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
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>トポロジ</u>
<u>コンフィギュレーション</u>
<u>ISEの検証</u>
<u>WLCの検証</u>
<u>ファブリックENの検証</u>
<u>パケットの検証</u>

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:

Fabric Infrastructure	Host Onboarding)				More Actions
Authentication Virtu	al Networks	Wireless SSIDs	Port Assignm	nent		
Enable Wireless Multicast						
						ΞQ
SSID Name	Туре	Security	Traffic Type	Address Pool		Scalable Group 🔵
TC2E-druedahe-PSK	Enterp	vrise WPA2	Voice +	Choose Pool Pegasus_Read_Only	~	Assign SGT
		i croonal	Data			No Scalable group associat

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。

I	VLAN Name 🔺	IP Address Pool	VLAN ID	Layer 2 VNID 🕕	Traffic Type	Security Group	Wireless Pool
	10_10LY_VN		1031	8199	Data	-	Enabled

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。

lyst 9800	-CL Wireless Controlle	r		Welco Last login	me <i>dnacadmin</i> 11/28/2023 19:08:26		
Configura	ation > Wireless > Fab	ric					
General	General Control Plane Profiles						
Fabr	Fabric Status						
Fa	Fabric VNID Mapping						
	Add × Delete						
L2 V	/NID "Contains" 819 🗙 🏋						
	Name	T	L2 VNID	\mathbf{T}	L3 VNID		
	Pegasus_APs		8196		4097		
	Pegasus_Read_Only		8198		0		
D	10_10_30_0-READONLY_VN		8199		0		
м	< 1 ► ► 10 ▼	iten	ns per page				

「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。

sco Ide	ntity Services Engine	Home + Contex	t Visibility	Operations Policy	 Administration 	► Work Centers				1 License
- RADIUS	Threat-Centric NAC Live L	.ogs + TACACS	Troubleshoo	t Adaptive Network Co	ontrol Reports					Click here to do visibility
Live Logs	Live Sessions									
	Misconfig	ured Supplicants 🕄	Misc	onfigured Network Device	es 🛈	RADIUS Drops		Client Stopped F	Responding 🚯	Repeat Cou
		0		0		1		0)	0
								Refresh	Every 10 second	s 🗸 Show Latest 100 re
C Refres	h 🗢 Reset Repeat Count	ts 🛃 Export To 🕶								
Tin	ne	Status	Details	Repeat Count	Identity	Endpoint ID		Endpoint P	Authenticat	Authorization Profiles
×		~	/	•	Identity	08:BE:AC:18:C4:D	9 ×	Endpoint Prof	Authentication	Authorization Profiles
No	v 28, 2023 07:19:52.040 PM	0		0	druedahe	08:BE:AC:18:C4:D9)	Microsoft-W	TC2E-Wirele	TC2E-8021X
No	v 28, 2023 07:19:52.009 PM		ò		druedahe	08:BE:AC:18:C4:D9)	Microsoft-W	TC2E-Wirele	TC2E-8021X

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	
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

<#root>

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。

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: IP-address Name Key Status ------172.16.201.4 default-control-plane f9afa1 Up Fabric VNID Mapping: Subnet Control plane n L2-VNID L3-VNID IP Address Name _____ _____ _____ Pegasus_APs 8196 Pegasus_Extended 8207 4097 10.10.99.0 255.255.255.0 default-cont 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

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/configguide/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 1	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-Authenticate	or[80]	18		
{wncd_x_R0-0}{1}:	[radius]	[21860]:	(info):	01:					
{wncd_x_R0-0}{1}:	[radius]	[21860]:	(info):	RADIUS:					
Tunnel-Private-Gro	oup-Id[81]	25 '	10_10_30)_0-READON	NLY_VN"				
$\{wncd \times RO_0\}$	Fradiusl	[21860].	(info).	ΡΔΠΤΠ Σ·	FAP-Key-Name	F1021	67	*	
$\{$ when $x \in \mathbb{R}^{-0}$	[radius]	[21860].	(info).	RADIUS.	Vendor Cisco	[102]	38		
$\{wncd x R0-0\}\{1\}$:	[radius]	[21860]	(info):	RADTUS.	vendor, erseo	[20]	50		
	Ligarabl	[21000].	(1110).	10101051					
Cisco AVpair	[1]	32 "cts:	security	y-group-ta	ag=0012-01"				
<pre>{wncd_x_R0-0}{1}:</pre>	[radius]	[21860]:	(info):	RADIUS:	Vendor, Cisco	[26]	34		
{wncd_x_R0-0}{1}:	[radius]	[21860]:	(info):	RADIUS:	,				
Cisco AVpair	[1]	28 "cts:	sgt-name	e=TC2E Lea	arners"				
_			-						
{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-miso	c] [21860]]: (info]): [08be.a	ac18.c4d9:capwap_9000	0000a]	Userna	ame druedahe receiv	v
{wncd_x_R0-0}{1}:	[epm-miso	[21860]]: (info): [08be.a	ac18.c4d9:capwap_9000	0000a]	VN REA	ADONLY_VN received	
\dots	[auth_mou	r] [21860 ⁻	l. (info) \cdot $\Gamma 0.8 he^{-1}$	ac18 c4d9 canwar 0000	100021	llsor [Profile annlied sur	c
$\sum_{wncd} x R0_0 \{1\}$	[cliont_	uth] [21000]	3. (1110) 860]• (n/). [UODE.α ητα). ΜΔΓ	\cdot 08he ac18 c4d0 ADI) MORTI	F cont	- Client state fl	2
$\lim_{\to \infty} \nabla^- \nabla_1 \nabla_2 \nabla_2 \nabla_2 \nabla_2 \nabla_2 \nabla_2 \nabla_2 \nabla_2 \nabla_2 \nabla_2$	Le ment-a		500]. (III	JUEJ. MAC	. 0052.ac10.c409 AD		L Selli	L. CHEIL State Ha	a

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_APsactiveTu0:8196, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/10, Gi1/0/181030 Pegasus_Read_OnlyactiveTu0:8198, 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

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。

> 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

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。

 Virtual eXtensible Local Area Network
\sim Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
1 = GBP Extension: Defined
<pre> 1 = VXLAN Network ID (VNI): True</pre>
<pre> 0 = Policy Applied: False</pre>
.000 .000 0.00 .000 = Reserved(R): 0x0000
Group Policy ID: 18 ┥
VXLAN Network Identifier (VNI): 8199 ┥
Reserved: 0

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。