# 了解SDA无线上的动态SGT/L2VNID分配

## 目录



## 简介

本文档介绍在启用交换矩阵的无线802.1x SSID上分配动态SGT和L2VNID的过程。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 远程用户拨入认证系统(RADIUS)
- 无线局域网控制器(WLC)
- 身份服务引擎 (ISE)
- 安全组标记(SGT)
- L2VNID（第2层虚拟网络标识符）
- 支持SD访问交换矩阵的无线（SDA少）
- 定位器/ID分离协议(LISP)
- 虚拟可扩展局域网(VXLAN)
- 交换矩阵控制平面(CP)和边缘节点(EN)
- Catalyst Center（CatC，以前称为Cisco DNA Center）

### 使用的组件

WLC 9800 Cisco IOS® XE版本17.6.4

思科IOS® XE

ISE版本2.7

CatC版本2.3.5.6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 背景信息

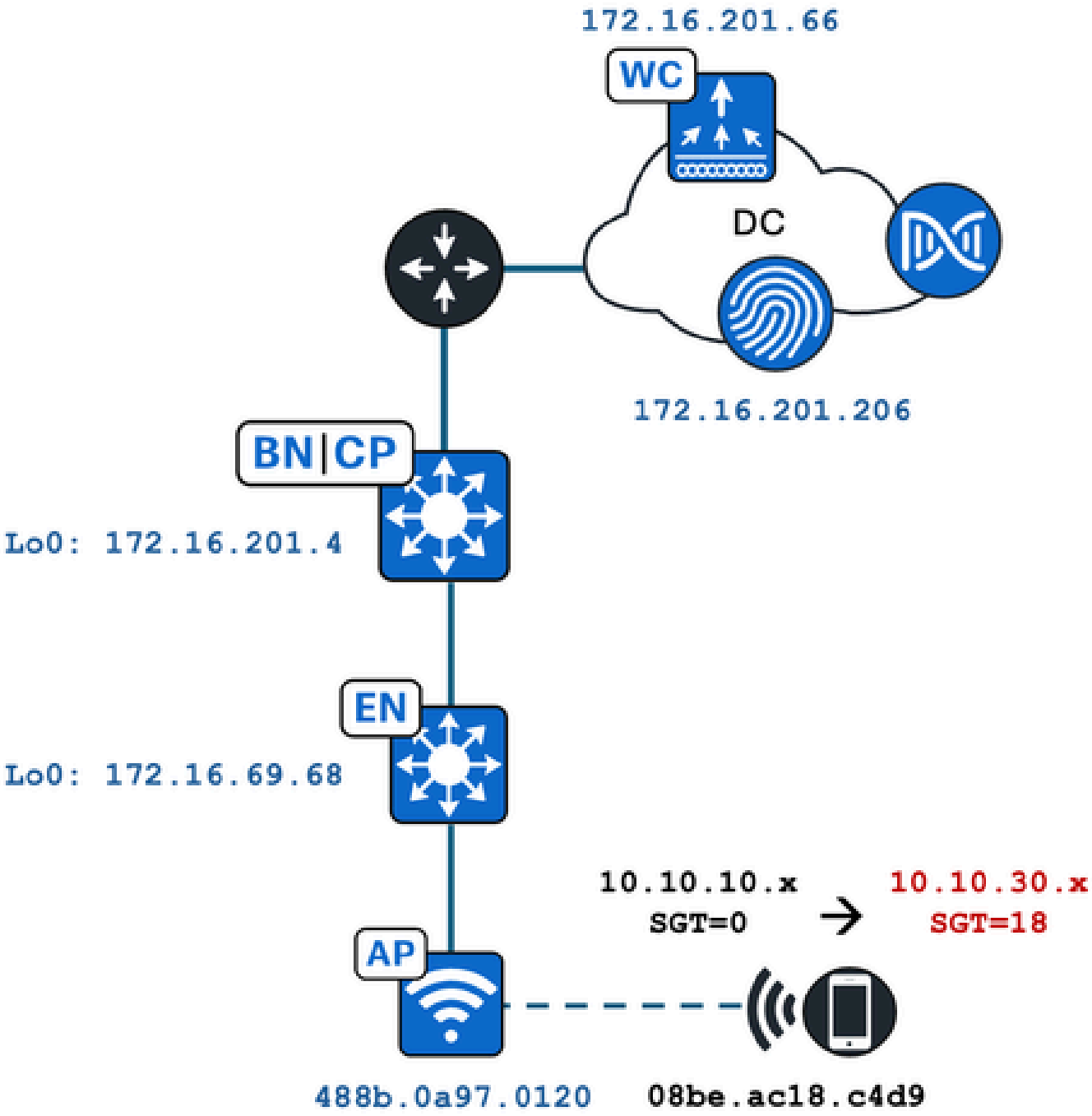
SD-Access的关键方面之一是通过Scalable Groups实现的VN中的微分段。

SGT可按支持交换矩阵的WLAN或SSID静态分配（虽然它们不同，但它们的差异不会影响本文档的主要目标，因此我们可互换使用两个具有相同含义的术语以增强可读性）。但是，在许多实际部署中，通常有连接到同一WLAN的用户需要一组不同的策略或网络设置。此外，在某些情况下，需要为同一交换矩阵WLAN内的特定客户端分配不同的IP地址，以便向其应用基于IP的特定策略或满足公司的IP寻址要求。L2VNID（第2层虚拟网络标识符）是FEW基础设施用于将无线用户置于不同子网范围的参数。接入点将VxLAN报头中的L2VNID发送到交换矩阵边缘节点(EN)，然后将其关联到对应的L2 VLAN。

要在同一WLAN中实现此粒度，需要利用动态SGT和/或L2VNID分配。WLC收集终端的身份信息，将其发送到ISE进行身份验证，ISE使用它来匹配要应用于此客户端的适当策略，并在身份验证成功后返回SGT和/或L2VNID信息。

# 拓扑

为了了解此过程的工作原理，我们使用本实验拓扑开发了一个示例：




在本示例中，WLAN静态配置为：

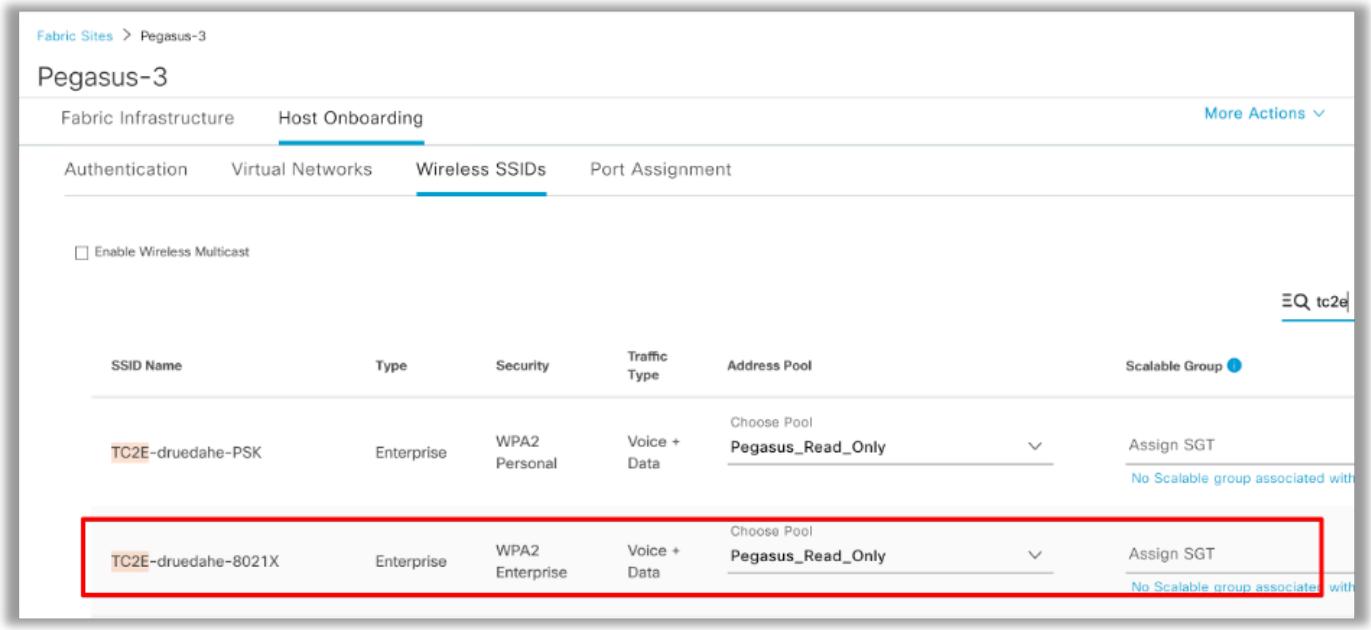
- L2VNID = 8198 / IP池名称= Pegasus_Read_Only —> VLAN 1030 (10.10.10.x)
- 无SGT

连接无线客户端动态获取以下参数：

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

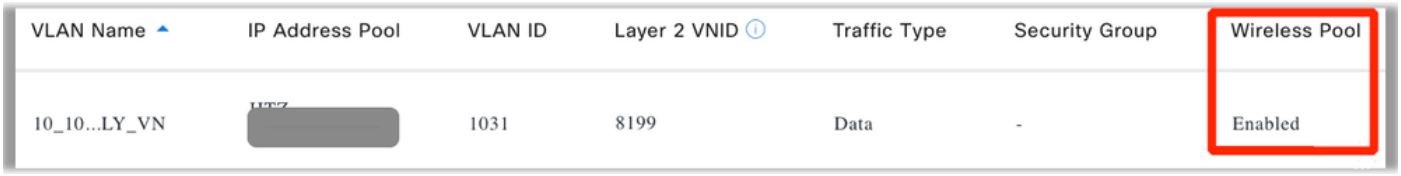
## 配置

首先，我们需要确定相关的WLAN并检查其配置方式。本例中使用的是“TC2E-druedahe-802.1x”SSID。在本文档进行编辑时，SDA仅通过CatC受支持，因此我们必须检查其中配置的内容。在Provision/SD-Access/Fabric Sites/<specific Fabric site>/Host Onboarding/Wireless SSIDs下：

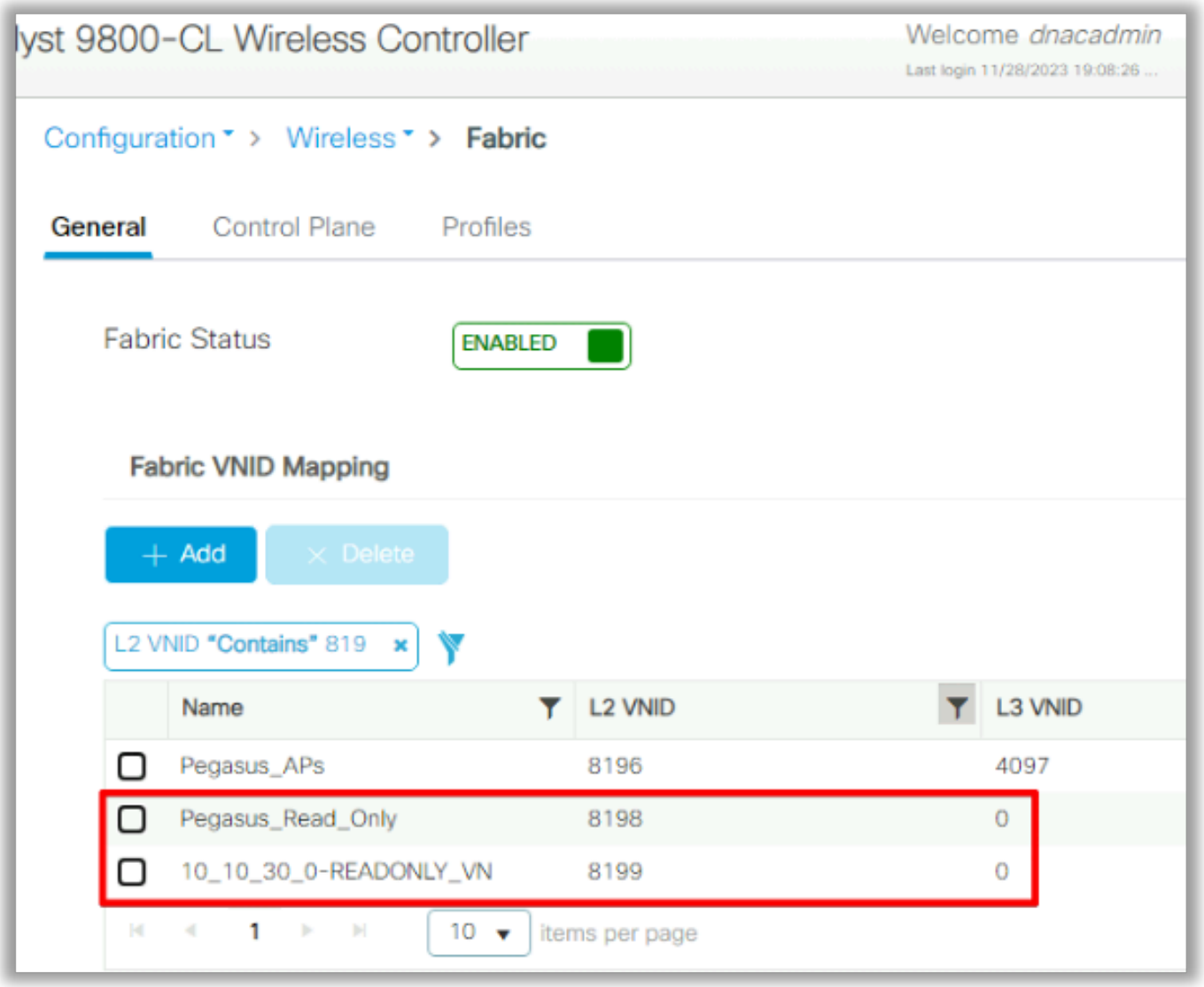



SSID映射了名为“Pegasus_Read_Only”的IP池，并且没有静态分配SGT，这意味着SGT=0。这意味着，如果无线客户端成功连接并身份验证，而ISE不发送任何属性返回进行动态分配，则这是无线客户端设置。

动态分配的池必须存在于WLC配置之前。这可以通过在CatC的虚拟网络中将IP池添加为“Wireless Pool”来完成：




在WLC GUI中的Configuration/Wireless/Fabric下，此设置反映以下方式：




“Pegasus_Read_Only”池等同于8198 L2VNID，我们希望我们的客户端位于8199 L2VNID上，这意味着ISE需要通知WLC为此客户端使用“10_10_30_0-READONLY_VN”池。请注意，WLC不包含交换矩阵VLAN的任何配置。它只知道L2VNID。然后，每个映射到SDA交换矩阵EN中的特定VLAN。

# 确认

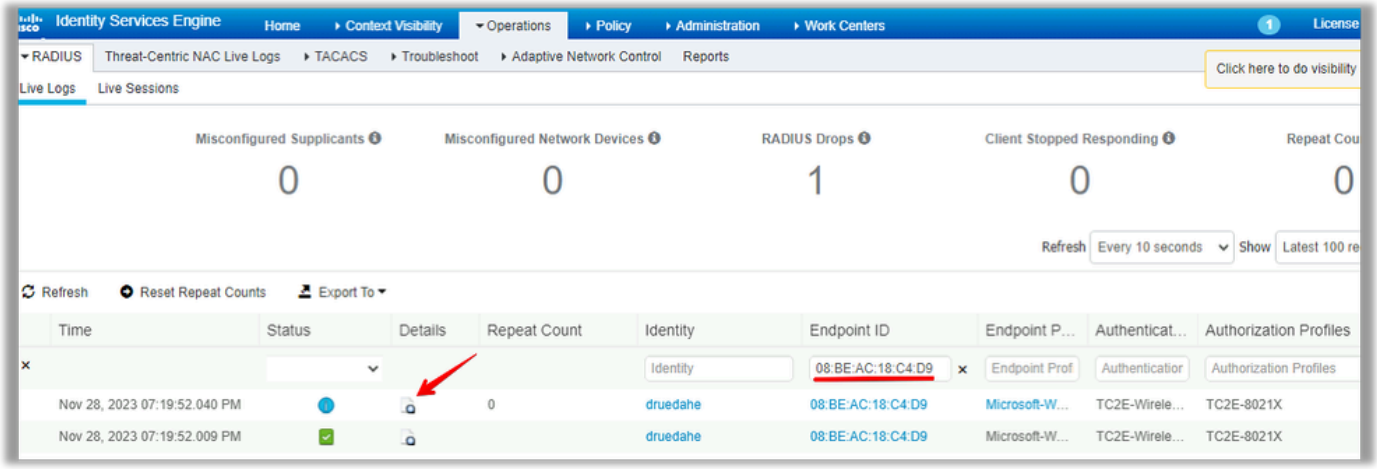
报告的涉及SGT/L2VNID动态分配问题的症状为以下症状之一：

1. 在连接到特定WLAN的无线客户端上不实施SG策略。（动态SGT分配问题）。
2. 无线客户端未通过DHCP获取IP地址，或者未从特定WLAN上的所需子网范围获取IP地址。（动态L2VNID分配问题）。

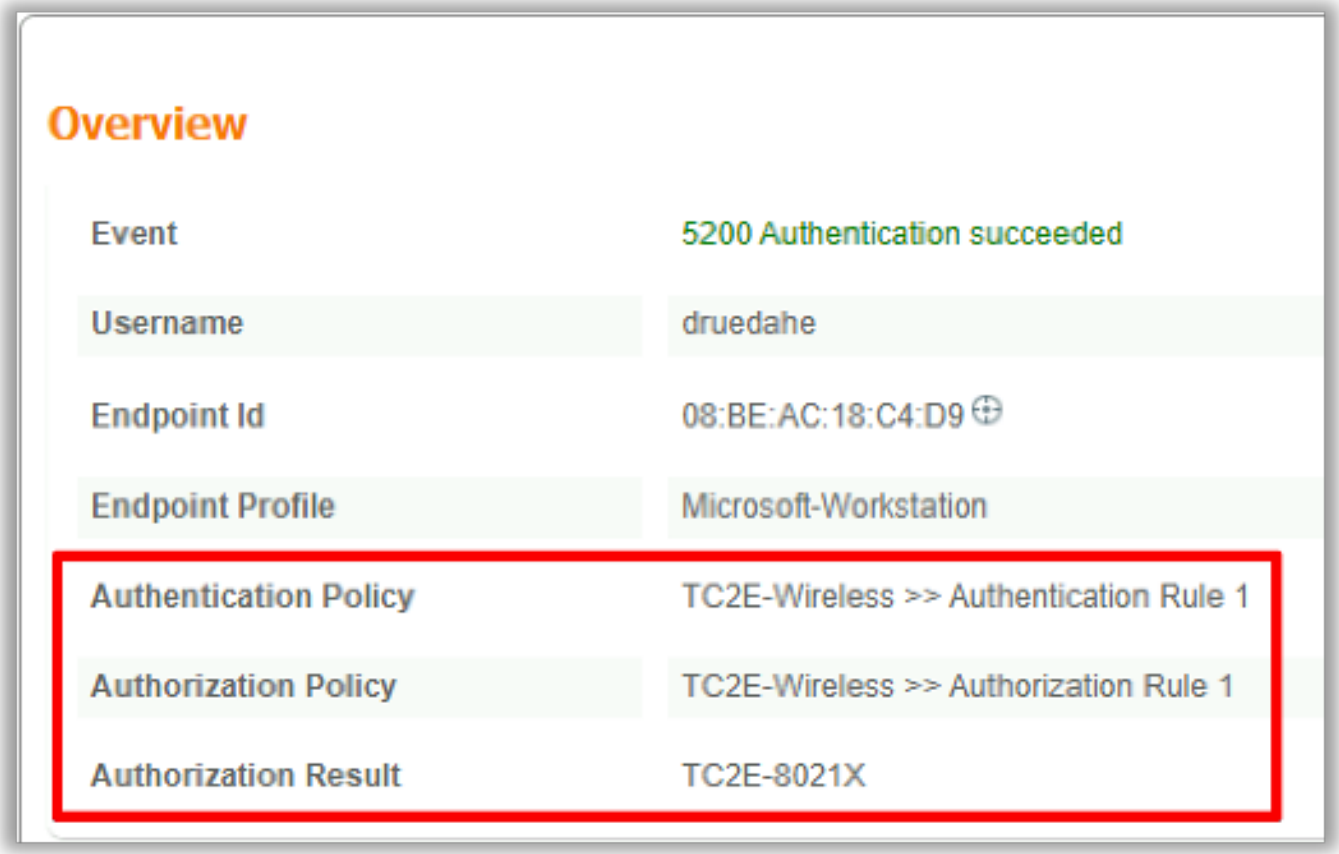
现在描述了在这个过程中各个相关节点的验证。

## ISE验证

首先是ISE。转至ISE GUI的Operation/RADIUS/Live Logs/并使用无线客户端MAC地址作为Endpoint ID字段中的过滤器，然后点击Details图标：




然后会打开另一个包含身份验证详细信息的选项卡。我们主要关注两个部分，概述和结果：




概述显示为此无线客户端身份验证使用了预期策略还是预期策略。如果没有，则需要重新查看ISE策略配置，但此内容不在本文档的讨论范围之内。

结果显示了ISE返回到WLC的内容。目标是动态分配SGT和L2VNID，因此这些数据必须包含在此处，并且它是。请注意两点：

1. L2VNID名称作为“Tunnel-Private-Group-ID”属性发送。ISE必须返回名称(10_10_30_0-READONLY_VN)而不是id (8199)。

2. SGT作为“cisco-av-pair”发送。在cts：security-group-tag属性中，请注意，SGT值以十六进制(12)表示不在ascii (18)中，但它们相同。TC2E_Learger是ISE内部的SGT名称。

## WLC验证

在WLC中，我们可以使用show wireless fabric client summary命令检查客户端状态，并使用show wireless fabric summary双击确认交换矩阵配置和存在动态分配的L2VNID：

<#root>

eWLC#

**show wireless fabric client summary**

Number of Fabric Clients : 1

MAC Address AP Name WLAN State Protocol Method L2 VNID

---

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

如果未反映预期信息，我们可以在WLC中启用无线客户端MAC地址的RA跟踪，以准确查看从ISE接收的数据。有关如何获取特定客户端的RA Traces输出的信息，请参阅以下文档：

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

在客户端的RA Trace输出中，ISE发送的属性在RADIUS Access-Accept数据包中传输：

<#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
```

然后，WLC将SGT和L2VNID信息发送到：

1. 通过CAPWAP（无线接入点的控制和调配）的接入点(AP)。

2. 通过LISP的交换矩阵CP。

然后，交换矩阵CP通过LISP将SGT值发送到连接AP的交换矩阵EN。

## 交换矩阵企业网络验证

下一步是验证交换矩阵EN是否反映动态接收的信息。show vlan命令确认与L2VNID 8199关联的

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
```

我们可以看到L2VNID 8199映射到VLAN 1031。

并且show device-tracking database mac <mac address>会显示无线客户端是否位于所需的VLAN上：

```
<#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)
```

最后，show cts role-based sgt-map vrf <vrf name> all命令提供分配给客户端的SGT值。在本例中，VLAN 1031是“READONLY_VN” VRF的一部分：

<#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

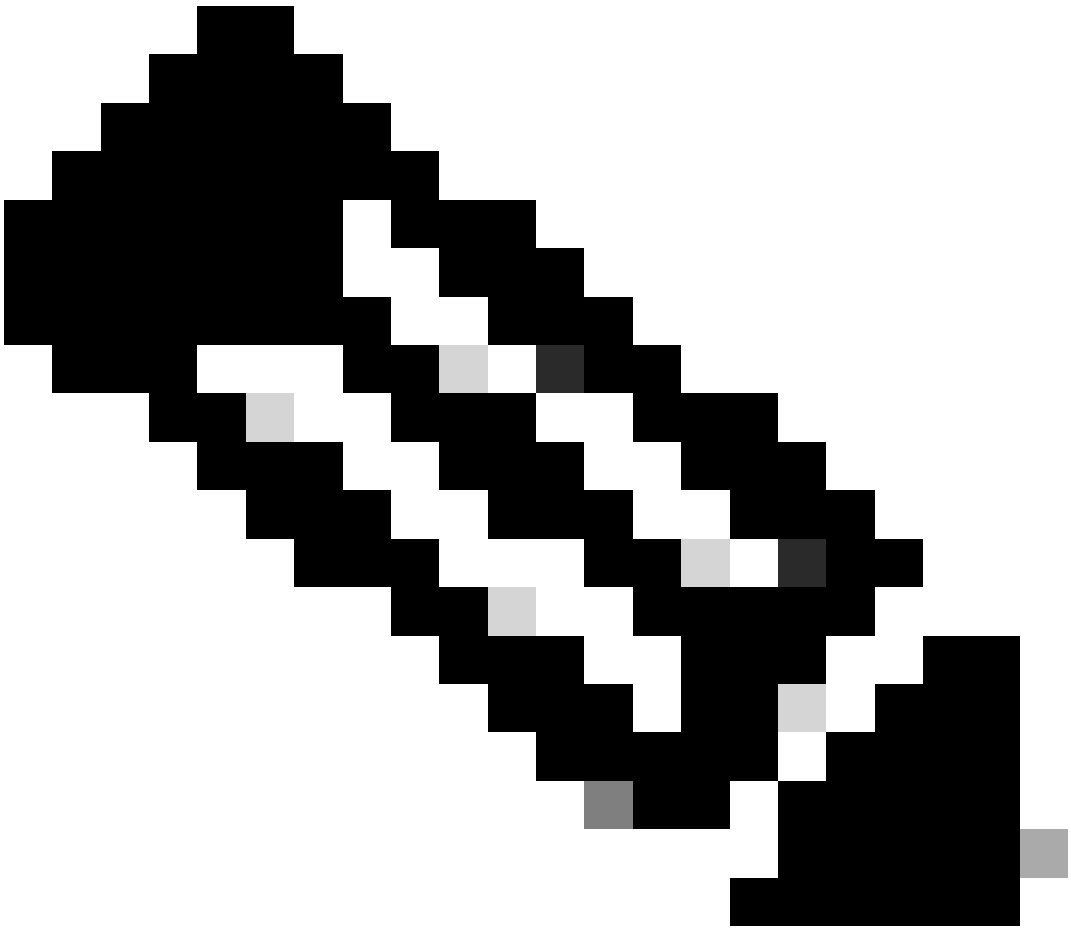
IP Address SGT Source
==========

**10.10.30.12**

**18**

LOCAL
10.10.30.14 4 LOCAL

---



---

注意：SDA交换矩阵中针对无线客户端（类似于有线客户端）的思科TrustSec (CTS)策略实施由EN完成，而不是AP或WLC。

这样，EN可以应用为指定SGT配置的策略。

如果这些输出未正确填充，则可以在EN中使用debug lisp control-plane all命令检查其是否接收来自WLC的LISP通知：

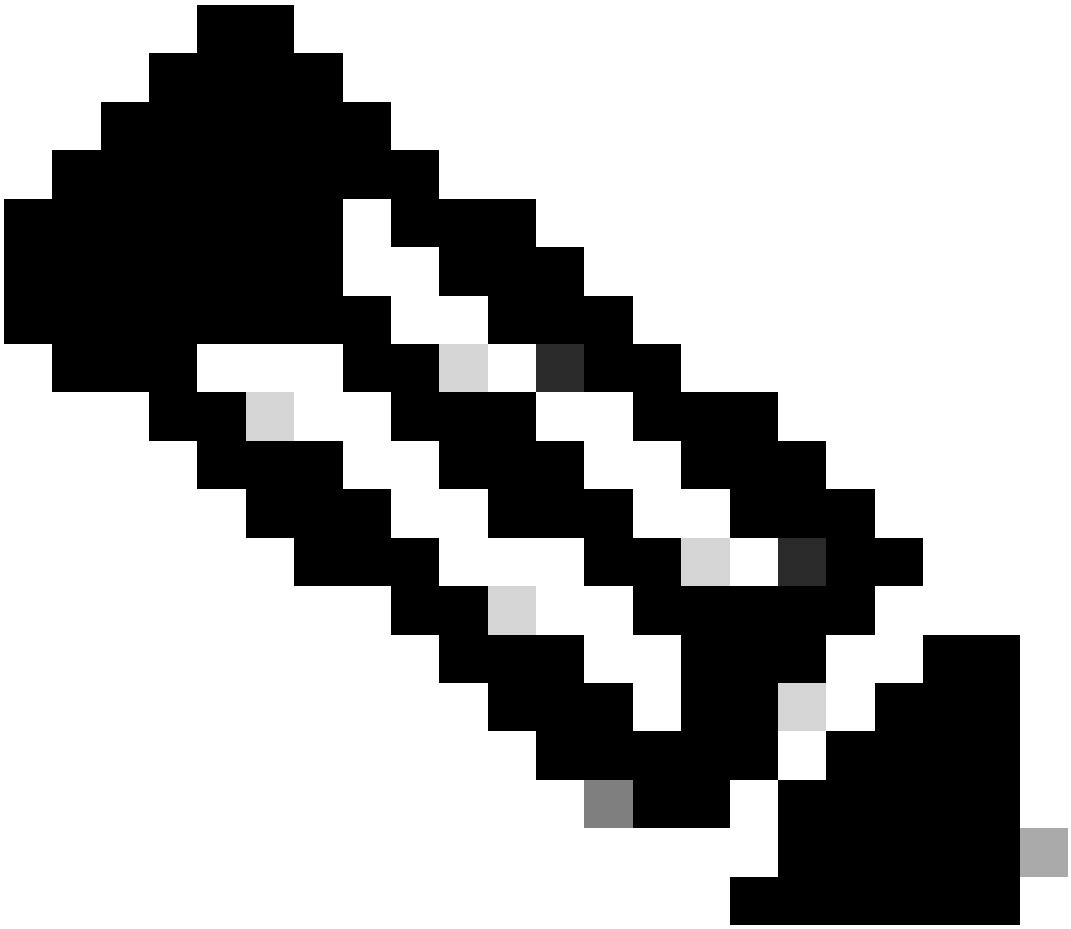
```
<#root>

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.
```

请注意，LISP通知首先由CP接收，然后由CP将其中继到EN。收到此LISP通知时创建SISF或设备跟踪条目，这是该过程的重要部分。您也可以通过以下方式查看此通知：

```
<#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
```

---



注意：元数据部分中突出显示的值12是我们最初打算分配的SGT 18的十六进制版本。这证实整个过程已经顺利完成。

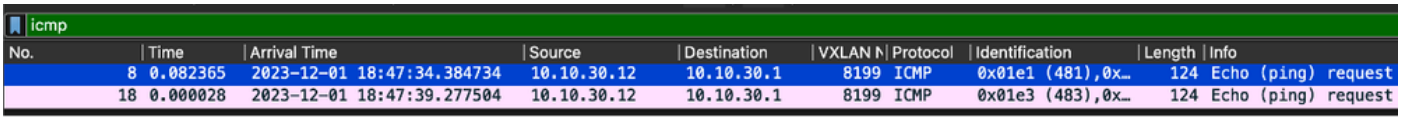
---

## 数据包验证

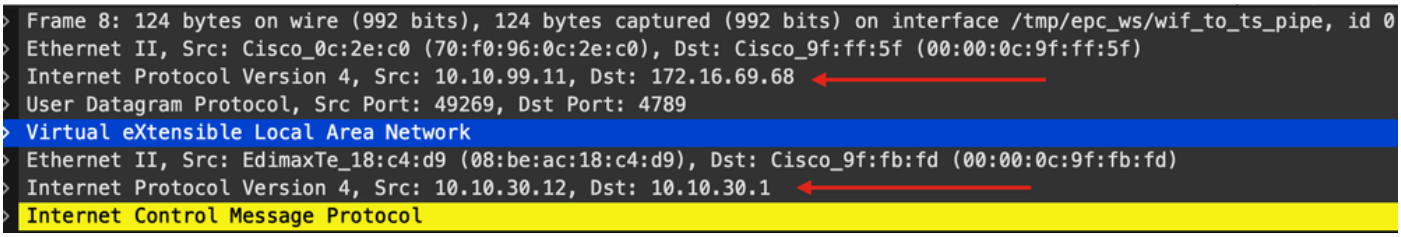
最后，我们还可以使用EN交换机中的嵌入式数据包捕获(EPC)工具，查看此客户端的数据包如何通过AP传输。有关如何通过EPC获取捕获文件的信息，请参阅：

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

在本例中，无线客户端自身发起了对网关的ping：

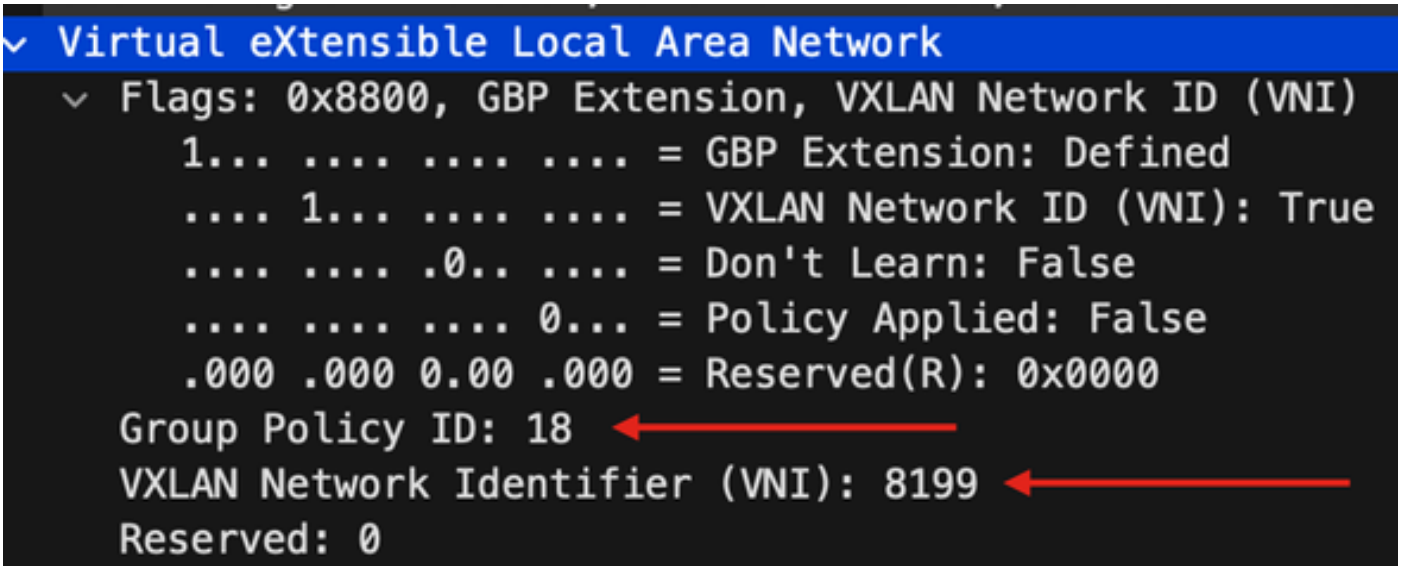



请注意，由于AP和EN为交换矩阵无线客户端在数据包之间形成VXLAN隧道，因此预计数据包将附带来自AP的VXLAN报头：




隧道源是AP IP地址(10.10.99.11)，目标是EN Loopback0 ip地址(172.16.69.68)。在VXLAN报头中，我们可以看到实际的无线客户端数据，本例中为ICMP数据包。

最后，检查VXLAN报头：




注意SGT值作为组策略ID -在本例中，采用ascii格式，L2VNID值作为VXLAN网络标识符(VNI)。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。