Understand Dynamic SGT/L2VNID Assignment on SDA Wireless

Contents

Introduction

This document describes the process of Dynamic SGT and L2VNID assignment on Fabric Enabled Wireless 802.1x SSIDs.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Remote Authentication Dial-In User Service (RADIUS)
- Wireless LAN Controller (WLC)
- Identity Services Engine (ISE)
- Security Group Tag (SGT)
- L2VNID (Layer 2 Virtual Network Identifier)
- SD-Access Fabric Enabled Wireless (SDA FEW)
- Locator/ID Separation Protocol (LISP)
- Virtual eXtensible Local Area Network (VXLAN)
- Fabric Control Plane (CP) and Edge Node (EN)
- Catalyst Center (CatC, formerly known as Cisco DNA Center)

Components Used

WLC 9800 Cisco IOS® XE version 17.6.4

Cisco IOS® XE

ISE version 2.7

CatC version 2.3.5.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

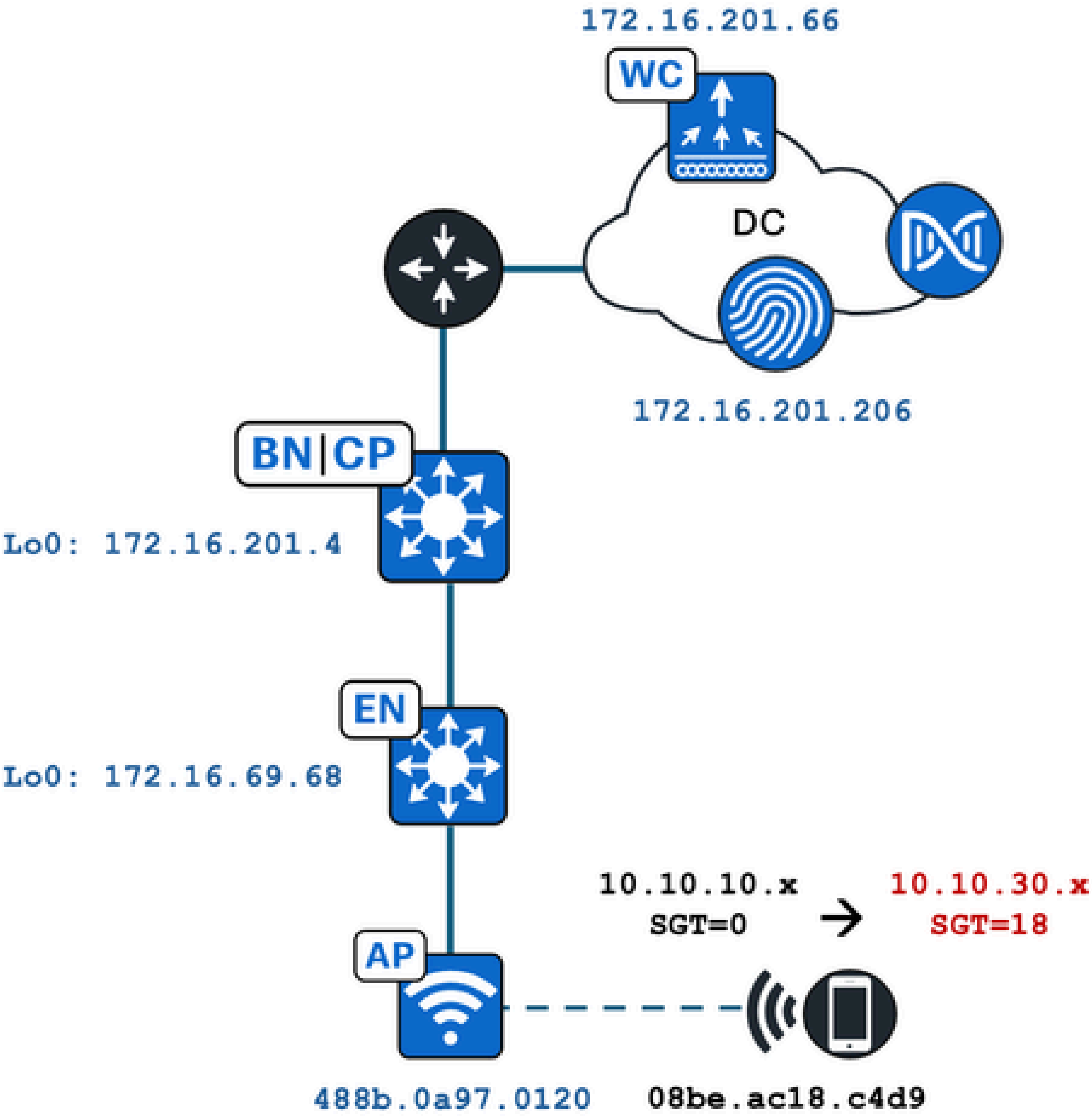
One of the key aspects of SD-Access is the micro-segmentation within a VN achieved via the Scalable Groups.

The SGT can be assigned statically per Fabric Enabled WLAN or SSID (although they are not the same, their difference does not impact the main goal of this document, so we interchangeably use the two terms for the same meaning to enhance readability). However, in many real deployments, there are often users connecting to the same WLAN who require a different set of policies or network settings. Additionally, in some scenarios, there is a need to allocate different IP addresses to specific clients within the same Fabric WLAN to either apply specific IP-based policies to them or meet the company IP addressing requirements. The L2VNID (Layer 2 Virtual Network Identifier) is the parameter that the FEW infrastructure uses to place wireless users in different subnet ranges. The Access Points send the L2VNID in the VxLAN header to the Fabric Edge Node (EN), which then correlates it to the corresponding L2 VLAN.

To achieve this granularity within the same WLAN, Dynamic SGT and/or L2VNID assignment is leveraged. The WLC collects the identity information of the endpoint, sends it to ISE for authentication, which uses it to match the proper policy to be applied to this client and returns the SGT and/or L2VNID information upon successful authentication.

Topology

To understand how this process works we developed an example using this lab topology:



In this example the WLAN is configured statically with:

- L2VNID = 8198 / IP Pool Name = Pegasus_Read_Only ---> VLAN 1030 (10.10.10.x)
- No SGT

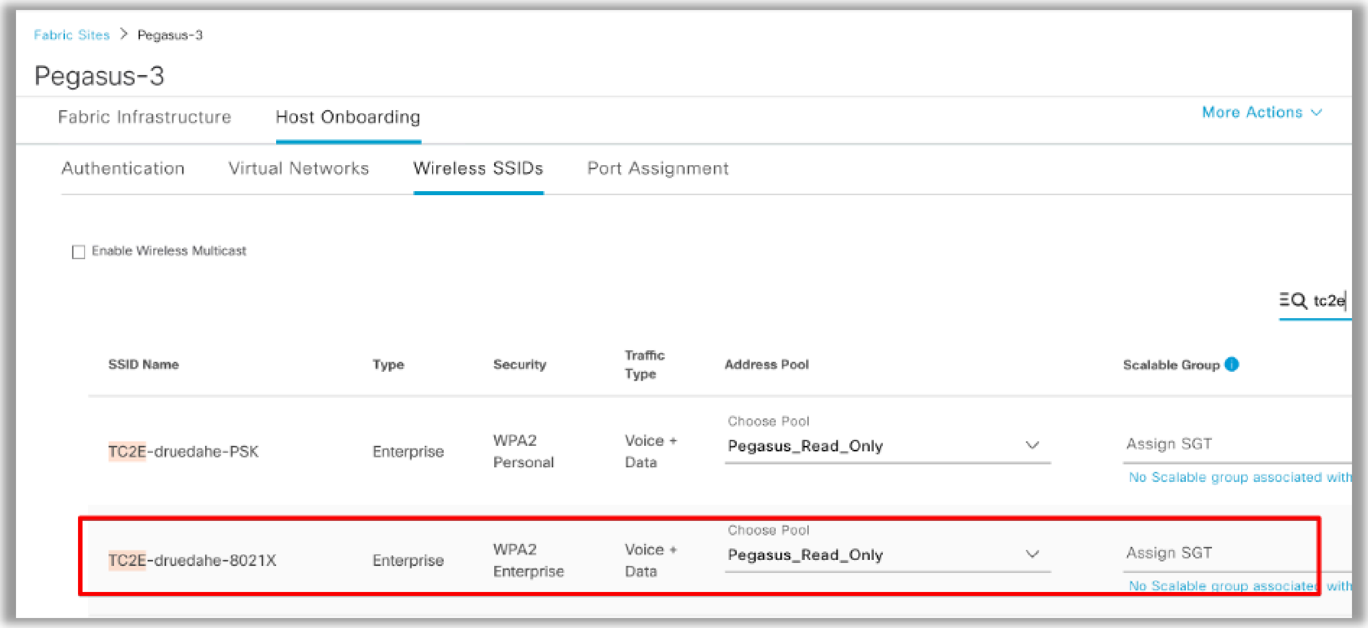
And the wireless client connecting to it, dynamically gets these parameters:

- L2VNID = 8199 / IP Pool Name = 10_10_30_0-READONLY_VN ---> VLAN 1031 (10.10.30.x)
- SGT = 18

Configuration

First off, we need to identify the involved WLAN and check how it is configured. In this example the

"TC2E-druedahe-802.1x" SSID is used. At the time of this document redaction, SDA is only supported via CatC so we must check what is configured there. Under Provision/SD-Access/Fabric Sites/<specific Fabric site>/Host Onboarding/Wireless SSIDs:

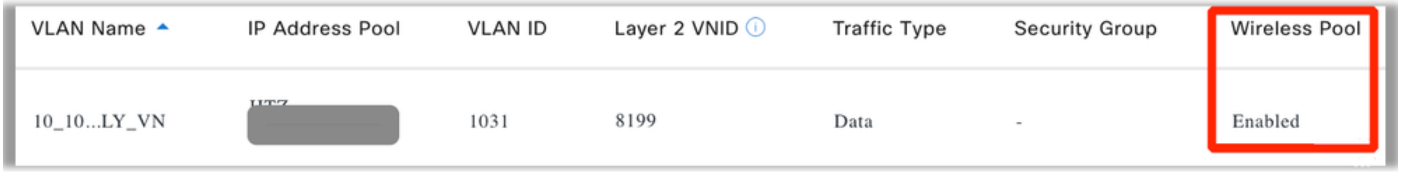


☐ Enable Wireless Multicast

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

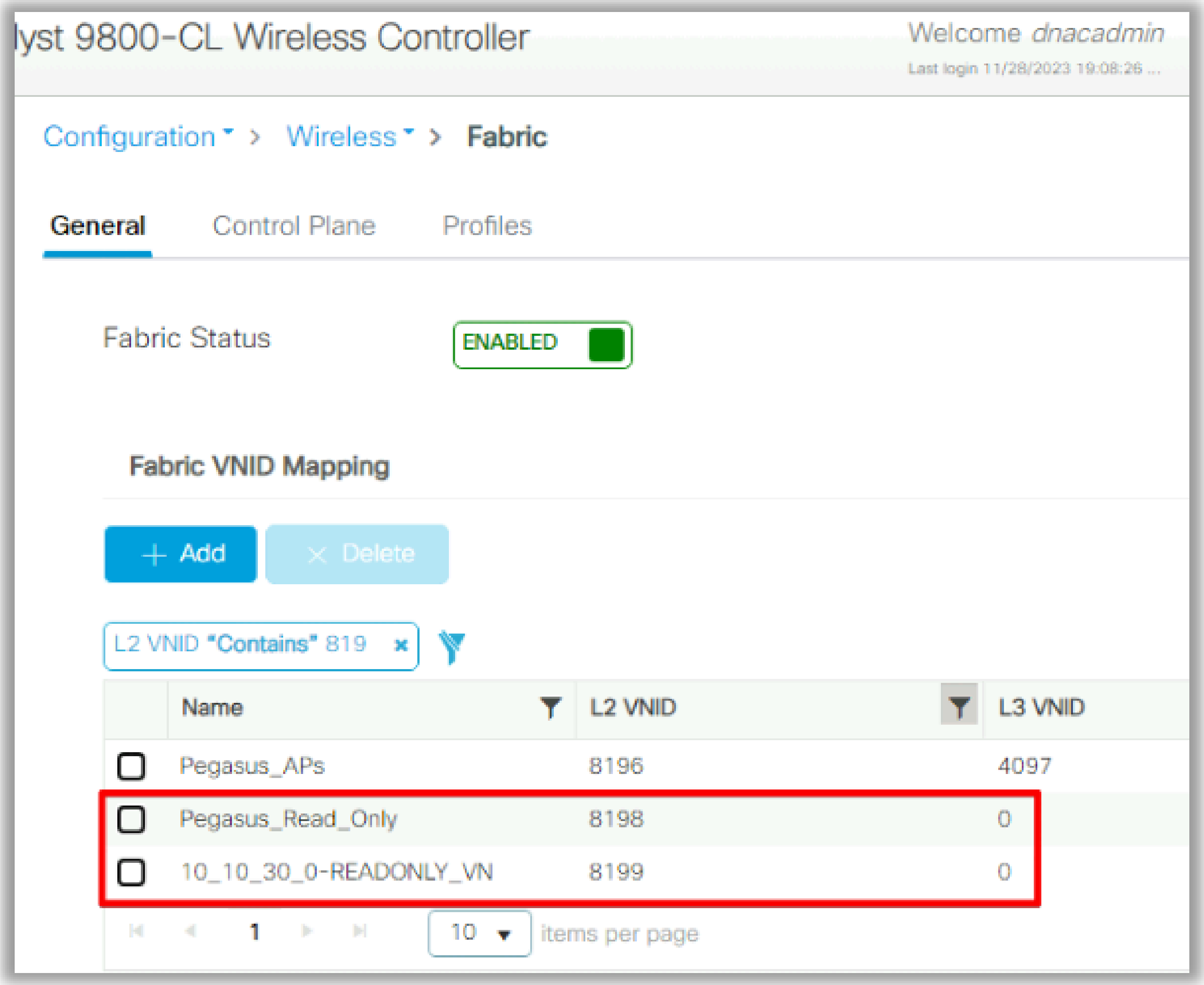
The SSID has the IP Pool named “Pegasus_Read_Only” mapped to it and has no SGT statically assigned which means SGT=0. This means that, if a wireless client connects and authenticates successfully without ISE sending any attribute back for dynamic assignment, this is what the wireless client settings are.

The pool that is dynamically assigned must be present prior in the WLC configuration. And this is done by adding the IP Pool as "Wireless Pool" in the Virtual Network on the 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

In the WLC GUI under Configuration/Wireless/Fabric, this setting reflects this way:



	Name	L2 VNID	L3 VNID
□	Pegasus_APs	8196	4097
□	Pegasus_Read_Only	8198	0
□	10_10_30_0-READONLY_VN	8199	0

The "Pegasus_Read_Only" pool equates to the 8198 L2VNID and we want our client to be on the 8199 L2VNID, which means ISE needs to tell the WLC to use the "10_10_30_0-READONLY_VN" pool for this client. Worth to remember that the WLC does not hold any configuration for the Fabric VLANs. It is only aware of the L2VNIDs. Each one is then mapped to a specific VLAN in the SDA Fabric ENs.

Verification

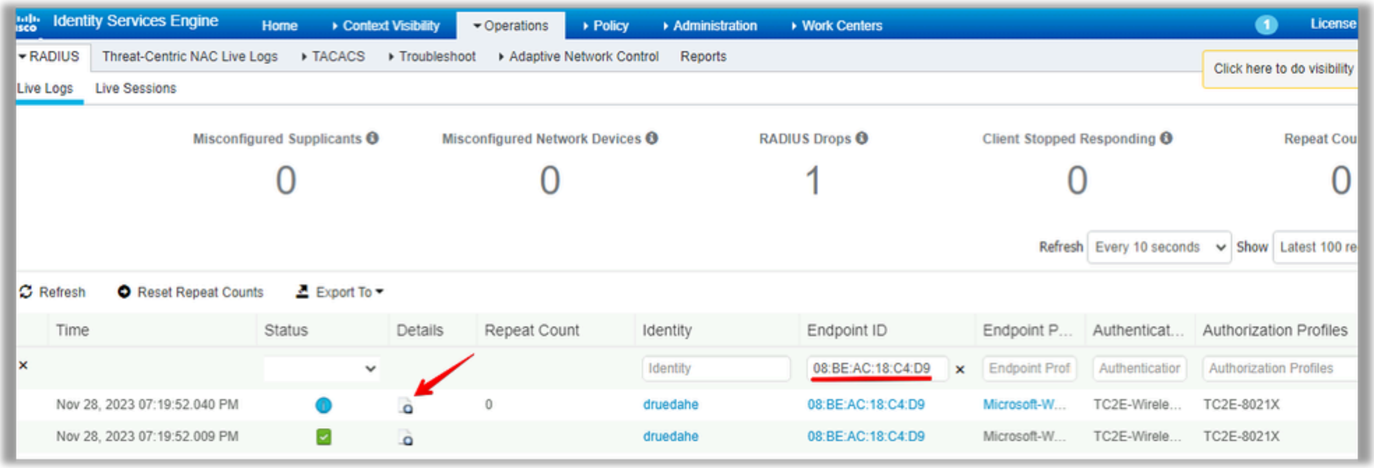
The symptoms reported for problems involving the Dynamic Assignment of SGT/L2VNID are either:

1. SG Policies are not enforced on wireless clients that connect to a specific WLAN. (Dynamic SGT Assignment problem).
2. Wireless clients are not obtaining IP address via DHCP, or they are not obtaining an IP address from the desired subnet range on a specific WLAN. (Dynamic L2VNID Assignment problem).

Now the verification of each relevant node in this process is described.

ISE Verification

The starting point is ISE. Go to the ISE GUI under Operation/RADIUS/Live Logs/ and use the wireless client mac address as filter in the Endpoint ID field, then click on the Details icon:

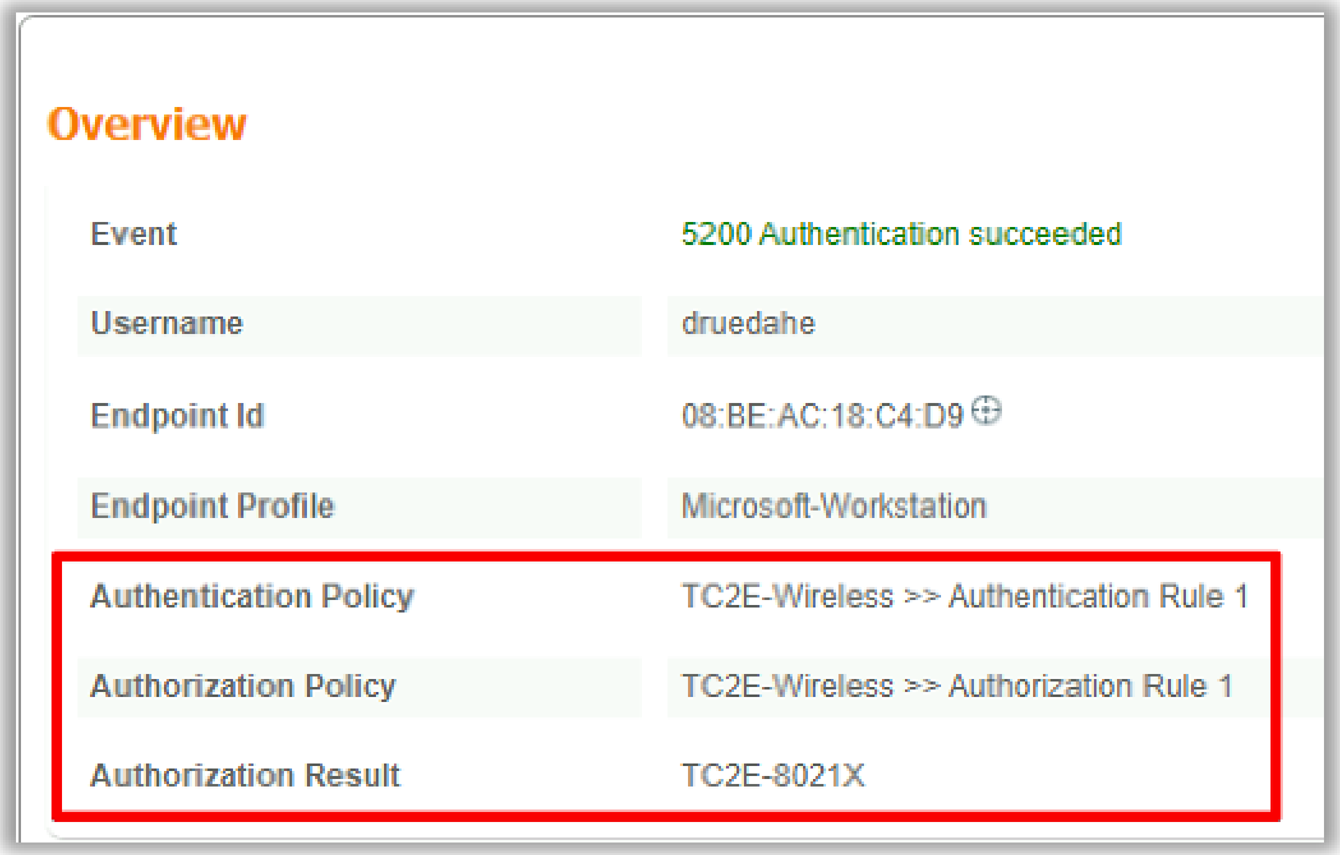


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Cou
0	0	1	0	0

Refresh Every 10 seconds Show Latest 100 re

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Profiles
×				Identity	08:BE:AC:18:C4:D9 ×	Endpoint Prof	Authenticatior	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

It then opens up another tab with the authentication details. We are interested mainly in two sections, **Overview** and **Result**:



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

Overview shows whether the intended or desired policy was used for this wireless client authentication. If not, the ISE policies confiuration needs to be revisited, however this is outside of the scope of this document.

Result shows what was returned by ISE to the WLC. The goal is to have the SGT and the L2VNID dynamically assigned, so this data must be included here, and it is. Notice two things:

1. The L2VNID name is sent as a "Tunnel-Private-Group-ID" attribute. ISE must return the name (10_10_30_0-READONLY_VN) not the id (8199).

2. The SGT is sent as a "cisco-av-pair". In the cts:security-group-tag attribute, note that the SGT value is in

hex (12) not in ascii (18), but they are the same. TC2E_Learners is the SGT name in ISE internally.

WLC Verification

In the WLC we can use the **show wireless fabric client summary** command to check the client status and the **show wireless fabric summary** to double confirm the Fabric configuration and the presence of the dynamically assigned L2VNID:

<#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-cont
  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
```

If the expected information is not reflected, we can enable RA Traces for the wireless client mac address in the WLC to see exactly the data received from ISE. Information on how to obtain the RA Traces output for a specific client can be found in this document:

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

In the RA Trace output for the client, the attributes sent by ISE are carried in the RADIUS Access-Accept packet:

<#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
```

The WLC then sends the SGT and L2VNID information to:

1. The Access Point (AP) via CAPWAP (Control And Provisioning of Wireless Access Points).

2. The Fabric CP via LISP.

The Fabric CP then sends the SGT value via LISP to the Fabric EN where the AP is connected.

Fabric EN Verification

The next step is to validate if the Fabric EN is reflecting the dynamically received information. The **show**

vlan command confirms the VLAN associated to the 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
```

We can see that the L2VNID 8199 is mapped to VLAN 1031.

And the **show device-tracking database mac <mac address>** displays if the wireless client is on the desired VLAN:

<#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)
```

Lastly, the **show cts role-based sgt-map vrf <vrf name> all** command provides the SGT value assigned to the client. In this example, the VLAN 1031 is part of the "READONLY_VN" VRF:

<#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
```

Note: The Cisco TrustSec (CTS) policy enforcement in a SDA Fabric for Wireless Clients (like for Wired clients), is done by the ENs, not by the APs nor the WLC.

With this the EN is able to apply the policies configured for the specified SGT.

If these outputs are not populating properly, we can use the **debug lisp control-plane all** command in the EN to check whether it is receiving the LISP notification coming from the 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.
```

Note that the LISP notification is first received by the CP who then relays it to the EN. The SISF or Device-tracking entry is created upon receiving this LISP notification, which is an important part of the process. You can also see this notification with:

<#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
```

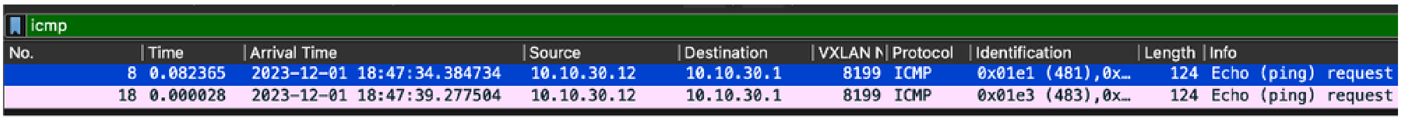
Note: The highlighted value 12 in the Metadata section is the hex version of the SGT 18 we initially intended to assign. And this confirms the whole process finished properly.

Packets Verification

As a last confirmation step, we can also use the Embedded Packet Capture (EPC) tool in the EN switch and see how the packets of this client are transmitted by the AP. For information on how to get a capture file with EPC, refer to:

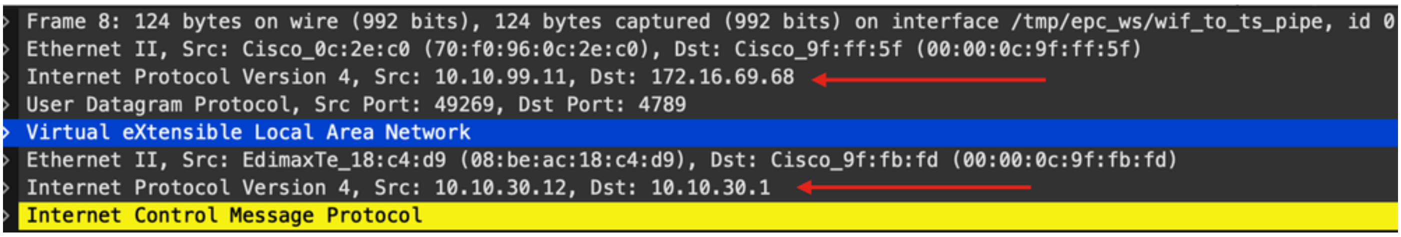
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_packet_capture.html

For this example, a ping to the gateway was initiated in the wireless client itself:



```
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
```

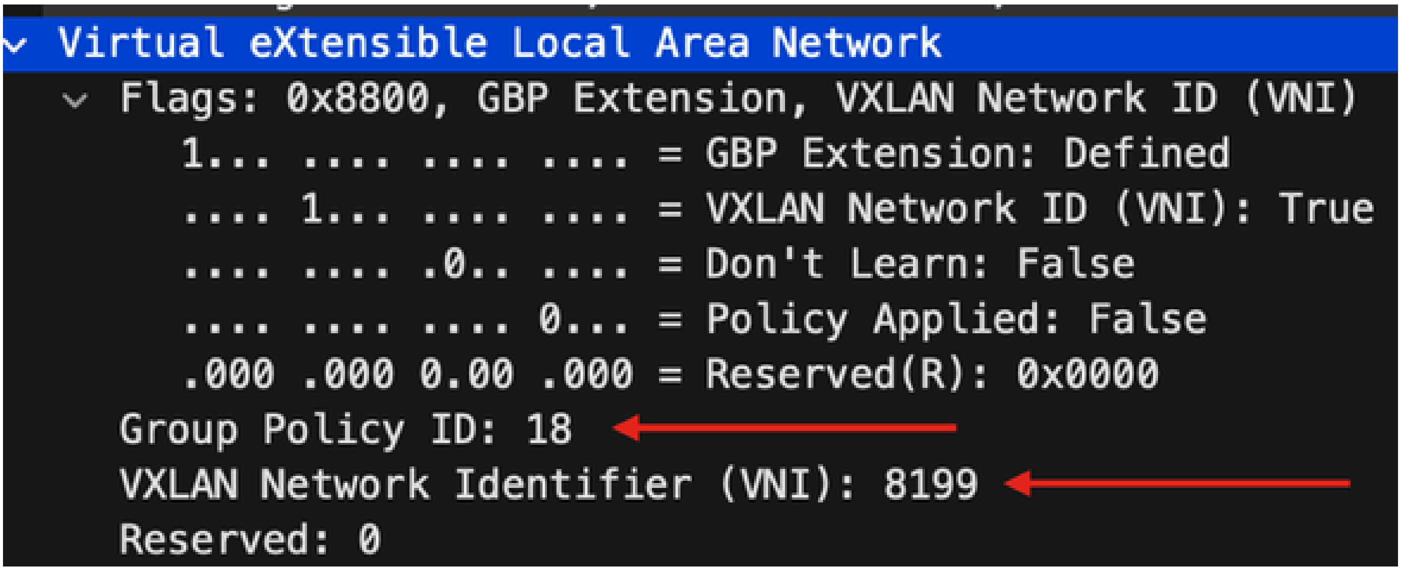
Note that the packet is already expected to come with a VXLAN header from the AP, as the AP and EN form a VXLAN tunnel between them for the Fabric wireless clients:



```
> 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
```

The source of the tunnel is the AP ip address (10.10.99.11) and the destination is the EN Loopback0 ip address (172.16.69.68). Inside of the VXLAN header we can see the actual wireless client data, in this case the ICMP packet.

Finally, inspect the VXLAN header:



```
v Virtual eXtensible Local Area Network
  v 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
```

Note the SGT value as Group Policy ID -- in this case, in ascii format and the L2VNID value as VXLAN Network Identifier (VNI).