Comprendere l'assegnazione dinamica di SGT/L2VNID su SDA Wireless

Sommario

Introduzione

In questo documento viene descritto il processo di assegnazione di SGT e L2VNID dinamici su SSID wireless 802.1x abilitati per la struttura.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- RADIUS (Remote Authentication Dial-In User Service)
- Controller LAN wireless (WLC)
- Identity Services Engine (ISE)
- SGT (Security Group Tag)
- L2VNID (identificatore di rete virtuale di livello 2)
- Wireless abilitato per fabric ad accesso SD (SDA SOME)
- Locator/ID Separation Protocol (LISP)
- VXLAN (Virtual Extensible Local Area Network)
- Fabric Control Plane (CP) e Edge Node (EN)
- Catalyst Center (CatC, in precedenza Cisco DNA Center)

Componenti usati

WLC 9800 Cisco IOS® XE versione 17.6.4

Cisco IOS® XE

ISE versione 2.7

CatC versione 2.3.5.6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

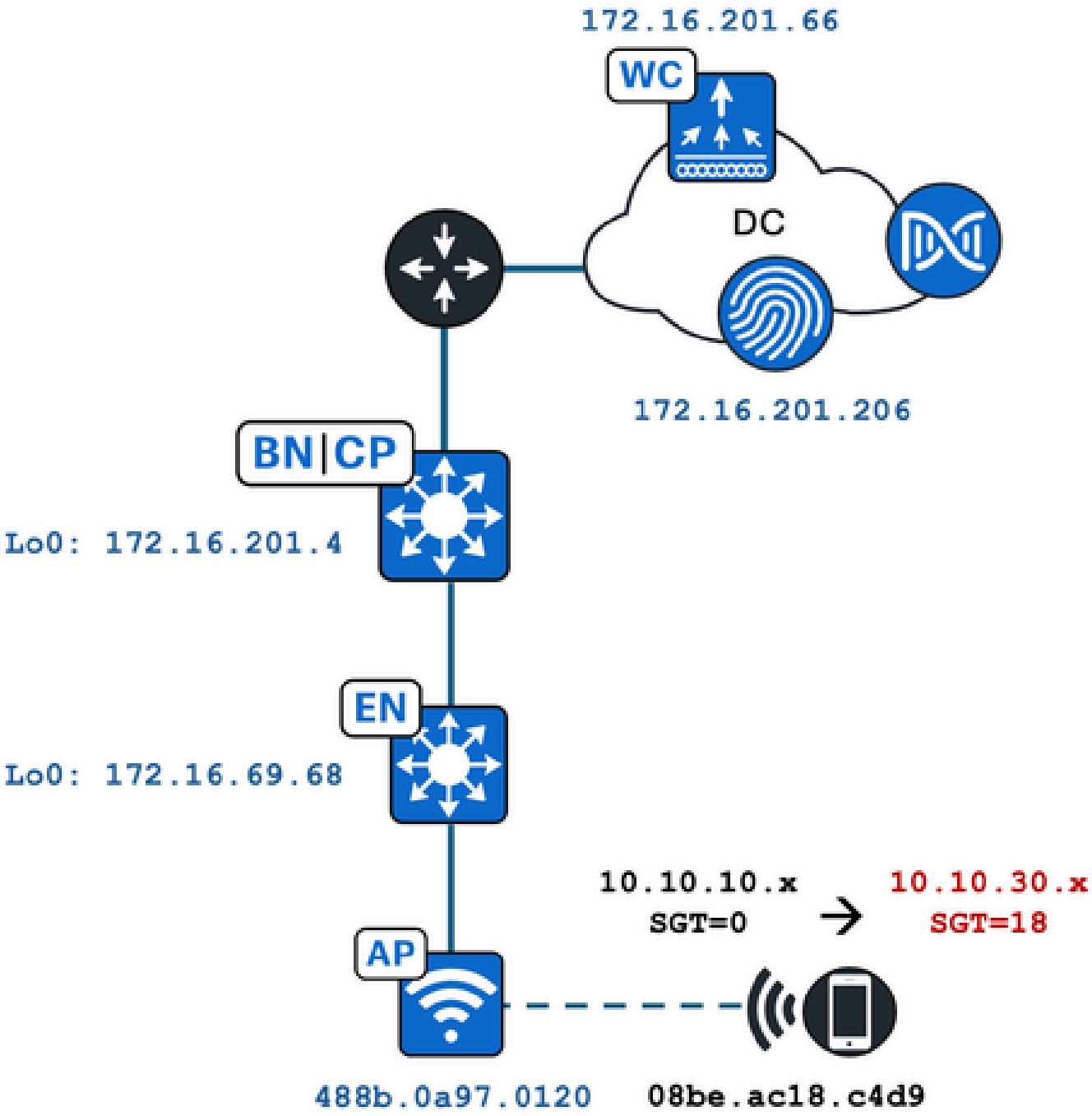
Uno degli aspetti chiave di SD-Access è la micro-segmentazione all'interno di una VPN ottenuta tramite i gruppi scalabili.

L'SGT può essere assegnato in modo statico per WLAN o SSID abilitati per il fabric (sebbene non siano gli stessi, la loro differenza non influisce sull'obiettivo principale di questo documento, quindi utilizziamo in modo intercambiabile i due termini per lo stesso significato per migliorare la leggibilità). Tuttavia, in molte implementazioni reali, spesso gli utenti che si connettono alla stessa WLAN richiedono un insieme diverso di criteri o impostazioni di rete. Inoltre, in alcuni scenari, è necessario allocare diversi indirizzi IP a client specifici all'interno della stessa WLAN di fabric per applicare a tali client criteri specifici basati su IP o soddisfare i requisiti di indirizzamento IP dell'azienda. L2VNID (Layer 2 Virtual Network Identifier, identificatore di rete virtuale di livello 2) è il parametro utilizzato da POCHE infrastrutture per collocare gli utenti wireless in intervalli di subnet diversi. Gli access point inviano l'L2VNID nell'intestazione VxLAN al Fabric Edge Node (EN), che quindi lo mette in correlazione con la VLAN L2 corrispondente.

Per ottenere questa granularità all'interno della stessa WLAN, viene sfruttata l'assegnazione di Dynamic SGT e/o L2VNID. Il WLC raccoglie le informazioni sull'identità dell'endpoint, le invia all'ISE per l'autenticazione, che le utilizza per soddisfare i criteri appropriati da applicare al client e restituisce le informazioni SGT e/o L2VNID al completamento dell'autenticazione.

Topologia

Per comprendere come funziona questo processo, abbiamo sviluppato un esempio utilizzando questa topologia di laboratorio:



Nell'esempio, la WLAN è configurata in modo statico con:

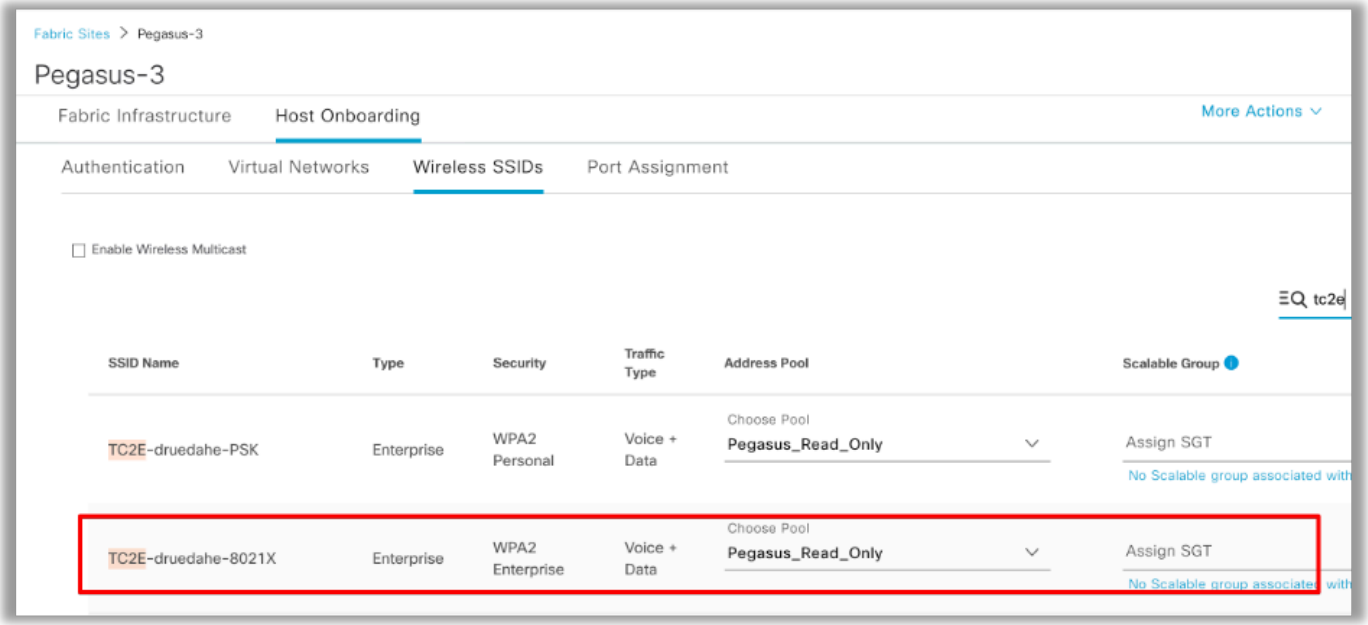
- L2VNID = 8198 / Nome pool IP = Pegasus_Read_Only —> VLAN 1030 (10.10.10.x)
- Nessun SGT

E il client wireless che si connette ad esso, ottiene dinamicamente questi parametri:

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

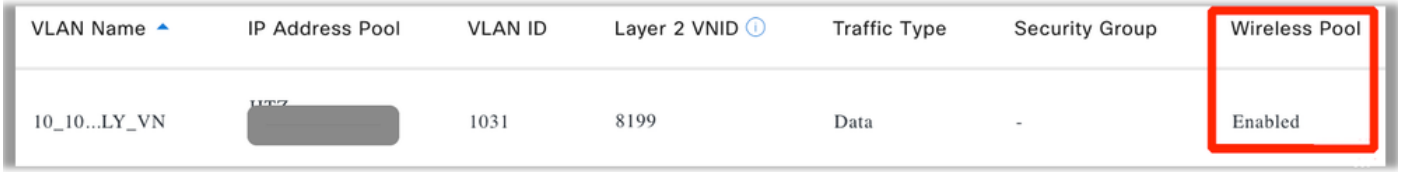
Configurazione

Innanzitutto, è necessario identificare la WLAN interessata e verificare come è configurata. Nell'esempio viene usato il SSID "TC2E-druedahe-802.1x". Al momento della redazione di questo documento, l'SDA è supportata solo tramite CatC, quindi dobbiamo controllare cosa vi è configurato. In Provisioning/Accesso SD/Siti fabric/<sito fabric specifico>/Host Onboarding/SSID wireless:



All'SSID è mappato il pool IP denominato "Pegasus_Read_Only" e non è assegnato staticamente alcun SGT, ovvero SGT=0. Ciò significa che, se un client wireless si connette e si autentica correttamente senza che ISE invii indietro alcun attributo per l'assegnazione dinamica, le impostazioni del client wireless sono così.

Il pool assegnato in modo dinamico deve essere presente prima nella configurazione WLC. A tale scopo, aggiungere il pool IP come "pool wireless" nella rete virtuale della scheda CatC:



Nell'interfaccia utente del WLC in Configuration/Wireless/Fabric, questa impostazione riflette questo modo:

Il pool "Pegasus_Read_Only" equivale allo 8198 L2VNID e vogliamo che il nostro client si trovi sullo 8199 L2VNID, il che significa che ISE deve dire al WLC di utilizzare il pool "10_10_30_0-READONLY_VN" per questo client. Vale la pena ricordare che il WLC non contiene alcuna configurazione per le VLAN del fabric. È a conoscenza solo degli L2VNID. Ciascuna viene quindi mappata a una VLAN specifica nelle VLAN del fabric SDA.

Verifica

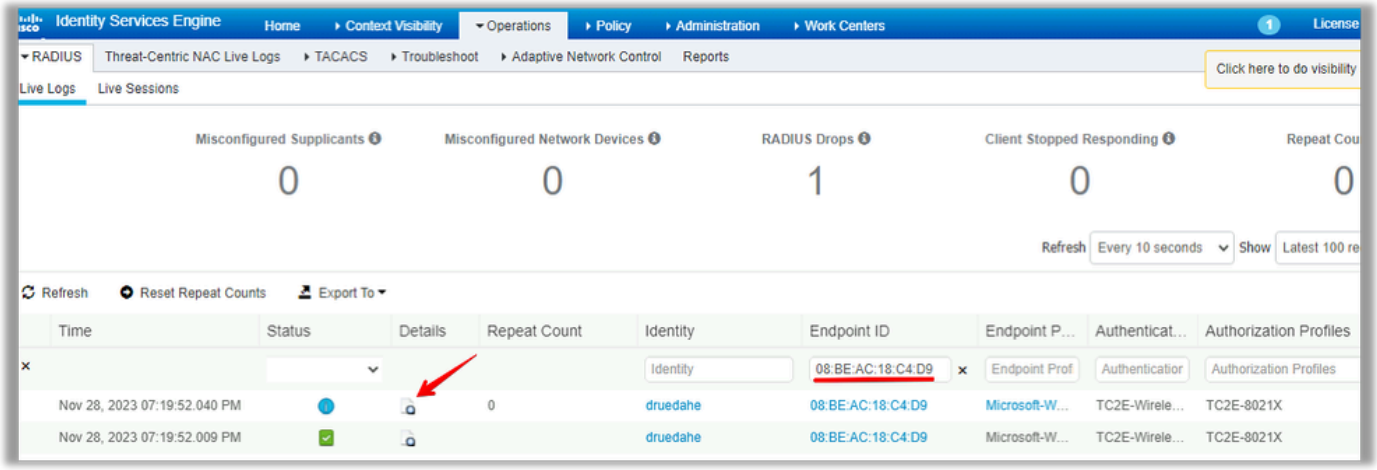
I sintomi segnalati per problemi relativi all'assegnazione dinamica di SGT/L2VNID sono:

1. I criteri SG non vengono applicati ai client wireless che si connettono a una WLAN specifica. (Problema di assegnazione SGT dinamico).
2. I client wireless non ottengono l'indirizzo IP tramite DHCP oppure non ottengono un indirizzo IP dall'intervallo di subnet desiderato in una WLAN specifica. (Problema di assegnazione dinamica L2VNID).

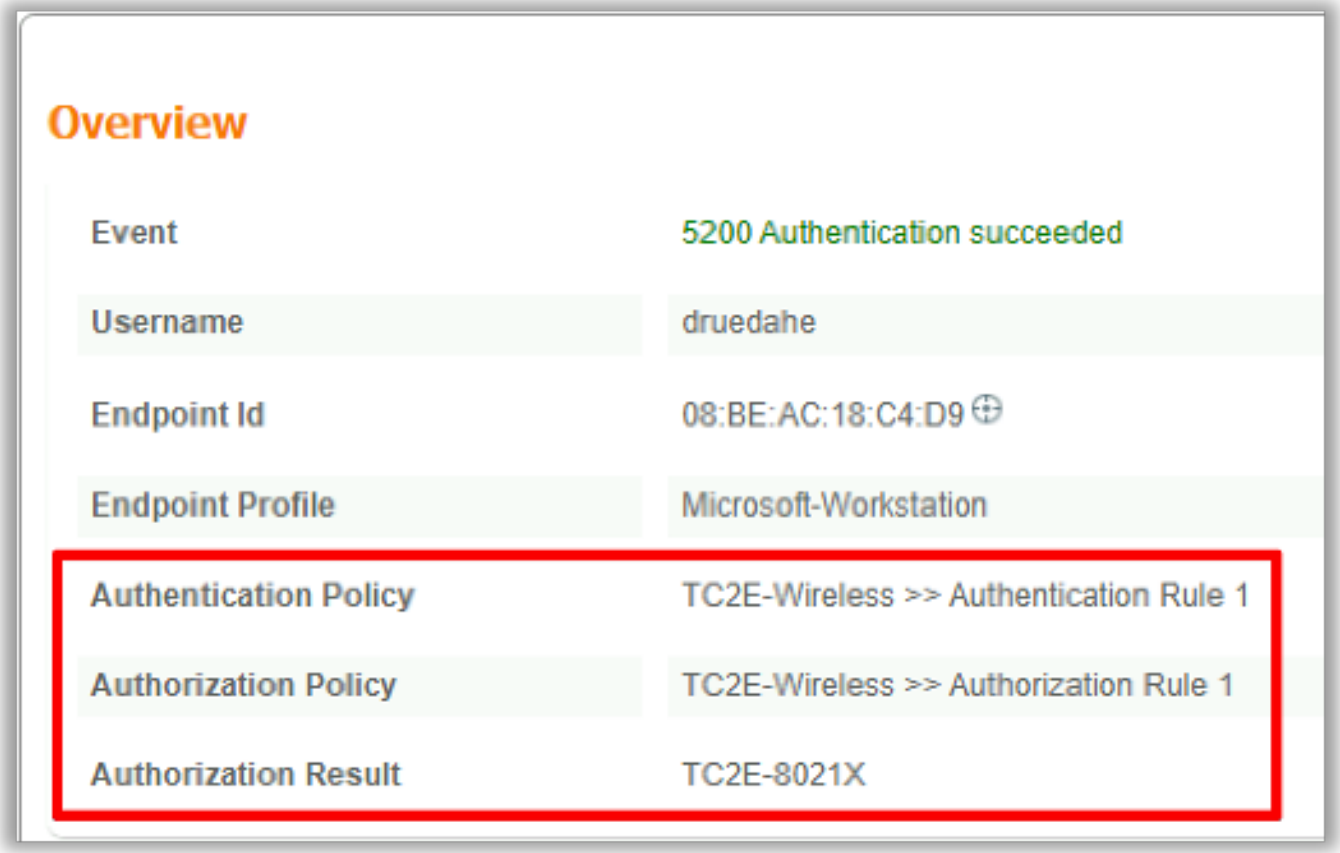
Ora viene descritta la verifica di ogni nodo rilevante in questo processo.

Verifica ISE

Il punto di partenza è ISE. Andare alla GUI di ISE in Operation/RADIUS/Live Logs/ e usare l'indirizzo MAC del client wireless come filtro nel campo ID endpoint, quindi fare clic sull'icona Dettagli:



Viene quindi aperta un'altra scheda con i dettagli di autenticazione. L'interesse è rivolto principalmente a due sezioni, Panoramica e Risultato:



Panoramica mostra se il criterio desiderato è stato utilizzato per l'autenticazione del client wireless. In caso contrario, la configurazione delle policy ISE deve essere rivista, ma ciò esula dalle finalità del presente documento.

Result mostra ciò che è stato restituito da ISE al WLC. L'obiettivo è l'assegnazione dinamica di SGT e L2VNID, in modo che questi dati vengano inclusi in questo contesto. Si notino due cose:

1. Il nome L2VNID viene inviato come attributo "Tunnel-Private-Group-ID". ISE deve restituire il nome (10_10_30_0-READONLY_VN) non l'ID (8199).

2. L'SGT viene inviato come "cisco-av-pair". Nell'attributo cts:security-group-tag si noti che il valore SGT è in formato esadecimale (12) e non in formato ascii (18), ma sono identici. TC2E_Learners è il nome SGT in ISE internamente.

Verifica WLC

Nel WLC, è possibile utilizzare il comando show wireless fabric client summary per controllare lo stato del client e il show wireless fabric summary per verificare due volte la configurazione dell'infrastruttura e la presenza dell'L2VNID assegnato in modo dinamico:

```
<#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
```

Se le informazioni previste non vengono riflesse, è possibile abilitare le tracce RA per l'indirizzo MAC del client wireless nel WLC per vedere esattamente i dati ricevuti da ISE. Per informazioni su come ottenere l'output di RA Traces per un client specifico, vedere questo 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

Nell'output di RA Trace per il client, gli attributi inviati da ISE vengono inseriti nel pacchetto 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_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
```

Il WLC invia quindi le informazioni SGT e L2VNID a:

1. Il punto di accesso (AP) tramite CAPWAP (controllo e provisioning di punti di accesso wireless).

2. Il PC fabric tramite LISP.

Il Fabric CP invia quindi il valore SGT tramite LISP al Fabric EN a cui è collegato l'AP.

Verifica Fabric EN

Il passaggio successivo consiste nel verificare se la tecnologia Fabric EN riflette le informazioni ricevute in modo dinamico. Il comando show vlan conferma la VLAN associata all'ID 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
```

Si noti che l'ID L2VNID 8199 è mappato alla VLAN 1031.

Inoltre, il comando show device-tracking database mac <mac address> viene visualizzato se il client wireless si trova sulla VLAN desiderata:

```
<#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     T
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)

Infine, il comando show cts role-based sgt-map vrf <vrf name> all restituisce il valore SGT assegnato al client. Nell'esempio, la VLAN 1031 fa parte della 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

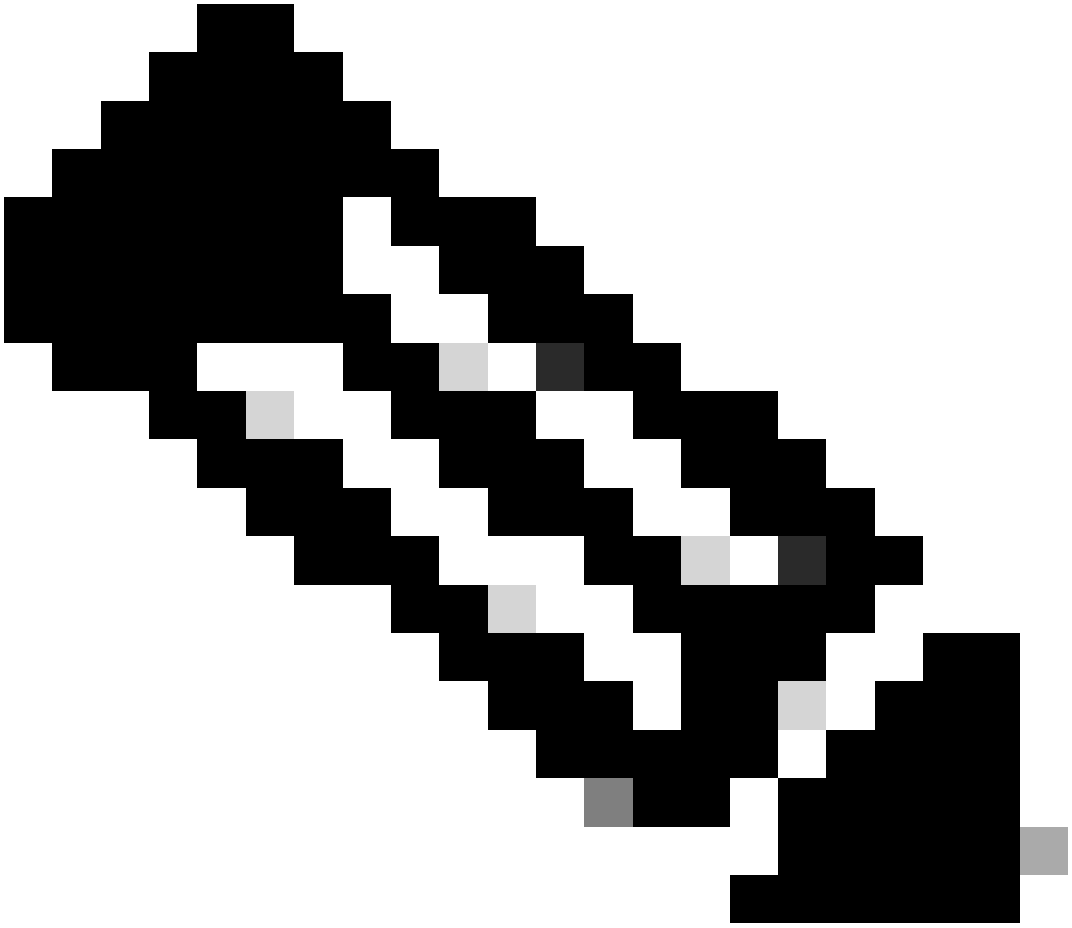
Active IPv4-SGT Bindings Information

IP Address SGT Source
==========

10.10.30.12

18

LOCAL
10.10.30.14 4 LOCAL



> Nota: l'applicazione della policy Cisco TrustSec (CTS) in un'infrastruttura SDA per client wireless (come per i client cablati) viene eseguita dagli endpoint, non dagli access point né dai WLC.

Con questo l'EN è in grado di applicare le politiche configurate per il SGT specificato.

Se questi output non vengono popolati correttamente, è possibile usare il comando debug lisp control-plane all nella EN per verificare se sta ricevendo la notifica LISP proveniente dal 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.
```

Si noti che la notifica LISP viene prima ricevuta dal CP che la trasmette poi alla EN. La voce SISF o Device-tracking viene creata alla ricezione di questa notifica LISP, che è una parte importante del processo. È inoltre possibile visualizzare questa notifica con:

<#root>

```
EDGE-01#
```

show lisp instance-id 8199 ethernet database wlc clients detail

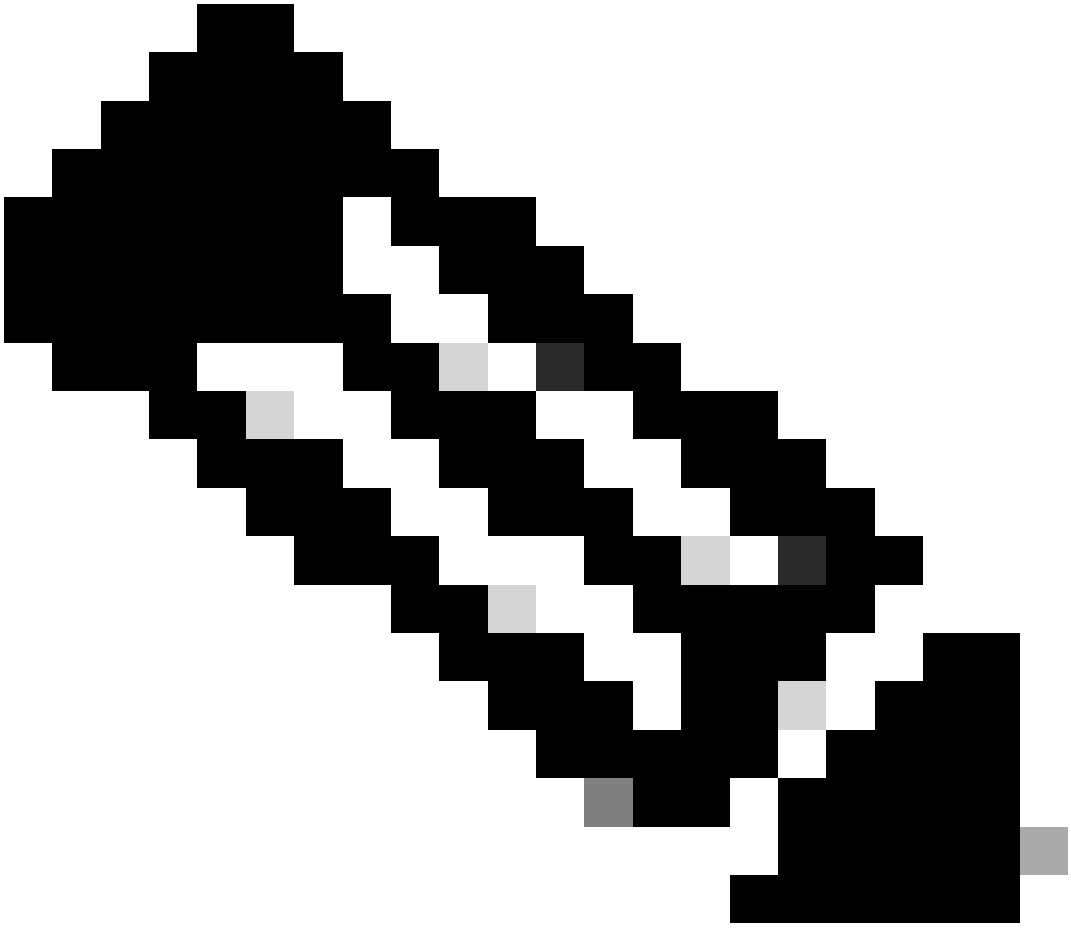
```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 21:23:31.737 UTC Wed Nov 29 2023


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: il valore evidenziato 12 nella sezione Metadati è la versione esadecimale dell'SGT 18 che si intendeva assegnare inizialmente. E questo conferma che l'intero processo è stato completato correttamente.

Verifica pacchetti

Come ultima conferma, possiamo usare lo strumento Embedded Packet Capture (EPC) nello switch EN e vedere come i pacchetti di questo client vengono trasmessi dall'access point. Per informazioni su come ottenere un file di acquisizione con EPC, consultare:

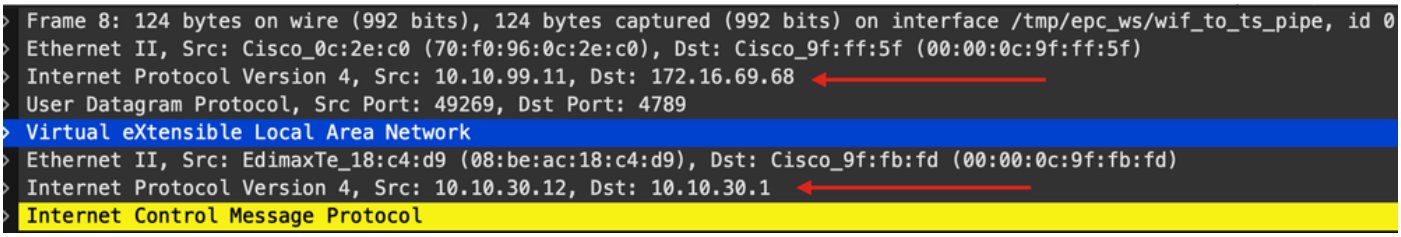
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_packet_capture.html

Per questo esempio, è stato avviato un ping sul gateway nel client wireless stesso:

icmp

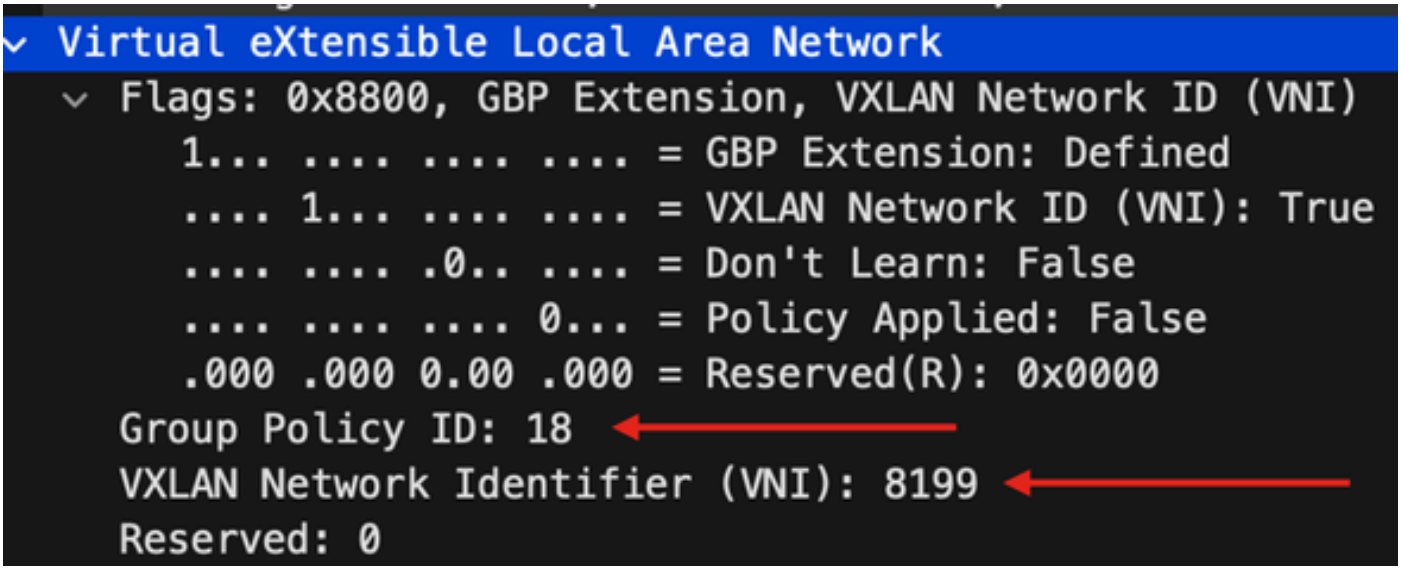
No.	Time	Arrival Time	Source	Destination	VXLAN N	Protocol	Identification	Length	Info
8	0.082365	2023-12-01 18:47:34.384734	10.10.30.12	10.10.30.1	8199	ICMP	0x01e1 (481),0x…	124	Echo (ping) request
18	0.000028	2023-12-01 18:47:39.277504	10.10.30.12	10.10.30.1	8199	ICMP	0x01e3 (483),0x…	124	Echo (ping)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

Notare che il pacchetto deve già essere fornito con un'intestazione VXLAN dall'access point, poiché l'access point e l'endpoint formano un tunnel VXLAN tra di essi per i client wireless fabric:



L'origine del tunnel è l'indirizzo ip del punto di accesso (10.10.99.11) e la destinazione è l'indirizzo ip del punto di accesso (172.16.69.68). All'interno dell'intestazione VXLAN è possibile visualizzare i dati effettivi del client wireless, in questo caso il pacchetto ICMP.

Infine, controllare l'intestazione della VXLAN:



Prendere nota del valore SGT come ID di Criteri di gruppo, in questo caso in formato ascii e del valore L2VNID come VXLAN Network Identifier (VNI).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).