SDA 무선에서 동적 SGT/L2VNID 할당 이해

목차

소개

이 문서에서는 Fabric Enabled Wireless 802.1x SSID에서 동적 SGT 및 L2VNID 할당 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS(Remote Authentication Dial-In User Service)
- 무선 LAN 컨트롤러(WLC)
- Identity Services Engine(ISE)
- SGT(보안 그룹 태그)
- L2VNID(레이어 2 가상 네트워크 식별자)
- SD-Access Fabric Enabled Wireless(SDA 소수)
- LISP(Locator/ID Separation Protocol)
- VXLAN(Virtual eXtensible Local Area Network)
- CP(패브릭 제어 평면) 및 EN(에지 노드)
- Catalyst Center(CatC, 이전의 Cisco DNA Center)

사용되는 구성 요소

WLC 9800 Cisco IOS® XE 버전 17.6.4

Cisco IOS® XE

ISE 버전 2.7

CatC 버전 2.3.5.6

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

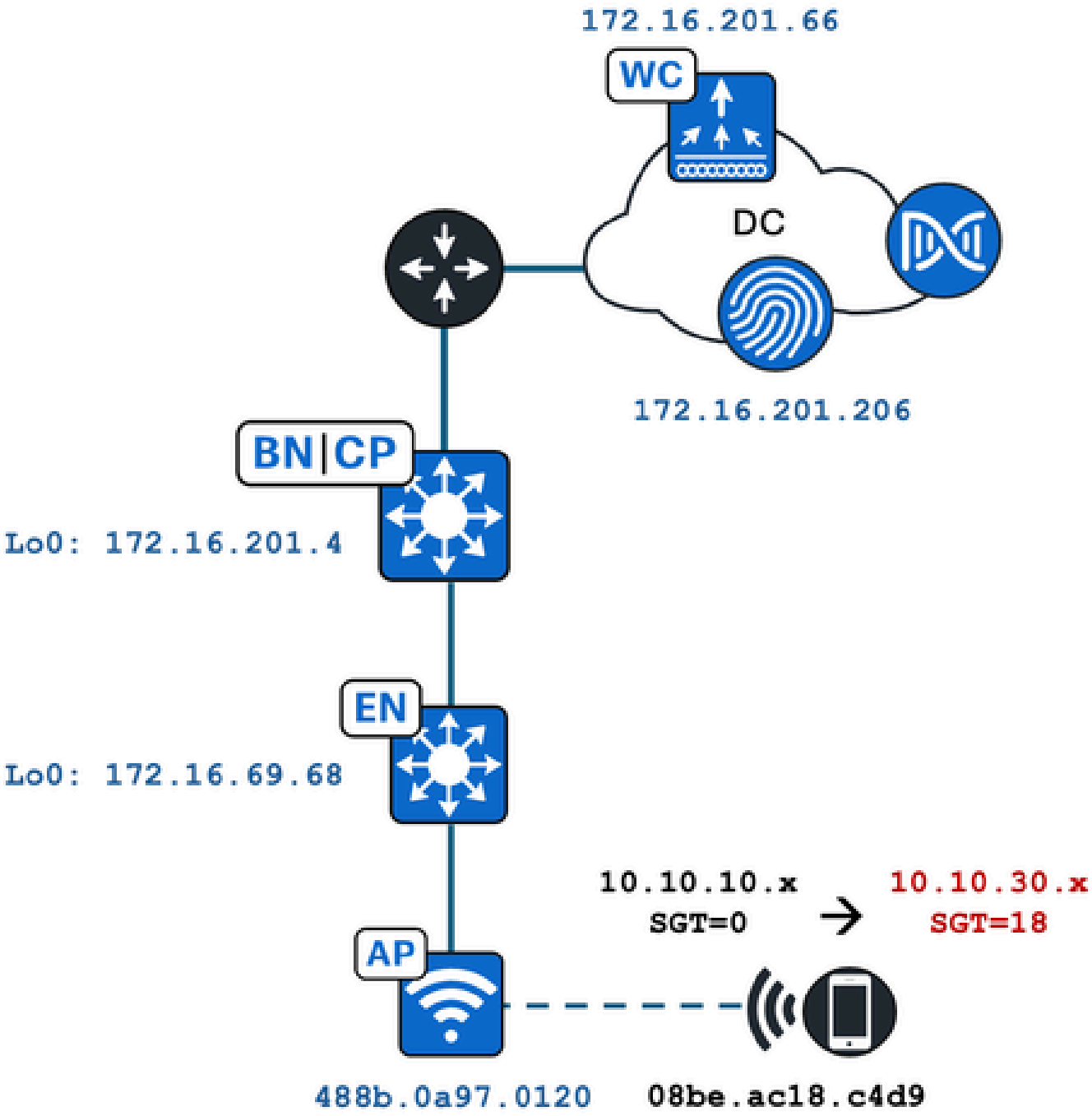
SD-Access의 핵심 요소 중 하나는 Scalable Groups를 통해 달성되는 VN 내의 마이크로 세그멘테이션입니다.

SGT는 Fabric Enabled WLAN 또는 SSID마다 정적으로 할당할 수 있습니다(동일한 것은 아니지만 차이가 이 문서의 기본 목표에 영향을 미치지 않으므로 가독성을 높이기 위해 동일한 의미로 두 용어를 교대로 사용합니다). 그러나 실제 구축의 경우 동일한 WLAN에 연결하는 사용자가 종종 있으며, 이러한 사용자들은 서로 다른 정책 또는 네트워크 설정을 요구합니다. 또한 일부 시나리오에서는 동일한 패브릭 WLAN 내의 특정 클라이언트에 특정 IP 기반 정책을 적용하거나 회사 IP 주소 지정 요건을 충족하기 위해 서로 다른 IP 주소를 할당해야 합니다. L2VNID(L2VNID(Layer 2 Virtual Network Identifier)는 FEW 인프라에서 무선 사용자를 서로 다른 서브넷 범위에 배치하는 데 사용하는 매개변수입니다. 액세스 포인트는 VxLAN 헤더의 L2VNID를 Fabric Edge Node(EN)로 전송한 다음 해당 L2 VLAN과 상관관계를 맺습니다.

동일한 WLAN 내에서 이러한 세분화를 달성하기 위해 동적 SGT 및/또는 L2VNID 할당을 활용합니다. WLC는 엔드 포인트의 ID 정보를 수집 하고 인증을 위해 ISE에 전송 하고, 이 클라이언트에 적용할 적절 한 정책을 일치 하는 데 사용 하고 성공 적 인 인증에 SGT 및/또는 L2VNID 정보를 반환 합니다.

토폴로지

이 프로세스의 작동 방식을 파악하기 위해 이 Lab 토폴로지를 사용하여 예시를 개발했습니다.



이 예에서는 WLAN이 다음으로 정적으로 구성됩니다.

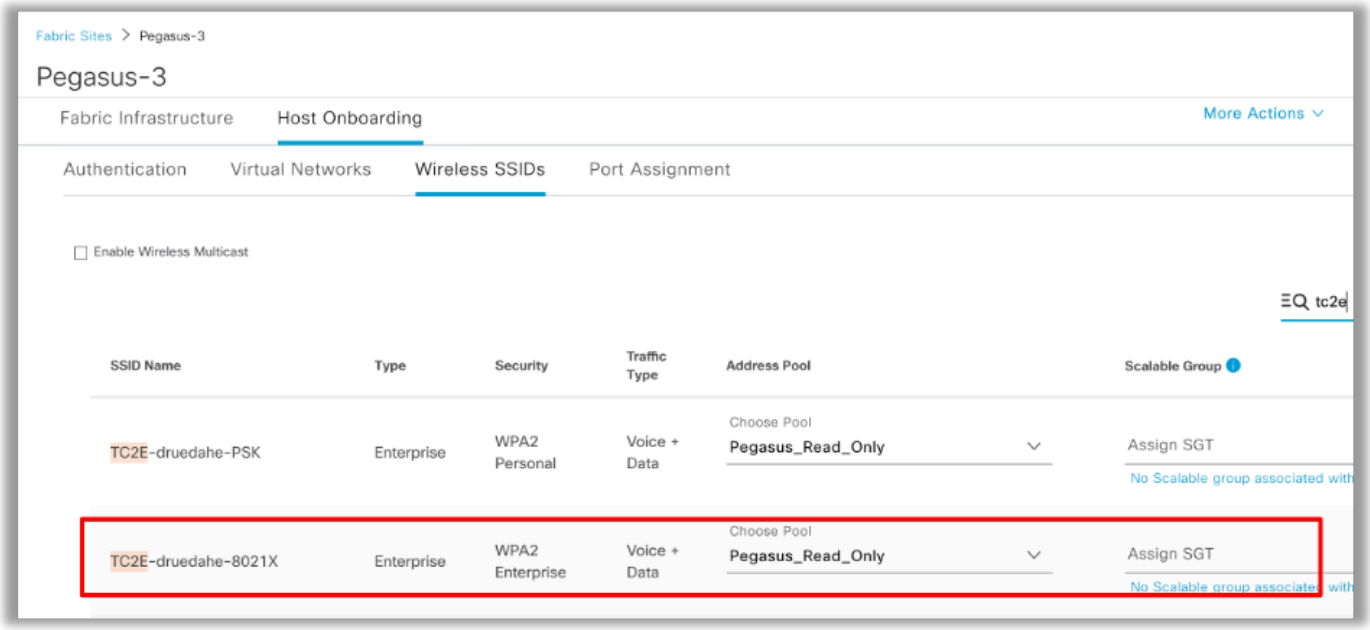
- L2VNID = 8198 / IP 풀 이름 = Pegasus_Read_Only —> VLAN 1030(10.10.10.x)
- SGT 없음

그리고 여기에 연결하는 무선 클라이언트는 다음 매개변수를 동적으로 가져옵니다.

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

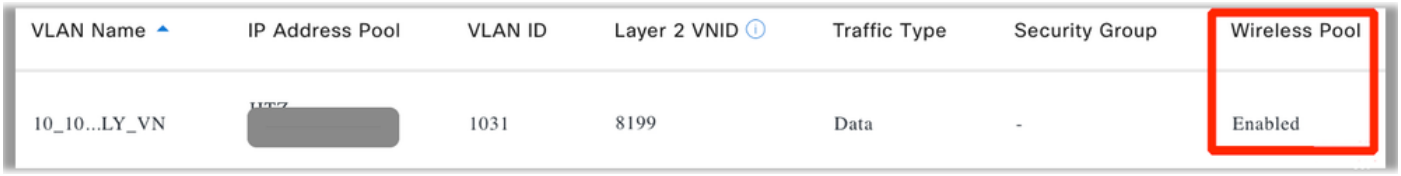
설정

먼저, 관련 WLAN을 식별하고 구성된 방법을 확인해야 합니다. 이 예에서는 "TC2E-druedahe-802.1x" SSID가 사용됩니다. 이 문서를 수정할 때 SDA는 CatC를 통해서만 지원되므로 어떤 구성이 되어 있는지 확인해야 합니다. Provision/SD-Access/Fabric Sites/<특정 패브릭 사이트>/Host Onboarding/Wireless SSIDs 아래에서 다음을 수행합니다.



SSID에는 "Pegasus_Read_Only"라는 이름의 IP 풀이 매핑되어 있으며 SGT가 정적으로 할당되어 있지 않습니다. 이는 SGT=0을 의미합니다. 즉, ISE가 동적 할당을 위해 어떤 특성도 다시 전송하지 않고 무선 클라이언트가 성공적으로 연결 및 인증하면 무선 클라이언트 설정은 다음과 같습니다.

동적으로 할당되는 풀은 WLC 컨피그레이션 이전에 있어야 합니다. 이는 CatC의 가상 네트워크에서 IP 풀을 "무선 풀"로 추가하는 방식으로 수행됩니다.



Configuration/Wireless/Fabric(컨피그레이션/무선/패브릭) 아래의 WLC GUI에서 이 설정은 다음 방법을 반영합니다.

"Pegasus_Read_Only" 풀은 8198 L2VNID와 동일하며, 클라이언트가 8199 L2VNID에 있기를 원합니다. 즉, ISE가 WLC에 이 클라이언트에 대해 "10_10_30_0-READONLY_VN" 풀을 사용하도록 지시해야 합니다. WLC는 패브릭 VLAN에 대한 컨피그레이션을 보유하지 않습니다. L2VNID만 인식합니다. 그런 다음 각 VLAN은 SDA 패브릭 EN의 특정 VLAN에 매핑됩니다.

확인

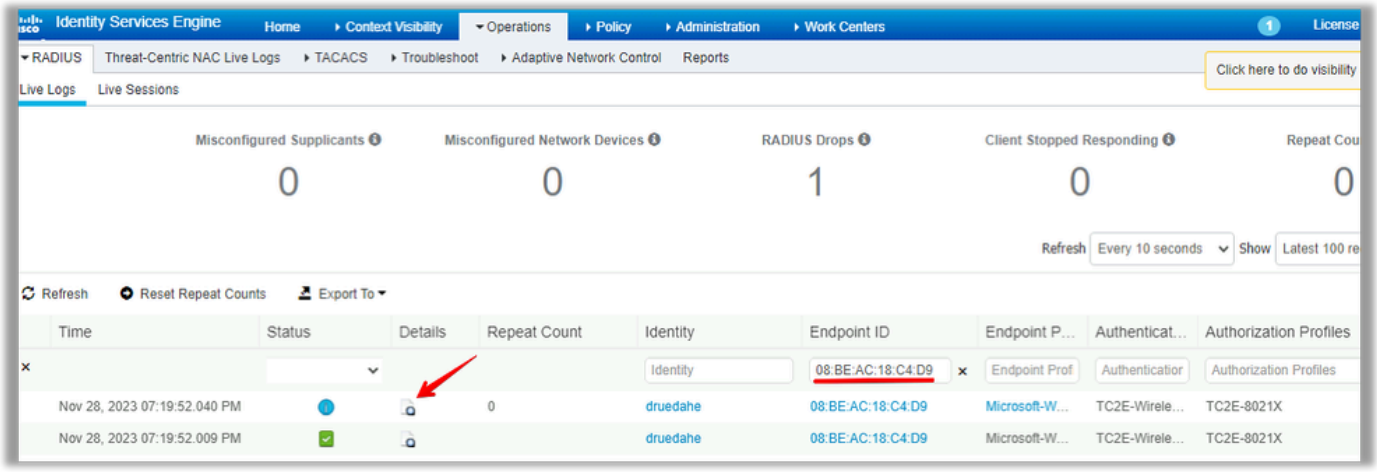
SGT/L2VNID의 동적 할당과 관련된 문제에 대해 보고된 증상은 다음 중 하나입니다.

1. SG 정책은 특정 WLAN에 연결하는 무선 클라이언트에 적용되지 않습니다(동적 SGT 할당 문제).
2. 무선 클라이언트가 DHCP를 통해 IP 주소를 가져오지 않거나 특정 WLAN의 원하는 서브넷 범위에서 IP 주소를 가져오지 않습니다(동적 L2VNID 할당 문제).

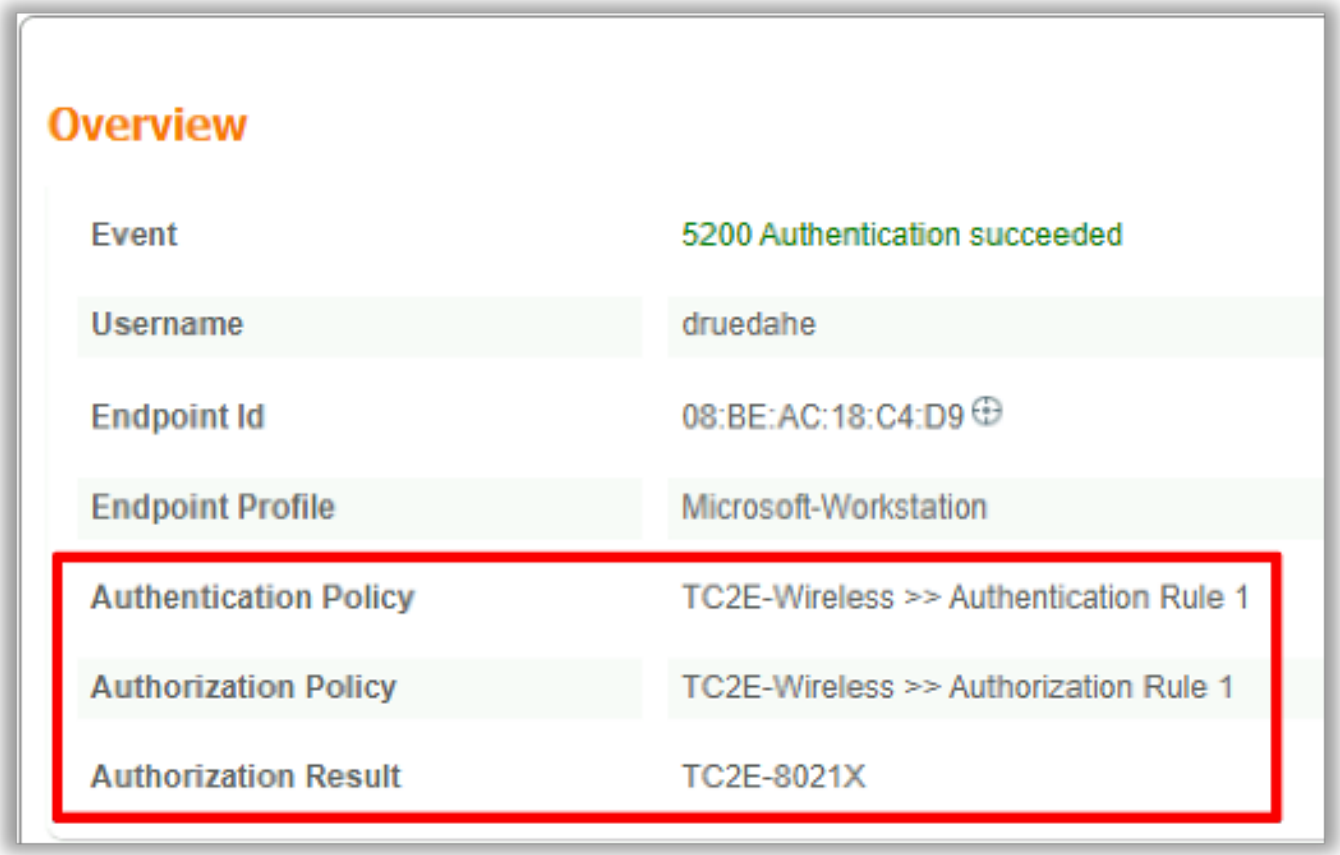
이제 이 프로세스에서 각 관련 노드의 검증에 대해 설명합니다.

ISE 확인

그 출발점은 ISE입니다. Operation/RADIUS/Live Logs/(작업/RADIUS/라이브 로그) 아래의 ISE GUI로 이동하여 무선 클라이언트 mac 주소를 Endpoint ID(엔드포인트 ID) 필드의 필터로 사용한 다음 Details(세부사항) 아이콘을 클릭합니다.



그런 다음 인증 세부사항이 있는 다른 탭이 열립니다. 여기서는 주로 개요 및 결과 두 섹션에 대해 알아봅니다.



개요는 이 무선 클라이언트 인증에 의도한 정책 또는 원하는 정책이 사용되었는지 보여줍니다. 그렇지 않은 경우 ISE 정책 컨피그레이션을 다시 방문해야 하지만, 이는 이 문서의 범위를 벗어납니다.

결과는 ISE에서 WLC로 반환된 내용을 보여줍니다. 목표는 SGT와 L2VNID가 동적으로 할당되는

것이므로 이 데이터는 여기에 포함되어야 하며, 이 데이터는 여기에 포함됩니다. 다음 두 가지 사항을 확인합니다.

1. L2VNID 이름이 "Tunnel-Private-Group-ID" 특성으로 전송됩니다. ISE는 ID(8199)가 아닌 이름(10_10_30_0-READONLY_VN)을 반환해야 합니다.

2. SGT는 "cisco-av-pair"로 전송됩니다. cts:security-group-tag 속성에서 SGT 값은 ascii(18)가 아니라 16진수(12)이지만 동일합니다. TC2E_Learners는 내부적으로 ISE의 SGT 이름입니다.

WLC 확인

WLC에서 show wireless fabric client summary 명령을 사용하여 클라이언트 상태를 확인하고 show wireless fabric summary를 사용하여 패브릭 컨피그레이션과 동적으로 할당된 L2VNID가 있는지 두 번 확인할 수 있습니다.

<#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
```

예상 정보가 반영되지 않으면 WLC에서 무선 클라이언트 mac 주소에 대한 RA 추적을 활성화하여 ISE에서 수신한 데이터를 정확하게 확인할 수 있습니다. 특정 클라이언트에 대한 RA 추적 출력을 얻는 방법에 대한 정보는 다음 문서에서 확인할 수 있습니다.

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

클라이언트에 대한 RA 추적 출력에서 ISE가 전송한 특성은 RADIUS Access-Accept 패킷에서 전달됩니다.

<#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
```

그런 다음 WLC는 SGT 및 L2VNID 정보를 다음으로 전송합니다.

1. CAPWAP(Control And Provisioning of Wireless Access Points)를 통한 액세스 포인트(AP)

2. LISP를 통한 패브릭 CP

그런 다음 패브릭 CP는 LISP를 통해 AP가 연결된 패브릭 EN에 SGT 값을 전송합니다.

패브릭 EN 확인

다음 단계는 패브릭 EN이 동적으로 수신한 정보를 반영하는지 확인하는 것입니다. show vlan 명령은 L2VNID 8199와 연결된 VLAN을 확인합니다.

<#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

우리는 L2VNID 8199가 VLAN 1031에 매핑된 것을 확인할 수 있습니다.

그리고 무선 클라이언트가 원하는 VLAN에 있는지 show device-tracking database mac <mac address>가 표시됩니다.

<#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

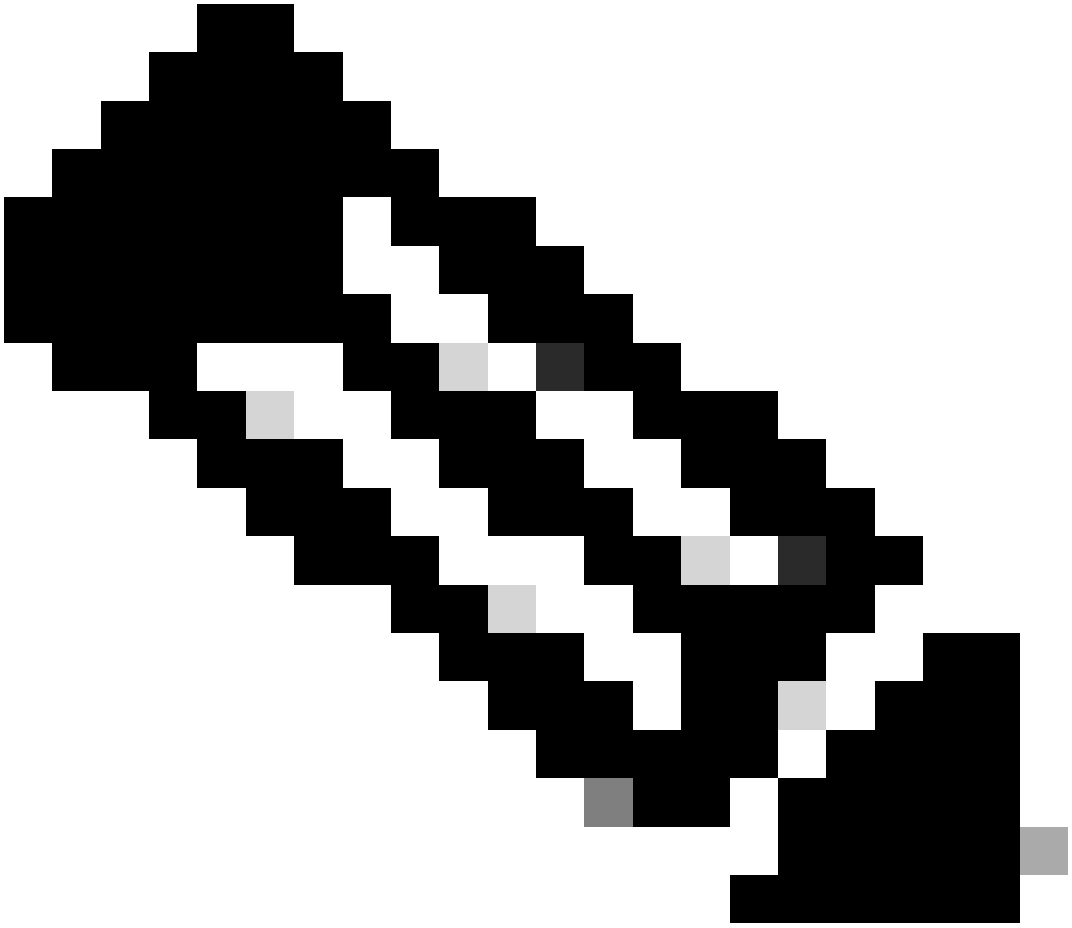
Network Layer Address Link Layer Address Interface vlan prlvl age state
macDB has 0 entries for mac 08be.ac18.c4d9,vlan 1028, 0 dynamic
macDB has 2 entries for mac 08be.ac18.c4d9,vlan 1030, 0 dynamic
DH4

10.10.30.12 08be.ac18.c4d9

```
     Ac1
1031
  0025  96s    REACHABLE 147 s try 0(691033 s)
```

마지막으로 show cts role-based sgt-map vrf <vrf name> all 명령은 클라이언트에 할당된 SGT 값을 제공합니다. 이 예에서 VLAN 1031은 "READONLY_VN" VRF의 일부입니다.

```
<#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
```



참고: 무선 클라이언트용 SDA 패브릭(예: 유선 클라이언트)에서 Cisco TrustSec(CTS) 정책을 적용하는 작업은 AP나 WLC가 아니라 EN에서 수행합니다.

이를 통해 EN은 지정된 SGT에 대해 구성된 정책을 적용할 수 있습니다.

이러한 출력이 제대로 입력되지 않으면 EN의 debug lisp control-plane all 명령을 사용하여 WLC에서 오는 LISP 알림을 수신하는지 확인할 수 있습니다.

<#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.
```

LISP 알림은 먼저 CP에 의해 수신되며, CP는 이를 EN에 중계합니다. 이 LISP 알림을 수신하면 SISF 또는 디바이스 추적 항목이 생성되며, 이는 프로세스의 중요한 부분입니다. 다음 항목을 사용하여 이 알림을 볼 수도 있습니다.

<#root>

```
EDGE-01#
```

show lisp instance-id 8199 ethernet database wlc clients detail

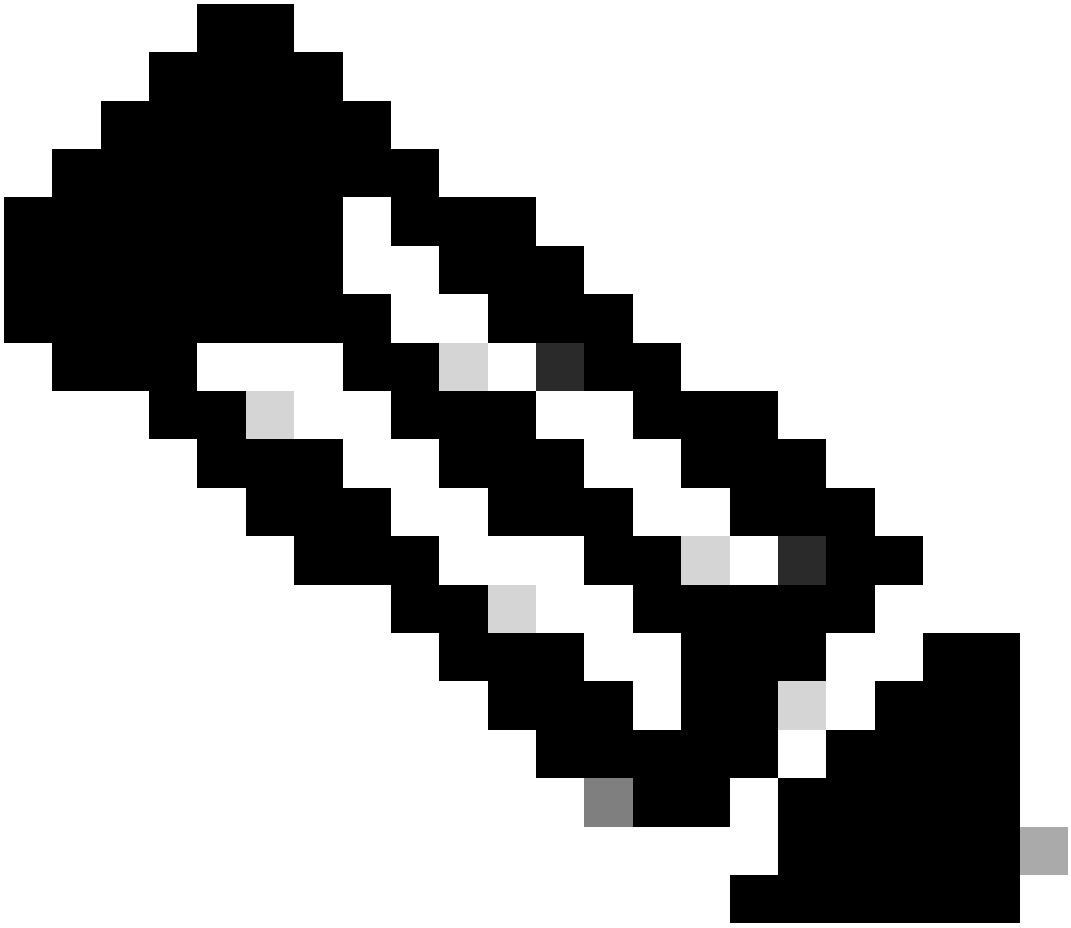
```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 21:23:31.737 UTC Wed Nov 29 2023


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
```



참고: Metadata(메타데이터) 섹션에서 강조 표시된 값 12는 처음에 할당하려고 했던 SGT 18의 16진수 버전입니다. 그리고 이것은 모든 과정이 제대로 끝났다는 것을 확인시켜줍니다.

패킷 확인

마지막 확인 단계에서는 EN 스위치에서 EPC(Embedded Packet Capture) 툴을 사용하여 이 클라이언트의 패킷이 AP에 의해 전송되는 방식을 확인할 수도 있습니다. EPC를 사용하여 캡처 파일을 가져오는 방법에 대한 자세한 내용은 다음을 참조하십시오.

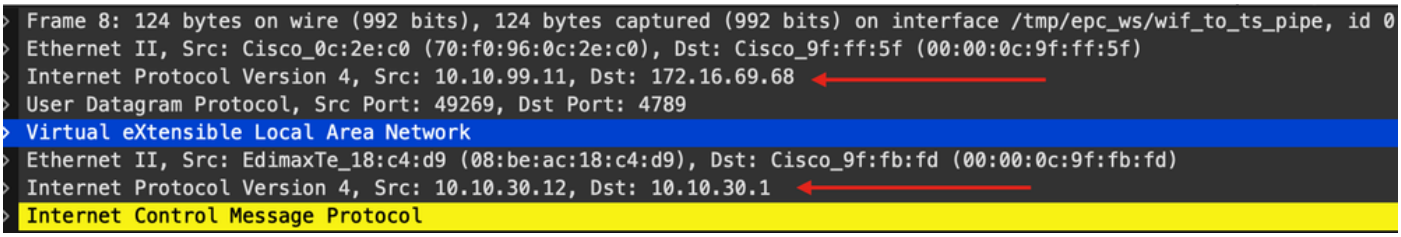
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_packet_capture.html

이 예에서는 무선 클라이언트 자체에서 게이트웨이에 대한 ping이 시작되었습니다.

icmp

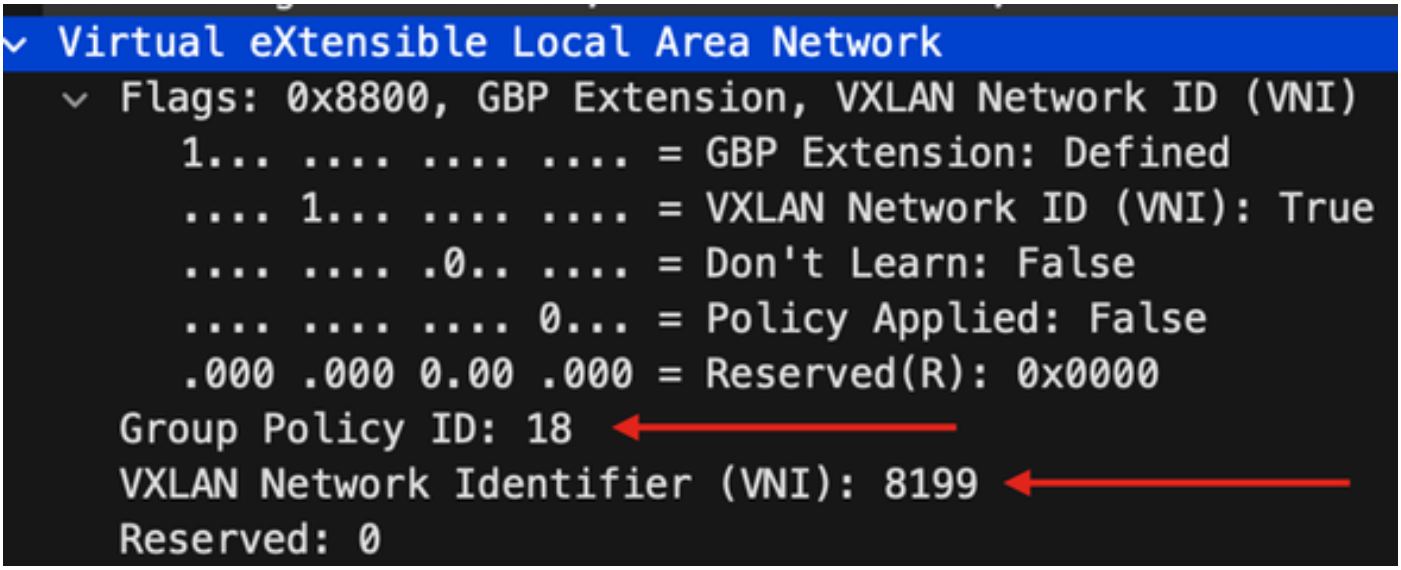
No.	Time	Arrival Time	Source	Destination	VXLAN N	Protocol	Identification	Length	Info
8	0.082365	2023-12-01 18:47:34.384734	10.10.30.12	10.10.30.1	8199	ICMP	0x01e1 (481),0x…	124	Echo (ping) request
18	0.000028	2023-12-01 18:47:39.277504	10.10.30.12	10.10.30.1	8199	ICMP	0x01e3 (483),0x…	124	Echo (ping)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

AP와 EN이 패브릭 무선 클라이언트에 대해 VXLAN 터널을 형성하므로 패킷은 AP의 VXLAN 헤더와 함께 이미 와야 합니다.



터널의 소스는 AP ip 주소(10.10.99.11)이고 대상은 EN Loopback0 ip 주소(172.16.69.68)입니다. VXLAN 헤더 내부에는 실제 무선 클라이언트 데이터(이 경우 ICMP 패킷)가 표시됩니다.

마지막으로, VXLAN 헤더를 검사합니다.



SGT 값을 그룹 정책 ID로 기록합니다. 이 경우 ascii 형식으로, L2VNID 값을 VXLAN 네트워크 식별자(VNI)로 지정합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.