SDAワイヤレスでのダイナミックSGT/L2VNID割り当てについて

内容

はじめに

このドキュメントでは、ファブリック対応ワイヤレス802.1x SSIDでのダイナミックSGTおよびL2VNID割り当てのプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Remote Authentication Dial-In User Service（RADIUS）
- ワイヤレス LAN コントローラ（WLC）
- Identity Services Engine（ISE）
- セキュリティ グループ タグ（SGT）
- L2VNID（レイヤ2仮想ネットワーク識別子）
- SDアクセスファブリック対応ワイヤレス（SDA少数）
- ロケータ/ID分離プロトコル(LISP)
- Virtual eXtensible Local Area Network(VXLAN)
- ファブリックコントロールプレーン(CP)およびエッジノード(EN)
- Catalyst Center（CatC、旧称Cisco DNA Center）

使用するコンポーネント

WLC 9800 Cisco IOS® XEバージョン17.6.4

Cisco IOS® XE

ISE バージョン 2.7

CatCバージョン2.3.5.6

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

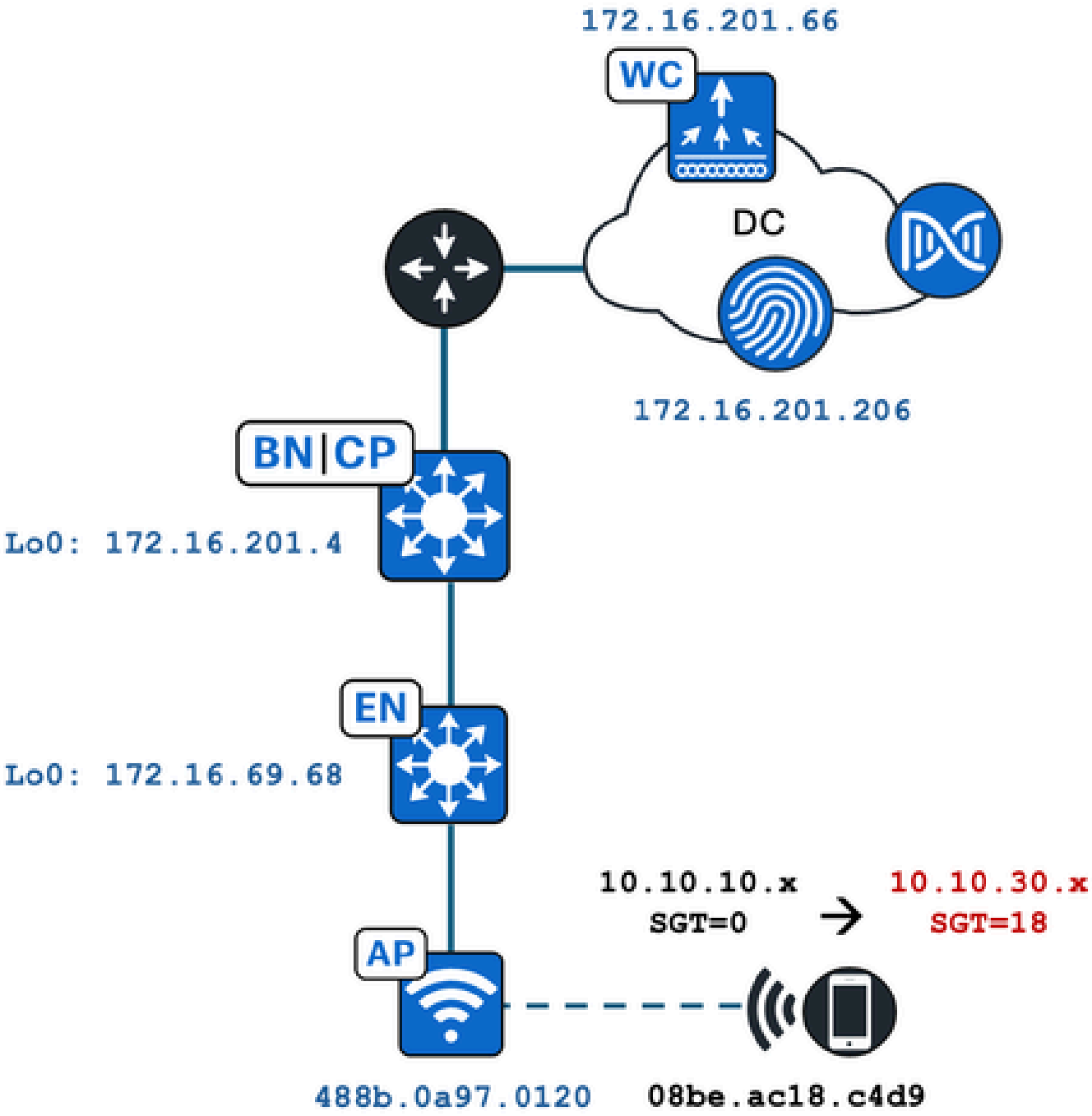
SD-Accessの重要な側面の1つは、VN内でのマイクロセグメンテーションがスケーラブルグループを介して実現することです。

SGTは、ファブリック対応WLANまたはSSIDごとに静的に割り当てることができます（これらは同じではありませんが、その違いはこのドキュメントの主な目的には影響しないため、読みやすさを向上させるために同じ意味で2つの用語を互換的に使用します）。しかし、実際の導入では、同じWLANに接続するユーザが異なるポリシーセットやネットワーク設定を必要とすることがよくあります。さらに、シナリオによっては、特定のIPベースのポリシーを適用するか、会社のIPアドレッシング要件を満たすために、同じファブリックWLAN内の特定のクライアントに異なるIPアドレスを割り当てる必要があります。L2VNID（レイヤ2仮想ネットワーク識別子）は、いくつかのインフラストラクチャが異なるサブネット範囲に無線ユーザを配置するために使用するパラメータです。アクセスポイント(AP)はVxLANヘッダー内のL2VNIDをファブリックエッジノード(EN)に送信し、対応するL2 VLANに関連付けます。

同じWLAN内でこの粒度を実現するには、ダイナミックSGTまたはL2VNID割り当てを使用します。WLCはエンドポイントのID情報を収集し、それを認証のためにISEに送信します。ISEはこの情報を使用して、このクライアントに適用される適切なポリシーを照合し、認証に成功すると、SGTやL2VNID情報を返します。

トポロジ

このプロセスの仕組みを理解するために、次のラボトポロジを使用して例を作成しました。



この例では、WLANは次のように静的に設定されています。

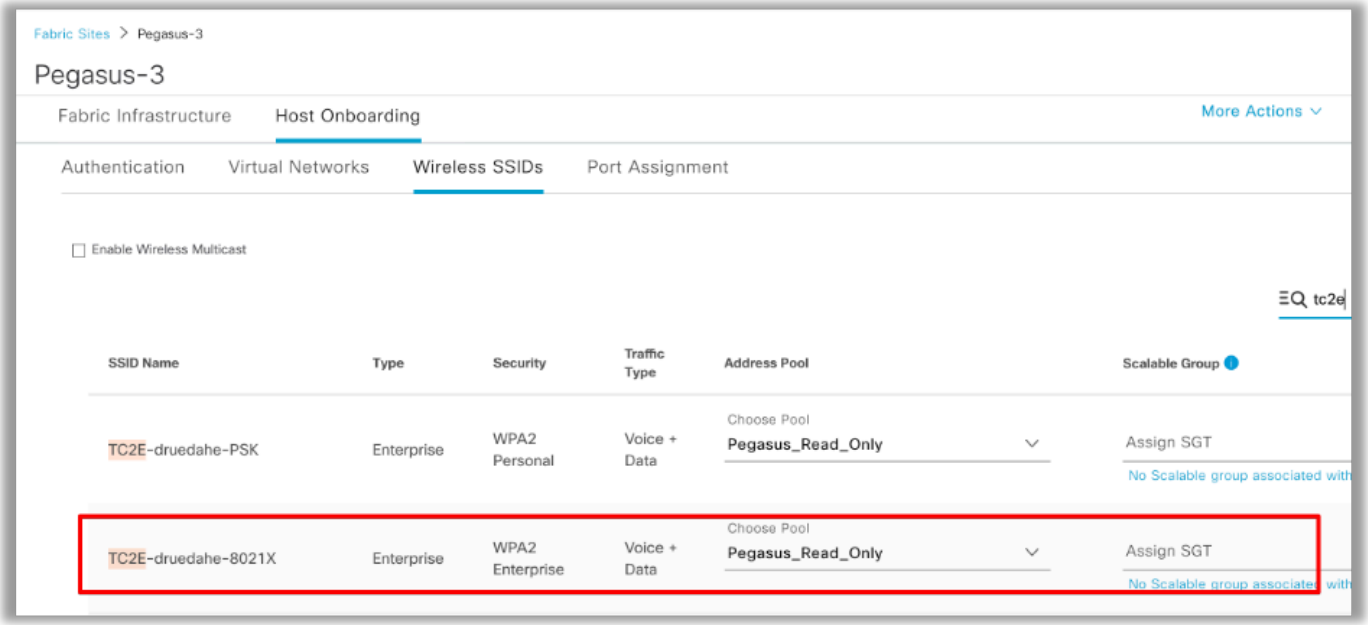
- L2VNID = 8198 / IPプール名= Pegasus_Read_Only —> VLAN 1030(10.10.10.x)
- SGTなし

また、それに接続しているワイヤレスクライアントは、動的に次のパラメータを取得します。

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

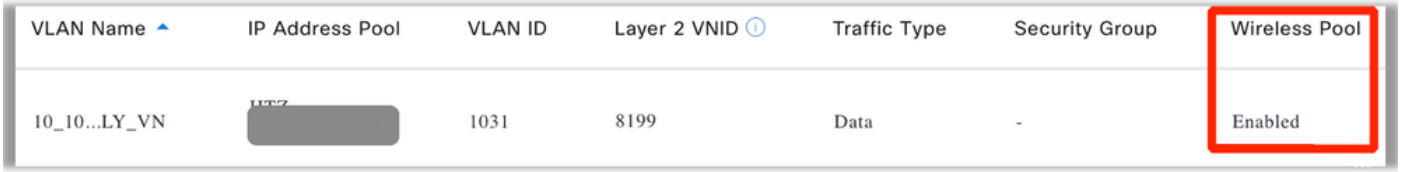
コンフィギュレーション

まず、関連するWLANを特定し、その設定方法を確認する必要があります。この例では、「TC2E-druedahe-802.1x」というSSIDが使用されます。このドキュメントの改訂時点では、SDAはCatC経由でのみサポートされているため、設定を確認する必要があります。プロビジョニング/SDアクセス/ファブリックサイト/<特定のファブリックサイト>/ホストオンボーディング/ワイヤレスSSIDの下：



SSIDには、「Pegasus_Read_Only」という名前のIPプールがマッピングされており、SGTが静的に割り当てられていません。これは、SGT=0を意味します。つまり、ISEがダイナミック割り当てのために属性を返送することなく、ワイヤレスクライアントが正常に接続および認証された場合、ワイヤレスクライアントの設定はこのようになります。

動的に割り当てられるプールは、WLC設定の前に存在している必要があります。これを行うには、CatC上の仮想ネットワークにIPプールを「ワイヤレスプール」として追加します。



WLCのGUIのConfiguration/Wireless/Fabricの下では、この設定は次のように反映されます。

「Pegasus_Read_Only」プールは8198 L2VNIDと同じであり、クライアントを8199 L2VNID上に配置します。つまり、ISEはWLCに対して、このクライアントに「10_10_30_0-READONLY_VN」プールを使用するように指示する必要があります。WLCではファブリックVLANの設定は保持されないことに注意してください。L2VNIDのみを認識します。それぞれは、SDAファブリックEN内の特定のVLANにマッピングされます。

検証

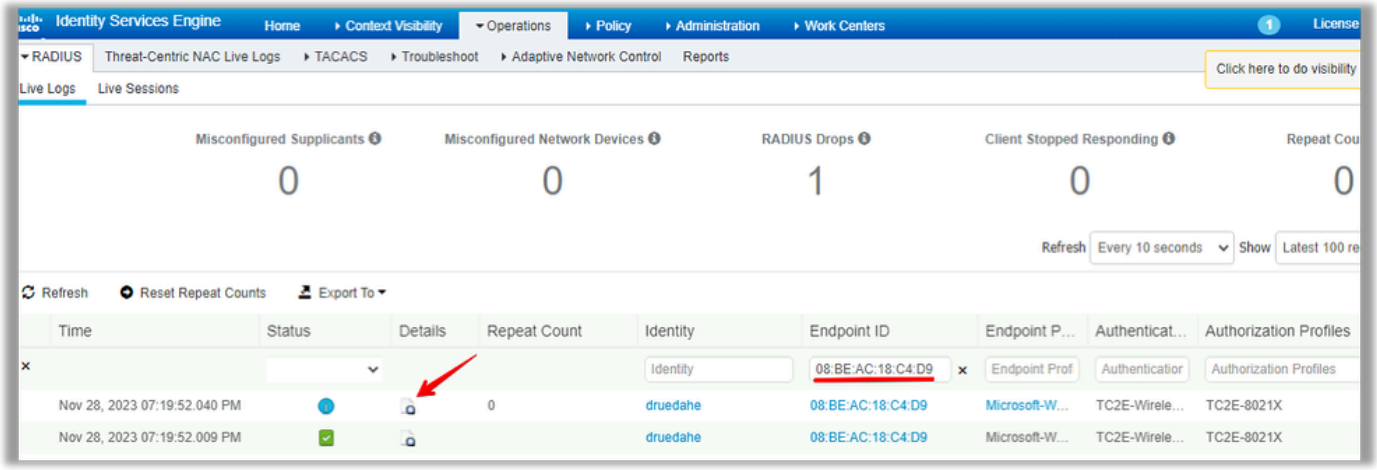
SGT/L2VNIDのダイナミック割り当てに関連する問題について報告される症状は次のいずれかです。

1. SGポリシーは、特定のWLANに接続するワイヤレスクライアントには適用されません（ダイナミックSGT割り当ての問題）。
2. ワイヤレスクライアントがDHCP経由でIPアドレスを取得していないか、特定のWLAN上の目的のサブネット範囲からIPアドレスを取得していない（ダイナミックL2VNID割り当ての問題）。

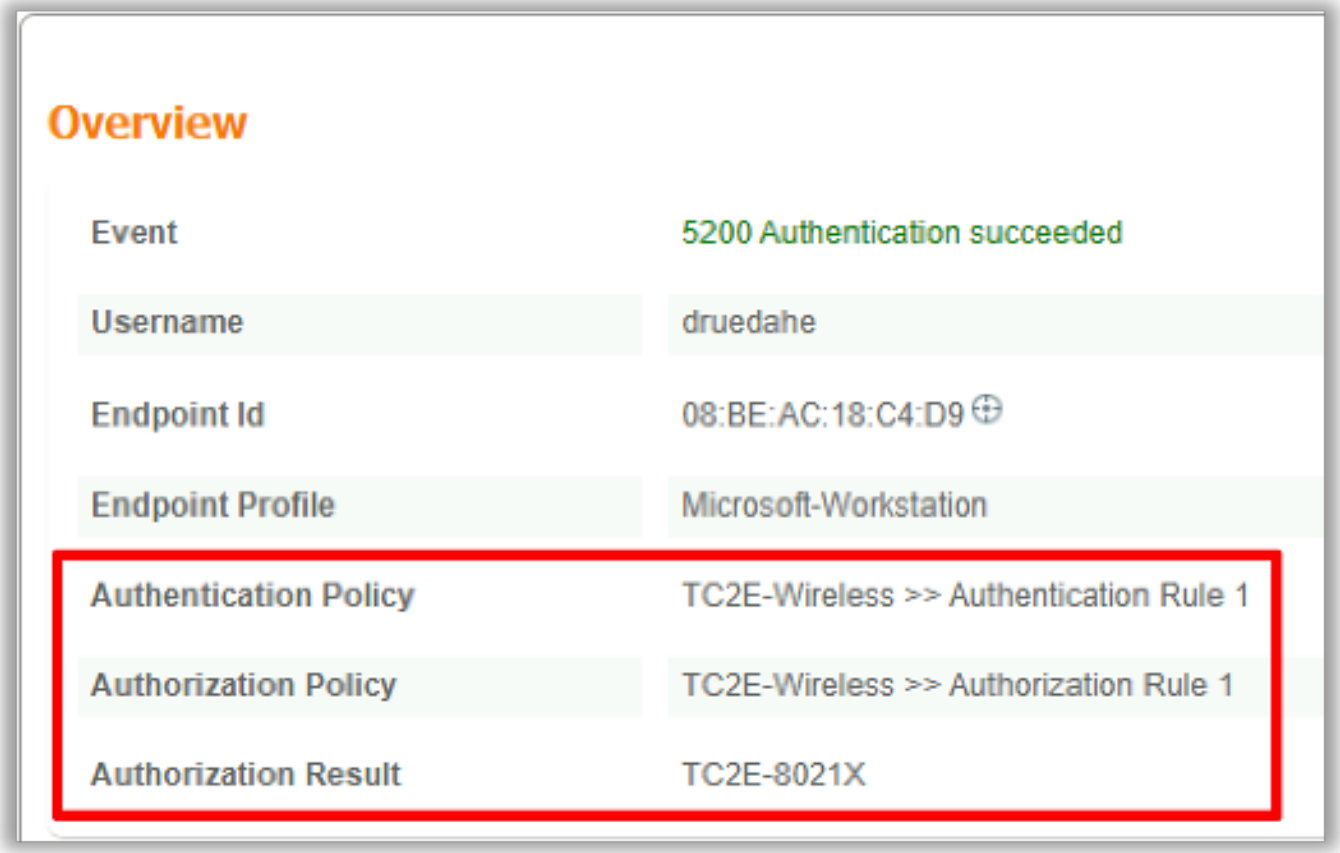
次に、このプロセスの関連する各ノードの検証について説明します。

ISEの検証

開始点はISEです。ISE GUIのOperation/RADIUS/Live Logs/に移動し、ワイヤレスクライアントのMACアドレスをEndpoint IDフィールドのフィルタとして使用し、Detailsアイコンをクリックします。



次に、認証の詳細が記載された別のタブが開きます。主に、概要と結果の2つのセクションに関心を持っています。



Overviewは、このワイヤレスクライアント認証に意図したポリシーまたは目的のポリシーのいずれが使用されたかを示します。そうでない場合は、ISEポリシー設定を見直す必要がありますが、このドキュメントでは説明しません。

Resultは、ISEからWLCに返された値を示します。目標はSGTとL2VNIDを動的に割り当てることであるため、このデータをここに含める必要があります。次の2点に注意してください。

1. L2VNID名は「Tunnel-Private-Group-ID」属性として送信されます。ISEは、ID(8199)ではなく、名前(10_10_30_0-READONLY_VN)を返す必要があります。

2. SGTは「cisco-av-pair」として送信されます。cts:security-group-tag属性で、SGT値が16進数(12)ではなくascii(18)であることに注意してください。ただし、これらは同じです。TC2E_Learnersは、内部的にはISEのSGT名です。

WLCの検証

WLCでは、show wireless fabric client summaryコマンドを使用してクライアントのステータスを確認し、show wireless fabric summaryを使用してファブリックの設定と、動的に割り当てられたL2VNIDの存在を再確認できます。

```
<#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
```

予想される情報が反映されない場合は、WLCでワイヤレスクライアントのMACアドレスのRAトレースを有効にして、ISEから受信したデータを正確に確認できます。特定のクライアントのRAトレース出力を取得する方法については、次のドキュメントを参照してください。

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

クライアントのRAトレース出力では、ISEから送信された属性がRADIUS Access-Acceptパケットで伝送されます。

<#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
```

WLCは、SGTおよびL2VNID情報を次の宛先に送信します。

1. CAPWAP(Control And Provisioning of Wireless Access Points)経由のアクセスポイント(AP)。

2. LISPによるファブリックCP。

次に、ファブリックCPはSGT値をLISP経由でファブリックENに送信します。ファブリックENではAPが接続されています。

ファブリックENの検証

次のステップでは、ファブリックENが動的に受信した情報を反映しているかどうかを検証します。show vlanコマンドを使用して、L2VNID 8199に関連付けられたVLANを確認します。

```
<#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
```

L2VNID 8199がVLAN 1031にマッピングされていることがわかります。

さらに、show device-tracking database mac <mac address>コマンドを使用すると、ワイヤレスクライアントが目的のVLAN上にあるかどうかが表示されます。

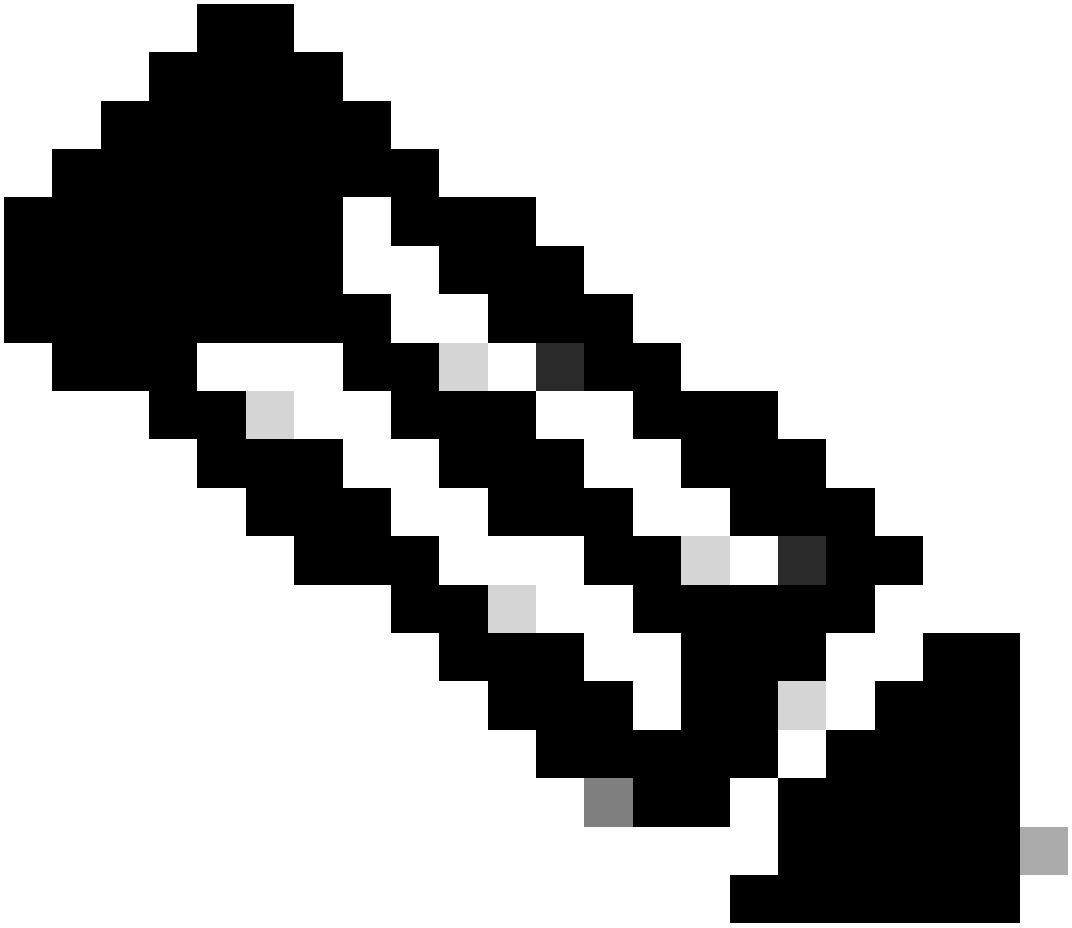
```
<#root>

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)
```

最後に、show cts role-based sgt-map vrf <vrf name> allコマンドは、クライアントに割り当てられたSGT値を提供します。この例では、VLAN 1031は「READONLY_VN」VRFの一部です。

<#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：ワイヤレスクライアント（有線クライアントなど）のSDAファブリックでのCisco TrustSec(CTS)ポリシーの適用は、APやWLCではなく、ENによって実行されます。

これにより、ENは指定されたSGTに設定されたポリシーを適用できます。

これらの出力が適切に入力されていない場合は、ENでdebug lisp control-plane allコマンドを使用して、WLCから送られてくるLISP通知を受信しているかどうかを確認できます。

<#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通知は、最初にCPによって受信され、次にENにリレーされることに注意してください。SISFまたはデバイストラッキングエントリは、このLISP通知を受信すると作成されます。この通知はプロセスの重要な部分です。この通知は、次の方法でも表示できます。

<#root>

```
EDGE-01#
```

show lisp instance-id 8199 ethernet database wlc clients detail

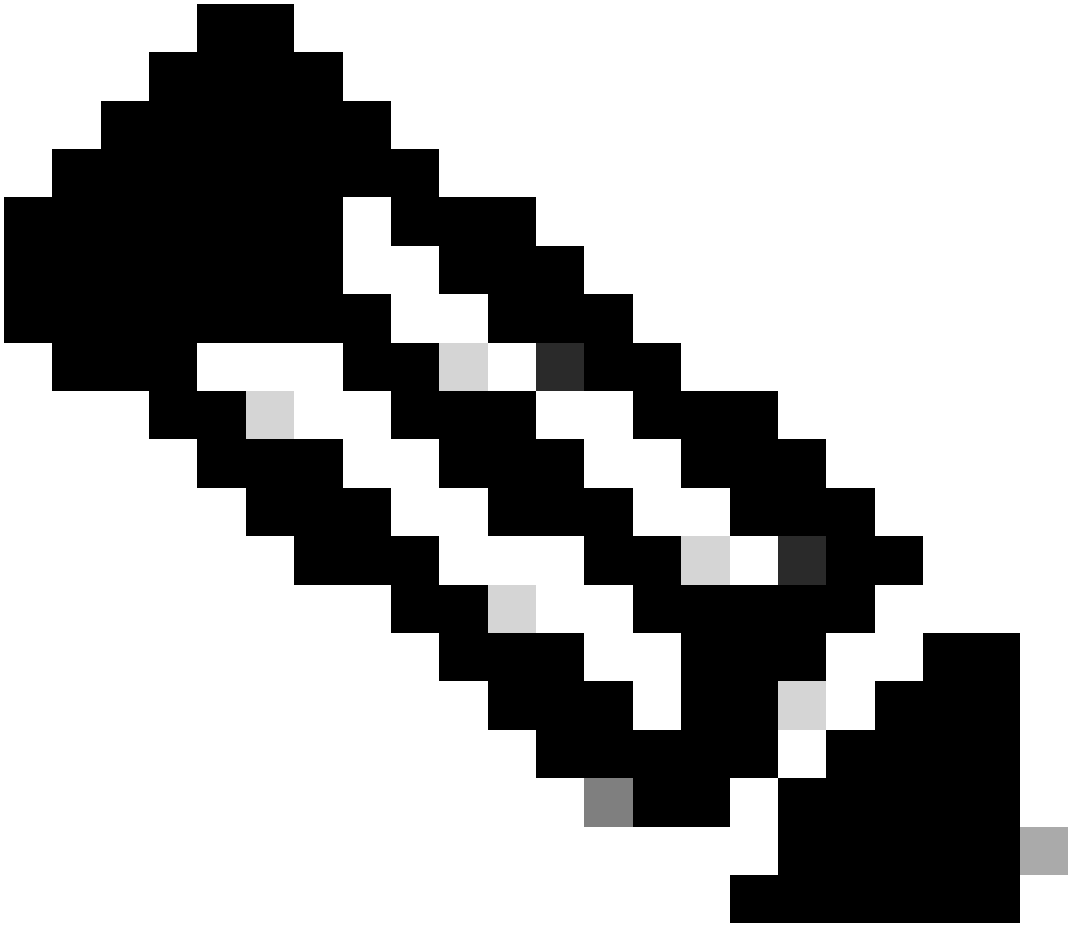
```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 21:23:31.737 UTC Wed Nov 29 2023


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：メタデータセクションで強調表示されている値12は、当初割り当てようとしたSGT 18の16進数バージョンです。これにより、プロセス全体が正常に終了したことが確認されます。

パケットの検証

最後の確認手順として、ENスイッチでEmbedded Packet Capture(EPC)ツールを使用して、このクライアントのパケットがAPによってどのように送信されるかを確認することもできます。EPCでキャプチャファイルを取得する方法については、次を参照してください。

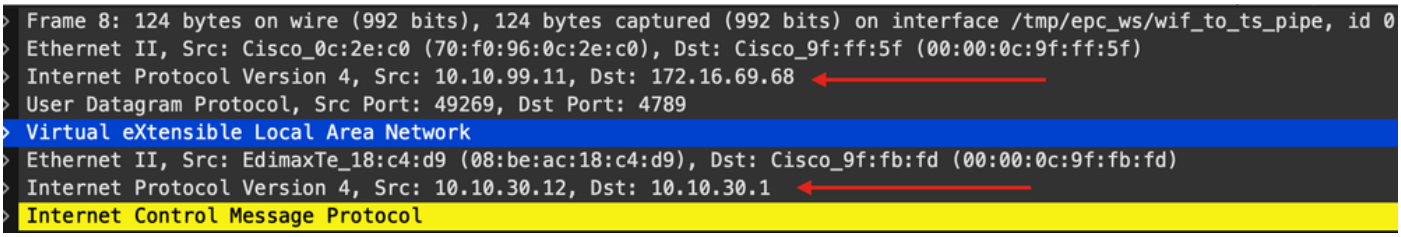
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_packet_capture.html

この例では、ゲートウェイへのpingがワイヤレスクライアント自体で開始されています。

icmp

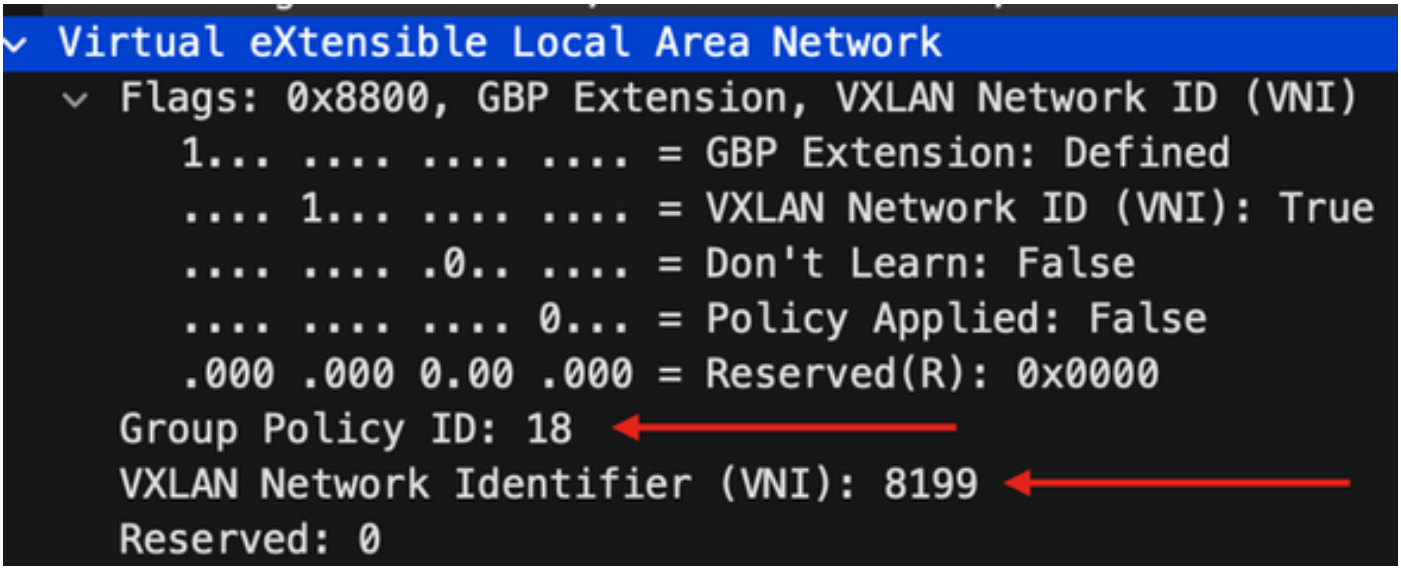
No.	Time	Arrival Time	Source	Destination	VXLAN N	Protocol	Identification	Length	Info
8	0.082365	2023-12-01 18:47:34.384734	10.10.30.12	10.10.30.1	8199	ICMP	0x01e1 (481),0x…	124	Echo (ping) request
18	0.000028	2023-12-01 18:47:39.277504	10.10.30.12	10.10.30.1	8199	ICMP	0x01e3 (483),0x…	124	Echo (ping)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

APとENはファブリックワイヤレスクライアント用にAP間のVXLANトンネルを形成するため、パケットにはAPからのVXLANヘッダーが付属することにすでに想定されています。



トンネルの送信元はAPのIPアドレス(10.10.99.11)で、宛先はEN Loopback0 IPアドレス(172.16.69.68)です。VXLANヘッダーの内部では、実際のワイヤレスクライアントデータ（この場合はICMPパケット）を確認できます。

最後に、VXLANヘッダーを調べます。



SGT値をグループポリシーIDとしてメモします。この場合はascii形式で、L2VNID値をVXLANネットワーク識別子(VNI)としてメモします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。