瞭解SDA無線上的動態SGT/L2VNID分配

目錄

簡介

本文檔介紹在啟用交換矩陣的無線802.1x SSID上動態SGT和L2VNID分配的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 遠端驗證撥入使用者服務(RADIUS)
- 無線LAN控制器(WLC)
- 身分識別服務引擎 (ISE)
- 安全組標籤(SGT)
- L2VNID（第2層虛擬網路識別符號）
- 支援SD訪問交換矩陣的無線（SDA少）
- Locator/ID Separation Protocol (LISP)
- 虛擬可擴充區域網路(VXLAN)
- 光纖控制平面(CP)和邊緣節點(EN)
- Catalyst Center（CatC，之前稱為Cisco DNA Center）

採用元件

WLC 9800 Cisco IOS® XE版本17.6.4

Cisco IOS® XE

ISE版本2.7

CatC版本2.3.5.6

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

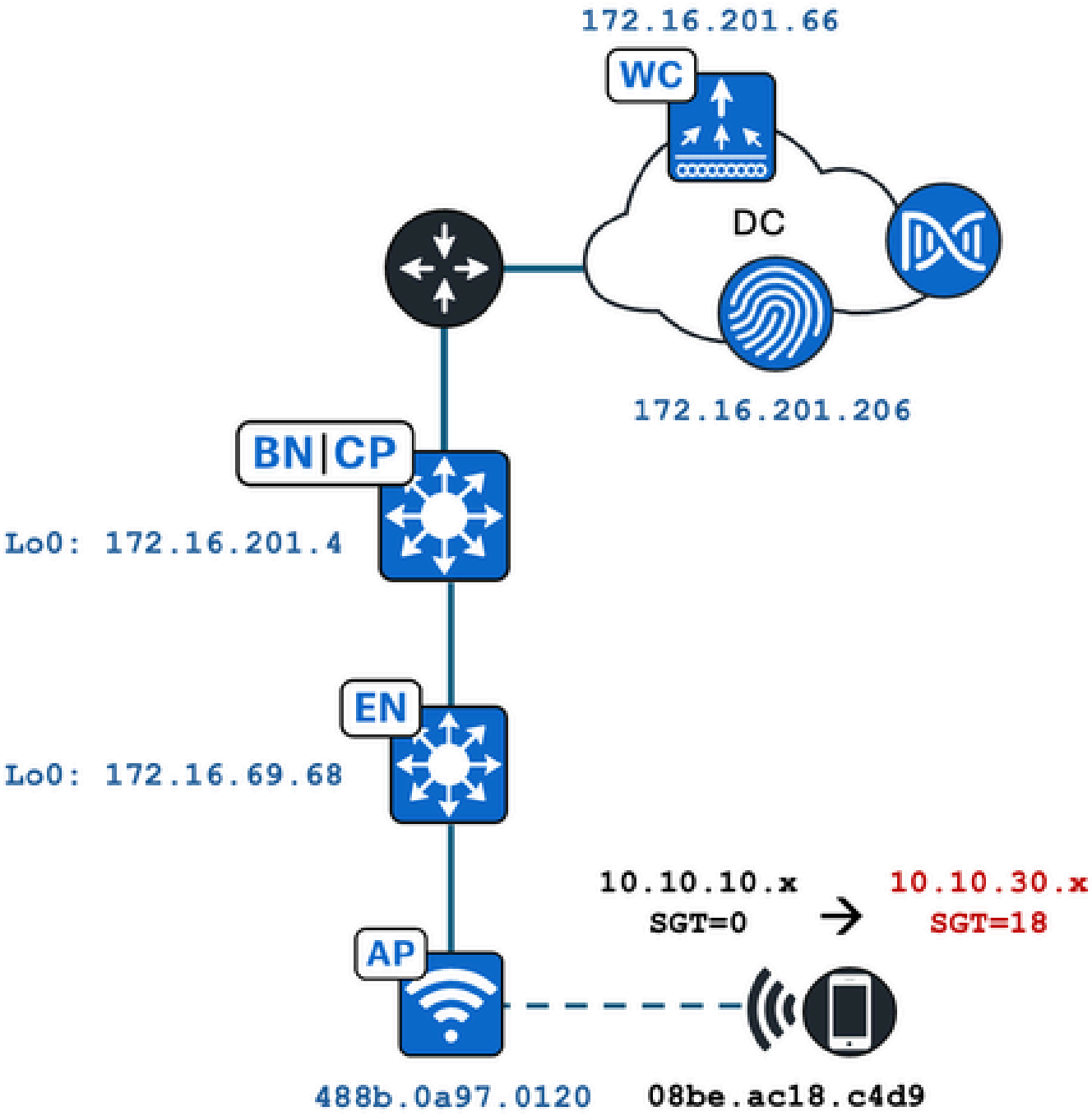
SD-Access的關鍵方面之一是透過Scalable Groups實現的VN中的微分段。

SGT可以按照支援交換矩陣的WLAN或SSID靜態分配（雖然它們不同，但它們的差異不會影響本文檔的主要目標，因此我們可互換使用兩個含義相同的術語以增強可讀性）。但是，在許多實際部署中，通常有連線到同一WLAN的使用者需要一組不同的策略或網路設定。此外，在某些情況下，需要為同一交換矩陣WLAN內的特定客戶端分配不同的IP地址，以便為其應用基於IP的特定策略或滿足公司的IP編址要求。L2VNID（第2層虛擬網路識別符號）是FEW基礎架構用於將無線使用者放置在不同子網範圍內的引數。存取點將VxLAN報頭中的L2VNID傳送到交換矩陣邊緣節點(EN)，然後由交換矩陣邊緣節點將其與相應的L2 VLAN關聯。

為了在同一WLAN中實現此粒度，使用動態SGT和/或L2VNID分配。WLC收集終端的身份資訊，將其傳送到ISE進行身份驗證，ISE使用它來匹配要應用於此客戶端的正確策略，並在身份驗證成功後返回SGT和/或L2VNID資訊。

拓撲

為了瞭解此過程的工作原理，我們使用本實驗拓撲製作了一個示例：



在本示例中，WLAN使用以下命令靜態配置：

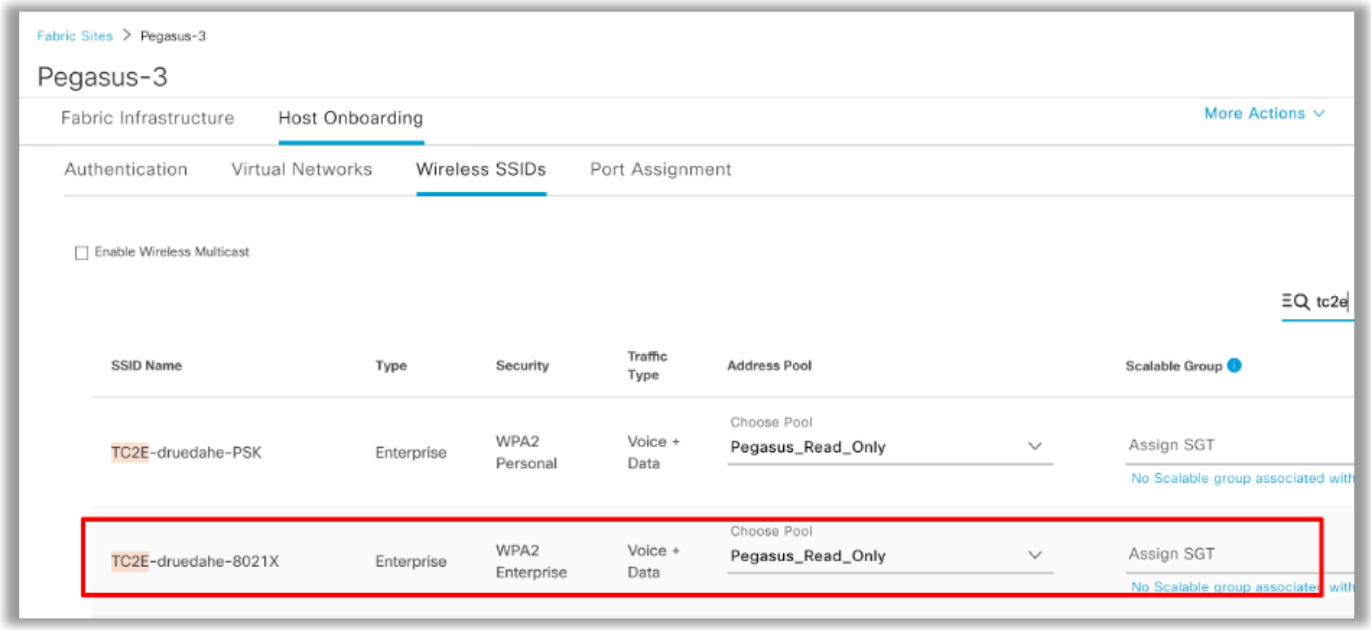
- L2VNID = 8198 / IP池名稱= Pegasus_Read_Only —> VLAN 1030 (10.10.10.x)
- 無SGT

連線的無線使用者端會動態取得下列引數：

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

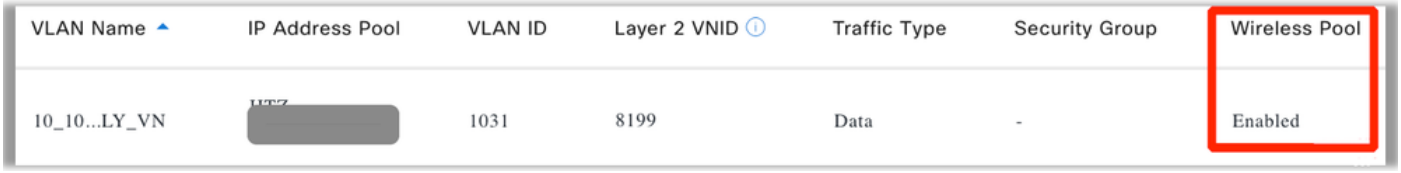
組態

首先，我們需要確定相關的WLAN並檢查其配置方式。本例中使用的是「TC2E-druedahe-802.1x」SSID。在本文檔進行密文時，SDA僅透過CatC受支援，因此我們必須檢查其中配置了什麼配置。在Provision/SD-Access/Fabric Sites/<specific Fabric site>/Host Onboarding/Wireless SSIDs下：



SSID對映了名為「Pegasus_Read_Only」的IP池，並且沒有靜態分配SGT，這意味著SGT=0。這意味著，如果無線客戶端成功連線和身份驗證而未通過ISE傳送任何屬性返回進行動態分配，則這是無線客戶端設定。

動態指定的池必須存在於WLC配置之前。這可以透過在CatC的虛擬網路中將IP池增加為「Wireless Pool」來完成：



在WLC GUI中的Configuration/Wireless/Fabric下，此設定反映以下方式：

「Pegasus_Read_Only」池相當於8198 L2VNID，我們希望我們的客戶端位於8199 L2VNID上，這意味著ISE需要通知WLC為此客戶端使用「10_10_30_0-READONLY_VN」池。請記得，WLC沒有保留光纖VLAN的任何配置。它只知道L2VNID。然後，每個對映到SDA交換矩陣EN中的特定VLAN。

驗證

所報告的涉及SGT/L2VNID動態分配問題的症狀為：

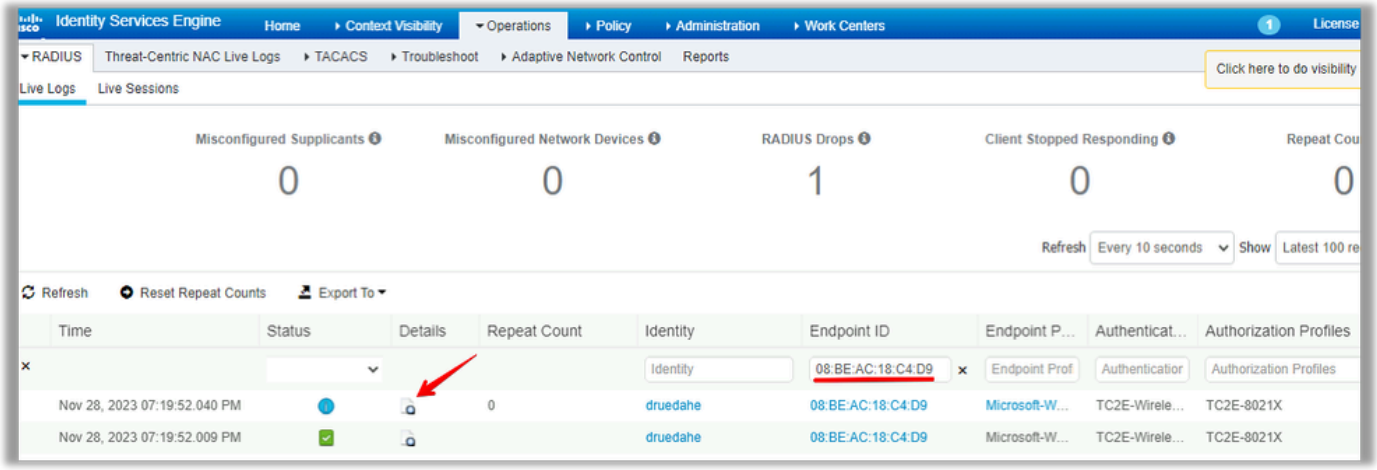
1. 在連線到特定WLAN的無線客戶端上未實施SG策略。（動態SGT分配問題）。
2. 無線客戶端未通過DHCP獲取IP地址，或者未從特定WLAN的所需子網範圍獲取IP地址。（動態L2VNID分配問題）。

現在描述了在這個過程中每個相關節點的驗證。

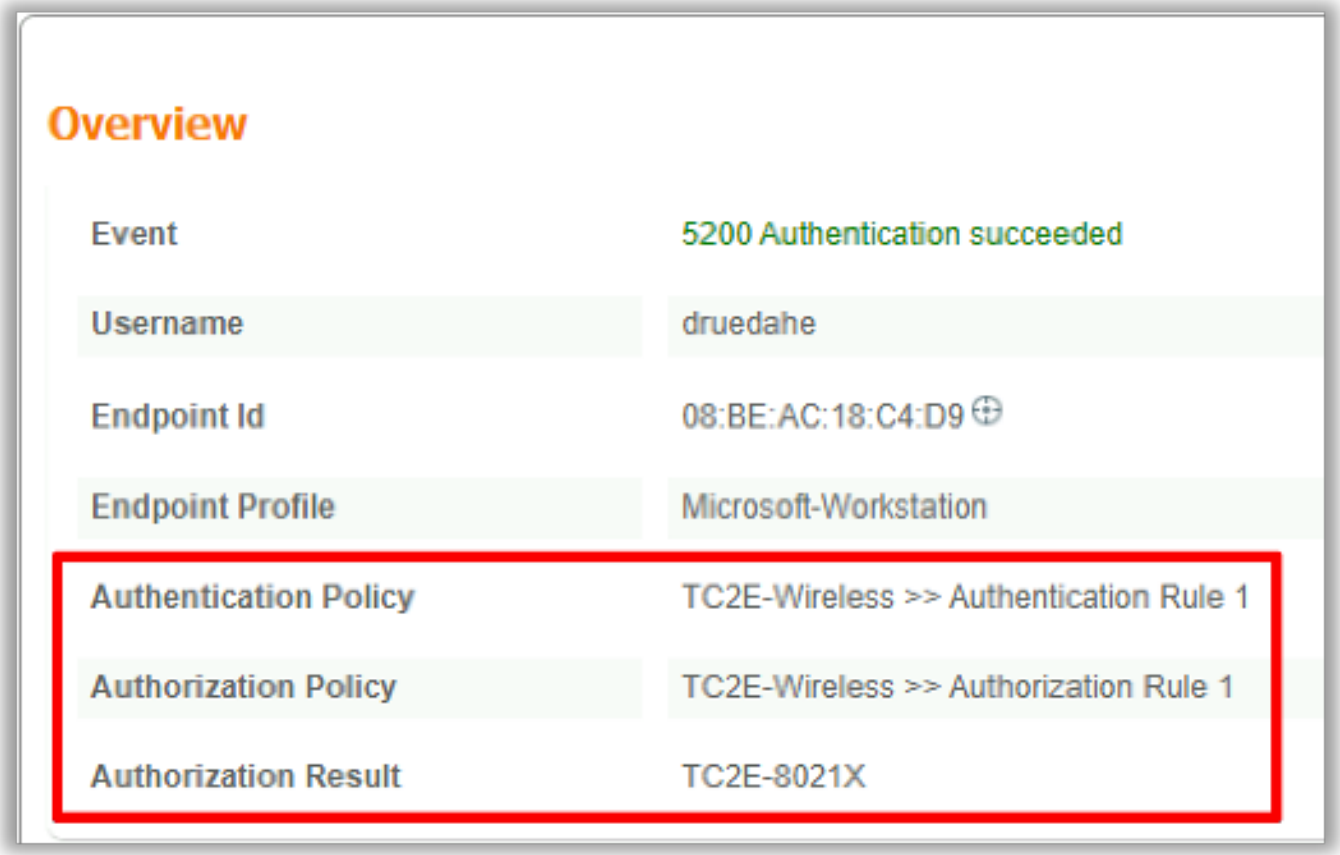
ISE驗證

起點是ISE。轉到ISE GUI的Operation/RADIUS/Live Logs/下並使用無線客戶端MAC地址作為

Endpoint ID欄位中的過濾器，然後點選Details圖示：



然後它會開啟另一個包含驗證詳細資訊的標籤。我們主要關注兩部分，概述和結果：



Overview顯示對此無線客戶端身份驗證使用的是預期策略還是期望策略。如果不是，則需要重新檢視ISE策略配置，但這超出了本文檔的範圍。

結果顯示ISE向WLC返回的內容。目標是動態分配SGT和L2VNID，因此這些資料必須包含在這裡，並且它是。請注意兩點：

1. L2VNID名稱作為「Tunnel-Private-Group-ID」屬性傳送。ISE必須返回名稱(10_10_30_0-READONLY_VN)而不是ID (8199)。

2. SGT作為「cisco-av-pair」傳送。在cts：security-group-tag屬性中，請注意SGT值以十六進位制(12)表示，而非ascii (18)，但它們相同。TC2E_Learers是ISE內部的SGT名稱。

WLC驗證

在WLC中，我們可以使用show wireless fabric client summary命令檢查客戶端狀態，並使用show wireless fabric summary按兩下確認交換矩陣配置和存在動態分配的L2VNID：

```
<#root>

eWLC#

show wireless fabric client summary

Number of Fabric Clients : 1

MAC Address    AP Name                          WLAN State              Protocol Method     L2 VNID    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
```

如果期望的資訊未反映出來，我們可以在WLC中啟用無線客戶端MAC地址的RA跟蹤，以準確檢視

從ISE接收的資料。有關如何獲取特定客戶端的RA Traces輸出的資訊，請參閱以下文檔：

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

在客戶端的RA Trace輸出中，ISE傳送的屬性在RADIUS Access-Accept資料包中傳輸：

<#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
```

然後，WLC將SGT和L2VNID資訊傳送到：

1. 透過CAPWAP（無線存取點的控制和調配）的存取點(AP)。

2. 透過LISP的交換矩陣CP。

交換矩陣CP然後透過LISP將SGT值傳送到連線AP的交換矩陣EN。

交換矩陣EN驗證

下一步是驗證交換矩陣EN是否反映動態接收的資訊。show vlan命令確認與L2VNID 8199關聯的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
```

我們可以看到L2VNID 8199對映到VLAN 1031。

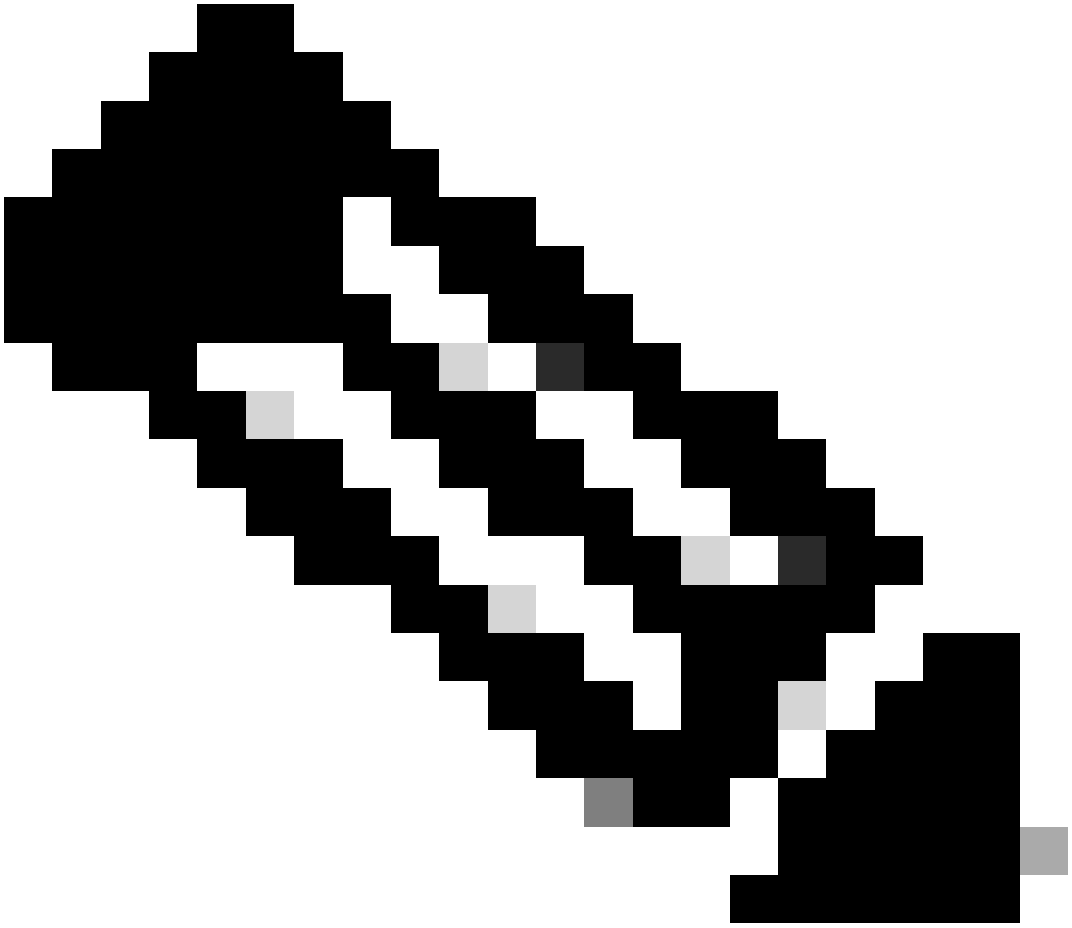
並且，如果無線客戶端位於所需的VLAN上，則會顯示show device-tracking database mac <mac address>：

```
<#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)
```

最後，show cts role-based sgt-map vrf <vrf name> all 命令提供分配給客戶端的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：在適用於無線客戶端的SDA交換矩陣（例如適用於有線客戶端）中，Cisco TrustSec (CTS)策略實施由EN進行，而不是AP或WLC。

這樣，EN可以應用為指定SGT配置的策略。

如果這些輸出填充不正確，我們可以使用EN中的debug lisp control-plane all命令檢查其是否收到來自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.
```

請注意，LISP通知首先由CP接收，然後由CP將其轉發給EN。SISF或裝置跟蹤條目是在收到此LISP通知時建立的，這是該過程的一個重要部分。您也可以檢視以下通知：

<#root>

```
EDGE-01#
```

show lisp instance-id 8199 ethernet database wlc clients detail

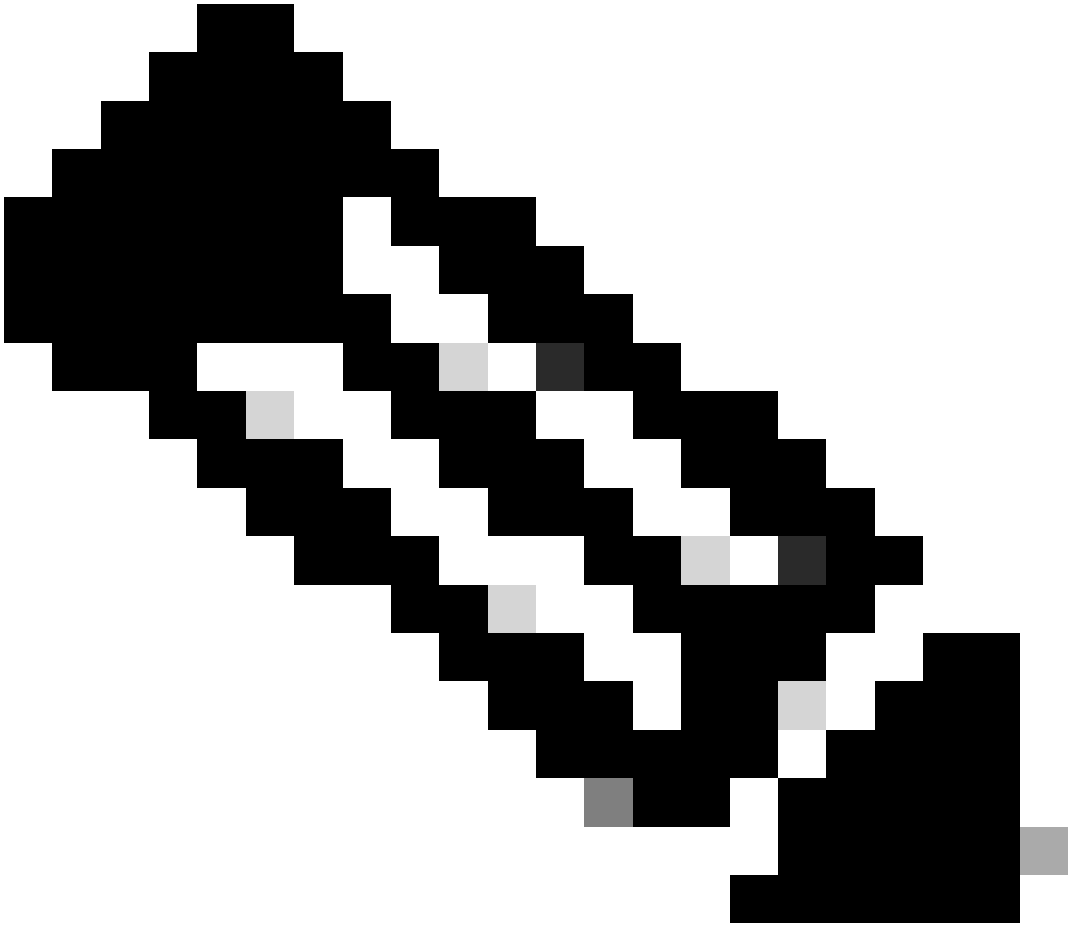
```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 21:23:31.737 UTC Wed Nov 29 2023


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：後設資料部分中突出顯示的值12是我們最初打算分配的SGT 18的十六進製版本。這證實了整個過程是正確完成的。

封包驗證

作為最後確認步驟，我們還可以使用EN交換機中的嵌入式資料包捕獲(EPC)工具，檢視此客戶端的資料包如何透過AP傳輸。有關如何透過EPC獲取捕獲檔案的資訊，請參閱：

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

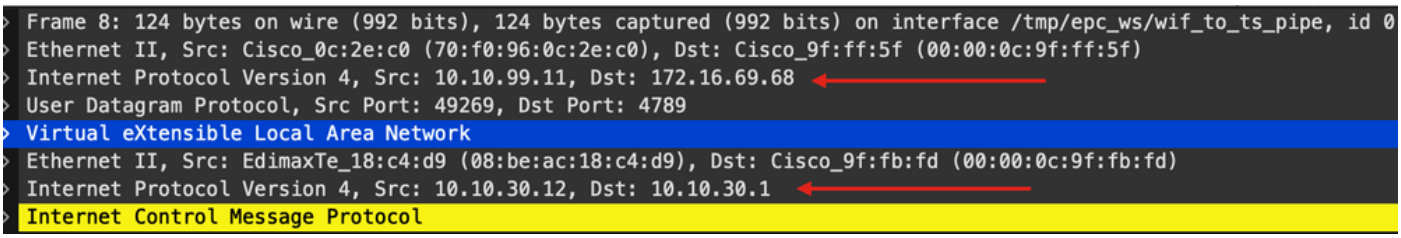
在本範例中，對閘道的ping是在無線使用者端本身中啟動：

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

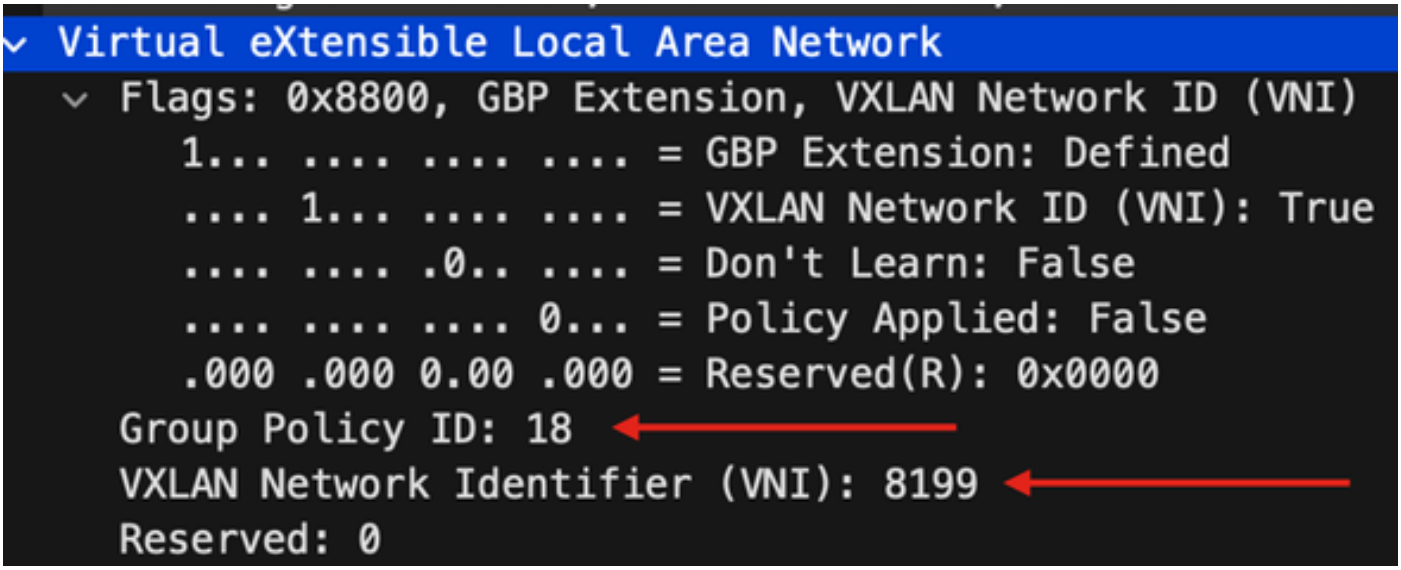
請注意，資料包預期會附帶來自AP的VXLAN報頭，因為AP和EN在它們之間為交換矩陣無線客戶端

形成VXLAN隧道：



隧道的源是AP IP地址(10.10.99.11)，目標是EN Loopback0 IP地址(172.16.69.68)。在VXLAN標頭中，我們可以看到實際的無線使用者端資料，在此案例中為ICMP封包。

最後，檢查VXLAN標頭：



將SGT值記為組策略ID —在本例中為ascii格式，並將L2VNID值記為VXLAN網路識別符號(VNI)。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。