

Comprensión de la asignación dinámica de SGT/L2VNID en conexiones inalámbricas SDA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Topología](#)

[Configuración](#)

[Verificación](#)

[Verificación de ISE](#)

[Verificación de WLC](#)

[Verificación EN de fabric](#)

[Verificación de paquetes](#)

Introducción

Este documento describe el proceso de asignación dinámica de SGT y L2VNID en SSID 802.1x inalámbricos habilitados para fabric.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)
- Controlador de LAN inalámbrica (WLC)
- Identity Services Engine (ISE)
- Security Group Tag (SGT)
- L2VNID (identificador de red virtual de capa 2)
- Red inalámbrica habilitada para acceso SD (SDA FEW)
- Protocolo de separación Localizador/ID (LISP)
- Red de área local extensible virtual (VXLAN)
- Plano de control de fabric (CP) y nodo de extremo (EN)
- Catalyst Center (CatC, anteriormente conocido como Cisco DNA Center)

Componentes Utilizados

WLC 9800 Cisco IOS® XE versión 17.6.4

Cisco IOS® XE

ISE versión 2.7

CatC versión 2.3.5.6

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

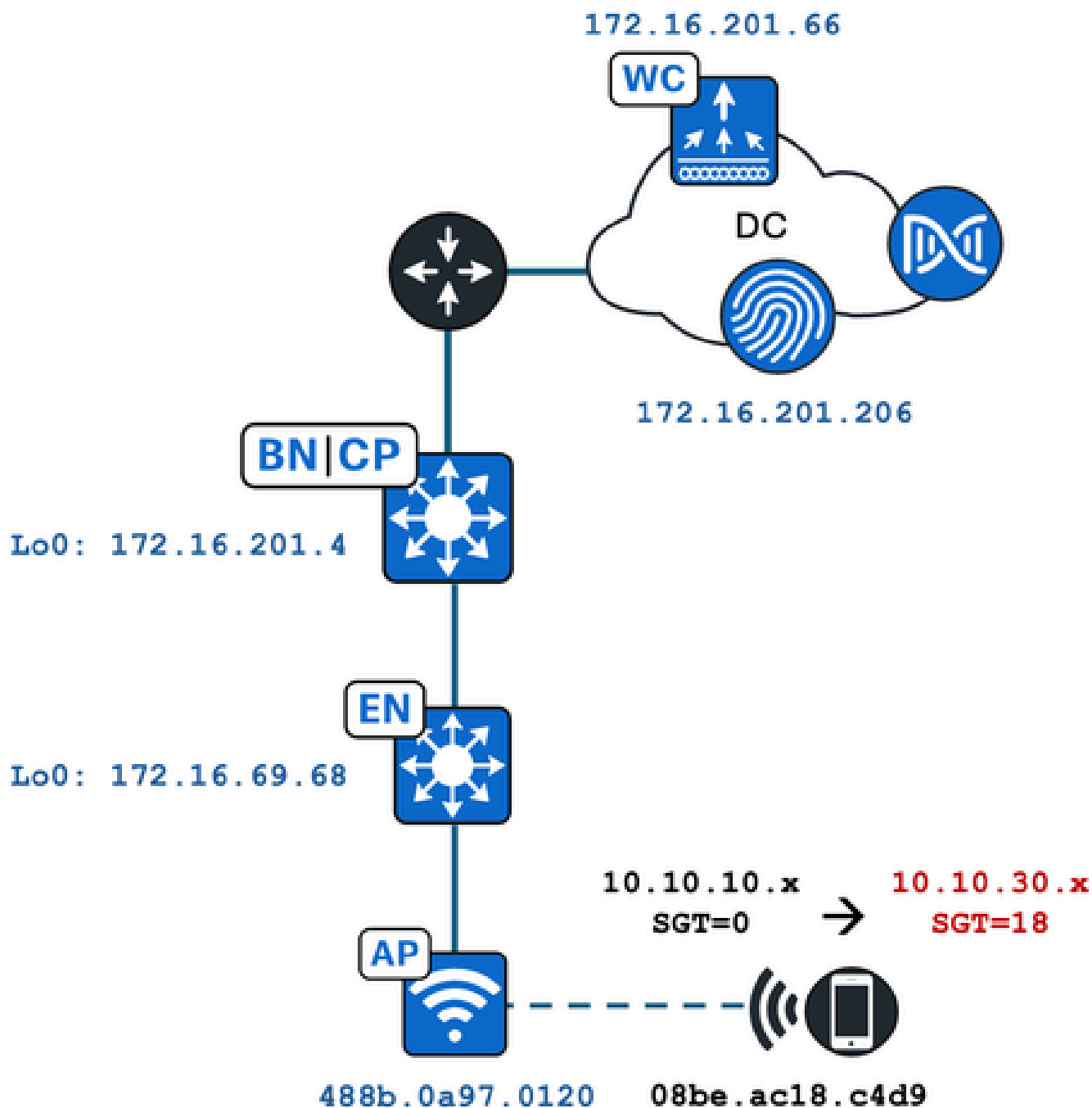
Uno de los aspectos clave de SD-Access es la microsegmentación dentro de una VPN conseguida a través de los grupos escalables.

La SGT se puede asignar de forma estática por WLAN o SSID habilitado para fabric (aunque no son iguales, su diferencia no afecta al objetivo principal de este documento, por lo que utilizamos indistintamente los dos términos para el mismo significado con el fin de mejorar la legibilidad). Sin embargo, en muchas implementaciones reales, a menudo hay usuarios que se conectan a la misma WLAN que requieren un conjunto diferente de políticas o configuraciones de red. Además, en algunos escenarios, existe la necesidad de asignar diferentes direcciones IP a clientes específicos dentro de la misma WLAN de fabric para aplicarles políticas específicas basadas en IP o cumplir con los requisitos de direccionamiento IP de la empresa. El L2VNID (identificador de red virtual de capa 2) es el parámetro que utiliza la infraestructura FEW para colocar a los usuarios inalámbricos en rangos de subred diferentes. Los puntos de acceso envían el L2VNID en el encabezado VxLAN al Fabric Edge Node (EN), que luego lo correlaciona con la VLAN L2 correspondiente.

Para lograr esta granularidad dentro de la misma WLAN, se aprovecha la asignación dinámica de SGT o L2VNID. El WLC recopila la información de identidad del terminal, la envía a ISE para su autenticación, que la utiliza para que coincida con la política adecuada que se aplicará a este cliente y devuelve la información de SGT o L2VNID tras una autenticación exitosa.

Topología

Para comprender cómo funciona este proceso, desarrollamos un ejemplo utilizando esta topología de laboratorio:



En este ejemplo, la WLAN se configura estáticamente con:

- L2VNID = 8198 / Nombre del conjunto IP = Pegasus_Read_Only → VLAN 1030 (10.10.10.x)
- Sin SGT

Y el cliente inalámbrico que se conecta a él obtiene dinámicamente estos parámetros:

- L2VNID = 8199 / Nombre del conjunto IP = 10_10_30_0-READONLY_VN → VLAN 1031 (10.10.30.x)
- SGT = 18

Configuración

En primer lugar, necesitamos identificar la WLAN involucrada y verificar cómo está configurada. En este ejemplo se utiliza el SSID "TC2E-druedahe-802.1x". En el momento de esta redacción del documento, SDA sólo se soporta a través de CatC, por lo que debemos verificar lo que está configurado allí. En Aprovisionamiento/Acceso SD/Sitios de fabric/<sitio de fabric específico>/Incorporación de host/SSID inalámbricos:

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 associate with

El SSID tiene asignado el conjunto IP denominado "Pegasus_Read_Only" y no tiene ninguna SGT asignada estáticamente, lo que significa SGT=0. Esto significa que, si un cliente inalámbrico se conecta y autentica correctamente sin que ISE envíe ningún atributo de vuelta para la asignación dinámica, esto es lo que es la configuración del cliente inalámbrico.

El conjunto que se asigna dinámicamente debe estar presente antes en la configuración del WLC. Y esto se logra agregando el conjunto IP como "conjunto inalámbrico" en la red virtual en el 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

En la GUI del WLC bajo la configuración/Wireless/Fabric, este ajuste refleja esta manera:

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

El conjunto "Pegasus_Read_Only" equivale al 8198 L2VNID y queremos que nuestro cliente esté en el 8199 L2VNID, lo que significa que ISE necesita decirle al WLC que utilice el conjunto "10_10_30_0-READONLY_VN" para este cliente. Vale la pena recordar que el WLC no contiene ninguna configuración para las VLANs del entramado. Solo es consciente de los L2VNID. A continuación, cada una se asigna a una VLAN específica en los EN del fabric SDA.

Verificación

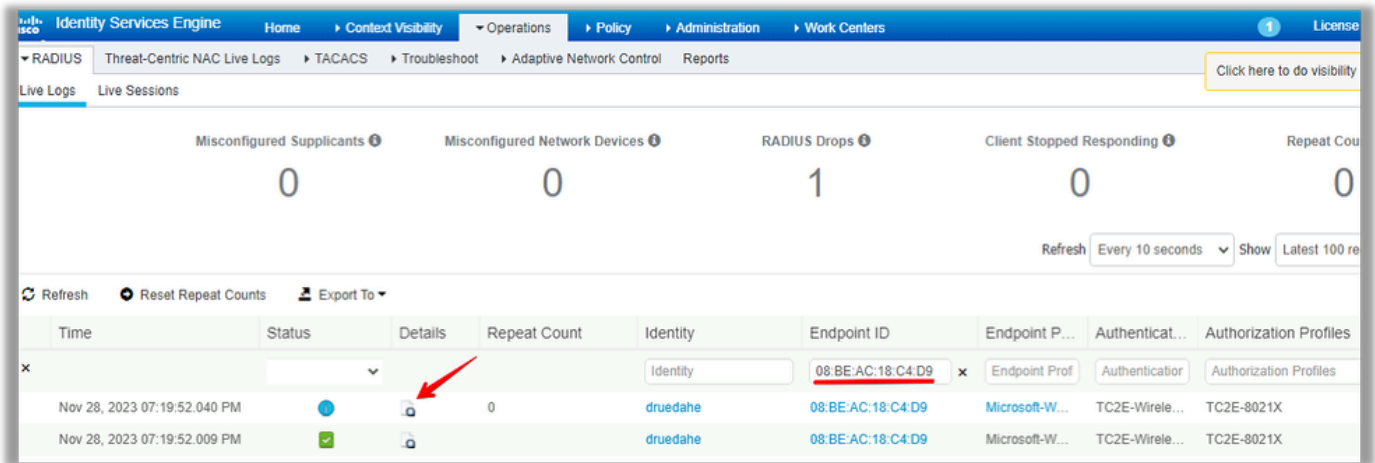
Los síntomas notificados para problemas relacionados con la asignación dinámica de SGT/L2VNID son:

1. Las políticas SG no se aplican en clientes inalámbricos que se conectan a una WLAN específica. (Problema de asignación de SGT dinámica).
2. Los clientes inalámbricos no están obteniendo la dirección IP a través de DHCP o no están obteniendo una dirección IP del rango de subred deseado en una WLAN específica. (Problema de asignación de L2VNID dinámico).

Ahora se describe la verificación de cada nodo relevante en este proceso.

Verificación de ISE

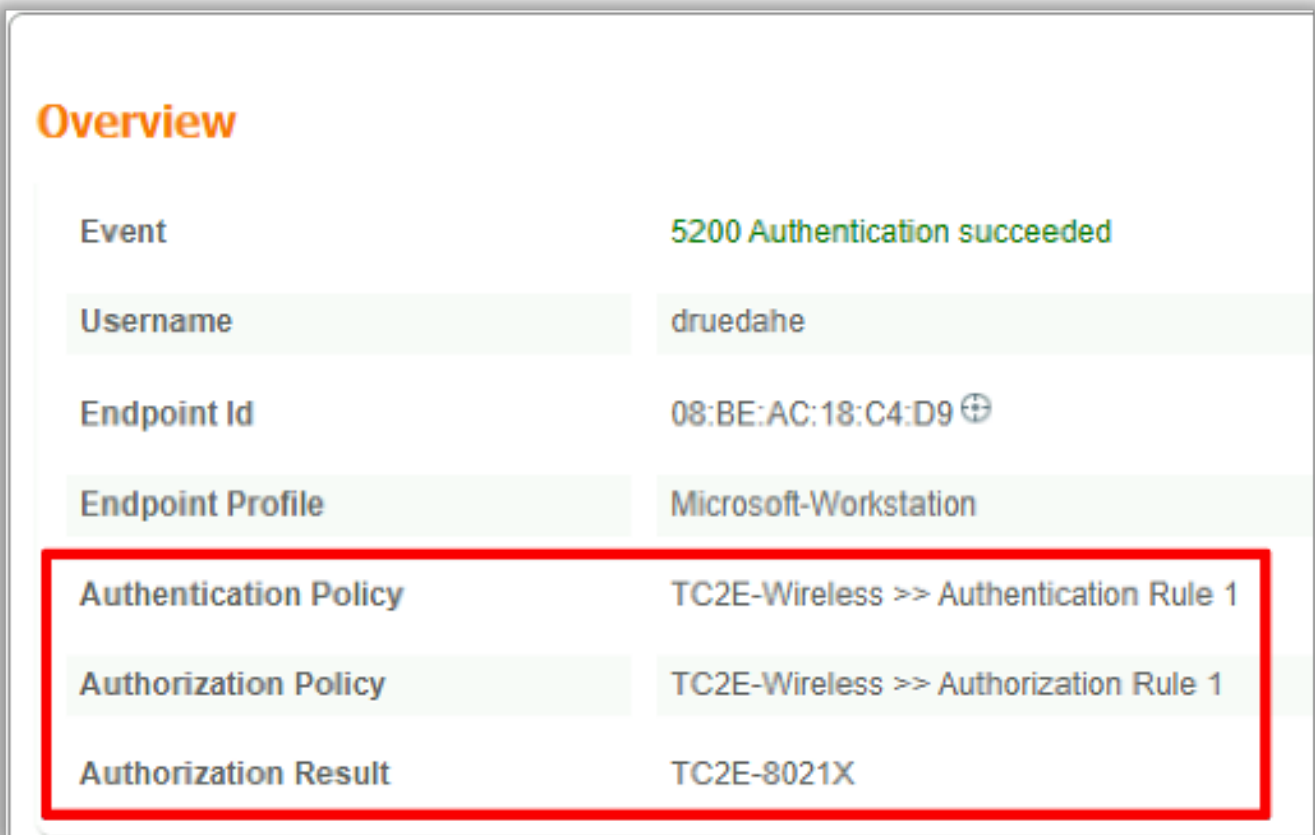
El punto de partida es ISE. Vaya a la GUI de ISE en Operation/RADIUS/Live Logs/ y utilice la dirección MAC del cliente inalámbrico como filtro en el campo Endpoint ID, luego haga clic en el icono Details (Detalles):



The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area displays several statistics: Misconfigured Suppliants (0), Misconfigured Network Devices (0), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counts (0). Below these statistics is a table with columns for Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, Authentication Profile, and Authorization Profiles. A red arrow points to the 'Details' icon in the first row of the table.

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

A continuación, abre otra ficha con los detalles de autenticación. Nos interesan principalmente dos secciones, Descripción general y Resultado:



The screenshot shows the Overview section of an authentication event in the Cisco Identity Services Engine (ISE) GUI. The section displays the following details:

- 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

La descripción general muestra si la política deseada se utilizó para esta autenticación de cliente inalámbrico. Si no es así, es necesario revisar la configuración de las políticas de ISE; sin embargo, esto queda fuera del alcance de este documento.

El resultado muestra lo que ISE devolvió al WLC. El objetivo es tener la SGT y el L2VNID dinámicamente asignados, por lo que estos datos deben incluirse aquí, y así es. Observe dos cosas:

1. El nombre L2VNID se envía como un atributo "Tunnel-Private-Group-ID". ISE debe devolver el nombre (10_10_30_0-READONLY_VN) y no la ID (8199).
2. La SGT se envía como un "par cisco-av". En el atributo cts:security-group-tag, observe que el valor SGT está en hexadecimal (12), no en ascii (18), pero son iguales. TC2E_Learners es el nombre de SGT de ISE de forma interna.

Verificación de WLC

En el WLC podemos utilizar el comando `show wireless fabric client summary` para verificar el estado del cliente y el `show wireless fabric summary` para confirmar dos veces la configuración del fabric y la presencia del L2VNID asignado dinámicamente:

```
<#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

Si la información esperada no se refleja, podemos habilitar Rastros de RA para la dirección MAC del cliente inalámbrico en el WLC para ver exactamente los datos recibidos de ISE. La información sobre cómo obtener la salida de Rastros de RA para un cliente específico se puede encontrar en este 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

En la salida de RA Trace para el cliente, los atributos enviados por ISE se transportan en el paquete de aceptación de acceso RADIUS:

```
<#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
```

El WLC entonces envía la información de SGT y L2VNID a:

1. El punto de acceso (AP) mediante CAPWAP (control y aprovisionamiento de puntos de acceso inalámbricos).
2. El Fabric CP vía LISP.

El Fabric CP luego envía el valor SGT a través de LISP al Fabric EN donde está conectado el AP.

Verificación EN de fabric

El siguiente paso consiste en validar si la norma EN del fabric refleja la información recibida dinámicamente. El comando show vlan confirma la VLAN asociada al 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 el L2VNID 8199 está mapeado a VLAN 1031.

Y el comando show device-tracking database mac <mac address> muestra si el cliente inalámbrico está en la VLAN deseada:

```
<#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 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 último, el comando `show cts role-based sgt-map vrf <vrf name> all` proporciona el valor SGT asignado al cliente. En este ejemplo, la VLAN 1031 es parte del 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

```

Nota: la aplicación de políticas de Cisco TrustSec (CTS) en un fabric SDA para clientes inalámbricos (como para clientes con cables) la realizan los EN, no los AP ni el WLC.

Con esto, EN puede aplicar las políticas configuradas para la SGT especificada.

Si estos resultados no se están llenando correctamente, podemos utilizar el comando debug lisp control-plane all en el EN para verificar si está recibiendo la notificación LISP que proviene del 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.

Tenga en cuenta que la notificación LISP la recibe primero el PC, que la transmite a la EN. La entrada SISF o Seguimiento de dispositivo se crea al recibir esta notificación LISP, que es una parte importante del proceso. También puede ver esta notificación con:

<#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



Nota: el valor destacado 12 en la sección Metadatos es la versión hexadecimal de la SGT 18 que inicialmente pretendíamos asignar. Y esto confirma que todo el proceso ha terminado correctamente.

Verificación de paquetes

Como último paso de confirmación, también podemos utilizar la herramienta Embedded Packet Capture (EPC) en el switch EN y ver cómo el AP transmite los paquetes de este cliente. Para obtener información sobre cómo obtener un archivo de captura con 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 ejemplo, se inició un ping al gateway en el propio cliente inalámbrico:

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

Tenga en cuenta que ya se espera que el paquete venga con un encabezado VXLAN del AP, ya que el AP y EN forman un túnel VXLAN entre ellos para los clientes inalámbricos Fabric:

```
> 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
```

El origen del túnel es la dirección IP del AP (10.10.99.11) y el destino es la dirección IP EN Loopback0 (172.16.69.68). Dentro del encabezado VXLAN podemos ver los datos reales del cliente inalámbrico, en este caso el paquete ICMP.

Por último, inspeccione el encabezado 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 el valor SGT como ID de política de grupo, en este caso, en formato ascii y el valor L2VNID como VXLAN Network Identifier (VNI).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).