

Entender a atribuição dinâmica de SGT/L2VNID no SDA Wireless

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Topologia](#)

[Configuração](#)

[Verificação](#)

[Verificação do ISE](#)

[Verificação de WLC](#)

[Verificação de EN de malha](#)

[Verificação de pacotes](#)

Introdução

Este documento descreve o processo de atribuição de SGT Dinâmico e L2VNID em SSIDs 802.1x Sem Fio Habilitados para Malha.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Serviço de Usuário de Discagem de Autenticação Remota (RADIUS)
- Controlador de LAN sem fio (WLC)
- Identity services engine (ISE)
- Tag de grupo de segurança (SGT)
- L2VNID (Identificador de rede virtual da camada 2)
- Rede sem fio habilitada para malha com acesso SD (SDA FEW)
- Protocolo de separação de localizador/ID (LISP)
- Rede local extensível virtual (VXLAN)
- Plano de controle de estrutura (CP) e nó de borda (EN)
- Catalyst Center (CatC, anteriormente conhecido como Cisco DNA Center)

Componentes Utilizados

WLC 9800 Cisco IOS® XE versão 17.6.4

Cisco IOS® XE

ISE versão 2.7

CatC versão 2.3.5.6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

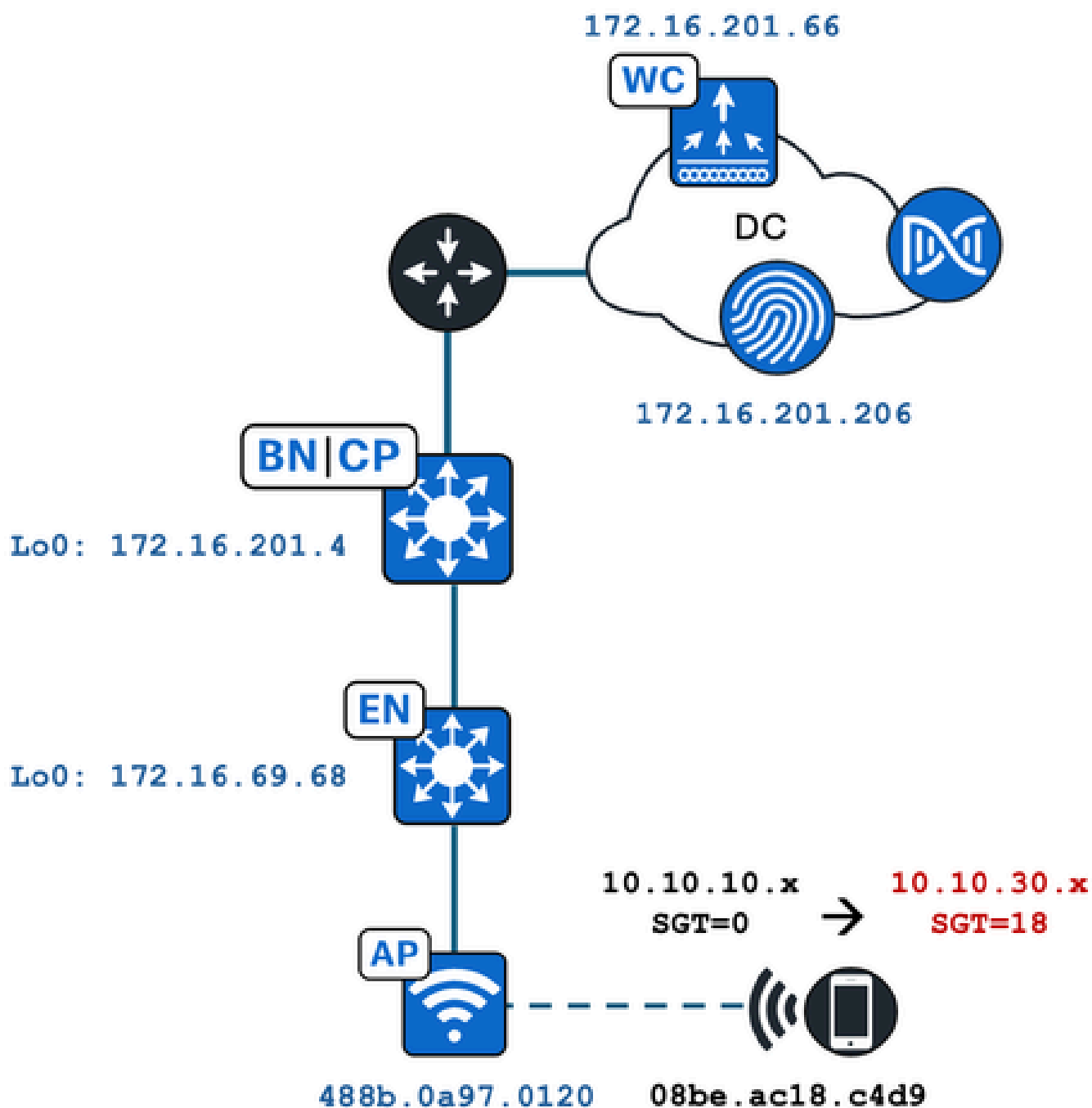
Um dos aspectos principais do SD-Access é a microssegmentação dentro de uma VPN obtida através dos grupos escaláveis.

O SGT pode ser atribuído estaticamente por WLAN ou SSID habilitado para estrutura (embora não sejam os mesmos, sua diferença não afeta o objetivo principal deste documento, então usamos intercambiavelmente os dois termos para o mesmo significado para melhorar a legibilidade). No entanto, em muitas implantações reais, muitas vezes há usuários se conectando à mesma WLAN que exigem um conjunto diferente de políticas ou configurações de rede. Além disso, em alguns cenários, há uma necessidade de alocar diferentes endereços IP para clientes específicos na mesma WLAN de estrutura para aplicar políticas específicas baseadas em IP a eles ou atender aos requisitos de endereçamento IP da empresa. O L2VNID (Layer 2 Virtual Network Identifier) é o parâmetro que a infraestrutura do FEW usa para colocar usuários sem fio em diferentes faixas de sub-rede. Os pontos de acesso enviam o L2VNID no cabeçalho VxLAN para o Fabric Edge Node (EN), que então o correlaciona à VLAN L2 correspondente.

Para atingir essa granularidade na mesma WLAN, a atribuição de SGT dinâmico e/ou L2VNID é aproveitada. A WLC coleta as informações de identidade do endpoint, envia-as ao ISE para autenticação, que as usa para corresponder à política apropriada a ser aplicada a esse cliente e retorna as informações SGT e/ou L2VNID após a autenticação bem-sucedida.

Topologia

Para entender como esse processo funciona, desenvolvemos um exemplo usando esta topologia de laboratório:



Neste exemplo, a WLAN é configurada estaticamente com:

- L2VNID = 8198 / Nome do pool de IP = Pegasus_Read_Only → VLAN 1030 (10.10.10.x)
- Sem SGT

E o cliente sem fio que se conecta a ele obtém dinamicamente estes parâmetros:

- L2VNID = 8199 / Nome do pool de IP = 10_10_30_0-READONLY_VN → VLAN 1031 (10.10.30.x)
- SGT = 18

Configuração

Primeiro, precisamos identificar a WLAN envolvida e verificar como ela está configurada. Neste exemplo, o SSID "TC2E-druedahe-802.1x" é usado. No momento da redação deste documento, o SDA é suportado apenas via CatC, portanto, devemos verificar o que está configurado lá. Em Provision/SD-Access/Fabric Sites/<specific Fabric site>/Host Onboarding/Wireless SSIDs:

SSID Name	Type	Security	Traffic Type	Address Pool	Scalable Group
TC2E-druedahe-PSK	Enterprise	WPA2 Personal	Voice + Data	Choose Pool Pegasus_Read_Only	Assign SGT No Scalable group associated with
TC2E-druedahe-8021X	Enterprise	WPA2 Enterprise	Voice + Data	Choose Pool Pegasus_Read_Only	Assign SGT No Scalable group associated with

O SSID tem o pool de IP chamado "Pegasus_Read_Only" mapeado para ele e não tem nenhum SGT atribuído estaticamente, o que significa SGT=0. Isso significa que, se um cliente sem fio se conectar e se autenticar com êxito sem que o ISE envie qualquer atributo de volta para atribuição dinâmica, essas serão as configurações do cliente sem fio.

O pool atribuído dinamicamente deve estar presente antes na configuração da WLC. E isso é feito adicionando-se o pool de IP como "Wireless Pool" na rede virtual no CatC:

VLAN Name	IP Address Pool	VLAN ID	Layer 2 VNID	Traffic Type	Security Group	Wireless Pool
10_10...LY_VN	[REDACTED]	1031	8199	Data	-	Enabled

Na GUI da WLC em Configuration/Wireless/Fabric, essa configuração reflete desta forma:

Configuration > Wireless > Fabric

General

Control Plane

Profiles

Fabric Status

ENABLED



Fabric VNID Mapping

+ Add

× Delete

L2 VNID "Contains" 819



	Name	L2 VNID	L3 VNID
<input type="checkbox"/>	Pegasus_APs	8196	4097
<input type="checkbox"/>	Pegasus_Read_Only	8198	0
<input type="checkbox"/>	10_10_30_0-READONLY_VN	8199	0



1



10

items per page

O pool "Pegasus_Read_Only" é igual ao L2VNID 8198 e queremos que nosso cliente esteja no L2VNID 8199, o que significa que o ISE precisa informar ao WLC para usar o pool "10_10_30_0-READONLY_VN" para esse cliente. Vale lembrar que a WLC não mantém nenhuma configuração para as VLANs de estrutura. Ele só reconhece os L2VNIDs. Cada uma é mapeada para uma VLAN específica nos ENs de estrutura SDA.

Verificação

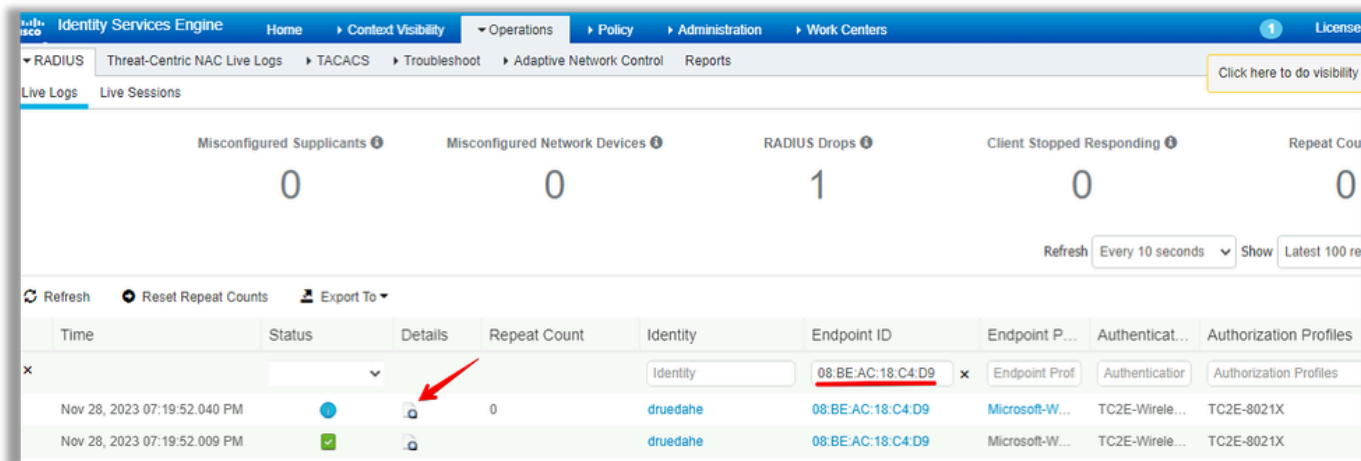
Os sintomas relatados para problemas que envolvem a Atribuição dinâmica de SGT/L2VNID são:



1. As Diretivas SG não são aplicadas em clientes sem fio que se conectam a uma WLAN específica. (Problema de Atribuição de SGT Dinâmico).
2. Os clientes sem fio não estão obtendo o endereço IP via DHCP ou não estão obtendo um endereço IP do intervalo de sub-rede desejado em uma WLAN específica. (Problema de atribuição de L2VNID dinâmica).

Agora, a verificação de cada nó relevante nesse processo é descrita.

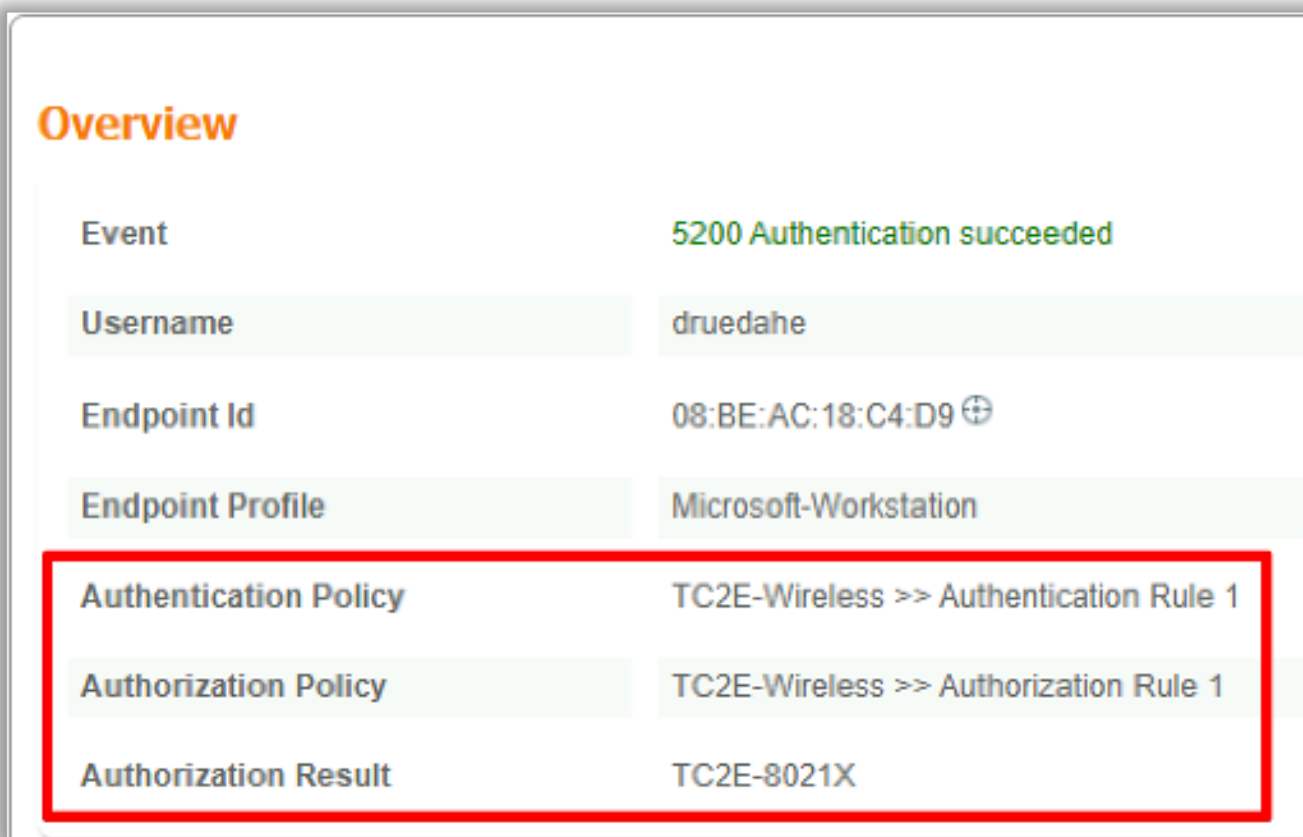
Verificação do ISE

O ponto de partida é o ISE. Vá para a GUI do ISE em Operation/RADIUS/Live Logs/ e use o endereço MAC do cliente sem fio como filtro no campo Endpoint ID e, em seguida, clique no ícone Details:



Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Profiles
Nov 28, 2023 07:19:52.040 PM	●		0	druedahe	08:BE:AC:18:C4:D9	Microsoft-W...	TC2E-Wirele...	TC2E-8021X
Nov 28, 2023 07:19:52.009 PM	■			druedahe	08:BE:AC:18:C4:D9	Microsoft-W...	TC2E-Wirele...	TC2E-8021X

Em seguida, ele abre outra guia com os detalhes de autenticação. Estamos interessados principalmente em duas seções, Visão geral e Resultado:



Overview

Event 5200 Authentication succeeded

Username druedahe

Endpoint Id 08:BE:AC:18:C4:D9

Endpoint Profile Microsoft-Workstation

Authentication Policy TC2E-Wireless >> Authentication Rule 1

Authorization Policy TC2E-Wireless >> Authorization Rule 1

Authorization Result TC2E-8021X

A visão geral mostra se a política desejada ou desejada foi usada para esta autenticação de cliente sem fio. Caso contrário, a configuração das políticas do ISE precisará ser revisitada, mas isso está fora do escopo deste documento.

O resultado mostra o que foi retornado pelo ISE para a WLC. O objetivo é ter o SGT e o L2VNID dinamicamente atribuídos, portanto, esses dados devem ser incluídos aqui, e são. Observe duas coisas:

1. O nome L2VNID é enviado como um atributo "Tunnel-Private-Group-ID". O ISE deve retornar o nome (10_10_30_0-READONLY_VN) e não o id (8199).
2. O SGT é enviado como um "cisco-av-pair". No atributo cts:security-group-tag, observe que o valor SGT está em hex (12), não em ascii (18), mas eles são iguais. TC2E_Learners é o nome SGT no ISE internamente.

Verificação de WLC

Na WLC, podemos usar o comando `show wireless fabric client summary` para verificar o status do cliente e o `show wireless fabric summary` para confirmar duas vezes a configuração da estrutura e a presença do L2VNID atribuído dinamicamente:

```
<#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 name
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

0

0.0.0.0

default-control-plane

Se as informações esperadas não forem refletidas, podemos habilitar Rastreamentos de RA para o endereço MAC do cliente sem fio na WLC para ver exatamente os dados recebidos do ISE. Informações sobre como obter a saída de Rastreamentos RA para um cliente específico podem ser encontradas neste documento:

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

Na saída do RA Trace para o cliente, os atributos enviados pelo ISE são transportados no pacote RADIUS Access-Accept:

<#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_VN"
```

```
{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 received
```

```
{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
```

Em seguida, a WLC envia as informações de SGT e L2VNID para:

1. O Ponto de Acesso (AP) através do CAPWAP (Control And Provisioning of Wireless Access Points).
2. O Fabric CP via LISP.

O Fabric CP envia o valor SGT via LISP para o Fabric EN onde o AP está conectado.

Verificação de EN de malha

A próxima etapa é validar se o EN de estrutura está refletindo as informações recebidas dinamicamente. O comando show vlan confirma a VLAN associada ao L2VNID 8199:

```
<#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
```

Podemos ver que o L2VNID 8199 está mapeado para a VLAN 1031.

E o comando show device-tracking database mac <mac address> será exibido se o cliente sem fio estiver na VLAN desejada:

```
<#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, DHCP - IPv4 DHCP
```

```
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)

```

Por fim, o comando `show cts role-based sgt-map vrf <vrf name> all` fornece o valor SGT atribuído ao cliente. Neste exemplo, a VLAN 1031 faz parte do VRF "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

```



Observação: a aplicação da política do Cisco TrustSec (CTS) em uma estrutura SDA para clientes sem fio (como para clientes com fio) é feita pelos ENs, não pelos APs nem pela WLC.

Com isso, o EN é capaz de aplicar as políticas configuradas para o SGT especificado.

Se essas saídas não estiverem sendo preenchidas corretamente, podemos usar o comando `debug lisp control-plane all` no EN para verificar se ele está recebendo a notificação LISP proveniente do WLC:

```
<#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.
```

Observe que a notificação LISP é recebida primeiro pelo CP, que depois a retransmite para o EN. A entrada SISF ou de rastreamento de dispositivo é criada após o recebimento dessa notificação LISP, que é uma parte importante do processo. Você também pode ver essa notificação com:

<#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
```

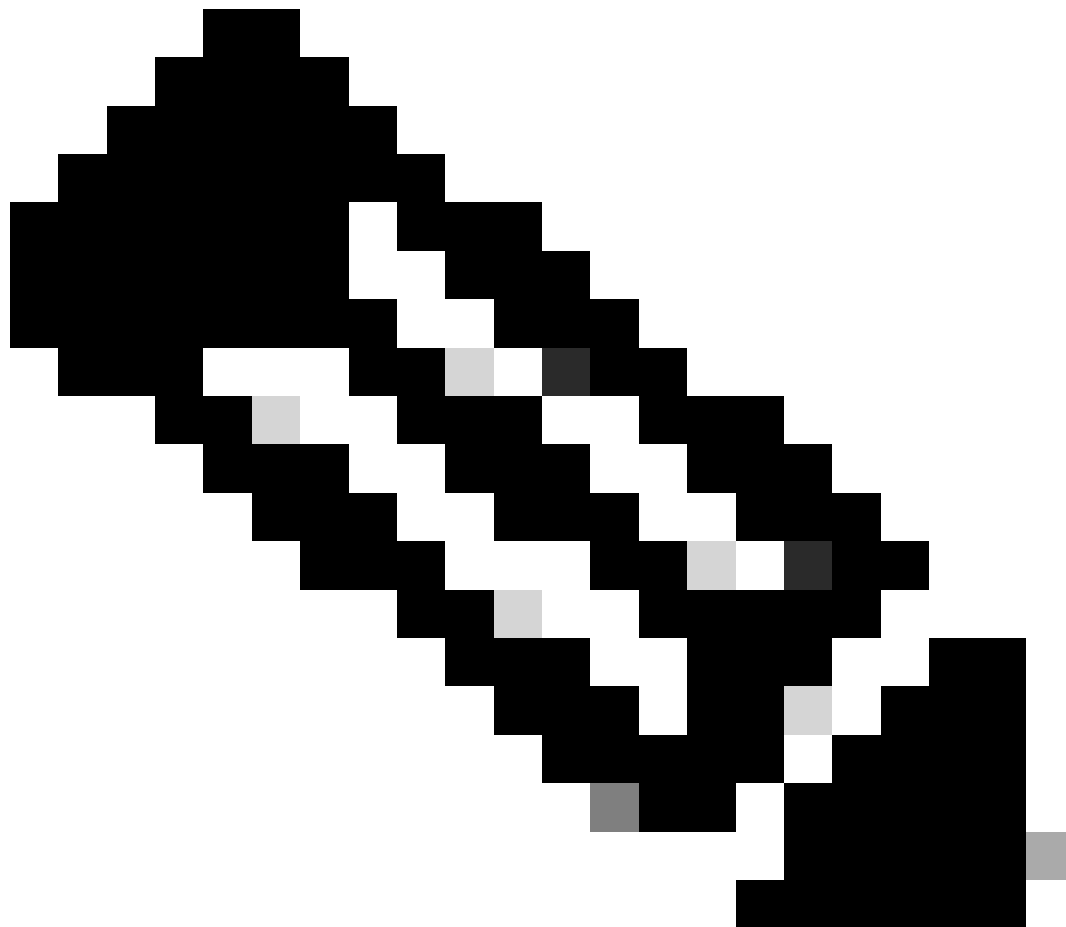
WLC clients/access-points information for router lisp 0 IID

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
```



Observação: o valor realçado 12 na seção Metadados é a versão hexadecimal do SGT 18 que inicialmente pretendemos atribuir. E isso confirma que todo o processo foi concluído corretamente.

Verificação de pacotes

Como última etapa de confirmação, também podemos usar a ferramenta Embedded Packet Capture (EPC) no switch EN e ver como os pacotes desse cliente são transmitidos pelo AP. Para obter informações sobre como obter um arquivo de captura com o EPC, consulte:

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

Para este exemplo, um ping para o gateway foi iniciado no próprio cliente sem fio:

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

Observe que já se espera que o pacote venha com um cabeçalho VXLAN do AP, já que o AP e o EN formam um túnel VXLAN entre eles para os clientes sem fio da estrutura:

```
> Frame 8: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
> Ethernet II, Src: Cisco_0c:2e:c0 (70:f0:96:0c:2e:c0), Dst: Cisco_9f:ff:5f (00:00:0c:9f:ff:5f)
> Internet Protocol Version 4, Src: 10.10.99.11, Dst: 172.16.69.68
> User Datagram Protocol, Src Port: 49269, Dst Port: 4789
> Virtual eXtensible Local Area Network
> Ethernet II, Src: EdimaxTe_18:c4:d9 (08:be:ac:18:c4:d9), Dst: Cisco_9f:fb:fd (00:00:0c:9f:fb:fd)
> Internet Protocol Version 4, Src: 10.10.30.12, Dst: 10.10.30.1
> Internet Control Message Protocol
```

A origem do túnel é o endereço IP do AP (10.10.99.11) e o destino é o endereço IP do EN Loopback0 (172.16.69.68). Dentro do cabeçalho VXLAN, podemos ver os dados reais do cliente sem fio, neste caso o pacote ICMP.

Finalmente, inspecione o cabeçalho VXLAN:

```
Virtual eXtensible Local Area Network
  Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    1... .. = GBP Extension: Defined
    .... 1... .. = VXLAN Network ID (VNI): True
    .... .. .0.. .. = Don't Learn: False
    .... .. .. 0... = Policy Applied: False
    .000 .000 0.00 .000 = Reserved(R): 0x0000
  Group Policy ID: 18
  VXLAN Network Identifier (VNI): 8199
  Reserved: 0
```

Observe o valor SGT como ID da política de grupo — nesse caso, no formato ascii e o valor L2VNID como VXLAN Network Identifier (VNI).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.