cisco.



8.5 EoGRE トンネリング導入ガイド

CUWN 8.5 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 4 設計1: WLC ベースの EoGRE トンネル 4 WLC EoGRE トンネリングの設定 6 ConfiguringWLC EoGRE トンネル パラメータの設定 7 一般的な展開:WLC EoGRE トポロジ 13 EoGRE トンネル DHCP オプション 82 の設計 18 リリース 8.2 のトンネリング ソースの変更 19 EoGRE トンネルの冗長性 20 EoGRE TGW フェールオーバーの設定手順 22 設計 2: FlexConnect AP ベースの EoGRE トンネル 25 EoGRE 機能の管理 28 トラブルシューティング コマンド 28 機能の設定手順 29 show コマンド 29 EoGRE 機能の設定例 30

参照 34

CUWN 8.5 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 IPv 6 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。

サポートされるコントローラと AP

- Cisco 3504、5508、5520 シリーズ、WiSM-2、および 8500 シリーズ ワイヤレス LAN コントローラ
- リリース 8.2 以降では、2500 シリーズおよび vWLC 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 8.4 のサポート対象アクセスポイント: 3800、2800、1800、3700、2700、1700、1600、3600、2600、2700、702i、3500、702w、1540、1560、1552、1532、1572。

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**リモート トンネル**や**ローカル**などの 2 種類のユーザ トラフィック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-Protocol-Type が [None] の場合、MPC プロトコル タイプはシンプル 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、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。

ステップ2 WLC のメイン メニューで、 [WLANs] を選択し、[Go] をクリックします。

Curr	ent Filter	None	[Change Filter] [Clear Filter]		Crea	ste New 🖌 Go
E v	WLAN ID	Туре	Profile Name	WLAN SSID	Admin Status	Security Policies
1	1	WLAN	POD2-PSK	POD2-PSK	Enabled	[WPA2][Auth(PSK)]

ステップ3 例えば POD4-EoGRE などの命名規則を持つ 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 における設定オプションの変更は、以下のセクションを参照してください。

uluulu cisco monitoi	WLANS CONTROLLER	Sage Configuration <u>P</u> ing Logout <u>R</u> efresh WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>E</u> EEDBACK A Home
WLANs	WLANs > Edit 'POD4	-EoGRE' <back apply<="" td=""></back>
WLANS	General Security	QoS Policy-Mapping Advanced
▶ Advanced	Profile Name Type SSID Status [Security Policies (POD4-EoGRE WLAN POD4-EoGRE POD4-EoGRE POD4-E
	Radio Policy Interface/Interface	All vanagement v
	Multicast Vlan Feature	Enabled
	Broadcast SSID NAS-ID	C Enabled 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。

neral	Security	QoS	Policy-Mapping Advanced	
ver 2	Laver 3	AAA S	ervers	
		94 - C C.		
Layer 2	Security f	lone		
Layer 2	Security f N	lone VC Filtering		

ConfiguringWLC EoGRE トンネルパラメータの設定



(注) EoGRE トンネルの設定は、GUI または CLI によって実行できます。

TGW リリース 8.3 での 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 アドレスをサポートしています。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 によって 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 トンネルのゲートウェイ 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。

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。3 つのキープアライブ ping の後に 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って、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、TWG が何回連続で応答をスキップできるか決定します。

- d) 例えば ASR1K などの [TGW Name] を追加します。
- e) 例えば 10.10.200.5 などの [TGW IP Address] を追加します。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS	Sage Configuration HELP <u>F</u> EEDBACK	Eing Logout Befre
Controller General Inventory	EoGRE General Apply Default			
Interfaces Interface Groups Multicast Multicast	Interface Name management Heartbeat Interval(Seconds) 60 Max Heartbeat Skip Count 3			
Redundancy Mobility Management	Add New TGW	Add New Domain Domain Name	domain4	
Ports > NTP	TGW IP Address 10.10.200.5	TGW-1 TGW-2	None +	
CDP PMIPv6	TGW List	Domain List		
 Tunneling EoGRE Profiles 	ASR1K 10.10.200.5 UP 0	Name TGW	1 TGW-2	Active Gateway
+ IPv6		domain4 ASR1K		ASR1K

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

					Sa <u>v</u> e Confi	guration
CISCO MONITOR	<u>W</u> LANS <u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	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	Seconds) 60 Count 3				
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) 例えば domain4 などの [Domain Name] を追加します。
- h) トンネル ゲートウェイ [TGW-1] を [ASR1K] と選択して、[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 リストのステータスは [UP] となります。

EoGRE General						
Apply Default						
Interface Name	management					
Heartbeat Interval(Seconds)	60					
Max Heartbeat Skip Count	3					
			Add New De	omain		
Add New TGW			Domain Na	me	domain4	-
TGW Name			TGW-1		ASR1K	-
TGW IP Address			TGW-2		None	
A00			Add			
TGW List			Domain List	t)		
Name IP Add	ress Statu	s Total Clients				A
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。 前述のように、単一のドメインに最大10個のトンネルが存在できます。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) プロファイル名、たとえば、pod6 を構成し、[Add] をクリックします。

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	6 HELP FEEDBACK
Controller	Profiles							
General Inventory	Profile Li	st						Add New
Interfaces	Profile Na	me	WLAN ID	(Mapped)				Profile Name pod6
Interface Groups								Copy of None 1
Network Routes								Add
Redundancy								1
Internal DHCP Server								/
Mobility Management								
Ports								
▶ NTP								
> CDP								
Tunneling								
EoGRE								

プロファイルは [Profile List] に表示されます。

Profiles			
Profile List			
Profile Name	WLAN IDs (Mapped)		
pod6	None		

- 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) 特定のレルムをプロファイルに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。 [Realm] に一致させるには、*を使用します(すべてのレルムを受け入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。

le Tunnel Par	ameters	
Drofile Name	nodd	
Prome name	pode	
Store Street Street		Turnel Trans. I and Junity On Coloural Durants - 1

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 Profile > Edit					< Back Apply
Rule Tunnel Parameters					-
Profile Name pod 6					
Realm *	Tunnel	Type EoGRE -	VLAN 0 Gatew	ay Domain domain4 👻	
Realm	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	Policy-Mapping	Advanced	
NAT-PAT En	sbied	HITP Protong	
Central Assoc	sbled	PMIP	
ync		PMIP Mobility Type	0
Lync Server Disabled	(1)	PMIP NAI Type	(Hexadecimal +)
1k		PMIP Profile	None ‡
Assisted Roaming Prediction Optimize	ation 🗌 Enabled	PMIP Realm	
Neighbor List	Enabled	Universal AP Admin Support	
Neighbor List Dual Band	Enabled	Universal AP Admin	۲
		11v BSS Transition Support	
		BSS Transition	•
		Disassociation Imminent	0
		Disassociation Timer(0 to 3000 T8TT)	200
		Optimized Roaming Disassociation Timer(0 to 40	(BTT) 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確な 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 が事前に設定されています。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) サンプルの設定は Ipv4 に向けたものです。

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





また、show client detail コマンドを POD WLC で実行することで、EoGRE トンネルによってクライアント が関連付けられていることを確認することもできます。

(POD2-WLC) >show client detail b8:f6:b1:11:7f:23 Client MAC Address. b8:f6:b1:11:7f:23 Client Username N/A AP Mame. N/A AP Name. POD2-APJ800 AP Name. POD2-APJ800 AP Intervention Associated Client User Group. Associated Client User Group. Access Client User Group. Access Client Nace OOB State. Access Wireless LAN Id. 2 Wireless LAN Pofile Name. PODX-EOGRE Hotspot (802.110) Not Supported BSSID. 3c:ce:73:38:24:70 Connected For 1363 secs Channel. 76 Policy Manager Rule Created. Yes Audit Session ID. none AAA Role Type. none IPv4 AcL Name. none IPv4 Act Applied Status. Unavailable IPv6 Act Applied Status. Unavailable EogRE AAA PGW Primary. <th></th> <th></th>		
Client MAC Address. b8:f6:b1:11:7f:23 Client Username N/A AP MAC Address. 3c:ce:73:38:24:70 AP Name. POD2-AP3600 AP radio slot Id. 1 Client State. Access Client State. Access Client State. Access Wireless LAN Pody Access Wireless LAN Proving Name (SSID). PODX-EOGRE Most Supported SSID. BSSID. Sc:ce:73:38:24:7e Connected For 1363 secs Address. 10.55.55.62 Policy Manager State. none Policy Manager State. none AAR Role Type. none Local Policy Applied. none Ipv4 Act. Applied Status. unavailable IPv4 Act. Applied Status. unavailable IPv6 Act. Applied Status. unavailable IPv6 Act. Name. none Inva Alable unavailable IPv6 Act. Name. none IPv6 Act. Name. none Invavailable unavailable IPv6 Act. Applied Status. unavailable	(POD2-WLC) >show client detail b8:f6:b1:11:7f:23	
Client Username N/A AP MAC Address 32:(c:73:38:24:70 AP Name. POO2-AP3600 1 Client User Group. Client State. Associated Client User Group. Client Vace Group. Client NAC OOB State. Access Wireless LAN Network Name (SSID). PODX-EOGRE Motspot (802.11u). PODX-EOGRE Motspot (802.11u). Box SID. PODX-EOGRE Motspot (802.11u). Constant State SSID. Connected For Client Vace State Channel. 36 Channel. 36 Channel. 36 Channel. 36 Channel. 36 Channel. 36 Policy Manager State. RUN Policy Manager State. RUN Policy Manager Rule Created. Yes Addit Session ID. none AAA Role Type. none IPv4 ACL Name. none IPv4 ACL Name. none IPv4 ACL Applied Status. Unavailable IPv4 ACL Name. none IPv4 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv4 ACL Name. none IPv6 ACL Name. none IPv6 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv4 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv6 ACL Applied Status. Unavailable IPv6 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv6 ACL Name. none IPv6 ACL Name. none	client MAC Address	b8:f6:b1:11:7f:23
AP MAC Address 3c:ce:73:38:24:70 AP Name. POD2-AP3600 AP Tate. POD2-AP3600 Client State. Associated Client User Group. Associated Client User Group. Associated Client State. Access Wireless LAN Id	Client Username	N/A
AP Name. PO02-AP3600 AP radio slot Id. 1 Client State. Associated Client State. Associated Client Nac OOB State. Access wireless LAN Id. 2 wireless LAN network Name (SSID). PODX-EOGRE Hotspot (802.11u). Box Supported BSSID. 3c:cc:73:38:24:7e Connected For 1363 secs Channel. 36 Policy Manager Rule Created. Yes Audit Session ID. none Accal Type. none Local Policy Applied unavailable IPv6 ACL Name. none IPv6 ACL Applied Status. unavailable IPv6 ACL Name. none EogRE AAA NSErvice. inone	AP MAC Address	3c:ce:73:38:24:70
AP radio slot Id. 1 Client State. Associated Client User Group. Associated Client User Group. Associated Client User Group. PODX-EGGRE Wireless LAN Id. 2 Wireless LAN Profile Name. PODX-EGGRE BSSID. PODX-EGGRE BSSID. Scice:73:38:24:7e Connected For 1363 secs Channel. 36 IP Address. 10.55.55.62 Policy Manager State. RUN Policy Manager State. none AAR Role Type. none Local Policy Applied. none IP Address. Unavailable IPv4 ACL Name. none IPv6 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv6 ACL Name. none Layer 2 ACL Applied Status. Unavailable EogRE AAA NSErvice. IPv4 EogRE AAA NSErvice. IPv4 EogRE AAA NAT Unavailable EogRE AAA Nat Group Tourged Not contructored	AP Name	POD2-AP3600
Client State. Associated Client State. Access Client NAC 00B State. 2 Wireless LAN Id. 2 Wireless LAN Profile Name. PODX-EOGRE Hotspot (802.11u) PODX-EOGRE Connected For 1363 Secs Channel. 36 IP Address. 10.55.55.62 Policy Manager Rule Created. Yes Audit Session ID. none Local Policy Applied none Flexconnect AcL Applied Status. Unavailable IPv4 AcL Name. none IPv6 AcL Applied Status. Unavailable	AP radio slot Id	1
Client User Group. Access Client NAC GOB State. 2 Wireless LAN 1d. 2 Wireless LAN Network Name (SSID). PODX-EOGRE PODX-EOGRE PODX-EOGRE Not Supported BSSID. BSSID. Scice:73:38:24:7e Connected For 1363 secs Channel. 36 IP Address. 10.55.55.62 Policy Manager State. RUN Policy Manager State. none AAR Role Type. none Local Policy Applied. none IP 4 ACL Name. none IPv4 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv6 ACL Name. none Izve2 ACL Applied Status. Unavailable IPv6 ACL Name. none Izve2 ACL Applied Status. Unavailable IPv6 ACL Name. none Izve2 ACL Applied Status. Unavailable IPv6 ACL Name. none Izve2 ACL Applied Status. Unavailable IPv6 ACL Name. none Izve2 ACL Applied Status. Unavailable	Client State	Associated
Client NAC 00B State. ACCess Wireless LAN 1d. 2 Wireless LAN Profile Name. PODX-EOGRE Hotspot (802.11u) PODX-EOGRE SSID. 3c:cc:73:38:24:7e Connected For 1363 secs Channel. 36 Policy Manager State. RUN Policy Manager Rule Created. Yes Audit Session ID. none Local Policy Applied none IPv4 ACL Name. none IPv6 ACL Applied Status. unavailable IPv6 ACL Name. none IPv6 ACL Applied Status. unavailable IPv6 ACL Applied Status. unavailable IPv6 ACL Applied Status. <t< td=""><td>Client User Group</td><td></td></t<>	Client User Group	
wireless LAN Id. 2 wireless LAN Network Name (SSID). PODX-EOGRE wireless LAN Profile Name. PODX-EOGRE Notspot (802.11u). Not Supported BSSID. 3C:CE?'3:38:24:7e Connected For 1363 secs Channel. 36 IP Address. 10.55.55.62 Policy Manager State. RUN Policy Manager Rule Created. Yes Audit Session ID. none AAR Role Type. none Local Policy Applied. none IPv4 ACL Name. none IPv6 ACL Name. none IPv6 ACL Name. none Layer2 ACL Applied Status. Unavailable Layer2 ACL Applied Status. Unavailable Client Type. EoGRE AAA NST EoGRE AAA NA NSErVICE. Unavailable EoGRE AAA NA PGW Primary. 10.10.200.55	Client NAC OOB State	Access
wireless LAN network Name (SSID). PODX-EOGRE wireless LAN Profile Name PODX-EOGRE HOTSpot (802.11u). Not Supported BSSID. 363 secs Connected For 1363 secs Channel. 36 Policy Manager State. RUN Policy Manager Rule Created. Yes Audit Session ID. none Local Policy Applied. none IPv4 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv6 ACL Name. none Layer 2 ACL Name. none Layer 2 ACL Name. none Client Type. EOGRE AAA NSEVICE. EogRE AAA NSEVICE. Unavailable EogRE AAA PGW Primary. 10.10.200.5 EogRE AAA PGW Primary. Not Count pured	Wireless LAN Id	2
wireless LAN Profile Name PODX-EOGRE Hotspot (802.11u) Not Supported BSSID	Wireless LAN Network Name (SSID)	PODX-EOGRE
Hotspot (802.11u). Hotspot (802.11u). BSSID. Connected For Channel. P Address. Policy Manager State. Policy Manager Rule Created. Policy Manager Rule Creater Rule Rule Rule Rule Rule Rule Rule Rule	Wireless LAN Profile Name	PODX-EOGRE
BSSID. 3c:ce:73:38:24:7e Connected For 1363 secs Channel. 36 IP Address. 10.55.55.62 Policy Manager State. RUN Policy Manager Rule Created. Yes Audit Session ID. none AAA Role Type. none Local Policy Applied. none IPv4 ACL Name. none IPv6 ACL Applied Status. unavailab	Hotspot (802.11µ).	Not Supported
Connected For 1363 secs Channel. 36 IP Address. 10.55.55.62 Policy Manager State. RUN Policy Manager Rule Created. Yes Audit Session ID. none Local Policy Applied. none IPv4 ACL Name. none IPv6 ACL Applied Status. Unavailable IPv6 ACL Applied Status. Unavailable IPv6 ACL Name. none ISVET CONSE AAA PON SERVICE. EOGRE EOGRE AAA NST. Unavailable EOGRE AAA PGW Primary. 10.10.200.5 EOGRE AAA PGW Primary. Not contrust	BSSTD	3c:ce:73:38:24:7e
Channel	Connected For	1363 Secs
IP Address. 10.55.55.62 Policy Manager State. RUN Policy Manager Rule Created. Yes Audit Session ID. none Local Policy Applied. none IPV4 ACL Name. none IPv4 ACL Name. none IPv6 ACL Name. none	Channel	36
Policy Manager State	TP address	10 55 55 62
Policy Manager State. RUN Policy Manager Rule Created. Yes Audit Session ID. none Local Policy Applied. none Ibcal Policy Applied. none IPV4 ACL Name. none IPv6 ACL Name. none ISVET CL Name. none ISVET CL Name. none ISVET CL Name. none ISVET CL NAME. unavailable ISVET CL NAME. unavailable EOGRE AAA NN SERVICE unavailable EOGRE AAA PGW Primary. 10.10.200.5 IONE CONTINUE NOT CONTINUE	AF MOU COST	10.33.33.02
Policý Manager Rule Created	Policy Manager State	RUN
Audit Session ID. none AAA Role Type. none Local Policy Applied. none IPv4 ACL Name. none IPv4 ACL Name. none IPv4 ACL Name. unavailable IPv4 ACL Name. none IPv4 ACL Name. none IPv6 ACL Name. none IPv6 ACL Name. none IPv6 ACL Name. none Layer2 ACL Name. none Layer2 ACL Name. none IPv6 ACL Name. unavailable EogRE AAA NN Service. IPv4 EogRE AAA NST unavailable EogRE AAA PGw Primary. 10.10.200.5 IPv4 IPv4 Forker Are Gw Primary. Nor contruct numed	Policy Manager Rule Created	Yes
AAA Role Typenone Local Policy Appliednone FlexConnect ACL Applied Statusnone IPv4 ACL Namenone IPv4 ACL Applied Statusunavailable IPv6 ACL Namenone IPv6 ACL Namenone Laver2 ACL Applied Statusunavailable Laver2 ACL Applied Statusunavailable Client TypeECGRE EOGRE AAA NAT	Audit Session ID.	none
Local Policy Applied	AAA Role Type	none
IPv4 ACL Name. none FlexConnect ACL Applied Status Unavailable IPv4 ACL Applied Status Unavailable IPv6 ACL Name. none IPv6 ACL Applied Status Unavailable IPv6 ACL Applied Status Unavailable Laver2 ACL Name. none Laver2 ACL Name. unavailable Client Type. EOGRE EOGRE AAA MN Service. Unavailable EOGRE AAA NAT. Unavailable EOGRE AAA PGW Primary. 10.10.200.5 EOGRE AAA PGW Service Not contrustered	Local Policy Applied	none
FlexConnect ACL Applied Status Unavailable IPv4 ACL Applied Status Unavailable IPv6 ACL Name none IPv6 ACL Namities Unavailable IPv6 ACL Name none Laver2 ACL Name unavailable Client Type EoGRE EoGRE AAA NAT Unavailable EoGRE AAA PGW Primary 10.10.200,5 EoGRE AAA PGW Primary Not control pured	TPv4 ACL Name	none
IPv4 ACL Applied Status. Unavailable IPv6 ACL Name. none Ipv6 ACL Applied Status. Unavailable Layer2 ACL Name. none Layer2 ACL Applied Status. Unavailable Client Type. EOGRE EOGRE AAA MAN Service. Unavailable EOGRE AAA PGW Primary. 10,10,200.5 FORME AGG AGG ACT STUDERED Not controlured	ElexConnect ACL Applied Status	Unavailable
IPv6 ACL Name	TPv4 ACL Annlied Status	Unavailable
IPV6 ACL Applied Status. Unavailable Layer2 ACL Applied Status. none Layer2 ACL Applied Status. unavailable Client Type. EOGRE EOGRE AAA MN Service. unavailable EOGRE AAA NAT. unavailable EOGRE AAA PGW Primary. 10,10,200.5 EOGRE AAA PGW Primary. Not controlured	TPUS ACL Name	none
Laver2 ACL Name	TPu6 ACL Annlied Status	Unavailable
Layer2 ACL Applied Status. Client Type. EOGRE AAA NAI EOGRE AAA NAI EOGRE AAA PGW Primary. EOGRE	1 svor? ACL Namo	none
Cient Type. Events States the Correct States	Layer2 ACL Applied Status	Unavailable
EOGRE AAA NAI UNAVIECE. IPVA EOGRE AAA NAI UNAVAIlable EOGRE AAA PGW Primary. 10.10.200.5 EOGRE AAA PGW Secondary. Not controlmed	Client Time	Cacop
EOGRE AAA NAT. Unavailable EOGRE AAA PGW Primary. 10,10,200,5 EOGRE AAA PGW Servorary Not controllered		EVOKE
EOGRE AAA PGU Primary	COCOF ANA NAT	Unavailable
EOURE AAA POW PTIMA 9	FOORE ANA DESI DESIMONY	10 10 200 5
ECONE AND POW SECONDAL V	EOURE ANA POW PT INdi Y	10.10.200.3
could retrie been a great from the could gut ea	EOOKE AAA POW Secondary	Not com igured

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							Configurat	tion Ping	Logout Be	fresh
cisco	MONITOR WLAN		WIRELES	S SECURITY	MANAGEMENT	COMMANDS	HELP	EEEOBACK	6 E	<u>l</u> ome
Controller	EoGRE General									
General Inventory Interfaces Interface Groups Multicast Network Routes	Apply De Interface Name Heartbeat Interva Max Heartbeat Sk	fault mana I(Seconds) 60 ip Count 3	gement							
 Redundancy Internal DHCP Server Mobility Management Ports NTP CDP DMIPee6 	Add New TGW TGW Name TGW IP Address Add TGW List	tgw2 4	6		Add New Doma Domain Name TGW-1 TGW-2 Add Domain List	dom) dom) tgw1 None	~			
Tunneling EoGRE Profiles	Name tgw1	IP Address 9.9.89.100	Status DOWN 0	Total Clients	Name	TGW-1	TGW	1-2 No	Active Gateway	

CLI から EoGRe ハートビートを設定します。

config tunnel eogre heart-beat interval 30

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

CLIから EoGRE トンネルを設定します。

config tunnel eogre gateway add tgwl 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 でドメイン dom1 を tgw1 と tgw2 に設定します。

du New Di	onium		1		
Domain Na	ime	dom1	-		
TGW-1		None	*	1	
TGW-2		None			
		TOW1	- mark		
Add		tgw2	_		
Add		tgw2	_		
Add	t	tgw2			
Add Oomain List	t	tgw2			
Add)omain List	t	tgw2			Active
Add Oomain List	t TGW-1	tgw2	TGW-2		Active Gateway

CLI からトンネル ドメインを作成します。

config tunnel eogre domain create domlcon config tunnel eogre domain add doml tgwl config tunnel eogre domain add doml tgw2

ステップ3 プロファイルの作成とルールの追加:

a) 例えば prof-att などのプロファイルを設定します。

CISCO MONITOR	WLANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Configu C <u>O</u> MMANDS	HELP	<u>P</u> ing Logou <u>F</u> EEDBACK
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Network Routes Redundancy Mobility Management Ports NTP CDP PMIPv6	Profiles Profile List Profile Name prof1 prof-att	WLAN ID None None	s (Mapped)	Add Nev Profile Copy o Add	V Name prof-at f None		

b) WLC GUI から、ドメイン dom1 で VLAN1 に向けたレルム att.com と VLAN2 に向けた att.net を作成し、 プロファイル prof-att にそれらを適用します。

Realm att.net	prof-att		VLAN 2 Gat	teway Domair	n dom1 💌
Add					
	Tunnal Tuna	VLAN	Gateway Doma	ain	

CLIからのプロファイルとレルムを作成します。

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のユーザをドロップします。
- ステップ4 トンネル パラメータを設定します。

以下の図は、AAA プロキシGW と DHCP オプション 82 を有効にしたトンネル パラメータの、GUI からの 設定例を示しています。

cisco	MONITOR WLANS CONTROLLER W	IRELESS SECURITY	MANAGEMENT COMMANDS	Gage HELP EE	Configuration Bing Log (DBACK	out Befresh
Controller General Inventory Interfaces Interface Groups Multicast > Network Routes > Redundancy Mobility Management Ports > 200	Tunnel Profile > Edit Rule Tunnel Parameters EGGRE @atevay as AAA Proxy @atevay as Accounting Proxy DHCP Option 62 Format DHCP Option 62 Format DHCP Option 82 Delimiter 2	· · · · · · · · · · · · · · · · · · ·			C Back	Apply
 CDP PNIPv6 Tunneling CoRt Profiles IPv6 mDNS Advanced 	Circuit-1D Fields Available AP radio MAC address AP Rome AP Group Name AP Flex Group Name AP Flex Group Name AP Flex Group Name AP Iotation VLAV-1D net Sisto-TYPE Client MAC	Fields Selected	Remote-ID Fields Available AP Bithemet MAC address AP Group Name AP Flex Group Name AP Flex Group Name AP Flex Group Name SSD-TYPE Client MAC		Fields Selected	Up Down

ステップ5 GUI からの EoGRE トンネルの設定

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。

NT

cisco	MONITOR WLA	Ns <u>C</u> ONTROLLER	WIRELESS	<u>S</u> ecurity	M <u>A</u> NAGEME
Controller	EoGRE Gener	al			
General Icons Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Mobility Management Ports NTP	Apply C Interface Name Heartbeat Inter Max Heartbeat Add New TGW TGW Name TGW IP Address Add	val(Seconds) mana chrom Skip Count eogre mana	gement V lecast20 lecast73 -test gement]	
▶ PMIPv6	Name	IP Address	Status	Total Clients	
r Tunneling	tgw1	9.9.89.100	DOWN	0	75
EoGRE Profiles	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」を WLAN にマッピングします。

uludu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAG	Saza Configu IMENT COMMANDS HELP EEEDBACK	iration Eing Logout Befresh 🏟 Home
WLANs	WLANs > Edit '5520-test' General Security QoS Policy-Mapping Advanced		< Back Apply
 Advanced 	Vian based Central Enabled	HTTP Profiling 🗐 PMIP	Î
	Central DHCP Processing Enabled Override DNS Enabled NAT-PAT Enabled	PMIP NAI Type Hexadecimal *	
	Central Assoc Enabled Lync Lync Disabled	PMIP Profile None PMIP Realm Universal AP Admin Support	
	Ik Arristed Reaming Prediction Optimization III Eachied	Universal AP Admin 🔲	
	Neighbor List Dual Band Enabled	BSS Transition Disassociation Imminent Disassociation Timer(0 to 3000 200	
		Optimized Roaming Disassociation 40 Timer(0 to 40 TBTT)	
		Tunneling Tunnel Profile prof-att •	
	4		•

CLI から WLAN2 にプロファイルをマッピングします。

config wlan tunnel profile prof1 2

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、ブリッジモードの WLC に挿入されています。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 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します。グローバル DHCP の設定は、EoGRE クライアントに影響を与え 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、サポート対象の最大 5 個の異なるパラメータ ID を提示することで簡単に設 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。

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 インターフェイスからの DHCP オプション 82 の設定

ahaha				Sa	ge Configuration Bing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP E	EEDBACK	🔒 Home
Controller	Tunnel Profile > Edit				< Bac	k Apply
General Inventory	Rule Tunnel Parameter	B				
Interfaces Interface Groups Multicast F Network Routes	EOGRE Gateway as AAA Proxy Gateway as Accounting Prox					
 Redundancy Mobility Management Ports 	DHCP Option-82 DHCP Option 82 Format DHCP Option 82 Delimiter	Binary V				
NTP CDP	Circuit-ID		Remote-ID		_	
PMIPv6	Fields Available	Fields Selected	Fields Available		Fields Selected	
 Tunneling Footes TPv6 mDNS Advanced 	AP radio MAC address AP Ethernet MAC address AP Name AP Group Name AP Flex Group Name AP Flex Group Name AP Iox Group Name SSID-TYPE Client MAC		AP Ethernet MAC address AP Name AP Group Name AP Flax Group Name AP Ica Group Name AP Ication VLAN-ID SSID-TYPFC Client MAC		AP radio MAC address	Up Down

CLI からの DHCPオプション 82 の設定:

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 からの AAA プロキシとしてのゲートウェイの設定:

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

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

リリース8.2のトンネリングソースの変更

リリース 8.2 以前は、EoGRE、PMIPV6 などのすべてのトンネルで、トンネルのエンドポイントとして管理 インターフェイスのみを使用できました。リリース8.2 では、管理インターフェイス以外のトンネルソースを指定する機能が追加されたため、ネットワークのデータトラフィックと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ます。

- ・設定には4094 L3 インターフェイスを利用できます。
- 管理者は、EoGREのようなトンネルに向けて、ダイナミックインターフェイスをトンネルエンドポイントとして 設定できます。
- •前述のトンネリングプロトコルを除いて、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 と 2500 を含むすべてのコントローラがサポートされています。

リリース 8.2 では、すべての 4094 インターフェイスが、サポート対象のコントローラ タイプに向けた L3 ダイナミッ クインターフェイス (IPv4 が IPv6 として設定されている場合は、8.2 のこれらのインターフェイスではサポートされ ていません)です。ただし、vWLC の場合は、512 L3 インターフェイスのみがサポートされます。IP アドレスが設定 されていない場合、L2インターフェイスのままとなります。これらのL2インターフェイスは、すでにフィールドに導 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 インスタンスの IP を取得する DHCP のサポート)の変更 を避けるために、このリリースではクライアント インターフェイスとして使用されません。要求に応じて、これらの L2 インターフェイスは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でき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 は、トンネル ソースは常に AP の IP アドレスを関連付けられたインターフェイスとなります。トンネルの外部 VLAN は、IP が関連付けられたこの AP インターフェイスの VLAN となります。

EoGRE トンネルの冗長性

2つ以上のトンネルに冗長性を設定できるため、プライマリまたはアクティブのトンネルに障害が発生した場合、セカ ンダリまたはスタンバイのトンネルが 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、その周期、つまり、トンネルがダウンしたと判断する前に、何回のキープ アライブの応答に失敗できる かを設定できます。これはグローバルなコマンドで、すべてのトンネルのタイプに適用されます。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 エコーの応答が返送され、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が使用可能な場合は、コントローラによってセカンダリトンネルが確立され、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、セカンダリWAGに再接続されます。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サーバーから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に接続されたま まです。

ahahi								Sa <u>v</u> e Conf	iguration	<u>P</u> ing Logou	t <u>R</u> efresh
CISCO	MONITOR WLANS		r wire	ELESS	SECURIT	MANAGE	MENT	COMMANDS	HELP	EEEDBACK	Home
Controller	EoGRE Genera	d									
General Inventory Interfaces Interface Groups Multicast	Apply D Interface Name Heartbeat Interv Max Heartbeat S	efault m al(Seconds) 60 kip Count 3	anageme	nt							
 Redundancy Internal DHCP Server Mobility Management Ports NTP CDP 	Add New TGW TGW Name TGW IP Address Add				Add D TC TC Ac	New Dom omain Name 3W-1 3W-2 Id	ain	None	v		
 PMIPv6 Tunneling 	IGW List	IP Address	Status	Total	Don	nain List				Active	
EoGRE Profiles	ASR1K-PR	10.10.200.5	UP	0		lame Iomain4	TGW ASR1	/-1 <-PR AS	TGW-2 R1K-SEC	Gatew	ay

リリース 8.5 の冗長性とフェールオーバー

リリース 8.5 以前では、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 または冗長性に向けた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 オーバーの目的で、TGW-1 と TGW-2 をプライマリとセカンダリとする新しいオプションを利用できます。



ドメインでは、プライマリ ゲートウェイが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または完了後に、WLC はプライマリ ゲート ウェイを ping し続けます。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 ゲートウェイとなります。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。



同じオプションが、ローカル スイッチング モードの Flex Connect AP からの TGW でも利用できます。



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 から 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	<u>P</u> ing	Logout	Refresh
CISCO	MONITOR WLANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COM	IMANDS	HELF	<u>F</u> EEDBACK				🔒 <u>H</u> ome
Controller	EoGRE General												
General Icons Inventory	Apply Def	ault											
Interfaces Interface Groups Multicast	Interface Name Heartbeat Interva Max Heartbeat Sk	I(Seconds) 60 ip Count 3	igement V										
Network Routes													
Fabric Configuration													
Redundancy													
Mobility Management								Ad	d New Domain				
Ports	Add New TGW							AU	la New Domain	damt			
▶ NTP	TGW Name	tgw1							Domain Name	domi			
▶ CDP	TGW IP Address									Gateway Name	Ro	le	_
▶ PMIPv6									TGW-1	tgw1 🔻	P	rimary 🔻]
▼ Tunneling	Add								TGW-2	tgw2 🔻	N	one 🔻]
EoGRE Profiles	TGW List							A	bb				_
▶ IPv6								Do	main List				
▶ mDNS	Name ¹	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 から、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	N WIRELESS SECU	IRITY MANAGEMENT				
WLANs	WLANs > Edit 'eogre'							
VLANs	General Security Q	20S	Policy-Mapping	Advanced				
Advanced	FlexConnect							
	FlexConnect Local Switching ²		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、EoGRE トンネル プロファイルをバインドします。

սիսիս					Save Configuration Ping
CISCO	<u>MONITOR WLANS CONTROLLER</u>	WIRELESS SECU	RITY M <u>A</u> NAG	EMENT C <u>O</u> MMANDS HE <u>L</u> F	P <u>F</u> EEDBACK
WLANs	General Security QoS	Policy-Mapping	Advanced		
WLANs	Lync Server Enable	d 🔻	1	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 Disasted Multicast Service	200 40
				Funneling	
				Tunnel Profile	eogre-psk 🔻
			4 <u> </u>	nDNS	
			1	mDNS Snooping TrustSec	Enabled
				Security Group Tag OpenDNS	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 WLA	Ns <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK			Say	e Configu	ration
Controller	Profiles												
General													
Icons	Profile List										New		
Inventory	Profile Name								\rightarrow	WLAN IDs (Mapped)	Profile		
Interfaces											Сору	None	T
Interface Groups	profi								None	e 📔	of	None	
Multicast	prof-att	1							None	e 🔽	Add		
Network Routes	eogre-psk								8,9				

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、レルムは、WLC-EoGREの導入シナリ オとまったく同様に設定されています。唯一の変更は、FC AP が、ローカル スイッチング モードで設定されて いることです。

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

- alulu			Sayı				
CISCO	MONITOR WLANS CONTR	OLLER WIRELESS SECURITY MANAG	EMENT COMMANDS HELP FEEDBACK				
WLANs	WLANs > Edit 'Pod1-ate	98'					
- WLANS	Conoral Security (Dos Dolicy-Manning Advanced					
WLANs	General Security (203 Poncy Happing Advanced					
Advanced	FlexConnect	DHCP Profiling					
	FlexConnect Local		HTTP Profiling				
	Switching ²		Local Client Profiling				
	FlexConnect Local Auth 🔽	Enabled					
	Learn Client IP Address 2	Enabled	HTTP Profiling				
	Vian based Central		PMIP				
	Switching 🚨	L Enabled	DMID Mability Type				
	Central DHCP Processing	Enabled	PMIP NAI Type PMIP Profile PMIP Realm				
	Override DNS	Enabled					
	NAT-PAT	Enabled					
	Central Assoc	Enabled					
	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、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/アプリケーションに関連するデバッグが再利用されます。以下は、パケットフロー、トンネル、IPv6 関連の問題に使用されるデバッグおよび show コマンドです。

```
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 eogre
debug Tunnel errors/events
Show commands:
debug fastpath dump vlandb
debug fastpath dump portdb
show system route
show arp kernel
```

WLC 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> - - - トンネルが AP と TGW 間の場合は、トンネル情報を表示します。

FC AP 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インターフェイスなどをサポートするために新しいCLIの要件はありません。8.2以前のリリースでは、ユーザはトンネルエンドポイントとして管理以外の設定インターフェイスを選択できません。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、異なるトンネルタイプに対して個別に行う必要があります。

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

CLI からの EoGRE トンネルの設定

config tunnel eogre interface <interface-name>

show コマンド :

show tunnel eogre summary

CLI からの PMIPv6 トンネルの設定

config pmipv6 interface <interface-name> show $\exists \forall \mathcal{V} \not\models$: show pmipv6 mag globals

show コマンド

SWLC 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 dot11 eogre-tunnel domain summary
show dot11 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

```
[Intelligent Wireless Access Gateway Configuration Guide]
46 OL-30226-06
 Service Provider WiFi: Support for Integrated Ethernet Over GRE
例: EoGRE 機能の設定
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
!
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
!
!
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 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 12-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 l2-connected initiator unclassified mac-address initiator dhcp ١ 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 l2-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 例: EoGRE 機能の設定 ipv4-address 192.168.199.1 ! ipv6 mobile pmipv6-mag M1 domain D1 sessionmgr role 3GPP address ipv4 9.9.9.9 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/