# cisco.



# 8.8 EoGRE トンネリング導入ガイド

CUWN 8.8 WLC と FC AP - EoGRE トンネル ゲートウェイ導入ガイド 3 WLC EoGRE トンネリング 3 サポートされるコントローラとAP 4 EoGRE トンネル システムの設計オプション 5 設計1:WLC ベースの EoGRE トンネル 5 WLC EoGRE トンネリングの設定 6 WLC EoGRE トンネル パラメータの設定 8 一般的な展開:WLC EoGRE トポロジ 14 リリース 8.2 のトンネリング ソースの変更 19 EoGRE トンネル DHCP オプション 82 の設計 19 EoGRE トンネルの冗長性 21 EoGRE TGW フェールオーバーの設定手順 22 リリース 8.8 の VLAN オーバーライド機能付き EoGRE トンネル 25 設計2: FlexConnect AP ベースの EoGRE トンネル 29 EoGRE 機能の管理 32 トラブルシューティング コマンド 33 機能の設定手順 33 show コマンド 34

EoGRE 機能の設定例 34

参照 38

# **CUWN 8.8 WLC** と **FC AP - EoGRE** トンネル ゲートウェ イ導入ガイド

# WLC EoGRE トンネリング

Ethernet over GRE (EoGRE) は、ホットスポットからの Wi-Fi トラフィックを集約するための新しい集約ソリューショ ンです。このソリューションでは、顧客宅内機器 (CPE) デバイスで、エンドホストから届いたイーサネットトラ フィックをブリッジし、そのトラフィックを IP GRE トンネルでイーサネットパケットにカプセル化できます。IP GRE トンネルがサービス プロバイダーのブロードバンド ネットワーク ゲートウェイで終端すると、エンドホストのトラ フィックが終了し、エンドホストに対するサブスクライバ セッションが開始されます。



#### トンネリングの一般的なメリット

- クライアントは、さまざまなテクノロジーやベンダーが混在するアクセスネットワーク上で IP アドレスとポリシーを維持できます。
- •WLCに接続するL2スイッチでのMACアドレスのスケーリング制限を回避できます。
- 合法的傍受(LI)

#### EoGRE トンネリングが携帯電話事業者にもたらすメリット:

- •3Gおよび4GトラフィックをオフロードしてOpExの削減とネットワーク効率の向上を実現することによってネットワークの輻輳を軽減します。
- ・弱いセル信号がなくても 3G および 4G コアへのアクセスを提供し、サブスクライバの維持に寄与します。
- ・高密度のメトロ環境においてユーザベースまたは帯域幅ベースの CapEx を削減します。

#### EoGRE トンネリングが有線および Wi-Fi 事業者にもたらすメリット:

- •WiFiセキュリティとサブスクライバ制御を提供します。
- スケーラブルで管理しやすく安全なワイヤレス接続を提供します。
- 新しい収益分配ビジネスモデルを実現します。
- ・新しいロケーションベースのサービスを提供する WiFi プラットフォームを提供します。

EoGRE トンネリングがサブスクライバにもたらすメリット:

- •WiFiネットワーク上のサブスクライバに高品質のエクスペリエンスを提供します。
- アクセスネットワーク全体にわたって統一された方法で課金します。
- •3G または 4G から WiFi、WiFi から WiFi などの無線アクセス テクノロジーをまたがるモビリティを提供します。
- •Wi-Fi プラットフォーム内で複数のオプションを提供し、ロケーションベースのサービスを実現します。
- ・リリース 8.2 以降では、EoGRE トンネリングはダイナミック インターフェイスでサポートされます。
- ・ダイナミックな IPv6 AP 管理インターフェイスはサポートされていません。
- リリース 8.3 では、IPv6 ダイナミック インターフェイスはトンネル インターフェイスとしてのみサポートされます。
- ・リリース 8.3 では、IPv6 アドレスを割り当てることができるダイナミック インターフェイスの最大数は 16 です。
- ・リリース 8.3 の TGW では、IPv4 と IPv6 の両方のアドレス形式がサポートされます。最大で 10 個のトンネル ゲートウェイを作成できます。
- ・リリース 8.4 では、WLC および Flex Connect AP から TGW への EoGRE IPv4 および IPv6 トンネルがサポートされます。
- リリース 8.5 では、プライマリおよびセカンダリ TGW のフェールオーバーと冗長性のサポートが追加されました。
- ・リリース 8.5 では、EoGRE トンネルを管理するための SNMP MIB が追加されています。
- リリース 8.6 では、Cisco Wave-2 AP での DHCP オプション 82 のサポートが追加されました。
- ・リリース 8.6 では、有効な WLAN にマッピングされた TGW にキープアライブを送信する拡張機能が追加されました。
- ・リリース 8.8 では、VLAN オーバーライド拡張機能が追加されて 10 VLAN のサポートが廃止され、特定のコント ローラモデルでサポートされる VLAN 数(5520 と 8540 は最大 4096 の VLAN をサポート)まで増加されました。

# サポートされるコントローラと AP

- Cisco 3504、5508、5520 シリーズ、および vWLC ワイヤレス コントローラ
- リリース 8.2 ~ 8.5 では 2500 シリーズで EoGRE がサポートされます
- •7500 コントローラでは、TGW への EoGRE 直接トンネルが設定されたフレックス接続 AP のみサポートされます。
- Cisco WLC 8.8 でサポートされるアクセス ポイント: 3700、2700、1700、702、702w、1530、1570
- Wave-2 AP: 1800 シリーズ、2800 シリーズ、3800 シリーズ、4800 シリーズ、1540、および 1560
- リリース 8.8、およびリリース 8.5 以降では、Cisco 3504、5520、8540、vWLC がサポートされます。
- (注) サポートされている AP のリストについては、8.8 のリリース ノートを参照してください。

# EoGRE トンネル システムの設計オプション

# 設計 1: WLC ベースの EoGRE トンネル

- CAPWAP 制御パス (AP WLC)
- CAPWAP データ パス (AP WLC)
- EoGRE データ フロー (WLC-TGW)

この設計モデルでは、WLC から ASR 1000 などトンネル ゲートウェイへのトンネルが生成されます。リリース 8.2 以降のコントローラでは、最大で 10 個のトンネル ゲートウェイ構成、10 個の EoGRE トンネル ゲートウェイ、そしてトンネルごとに 10 個のプロファイルがサポートされます。各プロファイルは、複数のレルムを使用して設定することもできます。レルムが設定されている場合は、@の後のユーザ名になります。レルムは @の後の文字列です(例:user\_name@realm)。冗長性を確保するために複数のトンネルを設定できます。その場合、プライマリまたはアクティブトンネルで障害が発生すると、セカンダリまたはスタンバイトンネルが EoGRE トンネルのオペレーションを引き継ぎます。EoGRE トンネル設定では、コントローラ内およびコントローラ間のモビリティもサポートされます。



リリース 8.1 以降の WLC では、ノースバウンドインターフェイスで次の2種類のトンネル設定がサポートされます。

- 1. PMIPv6 (RFC 5213) で定義されている IP/GRE L3
- **2.** Ethernet over GRE L2



WLAN ごとに1種類のトンネルのみサポートされます。EoGRE は、オープン WLAN または 802.1x ベースの WLAN で サポートされます。トンネル クライアントでは、EAP-SIM または EAP-AKA モードのみがサポートされます。その他 の認証モードは、トンネル クライアントでサポートされません。 オープン SSID の WLAN を使用する場合は、すべてローカル/シンプル クライアントまたはすべてトンネル クライアントがサポートされますが、同じ WLAN 上に混在させることはできません。ただし、802.1x で認証されたシンプルまた はトンネル EoGRE クライアントは同じ WLAN 上でサポートされます。

8.3 より前のリリースでは、オープンおよび WPA2-802.1X 用に設定された WLAN のみがサポートされました。

現在は、内部 WebAuth および WPA2-PSK 用に設定された WLAN に EoGRE トンネル プロファイルを割り当てること ができるようになりました、WPA2-PSK/WPA2-802.1X および内部 WebAuth が設定された WLAN もサポートされます。

クライアントは、認証に基づいてローカル モードまたはトンネル モードに分けられます。WLC では、同じ WLAN 上 で2種類のユーザ トラフィック(**リモート トンネル**と**ローカル**など)がサポートされます。

ローカル ユーザ トラフィックは、WLC によってローカルにブリッジされるトラフィックとして定義されます。

リモート トンネル ユーザ トラフィックは、リモートトンネル ユーザのトラフィックとして定義され、WLC によって TGW にトンネリングされます。

EoGRE ユーザの AAA のオーバーライドがサポートされています。トンネル ゲートウェイは AAA プロキシとして機能 することもできます。

#### コントローラで EoGRE EAP 認証済みクライアントの AAA オーバーライドが有効になっている場合:

- •WLC は、Access Accept を解析し、EoGRE、GTPv2、PMIPv6 などの MPC プロトコル タイプを探します。
- Protocol-Type AVP が存在する場合、WLC はそのトンネルタイプに関連するすべてのパラメータを探します。スタ ティックプロファイルは無視され、AAA によって提供されるパラメータがトンネルの設定に使用されます。
- AVP が存在しない場合、WLC は WLC のスタティック プロファイルを使用し、ユーザ名から抽出したレルムに基づいてトンネル タイプを判断します。
- 一部のパラメータが存在しない場合、認証は失敗します。たとえば、T-GWIP以外のパラメータがすべて存在する 場合でも、クライアント認証は失敗します。
- MPC プロトコル タイプが None の場合はシンプル IP になります。

AAA サーバから返される可能性がある属性には、User-Name、Calling-Station-Id、gw-domain-name、mn-service、cisco-mpc-protocol-interface、eogre\_vlan\_id などがあります。

# WLC EoGRE トンネリングの設定

EoGRE トンネルを設定するには、次の手順を実行します。

#### 手順

ステップ1 EoGRE 機能を設定するには、SSID を作成します。 ステップ2 WLC のメイン メニューで、[WLANs] を選択して [Go] をクリックします。

Current Filter: N	one [Change Filter]	[Clear Filter]	Crea	ate New 👻 Go
WLAN ID Type	Profile Name POD2-PSK	WLAN SSID POD2-PSK	Admin Status Enabled	Security Policies [WPA2][Auth(PSK)]

ステップ3 命名規則を使用して POD4-EoGRE などの WLAN を作成し、[Apply] をクリックします。

WLANs > New		< Back Apply
Туре	WLAN +	
Profile Name	PODX-EoGRE	
SSID	PODX-EoGRE	
ID	2 •	

- **ステップ4** [General] タブで、WLAN を管理インターフェイスにマッピングするか、リリース 8.2 以降の場合は管理またはダイナミック インターフェイスを選択します。
  - (注) リリース 8.2 での設定オプションの変更については、以下の項を参照してください。

CISCO MONITO	DR WLANS CONTROLLE	Sage Configuration   Ding   Logout Refresh R WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK A Home
WLANs	WLANs > Edit 'POD	4-EoGRE' <back apply<="" td=""></back>
WLANS WLANS	General Securit	y QoS Policy-Mapping Advanced
▶ Advanced	Profile Name Type SSID Status	POD4-EoGRE WLAN POD4-EoGRE TO THE POD4-EoGRE TOT
	Security Policies	None (Modifications done under security tab vill appear after applying the changes.)
	Radio Policy	All
	Interface/Interface Group(G)	management 👻
	Multicast Vlan Feature	Enabled
	Broadcast SSID	🗹 Enabled
	NAS-ID	POD4-WLC

ステップ5 [Security] タブで [Layer 2 Security] を [None] に設定し、[Apply] をクリックします。

ANs > E	dit 'PODX-	EoGRE'	< Back Appl
Seneral	Security	QoS Policy-Mapping Adva	sced
Layer 2	Layer 3	AAA Servers	
Layer 2	Security 1	ne •	
Fast Tran	sition	- Filterings 🖂	

# WLC EoGRE トンネル パラメータの設定



#### リリース 8.3 での TGW 上の IPv6 アドレスのサポート

リリース 8.3 では、EoGRE トンネル ゲートウェイのクライアント IPv6 トラフィックと IPv6 アドレス形式のサポート を追加しました。クライアント IPv6 トラフィックは IPv4 と IPv6 両方の EoGRE トンネルでサポートしています。クラ イアントごとに、最大 8 つの異なる IPv6 アドレスがサポートされます。Cisco WLC は、アカウンティング サーバから アカウンティング更新メッセージで仕入れたすべてのクライアント IPv6 アドレスを送信します。Cisco WLC とトンネ ルゲートウェイ、または RADIUS サーバ間では、すべての RADIUS メッセージやアカウンティング メッセージが EoGRE トンネル外部で交換されます。

### IPv4 or IPv6 EoGRE Tunnel From WLC



GUI を使用して WLC EoGRE を設定するには、以下の手順を実行します。

#### 手順

- ステップ1 トンネルゲートウェイアドレスを割り当てます。
  - a) WLC のメイン メニューから、[CONTROLLER] > [Tunneling] > [EoGRE] の順に選択します。
  - b) [Heartbeat Interval] を 60 秒に設定します。

リリース 8.6 では、新しいキープアライブ拡張機能が追加されました。これより前のリリースでは、 Cisco WLC に設定されているすべてのトンネルゲートウェイ (TGW) にキープアライブ ping が送信さ れていました。このリリースでは、有効な状態の WLAN にマッピングされている TGW にのみキープ アライブ ping が送信されます。Cisco WLC で WLAN を無効にしたり削除したりすると、この WLAN にマッピングされている TGW への定期的なキープアライブ ping が停止されます。

コントローラは、キープアライブを 60 秒ごとに送信します。キープアライブ ping を 3 回送信しても TGW が応答しない場合、コントローラは TGW がダウンしていると判断します。

c) [Max Heartbeat Skip Count] を [3] に設定します。

スキップ カウント数により、コントローラによって TGW がダウンしていると認識される前に、TGW が連続で応答をスキップできる回数が決まります。

- d) [TGW Name] を追加します(例: ASR1K)。
- e) [TGW IP Address] を追加します(例: 10.10.200.5)。

abab							Sage	Configuration	Eing   Logout	Refresh
cisco	MONITOR WLANS		WIRELES	S SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		A Home
Controller	EoGRE General									1
General Inventory	Apply Defa	ult								
Interfaces Interface Groups Multicast > Network Routes	Interface Name Heartbeat Interval Max Heartbeat Ski	(Seconds) 60 p Count 3	agement							
Redundancy     Mobility	Add New TGW		/		Add New I	Domain Iame	dom	ain4		
Ports > NTP	TGW Name TGW IP Address Add	10.10.200			TGW-1 TGW-2 Add		None			
> PMIPv6	TGW List				Domain Li	st				
Tunneling EoGRE Profiles	ASR1K I	IP Address 10.10.200.5 U	Status IP 0	Total Clients	Name	TGW	1	TGW-2	Active Gatewray	_
> IPv6					domain4	ASR1K			ASR1K	•

f) リリース 8.3 以降では、[TGW IPv6 Address] を追加します(例: 2001::1010::1010)。

alulu					Sa <u>v</u> e Confi	guration
CISCO MONITOR	WLANS <u>C</u> ONTROLLER	WIRELESS	<u>SECURITY</u>	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	EoGRE General					
General Icons	Apply Defa	ult				
Inventory	Interface Name	man	agement	•		
Interfaces Interface Groups Multicast	Heartbeat Interval( Max Heartbeat Skip					
Network Routes						
Redundancy	Add New TGW					
Internal DHCP	TGW Name	ASR1K				
Server	TGW IP Address	2001::1010	::1010 🔺			
Mobility Management	Add					
Ports	TGW List					
▶ NTP						

- g) [Domain Name] を追加します(例:domain4)。
- h) トンネルゲートウェイ [TGW-1] で [ASR1K] を選択し、[Add] をクリックします。トンネルゲートウェ イが到達可能な場合は、[TGW List] でステータスが [UP] と表示されます。

EoGRE General							
Interface Name Heartbeat Interval(Seconds)	management						
Add New TGW TGW Name TGW IP Address Add	E		Ad	Id New Domai Domain Name TGW-1 TGW-2	n	domain4 ASR1K None	<
TGW List Name IP Add	ress Status	Total Clients		Add omain List			
ASR1K 10.10.200.	S UP 0			Name	TGW-1	TGW-2	Gateway

ドメインは、冗長性の目的で使用されている1つ以上のトンネルの仮想コレクションを表しています。 前述のとおり、単一のドメイン上に最大10のトンネルを存在させることができます。1つのトンネル で障害が発生すると、トラフィックは別のTGWにリダイレクトされます。

- ステップ2 ネットワーク プロファイルを作成します。
  - a) WLC のメイン メニューから、[CONTROLLER] > [Tunneling] > [Profiles] の順に選択します。
  - b) [Profile Name] を設定し(例: pod6)、[Add] をクリックします。

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP EEEDBACK
Controller General Inventory Interfaces Interface Groups Multicast > Network Routes > Redundancy > Internal DHCP Server > Mobility Management Ports > NTP > CDP > DPIPv6 Tunneling Focks	Profile List Profile Name	WLAN IDs (Mapped)		Add New Profile Name pod6 Copy of None 1 Add

[Profile List] にプロファイル名が表示されます。

Profiles			
Profile List			
Profile Name	WLAN IDs (Ma	apped)	
pod6	None		
pooe	None	ă.	

- ステップ3 トンネル プロファイル ルールを定義します。
  - a) 作成したプロファイル (pod6) をクリックします。
  - b) プロファイルに特定のレルムをマッピングするには、user\_name@realmなどのレルム名を入力します。 レルムに一致させるには、[Realm]で\*を使用します(\*はすべてのレルムが受け入れられることを意味します)。
  - c) [EoGRE] として [Tunnel Type] を選択します。
  - d) [VLAN] を [0] に設定します。
  - e) [Gateway Domain] として [domain4] を選択します。
  - f) [Add] をクリックします。

nnel Profile > Edit	
Rule Tunnel Parameters	
Profile Name pod4	

g) [Apply] をクリックして、プロファイルにルールを適用します。

nnel P	Profile > Edit					< Back Appl
tule	Tunnel Parameters					1
Profil	le Name pod 6					
Realn	n •	Tunnel	Type EoGRE - V	LAN 0 Gatewa	y Domain domain4 +	
Add						
Add	E.	Tunnel Type	VLAN	Gateway Domain		

ステップ4 WLAN にトンネル プロファイルを追加/関連付けします。

- a) WLC の GUI から、EoGRE (POD4-EoGRE) トンネルを有効化する WLAN に移動します。
- b) [Advanced] タブの [Tunneling] エリアで、[Tunnel Profile] として [pod6] を選択します。

General Security QoS Pr NAT-PAT Enable Central Assoc Enable	ed Advanced	MITP Profiling	U
Lync		PMIP Mobility Type	0
Lync Server Disabled		PMIP NAI Type	(Hexadecimal 1)
11k		PMIP Profile	None +
Assisted Roaming Prediction Optimizati	on 📄 Enabled	PMIP Realm	- Second second
Neighbor List	Enabled	Universal AP Admin Support	
Neighbor List Dual Band	Enabled	Universal AP Admin	۲
		11v BSS Transition Support	
		BSS Transition	0
		Disassociation Imminent	0
		Disassociation Timer(0 to 3000 TBTT)	200
		Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
		Tunneling	-
		Tunnel Profile	pod6 +

ステップ5 トンネルが適切に設定されたかどうかを検証するには、WLCのメインメニューから [CONTROLLER] > [Tunneling] > [Profiles] の順に選択し、プロファイル名が正しい WLAN に設定されているかどうかを確認します。

この例では、EoGREトンネルとDHCPプールに対してASR1Kが事前設定されています。参照用に、ASR1K のトンネル設定を以下に示します。

```
ip dhcp pool IPv4-EoGRE
network 10.55.55.0 255.255.255.0
default-router 10.55.55.1
dns-server 171.70.168.183
domain-name cisco.com
lease 0 0 10
interface Loopback0
ip address 11.11.11.11 255.255.255.255
interface Tunnel1
mac-address 0000.5e00.5213
ip address 10.55.55.1 255.255.255.0
no ip redirects
load-interval 30
tunnel source GigabitEthernet0/0/0.200
tunnel mode ethernet gre ipv4
interface GigabitEthernet0/0/0
no ip address
negotiation auto
interface GigabitEthernet0/0/0.200
encapsulation dot10 200
ip address 10.10.200.5 255.255.255.0
```

(注) サンプル設定は Ipv4 向けのものです。

ワイヤレスクライアントをSSID (POD4-EoGRE など)に接続します。ASR1Kに設定されている10.55.55.0 サブネットから IP アドレスを取得します。

Status:	Connected	Turn Wi-Fi Off
	Wi-Fi is connected the IP address 10.5	to PODX-EoGRE and has
etwork Name:	PODX-EoGRE	÷
/	Ask to join ne Known networks v If no known netwo	w networks will be joined automatically. orks are available, you will select a network



また、POD WLC で show client detail コマンドを実行すると、EoGRE トンネルを介してクライアントが関連 付けられていることを確認することもできます。



# 一般的な展開:WLC EoGRE トポロジ

この一般的な EoGRE の展開設定では、2人のユーザ MN1 と MN2 が Realm @att.com に接続し、他の2人のユーザ MN3 と MN4 が Realm @att.net に接続しています。次の図に示すように、ユーザ MN1 と MN2 は接続するときに VLAN1 および TGW1 上にいる必要があり、ユーザ MN3 と MN4 は VLAN2 および TGW2 に接続する必要があります。この設定では、それぞれ1つのレルムを含む2つのプロファイルが作成され、同じドメイン内の TGW1 と TGW2 に適切にマッピングされます。



WLC EoGRE を設定するには、以下の手順を実行します。

ステップ1 トンネルゲートウェイを作成し、ハートビートを設定します。

- a) WLC のメイン メニューから、[CONTROLLER] > [Tunneling] > [EoGRE] の順に選択します。
- b) [Heartbeat Interval] を 60 秒に設定します。
- c) [Max Heartbeat Skip Count] を [3] に設定します。
- d) [TGW-1] と [TGW-2] に適切な IP アドレスを設定します。

ahaha						Saye	Configurati	ion   <u>B</u> ing	Logout Be	frest
CISCO	MONITOR WLAN		WIRELES!	S <u>S</u> ECURIT	Y MANAGEMENT	COMMANDS	HELP	EEEOBACK	<b>6</b> 1	lome
Controller	EoGRE General									
General Inventory Interfaces Interface Groups Multicast > Network Routes	Apply De Interface Name Heartbeat Interva Nax Heartbeat Sk	fault mani Mani (Seconds) 60 ip Count 3	agement							
<ul> <li>Redundancy</li> <li>Internal DHCP Server</li> <li>Mobility Management</li> <li>Ports</li> <li>NTP</li> <li>CDP</li> <li>PMIPv6</li> </ul>	Add New TGW TGW Name TGW IP Address Add TGW List	tgw2			Add New Doma Domain Name TGW-1 TGW-2 Add Domain List	dom) tg#1 None	~			
Tunneling	Name	IP Address	Status	Total Clients	Name	TOWN	TOW	2	Active	
Profiles	tgw1	9.9.89.100	DOWN 0		dom1	tgw1	16.97	No	ine	1

#### CLI で EoGRe ハートビートを設定する場合:

config tunnel eogre heart-beat interval 30

config tunnel eogre heart-beat max-skip-count 3

#### CLI で EoGRE トンネルを設定する場合:

config tunnel eogre gateway add tgw1 ipv4-address 9.9.89.100

config tunnel eogre gateway add tgw2 ipv4-address 9.9.90.100

ステップ2 EoGRE トンネル ドメインを設定します。

図 1: GUI で tgw1 と tgw2のドメイン dom1 を設定する

dd New D	omain		/	
Domain Na	ime	dom1	*	
TGW-1		None 💌	//	
TGW-2		None taw1		
Add		tgw2	_	
Add omain List	t TGW-1	tgw2	GW-2	Active Gateway

#### CLI でトンネル ドメインを作成する場合:

config tunnel eogre domain create dom1
config tunnel eogre domain add dom1 tgw1
config tunnel eogre domain add dom1 tgw2

ステップ3 プロファイルを作成してルールを追加します。

a) たとえば prof-att などのプロファイルを設定します。

CISCO MONITOR		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Configur C <u>O</u> MMANDS	ation <u>P</u> ing Logout HELP <u>F</u> EEDBACK
Controller General Inventory Interfaces Interface Groups Multicast	Profiles Profile List Profile Name profil	WLAN ID	s (Mapped)	Add New Profile N Copy of	ame prof-att	
<ul> <li>Network Routes</li> <li>Redundancy</li> <li>Mobility Management</li> <li>Ports</li> <li>NTP</li> <li>CDP</li> <li>PMIPv6</li> <li>Tunneling EoGRE Profiles</li> </ul>	prof-ats	None		Add		

b) WLC の GUI で、ドメイン dom1 の VLAN1 に対して att.com、VLAN2 に対して att.net というレルムを 作成し、それらをプロファイル prof-att に適用します。

	l Parameters				
Profile Name	prof-att				
Realm att.ne	t Tunne	l Type EoGRE 💌	VLAN 2	ateway Domain	dom1 💙
Realm att.ne	t Tunne Tunnel Type	VLAN	VLAN 2 C	àateway Domain main	dom1 💌
Realm att.ne Add Realm att.com	t Tunne Tunnel Type EoGRE	VLAN	VLAN 2 C	Bateway Domain	dom1 💌

#### CLI でプロファイルとレルムを作成する場合:

config tunnel profile create prof-att
config tunnel profile rule add prof-att realm-filter att.com eogre vlan 1 dom1
config tunnel profile rule add prof-att realm-filter att.net eogre vlan 2 dom1
config tunnel profile rule add prof1 realm-filter \* eogre vlan 0 dom1

(注) \*は、他のルールに属していないすべてのユーザをキャッチするワイルドカードを意味しま す。これは順序の最後であり、VLAN0のユーザはドロップします。

ステップ4 トンネルパラメータを設定します。

次の図は、GUI で AAA プロキシ GW と DHCP オプション 82 を有効にしてトンネル パラメータを設定す る例を示しています。

cisco	MONITOR MLANS CONTROLLER V	VIRELESS SECURITY	MANAGEMENT COMMANDS	Says Configuration	i   Bing   Lagout   Befresh
CISCO Controller General Inventory Interfaces Interface Groups Multicast > Network Routes > Redundancy Mobility Management Ports	MONITOR WLANS CONTROLLER V Tunnel Profile > Edit Rule Tunnel Parameters EeGRE @stevay as AAA Proxy Gatevay as Accounting Proxy DHCP Option-82 DHCP Option 82 Format DHCP Option 82 Format DHCP Option 82 Format		MANAGEMENT COMMANDS	HELP FEEDBACK	C Back Apply
<ul> <li>NTP</li> <li>CDP</li> <li>PNIPu6</li> <li>Tonneling</li> <li>Tofilus</li> <li>Profilus</li> <li>Profilus</li> <li>Profilus</li> <li>Profilus</li> <li>Advanced</li> </ul>	Circuit-1D Fields Available AP Fadle MAC address AP Rome AP Group Name AP Floc Group Name AP Floc Group Name AP Floc Group Name AP Floc Statu-Name Satu-Name Satu-Name Client MAC	Fields Selected	Remote-ID Fields Available	AP radio MAC	selected address

ステップ5 GUI で EoGRE トンネルを設定します。

コントローラの一般的なインターフェイスでインターフェイス名を設定する際は、管理インターフェイス 以外を選択します。

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEME
Controller	EoGRE General				
General Icons Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Mobility Management Ports NTP	Apply Def Interface Name Heartbeat Interva Max Heartbeat Sk Add New TGW TGW Name TGW IP Address Add TGW List	fault	gement ecast ecast20 ecast73 test gement	]	
▶ PMIPv6	Name	IP Address	Status	Total Clients	
r Tunneling	tgw1	9.9.89.100	DOWN	0	10
EoGRE	tgw2	9.9.90.100	DOWN	0 🔽	

**ステップ6** プロファイルを WLAN にマッピングします。

図 2:プロファイル「prof-att」の WLAN へのマッピング

cisco	MONITOR WILANS CONTROLLER WIRELESS SECURITY MANAGE	EMENT COMMANDS HELP EEEDBA	Sage Configuration   Bing   Logout   Befres CK <b>n</b> Bom
VLANS WLANS WLANS WLANS WLANS WLANS WLANS	MONITOR       MULANS       CONTROLLER       WIPELESS       SECURITY       MANAGE         WLANS > Edit       "5520-test"       Advanced         General       Security       QoS       Policy-Mapping       Advanced         Vian based       Central       Enabled       Central DHCP Processing       Enabled         Override DHS       Enabled       Central Assoc       Enabled         Vanc       Enabled       Lync       Enabled         Lync       Enabled       Enabled       Enabled         Neighbor List       Enabled       Enabled       Enabled	EMENT CQMMMANDS HELP EEEDBA HTTP Profiling PHIP PMIP NAI Type PMIP NAI Type PMIP Profile PMIP Realm Universal AP Admin Support Universal AP Admin Support Universal AP Admin Support Universal AP Admin Support Disassociation Imminent Disassociation Imminent Disassociation Timer(0 to 3000 TBT)	CK Apply
		Optimized Roaming Disassociation Timer(0 to 40 TBTT) Tunneling Tunnel Profile	40

### CLI で WLAN2 にプロファイルをマッピングする場合:

config wlan tunnel profile prof1 2

# リリース8.2のトンネリングソースの変更

8.2 より前のリリースでは、EoGRE や PMIPV6 などのすべてのトンネルでエンド ポイントとして使用できるのは管理 インターフェイスのみでした。リリース 8.2 で、管理インターフェイス以外のトンネル送信元を指定する機能が追加さ れ、ネットワーク内のデータ トラフィックおよび管理トラフィックを異なるネットワーク セグメントに分離できるよ うになりました。

- ・設定には4094 個のL3インターフェイスを使用できます。
- 管理者は、EoGREのようなトンネルのトンネルエンドポイントとしてダイナミックインターフェイスを設定できます。
- ・前述のトンネリングプロトコルを除き、すべての機能の設定に変更はありません。
- ダイナミックインターフェイスでの IPv6 アドレスは、8.2 ではサポートされていません。
- AP マネージャは、トンネル(EoGRE、PMIPv6 など)をホストしている L3 インターフェイスでは有効にできません。
- •vWLC および 2500 を含むすべてのコントローラがサポートされます。

リリース 8.2 では、vWLC (512 個の L3 インターフェイスがサポートされる)を除く全種類のサポート対象コントロー ラで、4094 個のすべてのインターフェイスが L3 ダイナミック インターフェイスです(IPv4 が IPv6 として設定されて いる場合、8.2 のこれらのインターフェイスではサポートされません)。 IP アドレスが設定されていない場合は L2 イ ンターフェイスのままになります。すでに実環境に導入されているコントローラの動作、アップグレードまたはダウン グレード シナリオ、DHCP サポート(オプション 82 で L3 パラメータの代わりに L2 パラメータを使用して、L2 イン ターフェイスの IP を取得する DHCP のサポート)が変更されることを避けるために、このリリースではこれらの L2 インターフェイスがクライアント インターフェイスとして使用されることはありません。必要に応じて、これらの L2 インターフェイスが今後のリリースでクライアント インターフェイスとして使用される可能性もあります。

ダイナミックインターフェイス機能は、WLCからWAGへのトンネルに固有の機能です。APからのトンネルの場合、 トンネル送信元は常にAPのIPアドレスを割り当てられたインターフェイスです。トンネルの外部VLANは、IPが割 り当てられたこのAPインターフェイスのVLANとなります。

# **EoGRE** トンネル DHCP オプション 82 の設計

EoGRE クライアントの DHCP オプション 82 はブリッジモードで WLC に挿入されます。クライアントからの DHCP 要求パケットは、他の DHCP パケットと同様にコントローラにパントされます。コントローラでは、クライアントの タイプに基づいて EoGRE クライアントが特別に処理されます。EoGRE クライアントの場合、DHCPオプション 82 の 設定はトンネルプロファイルデータベースから選択されます。グローバル DHCP の設定は、EoGRE クライアントに影響しません。

コントローラの DHCP コードによって、トンネルのプロファイル設定に基づいて DHCPオプション 82 パラメータが挿 入されます。また、EoGRE トンネル ヘッダー情報がコントローラに追加されます。コントローラは完全な DHCP パ ケットと EoGRE トンネル ヘッダーを収集し、トンネルに送信します。

設定コマンドによって、オプション82のフォーマット、デリミタ文字、リモートID、サーキットIDを柔軟に設定できます。リモートIDとサーキットIDは、サポートされる最大5個の異なるパラメータIDを指定して簡単に設定できます。入力したパラメータによって、以前に入力された設定が上書きされます。パラメータが入力されない場合、リモートIDとサーキットIDは削除され、そのフィールドに対するパラメータは送信されません。

リリース 8.6 以降、EoGRE トンネルの DHCP オプション 82 は Cisco Wave 2 AP でサポートされています。

#### コンフィギュレーション コマンド

config tunnel profile eogre <profile name> dhCP-Opt-82 enable / disable

config tunnel profile eogre <profile name> dhCP-Opt-82 format binary / ascii

config tunnel profile eogre <profile name> dhCP-Opt-82 delimiter <delimiter character>

config tunnel profile eogre <profile name> dhCP-Opt-82 remote-id <Paramater ID - 1> <Paramater ID - 2> <Paramater ID - 3> <Paramater ID - 4> <Paramater ID - 5>

config tunnel profile eogre <profile name> dhCP-Opt-82 circuit-id <Paramater ID - 1> <Paramater ID - 2> <Paramater
ID - 3> <Paramater ID - 4> <Paramater ID - 5>

#### 図 3: GUI インターフェイスでの DHCP オプション 82 の設定

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT COMMANDS	Say HELP EE	e Configuration   Bing EDBACK	Logout   <u>R</u> efresh
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Mobility Management	Tunnel Profile > Edit           Rule         Tunnel Parameters           EoGRE         Gatevay as AAA Proxy         Image: Compare the second seco	ary 💌			< Bi	ick Apply
Ports NTP COP PMIPv6 Tunneling Forditas TPv6 PMDNS Advanced	Circuit-ID Fields Available Predis Available AP radio MAC address AP Name AP Roup Name AP Flocation Provide Group Name AP Flocation VLAN-ID SSID-Type Client MAC	Fields Selected	Prede Available Fields Available AP Ethernet MAC address AP Group Name AP Flock Group Name AP Iocation View Dure SSID-TYPE Client MAC		Fields Selected AP radio MAC address	Up Down

#### CLI で DHCP オプション 82 を設定する場合:

config tunnel profile eogre prof-att DHCP-Opt-82 format Binary config tunnel profile eogre prof-att DHCP-Opt-82 delimiter config tunnel profile eogre prof-att DHCP-Opt-82 enable config tunnel profile eogre prof-att DHCP-Opt-82 circuit-id ap-ethmac flex-group-name ap-group-name config tunnel profile eogre prof1 DHCP-Opt-82 remote-id ap-name ap-location

### CLI で AAA プロキシとしてゲートウェイを設定する場合:

config tunnel profile eogre prof-att gateway-radius-proxy enable config tunnel profile eogre prof-att gateway-radius-proxy accounting enable

# **EoGRE**トンネルの冗長性

冗長性を確保するために複数のトンネルを設定できます。この場合、プライマリ(またはアクティブ)トンネルに障害 が発生すると、セカンダリ(またはスタンバイ)トンネルが EoGRE トンネルの動作を引き継ぎます。キープアライブ メッセージが定期的に送信される周期(応答がない場合にトンネルがダウンしているとみなされるまでのキープアライ ブ数)を設定できます。これは、グローバル コマンドですべてのタイプのトンネルに適用されます。EoGRE トンネル の設計では、DTLS ICMP パケットはトンネル ゲートウェイに送信されます。EoGRE トンネルが作成されると、ICMP エコー リクエスト パケットがトンネル ゲートウェイに送信されます。受信後、ICMP エコー応答が返されてトンネル ゲートウェイのステータスが更新されます。

プライマリトンネルに障害が発生すると、クライアントはプライマリWAGから認証と関連付けを解除されます。セ カンダリWAGが使用可能な場合、コントローラはセカンダリトンネルを確立し、セカンダリトンネルが次の例に示 すように設定されている場合はセカンダリWAGに再接続します。セカンダリトンネルが確立された後、リモートク ライアントデバイスはWAGに再認証および再関連付けされ、セカンダリWAGのDHCPサーバからIPアドレスを更 新します。プライマリWAGがオンラインに戻っても、クライアントはセカンダリWAGに接続したままになります。

ahaha								onfiguration	<u>P</u> ing   Logoul	t <u>R</u> efresh
cisco	MONITOR WLANS		R WIRE	LESS	SECURITY	MANAGEME	NT COMMAN	IDS HELP	EEEDBACK	1 Home
Controller	EoGRE Genera	1								
General Inventory Interfaces Interface Groups Multicast Network Boutes	Apply Du Interface Name Heartbeat Interv Max Heartbeat Si	efault m al(Seconds) 60 kip Count 3	anagemen	nt						
<ul> <li>Redundancy</li> <li>Internal DHCP Server</li> <li>Mobility Management Ports</li> <li>NTP</li> <li>CDP</li> <li>PMIPv6</li> </ul>	Add New TGW TGW Name TGW IP Address Add TGW List				Add N Don TGV Add Doma	New Domain nain Name V-1 V-2 Din List	None	M M		
Tunneling	Name	IP Address	Status	Total Clients		22.24%		<b>T</b> CIII <b>D</b>	Active	202
Profiles -	ASR1K-PR	10.10.200.5	UP	0		me	10W-1	ACD1V.CEC	Gatewa	ay
🕨 IPv6 🛛 💳	ASR1K-SEC	10.10.201.5	UP	0	00	main <del>4</del>	ASKIK-PR	ASKIK-SEC	NORE	

### リリース8.5の冗長性とフェールオーバー

8.5 より前のリリースでは、EoGRE TGW フェールオーバーは上記のスクリーンショットで示すように、フェールオー バーまたは冗長性用のプライマリまたはセカンダリとして制御されていませんでした。リリース 8.5 では、フェール オーバーを目的として TGW-1 と TGW-2 をプライマリとセカンダリに指定する新しいオプションを利用できます。



ドメインでプライマリ ゲートウェイはデフォルトでアクティブになっています。プライマリ ゲートウェイがダウンす ると、セカンダリ ゲートウェイがアクティブまたはプライマリとなります。クライアントは、セカンダリ ゲートウェ イに再関連付けされる必要があります。フェールオーバーの実行中および完了後に、WLCは継続的にプライマリ ゲー トウェイに ping を実行します。プライマリ ゲートウェイがオンラインに戻ると、プライマリ ゲートウェイがアクティ ブ ゲートウェイになります。クライアントはプライマリ ゲートウェイにフォールバックします。

リリース 8.6 で追加された拡張機能により、キープアライブ ping のオーバーヘッドが削減されます。

8.6 より前のリリースでは、WLC に設定されているすべての TGW に「キープアライブ」が送信されていました。

リリース 8.6 では、有効な WLAN にマッピングされている TGW のみに「キープアライブ」が送信されます。

WLC で WLAN を無効にしたり削除したりすると、WLAN にマッピングされている TGW への定期的な「キープアライブ」が停止します。

WLC で WLAN が無効化または削除された場合、これらのゲートウェイの削除メッセージが AP および AP グループに送信されます。

ローカル スイッチング モードの Flex Connect AP でも同じオプションを TGW に対して使用できます。

# 

(注) AP 1040、1260、1140 は、リリース 8.5 以降ではサポートされていません。

# EoGRE TGW フェールオーバーの設定手順

#### 手順

ステップ1 CLI または GUI で EoGRE トンネルに IPv4 または IPv6 アドレスを設定します。

(WLC) >config tunnel eogre gateway add <TGW> ipv4-address <IP address>
(WLC) >config tunnel eogre domain <name><Pri/Sec TGW>

սիսիս										Save Configuration	Ping	Logout	Refresh
cisco	MONITOR WLA	ns <u>C</u> ontroller	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COM	IMANDS	HELF	P <u>F</u> EEDBACK				🔒 <u>H</u> ome
Controller	EoGRE Gener	al											
General Icons Inventory Interfaces Interface Groups Multicast > Network Routes > Fabric Configuration > Redundancy	Apply D Interface Name Heartbeat Inter Max Heartbeat	val(Seconds) 60 Skip Count 3	agement V										
<ul> <li>Mobility Management</li> <li>Ports</li> </ul>	Add New TGW							Ad	ld New Domain				
▶ NTP	TGW Name	tgw1							Domain Name	dom1			
▶ CDP	TGW IP Address									Gateway Name	Ro	le	_
▶ PMIPv6									TGW-1	tgw1 🔻	P	rimary 🔻	
▼ Tunneling	Add								TGW-2	tgw2 ▼	N	one 🔻	1
EoGRE Profiles	TGW List							P	bb				
▶ IPv6								Do	omain List				
▶ mDNS	Namel	IP Address			SI	tatus	Total Clients						
Advanced	tgw1	9.9.89.100			D	OWN	0		Name	TGW-1		TGW-2	
	tgw2	9.9.90.100			D	OWN	0		dom1	tgw1		tgw2	
	tgw4	2001::10:70	:0:21		D	OWN	0						

ステップ2 CLI または GUI で EoGRE プロファイルに VLAN とドメインを設定します。

(WLC)>config tunnel profile <prof -name>

ahah.									Sa <u>v</u> e C	Configuration   Ping   Logout   Refresh
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK	🔒 <u>H</u> ome
Controller	Tunnel F	Profile > E	Edit							< Back Apply
General	Rule	Tunnel I	Parameters							
Icons Inventory Interfaces Interface Groups Multicast > Network Routes > Redundancy	Profil Name Realm Add Real	e eogr mn@att.c	e-psk				Tunnel	Tunnel Type Type	Eogre VLAN	1 Gateway dom1 •
Porte	cisco	.com					EoGRE		70	dom1
NTP	*						EoGRE		0	dom1
▶ CDP	mn@	att.net					EoGRE		2	dom1
PMIPv6     Tunneling     EoGRE     Profiles										

ステップ3 WLAN に Flex Connect ローカル スイッチングを設定します。

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> ONTRO	OLLER	WIRELESS SECU	IRITY MANAGEMENT			
WLANs	WLANs > Edit 'eogre'						
VLANs	General Security Q	los	Policy-Mapping	Advanced			
Advanced	FlexConnect						
	FlexConnect Local Switching <sup>2</sup>		Enabled				
	FlexConnect Local Auth 12		Enabled				
	Learn Client IP Address 5		Enabled				
	Vlan based Central Switching 13		Enabled				
	Central DHCP Processing		Enabled				
	Override DNS		Enabled				
	NAT-PAT		Enabled				
	Central Assoc		Enabled				

### ステップ4 WLANを設定して EoGRE トンネル プロファイルをバインドします。

alulu					Save Configuration Ping
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURIT	Y M <u>A</u> NAGE	MENT C <u>O</u> MMANDS HE <u>L</u> F	P <u>F</u> EEDBACK
WLANs	General Security QoS	Policy-Mapping	Advanced		
WLANs WLANs	Lync Server Enable	ed 🔻	11	Universal AP Admin	
▶ Advanced	Assisted Roaming Prediction Optimization Neighbor List Neighbor List Dual Band Denial Maximum Count Prediction Minimum Count	Enabled Enabled Enabled 2		BSS Transition Disassociation Imminent Disassociation Timer(0 to 3000 TBTT) Optimized Roaming Disassociation Timer(0 to 40 TBTT) BSS Max Idle Service Directed Multicast Service Inneling Tunnel Profile	200 40 200 eogre-psk V
			m	DNS	
			Tr	mDNS Snooping	Enabled
			o	Security Group Tag	0

### ステップ5 以下に示すように、プロファイルを WLAN にバインドします。

ululu cisco	MONITOR WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK			Say	e Configu	iration
Controller	Profiles												
General													
Icons	Profile List										Add		
Inventory	Profile Name									WLAN IDs (Mapped)	Profile		
Interfaces											Conv		
Interface Groups	prof1								No	ne 🔽	of	None	•
Multicast	prof-att								No	ne 🔽	Add		
Network Routes	eogre-psk								8,9				

# リリース 8.8 の VLAN オーバーライド機能付き EoGRE トンネル

シスコのお客様によっては EoGRE トンネリングを導入する場合に、サポートされる VLAN 数に関して問題が発生しま す。お客様が直面する問題は、オープン SSID 向けの EoGRE 実装で WLC あたりの SSID/VLAN の最大数が 16 に制限 されていることです。お客様は B2B 顧客(ホテル、食品チェーン、カフェなど)にオープン SSID を提供します。

特に 5520 または 8540 コントローラが 512 個の WLAN および 4096 個の VLAN をサポートすることを考慮する場合、 これはサービス プロバイダー アプリケーションでの大きな制限となります。

この制限が生じるのは、オープン SSID の場合はワイルドカードを使用して特定し VLAN にマッピングしなければなら ないためです。これにより、トンネル プロファイルごとに 1 つの SSID/VLAN ペアのみ、つまりボックスあたり最大 10 の SSID/VLAN ペアに絞られます(トンネル プロファイルの数が最大 10 に制限されているため)。

シスコの特定のお客様は、WiFiGW上のVLANによってB2B顧客が識別されてポリシーが適用されるため、オープン SSIDとVLANの1対1のマッピングが必要です。

上記のサービスプロバイダーの問題を解決するために、リリース8.8で新しい拡張機能が導入されました。この拡張機 能では、WLAN と EoGRE VLAN の1対1マッピングが導入されます。8.8 より前のリリースでは、512 個の WLAN と 10 個の EoGRE プロファイルのみがサポートされていました。

この拡張機能により、コントローラから TGW への EoGRE VLAN が最大で 4096 個サポートされます。

オープン認証クライアントの場合は、EoGRE VLAN とその WLAN の他の設定を持つ1つの「\*」ルールのみが使用されます。

この新しい拡張機能を使用すると、EoGRE VLANの設定がWLAN内で上書きされ、既存のすべてのルールが適用され ます。ただし、この EoGRE VLAN オーバーライドオプションを有効にすると、AAA オーバーライドまたはプロファ イル ルールの一致に関係なく、EoGRE VLAN が上書きされます。

以下は優先順位であり、この機能の一環として変更が行われることはありません。優先順位が最も高いのは AAA オーバーライドです。

- 1. WLAN の EoGRE VLAN オーバーライド値
- 2. AAA オーバーライド値の後に AAA 値
- 3. プロファイル ルールに一致する NAI

### VLAN オーバーライド付き WLC EoGRE トンネリングの設定

EoGRE トンネルを設定するには、以下の手順を実行します。

#### 手順

ステップ1 EoGRE 機能を設定するには、SSID を作成します。命名規則を使用して「eogre-test」などの WLAN を作成し、[Apply] をクリックします。

WLANS WLANS	General Security Q	oS Policy-Mapping Advanced					
Advanced	Profile Name	eogre					
	Туре	WLAN					
	SSID	eogre-test					
	Status	C Enabled					
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the change					
	Radio Policy	All					
	Interface/Interface Group(G)	3) management T					
	Multicast Vlan Feature	Enabled					
	Broadcast SSID	Senabled					

ステップ2 トンネル ゲートウェイ アドレスを割り当てます。

- 1. WLC のメイン メニューから、[CONTROLLER] > [Tunneling] > [EoGRE] の順に選択します。
- 2. [Heartbeat Interval] を 60 秒に設定します。

リリース 8.6 では、新しいキープアライブ拡張機能が追加されました。以前のリリースでは、Cisco WLC に設定されているすべてのトンネル ゲートウェイ (TGW) にキープアライブ ping が送信されて いました。このリリースでは、有効な状態の WLAN にマッピングされている TGW にのみキープアラ イブ ping が送信されます。Cisco WLC で WLAN を無効にしたり削除したりすると、この WLAN にマッ ピングされている TGW への定期的なキープアライブ ping が停止されます。

3. [Max Heartbeat Skip Count] を [3] に設定します。

スキップ カウント数により、コントローラによって TGW がダウンしていると認識される前に、TGW が連続で応答をスキップできる回数が決まります。

- 4. [TGW Name] を追加します(例: ASR1K)。
- 5. TGW IPv4 または IPv6 アドレスを追加します(例: 10.91.104.87)。

,1 1,1 1, CISCO Monitor <u>w</u> lans <u>controller</u> wireless <u>s</u> ecurity managemen	Saye Configuration   Ping   Logout   Refres
Controller General Icons Inventory Interfaces Interfaces Interface Groups Multicast Fabric Configuration Ports Mobility Management Ports Multipod Ports Multipod COV IP Address Interface Groups Multicast Fabric Configuration Ports Multicast Fabric Configuration Ports Multicast COV IP Address Interface Groups Multicast Fabric Configuration Ports Multicast Interface Groups Multicast Fabric Configuration Fabric Configuration Fabric Configuration Fabric Configuration Fabric Configuration COV IP Address Igw1 9.9.89.100 Igw2 9.9.90.100 Igw2 9.9.90.100 Igw2 9.9.90.100 Igw3 10.91.104.89 Igw6 10.91.104.87 Igw6 10.91.104.87	Add New Domain Domain Name Gateway Name Role TGW-1 None  TGW-2 None TGW-2 None TGW-2 None TGW-2 None TGW-2 None TGW-2 None TGW-2 None TGW-2 None TGW-2 TGW-1 TGW-2 dom1 tgw1 tgw2 dom1 tgw1 tgw2 dom2 tgw3 tgw4 dom2 tgw3 tgw4 dom3 tgw5 tgw6 DOWN 0

- ステップ3 トンネル プロファイル ルールを定義します。
  - 1. 作成したプロファイル (eogre など) をクリックします。
  - 2. プロファイルに特定のレルムをマッピングするには、user\_name@realmなどのレルム名を入力します。 すべてのレルムに一致させるには、\* を使用します

(\*はすべてのレルムが受け入れられることを意味します)。

- 3. [EoGRE] として [Tunnel Type] を選択します。
- 4. [VLAN] を [0] に設定します。
- 5. [Gateway Domain] として [domain4] を選択します。
- **6.** [Add] をクリックします。

- aliala									Sa <u>v</u> e	e Configuration   Pi	ng   Logout   <u>R</u> efres
CISCO	MONITOR W	LANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEE	DBACK			🔒 <u>H</u> om
Controller	Tunnel Prof	ile > Edit								< Back	Apply
General Icons Inventory	Rule	unnel Parameters									*
Interfaces Interface Groups	Realm mi	ike@cable.com					Tunnel	FogRF V	VLAN 4	Gateway	dom3 T
Multicast <ul> <li>Network Routes</li> </ul>	Add						Туре	Look		Domain	
Fabric Configuration	Realm					Tun	inel Type	VLA	N	Gatewa	/ Domain
Redundancy	att.com					EoG	RE	1		dom2	
<ul> <li>Mobility Management</li> <li>Ports</li> <li>NTP</li> <li>CDP</li> </ul>	att.net					EoG	RE	2		dom2	
PMIPv6     Tunneling     EoGRE     Profiles											

ステップ4 WLAN にトンネルプロファイルを追加/関連付けします。

1. WLC の GUI から、EoGRE (eogre-test) トンネルを有効化する WLAN に移動します。

- 2. [Advanced] タブの [Tunneling] エリアで、例に示すように [Tunnel Profile] として [prof-att] を選択しま す。
- 3. リリース 8.8 では、VLAN オーバーライドを有効にするオプションと VLAN オーバーライド ID が表示 されることに注意してください。

allulu						Save Configuration	<u>P</u> ing	Logout
CISCO	MONITOR WLANS CONTRO	ller w <u>i</u> reless <u>s</u> ecurity	M <u>A</u> NAGEMENT	COMMANDS HELP	<u>F</u> EEDBACK			<u>,</u>
WLANS WLANS WLANS Advanced	Central DHCP Processing Override DNS NAT-PAT Central Assoc Lync Server 1 11k Neighbor List Neighbor List Neighbor List Dual Band	Enabled Enabled Enabled Enabled Enabled Enabled Enabled		PMIP NAI Type PMIP Profile PMIP Realm Universal AP Admin S Universal AP Admin S BSS Transition S Optimized Roaming Timer(0 to 40 TBTT Directed Ad Beservic Directed Hulticaet, S Tunnel Profile EOGRE VIan Overric EOGRE VIan Overric	Support upport Disassociation ) se envice de de te D 4	Hexadecimal V None V		

### EoGRE VLAN Overridencept の CLI コマンド

次の CLI を追加し、機能を有効化してオーバーライド VLAN を更新します。

# configure wlan tunnel profile eogre-vlan-override enable/disable

- •WLAN ごとに EoGRE VLAN オーバーライド機能を有効または無効にします。
- ・この設定を行うには、LAN が無効な状態である必要があります。

# configure wlan tunnel profile eogre-vlan-override <vlanId>

- •WLAN に VLAN ID を設定します。
- ・この VLAN ID は、トンネル プロファイルに設定されている EoGRE VLAN ID で上書きされます。
- ・この設定を行うには、WLAN が無効な状態である必要があります。

デフォルトでは、無効に設定されています。

Eogre VLAN オーバーライドのデフォルト値は0です。

### コンソール ログの例

(WLC-5520MA) >show wlan 3	
DHCP Address Assignment Required	Disabled
Static IP client tunneling	Disabled
Tunnel Profile	Prof1
EoGRE Override VLAN state	Enable
EOGRE Override VLAN ID	4
PMIPv6 Mobility Type	none
PMIPv6 MAG Profile	Unconfigured
PMIPv6 Default Realm	Unconfigured

PMIPv6 NAI Type	Hexadecimal	Service	blo
Den COID Date Limite	Migualicy OI	Dermetueen	501U
Per-SSID Rate Limits	opstream	Downstream	
Average Data Rate	0	0	
Average Realtime Data Rate	0	0	
Burst Data Rate	0	0	
Burst Realtime Data Rate	. 0	0	
Per-Client Rate Limits	Upstream	Downstream	
Average Data Rate	0	0	
Average Realtime Data Rate	0	0	
Burst Data Rate	0	0	
Burst Realtime Data Rate	. 0	0	
Scan Defer Priority	4,5,6		
Scan Defer Time	100 milliseco	onds	

# 設計 2: FlexConnect AP ベースの EoGRE トンネル

- CAPWAP 制御パス (フレックス AP と WLC 間)
- EoGRE データ パス (フレックス AP と TGW 間)
- ・トンネルが確立されると、データは FC AP から直接 TGW に流れます。

この設計では、AP からの直接トンネルにより、データプレーンとコントロールプレーンがコントローラと AP から分離されます。ネットワークのコアへのデータパスルーティングが最適化されるため、中央のデータスループットはコアネットワークの容量によってのみ制限されます。コントローラ内またはコントローラ間のモビリティはサポートされませんが、クライアントはローカルスイッチングモードの同じ FlexConnect グループに引き続きローミングできます。



• FlexConnect AP: EoGRE は、オープン WLAN および 802.1x ベースの WLAN でサポートされます。

- ・802.1x で認証された「シンプル」または「トンネル」EoGRE クライアントは同じ WLAN 上でサポートされます。
- ・クライアントは、認証に基づいてローカルモードまたはトンネルモードに分けられます。

- •トンネル クライアントでは、EAP-SIM または EAP-AKA モードがサポートされます。
- オープンSSID WLANでは、すべてローカルクライアントまたはすべてトンネルクライアントのいずれかがサポートされます。
- EoGRE ユーザの AAA のオーバーライドがサポートされています。
- ・トンネルGWはAAAプロキシとして機能することもできます。
- FlexConnect AP では、TGW 障害検出と代替 TGW へのスイッチオーバーがサポートされます。
- •TGW では、アクティブ/スタンバイ モードによるフォールト トレランスがサポートされます。
- •コントローラ内およびコントローラ間のモビリティは、FlexConnect AP モードでサポートされます。
- •スタンドアロンモードでは、モビリティは FlexConnect グループ内でのみサポートされ、トンネル GW は AAA お よびアカウンティング プロキシとして設定できます。
- •トンネル GW では、「設定可能」DHCP オプション 82 がサポートされます。
- ・リリース 8.4 以降では、FlexConnect で IPv6 アドレスがサポートされます。

### 基本的な Flex AP EoGRE 設定

Flex AP に EoGRE トンネルを設定する場合:

- •WLAN にプロファイルを適用すると、WLC または FC AP トンネルに同じトンネル設定が適用されます。
- •FC AP がローカル スイッチ モードになっている場合、FC AP ゲートウェイ トンネルが自動的に適用されます。
- ・ローカルモードのAPに接続しているクライアントは、WLC-TGWトンネルを介して通信します。
- •FC AP に接続しているクライアントは、FC AP-TGW トンネルを介して通信します。
- •クライアントの選択も、AAA またはプロファイル オーバーライドの影響を受けます。



(注) 冗長トンネル設定モードでは、EoGRE トンネル モードに設定されているすべての FC AP からキープアライブ ping が送信されます。

### 一般的な展開: FlexConnect AP - EoGRE トポロジ

この一般的な FC AP - EoGRE トンネル展開設定では、2人のユーザ MN1 と MN2 が Realm @att.com に接続し、他の2 人のユーザ MN3 と MN4 が Realm @att.net に接続しています。次の図に示すように、ユーザ MN1 と MN2 は接続する ときに VLAN1 および TGW1 上にいる必要があり、ユーザ MN3 と MN4 は VLAN-2 および TGW2 に接続する必要があ ります。この設定では、それぞれ1つのレルムを含む2つのプロファイルが作成され、同じドメイン内の TGW1 と TGW2 に適切にマッピングされます。この展開シナリオでは、トンネルはローカル スイッチング モードの FlexConnect AP と TGW1 および TGW2 間に直接設定され、データ トラフィックはすべてコントローラをバイパスして流れます。



(注) この設定では、EoGREトンネルTGW、ドメイン、プロファイルルール、およびレルムが、WLC-EoGREの導入 シナリオの場合とまったく同様にセットアップされます。唯一の変更点は、FC AP がローカル スイッチドモー ドで設定されることです。

1. AP を FlexConnect ローカル スイッチングに設定します。

uluilu cisco	MONITOR WLANS CONTRO	DLLER WIRELESS SEC	URITY MANAGE	Say EMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'Pod1-ate	98'		
WLANS	General Security Q	oS Policy-Mapping	Advanced	
Advanced	FlexConnect	1		DHCP Profiling
- Hurdineed	FlexConnect Local	Foabled		HTTP Profiling
	Switching 4			Local Client Profiling
	FlexConnect Local Auth 🔽	Enabled		DHCP Profiling
	Learn Client IP Address §	Enabled		HTTP Profiling
	Vian based Central	Enabled		PMIP
	Central DHCP Processing	D = 10.1		PMIP Mobility Type
	Override DNS	HCP Processing Enabled		PMIP NAI Type
	NAT-PAT			PMIP Profile
	Central Assoc	Enabled		PMIP Realm
	Lync			Universal AP Admin Support
	Lync Server	Disabled V		Universal AP Admin

(注)

FC AP-TGW トンネルを有効にするには、[FlexConnect Local Switching] オプションのみを FG AP または FC グルー プで設定する必要があります。その他の WLC EoGRE 設定は、FC AP EoGRE 設定に適用されます。

# **EoGRE** 機能の管理

リリース 8.5 以降では、以下の SNMP MIBS を EoGRE トンネルの管理に使用できます。

- ・\* ゲートウェイ/AP EoGRE トンネル Admin ステータス
- ・\* ゲートウェイ/AP EoGRE トンネルのキープアライブ損失
- ・\* ゲートウェイ/AP EoGRE トンネル稼働時間
- ・\* ゲートウェイ/AP EoGRE トンネル トラフィック
- ・\* コントローラ/ゲートウェイ EoGRE トンネル Admin ステータス
- ・\* コントローラ/ゲートウェイ EoGRE トンネルのキープアライブ損失
- ・\* コントローラ/ゲートウェイ EoGRE トンネル稼働時間
- •\* コントローラ/ゲートウェイ EoGRE トンネル トラフィック

# トラブルシューティング コマンド

既存のインターフェイス/アプリケーション関連のデバッグが再利用されます。以下に、パケットフロー、トンネル、および IPv6 関連の問題に使用されるデバッグと show コマンドを示します。

デバッグ:

```
debug arp all/detail/error/message enable/disable
debug packet logging enable all
debug pm rules enable/disable
debug ipv6 neighbor-binding
debug ipv6 address-learning
debug system printk
debug Tunnel eogre
debug Tunnel errors/events
Show commands:
debug fastpath dump vlandb
debug fastpath dump portdb
show system route
show arp kernel
```

## WLC でのトラブルシューティング:

- 1. show tunnel eogre gateway summary
- 2. debug tunnel eogre events/detail/errors enable
- 3. Show tunnel eogre statistics
- 4. Show ap eogre gateway <ap-name> - AP と TGW 間のトンネルの場合は、トンネル情報が表示されます。

### FC AP でのトラブルシューティング:

show tunnel eogre gateway summary show dot11 eogre-tunnel gateway debug dot11 eogre-tunnel event/packets

# 機能の設定手順

L3インターフェイス自体をサポートするための新しいCLI要件はありません。8.2より前のリリースでは、ユーザは管理以外の設定済みインターフェイスをトンネルエンドポイントとして選択できません。グローバルインターフェイスをトンネルエンドポイントとして使用するように設定するには、新しいCLIが必要です。この設定は、EoGRE、PMIPv6などのトンネルタイプごとに行う必要があります。

PMIPv6トンネルの設定の詳細については、以下の導入ガイドを参照してください。1http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113686-pmipv6-config-00.html

### **CLI** での EoGRE トンネルの設定

config tunnel eogre interface <interface-name>

show コマンド:

show tunnel eogre summary

### CLI での PMIPv6 トンネルの設定

config pmipv6 interface <interface-name>

show コマンド: show pmipv6 mag globals

# show コマンド

#### WLC の show コマンド

Show tunnel eogre summary show tunnel eogre gateway summary show tunnel eogre domain summary show tunnel profile summary show tunnel profile detail <profile name> show ap eogre domain <ap-name> Show ap eogre gateway <ap-name>

#### AP の show コマンド

show dotll eogre-tunnel domain summary show dotll eogre-tunnel gateway summary show capwap reap associations show capwap client detailrcb

# EoGRE 機能の設定例

#### ASR 1K の CLI 手順の概要

- 1. enable
- 2. configure terminal
- 3. interface interface-name
- 4. ip unnumbered loopback interface-name or ip address ip-address
- 5. tunnel source interface-type interface-number
- 6. (シンプル IP モードの場合) mac-address H.H.H
- 7. tunnel mode ethernet gre ipv4 or tunnel mode ethernet gre ipv6
- 8. (任意) tunnel vlan vlan-id
- **9.** end

#### ASR1K での設定例

aaa new-model

```
!
aaa group server radius AAA_SERVER_CAR
server-private 5.3.1.76 auth-port 2145 acct-port 2146 key cisco
!
aaa authentication login default none
aaa authentication login ISG_PROXY_LIST group AAA_SERVER_CAR
aaa authorization network ISG_PROXY_LIST group AAA_SERVER_CAR
aaa authorization subscriber-service default local group AAA SERVER CAR
aaa accounting network PROXY_TO_CAR
action-type start-stop
group AAA_SERVER_CAR
!
aaa accounting network ISG_PROXY_LIST start-stop group AAA_SERVER_CAR
١
 [Intelligent Wireless Access Gateway Configuration Guide]
46 OL-30226-06
Service Provider WiFi: Support for Integrated Ethernet Over GRE
Example: Configuring the EoGRE Feature
aaa server radius dynamic-author
client 5.3.1.76 server-key cisco
auth-type any
ignore server-key
!!
ip dhcp excluded-address 172.16.254.254
١
ip dhcp pool ISG_SIMPLE_IP
network 172.16.0.0 255.255.0.0
default-router 172.16.254.254
domain-name cisco.com
!
policy-map type control EOGRE_L2_ISG
class type control always event session-start
```

2 authorize aaa list ISG\_PROXY\_LIST password cisco identifier mac-address 4 set-timer IP\_UNAUTH\_TIMER 5 ! class type control always event service-start 1 service-policy type service identifier service-name 2 collect identifier nas-port ! 1 interface Loopback0 ip address 9.9.9.9 255.255.255.255 interface GigabitEthernet1/0/0 ip address 192.168.0.9 255.255.255.0 negotiation auto ! interface GigabitEthernet1/0/0.778 description "to ASR5K GGSN" encapsulation dot1Q 778 ip address 172.16.199.9 255.255.255.0 1 interface Tunnel10 description "EoGRE Tunnel for Simple IP subscribers" mac-address 0000.5e00.5213 iip address 172.16.254.254 255.255.0.0 no ip redirects tunnel source 172.16.199.9 tunnel mode ethernet gre ipv4 service-policy type control EOGRE\_L2\_ISG ip subscriber l2-connected initiator unclassified mac-address initiator dhcp interface Tunnel100 description "IPv4 EoGRE Tunnel for PMIP/GTP subscribers" ip unnumbered Loopback0 tunnel source GigabitEthernet1/0/0

tunnel mode ethernet gre ipv4 tunnel vlan 100 service-policy type control EOGRE\_L2\_ISG ip subscriber 12-connected initiator unclassified mac-address initiator dhcp

#### !

address ipv4 9.9.9.9

interface Tunnel200 description "IPv6 EoGRE Tunnel for PMIP/GTP subscribers" ip unnumbered Loopback0 tunnel source 2001:161::9 tunnel mode ethernet gre ipv6 tunnel vlan 200 service-policy type control EOGRE\_L2\_ISG ip subscriber 12-connected initiator unclassified mac-address initiator dhcp ! mcsa enable sessionmgr ! ipv6 mobile pmipv6-domain D1 replay-protection timestamp window 255 lma LMA\_5K [Intelligent Wireless Access Gateway Configuration Guide] OL-30226-06 47 Service Provider WiFi: Support for Integrated Ethernet Over GRE Example: Configuring the EoGRE Feature ipv4-address 192.168.199.1 ! ipv6 mobile pmipv6-mag M1 domain D1 sessionmgr role 3GPP

37

interface Tunnel100 interface Tunnel200 lma LMA\_5K D1 ipv4-address 192.168.199.1 encap gre-ipv4 ! ntp master ! gtp information-element rat-type wlan interface local GigabitEthernet1/0/0.778 apn 1 apn-name gtp.com ip address ggsn 172.16.199.1 fixed link-layer address 00ab.00cd.00ef default-gw 20.100.254.254 prefix-len 16 dns-server 20.100.254.254 dhcp-server 20.100.254.254 !

end

サブスクライバ セッション情報を確認および表示するには、以下のコマンドを使用します。 show ip dhep sip statistics show subscriber statistics show subscriber session show ipv6 mobile pmipv6 mag binding show gtp pdp-context all show interface tunnel-name



『Intelligent Wireless Access Gateway (IWAG) Configuration Guide』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意(www.cisco.com/jp/go/safety\_warning/)をご 確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、 日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合が ありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サ イトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、 弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, およびCisco Systems ロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。 本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。 「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R) この資料の記載内容は2008 年 10 月現在のものです。 この資料に記載された仕様は予告なく変更する場合があります。

# 

#### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
 http://www.cisco.com/jp
 お問い合わせ先:シスコ コンタクトセンター
 0120-092-255 (フリーコール、携帯・PHS含む)
 電話受付時間:平日 10:00~12:00、13:00~17:00
 http://www.cisco.com/jp/go/contactcenter/