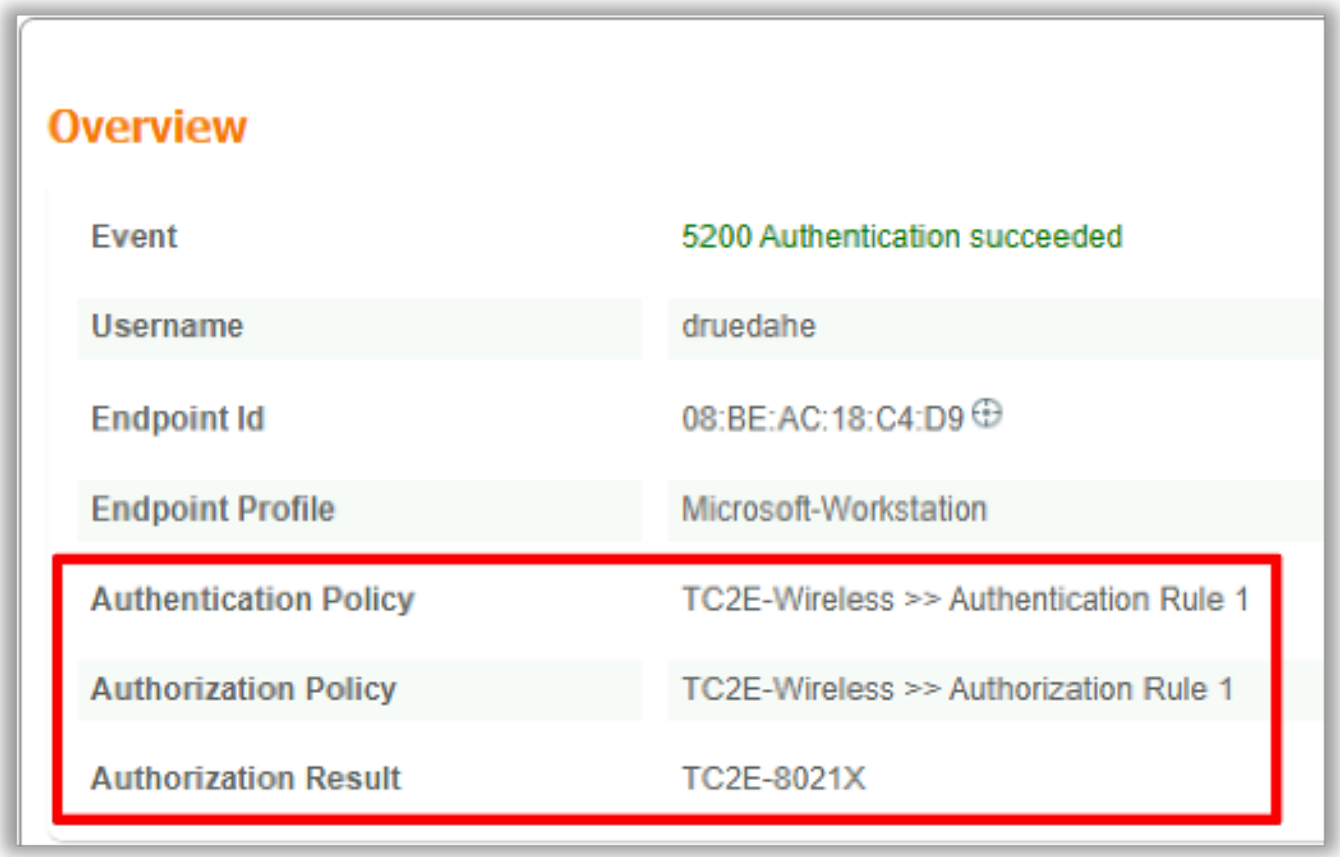
Nun wird die Verifizierung jedes relevanten Knotens in diesem Prozess beschrieben.

## ISE-Verifizierung

Ausgangspunkt ist die ISE. Öffnen Sie die ISE-GUI unter "Operation/RADIUS/Live Logs/", und verwenden Sie die MAC-Adresse des Wireless-Clients als Filter im Feld "Endpoint ID". Klicken Sie dann auf das Symbol Details:




Anschließend wird eine weitere Registerkarte mit den Authentifizierungsdetails geöffnet. Wir interessieren uns hauptsächlich für zwei Bereiche, Überblick und Ergebnis:




Die Übersicht zeigt, ob die beabsichtigte oder die gewünschte Richtlinie für diese Wireless-Client-

Authentifizierung verwendet wurde. Falls nicht, muss die ISE-Richtlinienkonfiguration überprüft werden. Dies ist jedoch nicht Bestandteil des vorliegenden Dokuments.

Das Ergebnis zeigt, was von der ISE an den WLC zurückgegeben wurde. Das Ziel besteht darin, das SGT und die L2VNID dynamisch zuzuweisen. Daher müssen diese Daten hier enthalten sein, und das ist auch der Fall. Beachten Sie dabei zwei Aspekte:

1. Der L2VNID-Name wird als "Tunnel-Private-Group-ID"-Attribut gesendet. ISE muss den Namen (10_10_30_0-READONLY_VN) und nicht die ID (8199) zurückgeben.

2. Das SGT wird als "cisco-av-pair" gesendet. Beachten Sie im Attribut cts:security-group-tag, dass der SGT-Wert in Hex (12) und nicht in ASCII (18) angegeben ist, jedoch identisch ist. TC2E_Learners ist der interne SGT-Name in der ISE.

## WLC-Verifizierung

Im WLC können wir den Befehl show wireless fabric client summary verwenden, um den Client-Status zu überprüfen, und den Befehl show wireless fabric summary, um die Fabric-Konfiguration und das Vorhandensein der dynamisch zugewiesenen L2VNID zu bestätigen:

```
<#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 na
-------------------------------------------------------------------------------------------------------
```

```
  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
```

Wenn die erwarteten Informationen nicht wiedergegeben werden, können RA Traces für die MAC-Adresse des Wireless-Clients im WLC aktiviert werden, um die von der ISE empfangenen Daten genau anzuzeigen. Informationen zum Abrufen der RA Traces-Ausgabe für einen bestimmten Client finden Sie in diesem Dokument:

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 der RA Trace-Ausgabe für den Client werden die von ISE gesendeten Attribute in das RADIUS Access-Accept-Paket übernommen:

<#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
```

Der WLC sendet dann die SGT- und L2VNID-Informationen an:

1. Der Access Point (AP) über CAPWAP (Control And Provisioning of Wireless Access Points).

2. Fabric-CP über LISP

Der Fabric-CP sendet dann den SGT-Wert über LISP an die Fabric EN, an der der AP angeschlossen ist.

## Fabric EN-Verifizierung

Im nächsten Schritt muss überprüft werden, ob die Fabric EN die dynamisch empfangenen Informationen wiedergibt. Der Befehl show vlan bestätigt das mit L2VNID 8199 verknüpfte VLAN:

```
<#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
```

Wie wir sehen, ist die L2VNID 8199 VLAN 1031 zugeordnet.

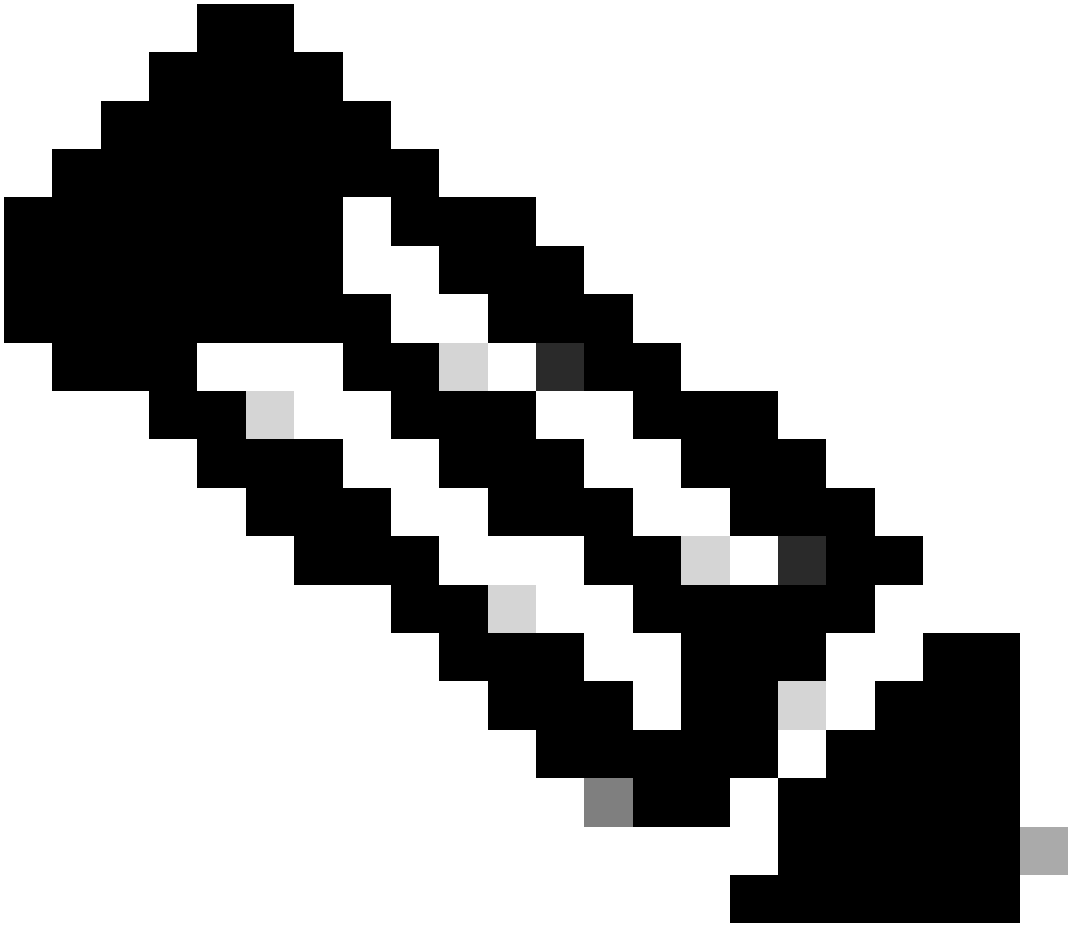
Und die MAC-Adresse der Datenbank zur Geräteverfolgung <MAC-Adresse> wird angezeigt, wenn sich der Wireless-Client im gewünschten VLAN befindet:

```
<#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)
```

Schließlich wird mit dem Befehl show cts role-based sgt-map vrf <vrf name> all der dem Client zugewiesene SGT-Wert bereitgestellt. In diesem Beispiel ist das VLAN 1031 Teil der VRF-Instanz "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
```



> Hinweis: Die Richtliniendurchsetzung von Cisco TrustSec (CTS) in einer SDA-Struktur für Wireless-Clients (wie für kabelgebundene Clients) wird von den ENs vorgenommen, nicht von den APs oder dem WLC.

Dadurch kann die EN die für das angegebene SGT konfigurierten Richtlinien anwenden.

Wenn diese Ausgaben nicht richtig aufgefüllt werden, können Sie mithilfe des Befehls debug lisp control-plane all in der EN prüfen, ob die LISP-Benachrichtigung vom WLC empfangen wird:

<#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.
```

Beachten Sie, dass die LISP-Benachrichtigung zuerst beim CP eingeht, der sie dann an die EN weiterleitet. Der SISF- oder Device-Tracking-Eintrag wird nach Erhalt der LISP-Benachrichtigung erstellt. Dies ist ein wichtiger Teil des Prozesses. Sie können diese Benachrichtigung auch sehen mit:

<#root>

```
EDGE-01#
```

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

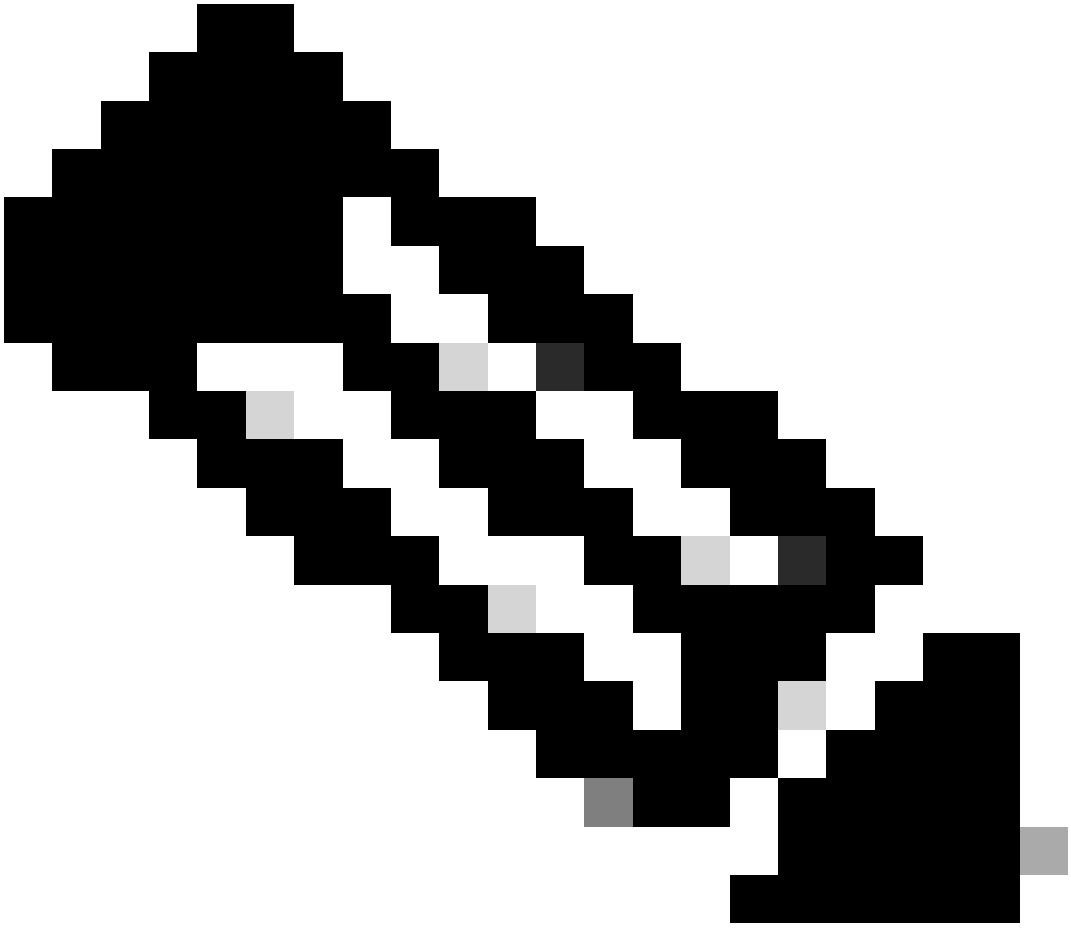
```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 21:23:31.737 UTC Wed Nov 29 2023


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
```



Hinweis: Der markierte Wert 12 im Abschnitt "Metadaten" ist die Hexadezimalversion des SGT 18, die wir ursprünglich zuweisen wollten. Und das bestätigt, dass der ganze Prozess richtig abgeschlossen ist.

## Paketverifizierung

Als letzten Bestätigungsschritt können wir auch das Embedded Packet Capture (EPC) Tool im EN Switch verwenden und sehen, wie die Pakete dieses Clients vom AP übertragen werden. Weitere Informationen zum Abrufen einer Erfassungsdatei mit EPC finden Sie unter:

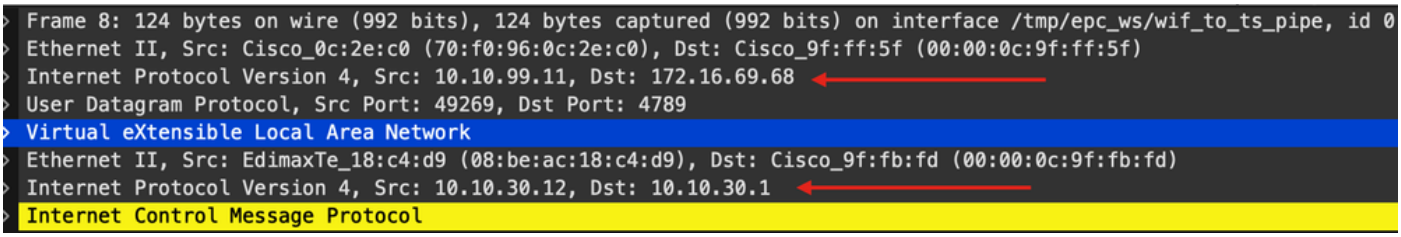
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_packet_capture.html

In diesem Beispiel wurde ein Ping an das Kabelmodem im Wireless-Client selbst initiiert:

icmp

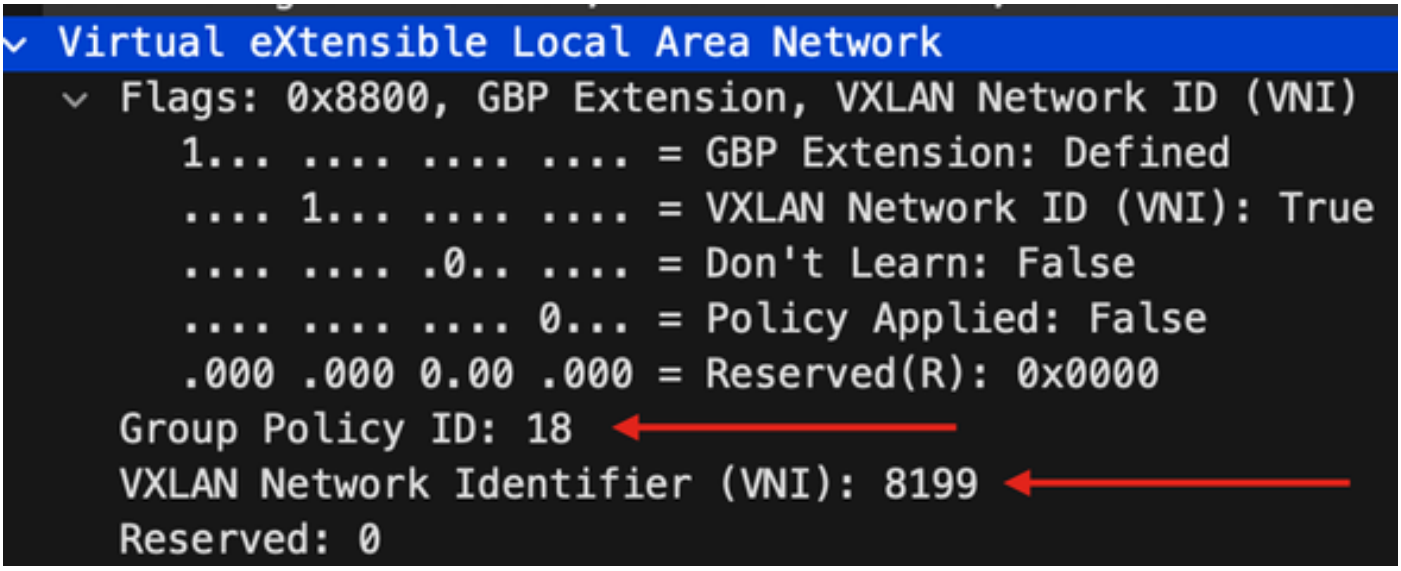
| No. | Time | Arrival Time | Source | Destination | VXLAN N | Protocol | Identification | Length | Info |
|---|---|---|---|---|---|---|---|---|---|
| 8 | 0.082365 | 2023-12-01 18:47:34.384734 | 10.10.30.12 | 10.10.30.1 | 8199 | ICMP | 0x01e1 (481),0x… | 124 | Echo (ping) request |
| 18 | 0.000028 |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

Beachten Sie, dass das Paket bereits mit einem VXLAN-Header vom WAP ausgeliefert werden muss, da der WAP und der EN zwischen sich einen VXLAN-Tunnel für die Fabric Wireless Clients bilden:




Die Quelle des Tunnels ist die AP-IP-Adresse (10.10.99.11) und das Ziel die EN Loopback0-IP-Adresse (172.16.69.68). Innerhalb des VXLAN-Headers können wir die tatsächlichen Wireless-Client-Daten sehen, in diesem Fall das ICMP-Paket.

Überprüfen Sie abschließend den VXLAN-Header:




Beachten Sie den SGT-Wert als Gruppenrichtlinien-ID - in diesem Fall im ASCII-Format und den L2VNID-Wert als VXLAN Network Identifier (VNI).

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.