



Ethernet over GRE の設定

Ethernet over GRE (EoGRE) は、IP コア ネットワーク上で GRE ヘッダーにカプセル化されたレイヤ 2 パケットのトンネリングを可能にするトンネリング プロトコルです。Generic Routing Encapsulation (GRE) は、レイヤ 3 IPv4 またはレイヤ 3 IPv6 アクセス ネットワーク上で仮想ポイントツーポイントリンクに多種多様なネットワーク レイヤ プロトコルをカプセル化するトンネリング プロトコルです。

前提条件

EoGRE を設定する際の前提条件は次のとおりです。

- IP ルーティングが有効にされている必要があります。IP ルーティングを有効にするためのコマンドは次のとおりです。

ip routing

- IP CEF が有効にされている必要があります。IP CEF を有効にするためのコマンドは次のとおりです。

ip cef

- VLAN タグを持つイーサネット フレームをトンネリングする、VLAN のサブインターフェイスを作成する必要があります。VLAN のサブインターフェイスを作成するためのコマンドは次のとおりです。

interface Dot11Radio *interface number.sub-interface number*

encapsulation dot1Q *vlan id*

bridge-group *bridge id*

interface GigabitEthernet0.*sub-interface number*

encapsulation dot1Q *vlan id*

bridge-group *bridge id*



(注) 同じ VLAN ID が設定されたインターフェイスには、同じブリッジ ID を設定する必要があります。

次はサポートされていません。

- SNMP、ACS コンフィギュレーションを使用した GUI
- IPv6 アドレスを使用したトンネルの確立

EoGRE の設定

トンネルのプロファイルを設定して、トンネルを作成するために設定可能なパラメータを定義します。次のパラメータは、dot11 トンネルに設定されます。

- トンネルアドレス モード
- 送信元アドレス
- 宛先アドレス
- 最大セグメント サイズ(MSS)
- 最大伝送ユニット(MTU)
- Type of Service (ToS) または Differentiated Services Code Point (DSCP)

dot11 トンネルのトンネルプロファイルを設定するには、特権 EXEC モードで次の手順に従います。

コマンド	目的
mode [ipv4 ipv6]	トンネルアドレス モードを IPv4 または IPv6 に設定します。
source address	送信元アドレス。デフォルトは AP の BVI アドレスです。
destination address	トンネル宛先アドレス
mss size	着信/発信 TCP syn および syn/ack パケットの TCP MSS 値を設定します。デフォルトのサイズは 1360 です。
mtu size	IP パケットのサイズがこの値より大きい場合、着信 IP パケットはフラグメント化され、ICMP Need Fragmentation エラーメッセージがクライアントに送信されます。デフォルトのサイズは 1400 です。
tos value	転送 IP アドレスの ToS または DSCP 値を設定します。デフォルト値は 0 です。

例

```
ap(config)# dot11 tunnel sample
ap(config-dot11-tunnel)# mode ipv4
ap(config-dot11-tunnel)# destination 1.1.1.1
ap(config-dot11-tunnel)# mss 1360
ap(config-dot11-tunnel)# mtu 1400
ap(config-dot11-tunnel)# tos 5
ap(config-dot11-tunnel)# end
```

SSID のトンネルへのマッピング

トンネルを WLAN にマッピングするには、SSID コンフィギュレーションでコマンド `tunnel tunnel_profile` を使用します。

SSID をトンネルにマッピングするには、特権 EXEC モードで次の手順に従います。

	コマンド	目的
ステップ 1	<code>dot11 ssid ssid</code>	SSID を設定します。
ステップ 2	<code>vlan vlan id</code>	VLAN ID を指定します。
ステップ 3	<code>tunnel tunnel profile</code>	使用するトンネルプロファイルを指定します。
ステップ 4	<code>authentication {open eap }</code>	認証のタイプを指定します。

例

```
ap(config)# dot11 ssid doc
ap(config-ssid)# tunnel sample
ap(config-ssid)# authentication open
ap(config-ssid)# end
```

EoGRE クライアントの DHCP スヌーピングの設定

DHCP スヌーピングは、信頼できないホストと信頼済み DHCP サーバとの間でファイアウォールのような役割を果たすセキュリティ機能です。AP 上で DHCP スヌーピングを有効にすると、AP は、回線 ID とリモート ID の 2 つのサブオプションを含むリレー エージェント情報オプション (DHCP オプション 82) を挿入します。



(注) DHCP スヌーピングは、デフォルトで無効になっています。

dot11 SSID の EoGRE クライアントの DHCP スヌーピングを有効にするには、特権 EXEC モードで次の手順に従います。

	コマンド	目的
ステップ 1	<code>dhcp-snoop enable</code>	DHCP スヌーピングを有効にします。 デフォルトでは、DHCP スヌーピングはディセーブルです。
ステップ 2	<code>dhcp-snoop circuit_id format {ap-mac client-mac eth-mac name ssid type vlan raw word_string}</code>	回線 ID として使用する文字列シーケンスの形式を指定します。指定する形式については、 回線 ID およびリモート ID の書式と文字列 (24-4 ページ) を参照してください。 回線 ID は DHCP パケットに挿入されます。
ステップ 3	<code>dhcp-snoop circuit_id circuit-id-string_sequence</code>	回線 ID として使用する文字列シーケンスを、設定した形式で指定します。区切り文字を使用して各文字列を区切ります。デフォルトの区切り文字は「;」です。

	コマンド	目的
ステップ 4	dhcp-snoop remote_id format {ap-mac client-mac eth-mac name ssid type vlan raw word_string}	リモート ID として使用する文字列シーケンスの書式を指定する必要があります。指定する値については、 回線 ID およびリモート ID の書式と文字列(24-4 ページ) を参照してください。
ステップ 5	dhcp-snoop remote_id remote-id-string_sequence	リモート ID として使用する文字列シーケンスを、設定した書式で指定する必要があります。区切り文字を使用して各文字列を区切ります。デフォルトの区切り文字は「;」です。

例

```
ap(config)# dot11 ssi
ap(config)# dot11 ssid doc
ap(config-ssid)# dhcp-snoop enable
ap(config-ssid)# dhcp-snoop circuit_id format ap-mac ssid type
ap(config-ssid)# dhcp-snoop circuit_id 00:10:A4:23:B6:C0;xfinityWiFi;s
ap(config-ssid)# dhcp-snoop remote_id format client-mac
ap(config-ssid)# dhcp-snoop remote_id 00:50:24:23:B7:D0
ap(config-ssid)# end
```

その他のコマンド

デフォルトの DHCP スヌーピングのエンコーディングはバイナリです。これを ASCII に設定するには、次のコマンドを使用します。

```
ap(config-ssid)# dhcp-snoop encoding ascii
```

デフォルトの DHCP スヌーピングの文字列シーケンスの区切り文字は単一の「;」文字です。これを変更するには、次のコマンドを使用します。

```
ap(config-ssid)# dhcp-snoop delimiter single_character_or_string
```

single_character_or_string は、最大 127 文字の長さになります。

回線 ID およびリモート ID の書式と文字列

回線 ID およびリモート ID に文字列を割り当てる前に、それぞれに文字列シーケンスの書式を指定する必要があります。

書式および文字列には、次の表に記載する 8 つの値のうち、最大 5 つの値を組み合わせることができます。文字列シーケンスを指定する際には、区切り文字で文字列を区切る必要があります。デフォルトの区切り文字は「;」です。

書式	対応する文字列の特性
ap-mac	AP 無線の MAC アドレス
client-mac	Client MAC address
eth-mac	AP イーサネット MAC アドレス
name	AP 名
raw word_string	任意の文字列。書式コマンドで raw を指定する場合は、入力する文字列も一緒に指定します。
ssid	SSID (Service Set Identifier)
type	SSID のタイプ。オープン SSID の場合は「o」、セキュア SSID の場合は「s」です。
vlan	VLAN 名

トンネルゲートウェイアドレスの冗長性の設定

トンネルの冗長性を設定すると、運用中のゲートウェイアドレスが失敗または到達不能になった場合、プライマリからセカンダリにスイッチオーバーできるようになります。

冗長性を設定するには、次のパラメータを dot11 トンネルで設定します。

- バックアップ宛先
- バックアップ タイムアウト
- キープアライブ パラメータ

トンネルの冗長アドレスを設定するには、特権 EXEC モードで次の手順に従います。

	コマンド	目的
ステップ 1	Backup destination address	バックアップの宛先アドレスを指定します。
ステップ 2	Backup timeout seconds	トンネルをバックアップからプライマリに切り替えるまでの秒数を指定します。
ステップ 3	Keepalive count interval dead-count timeout	<p><i>count</i> は、各 <i>interval</i> (秒数) で送信する ping パケットの数です。</p> <p><i>dead-count ping</i> が失敗すると、トンネルエンドポイントはデッド状態であるとみなされます。</p> <p><i>timeout</i> は、AP が <i>ping</i> を送信した後に <i>ping</i> の応答を待機する秒数です。</p> <p><i>count</i>、<i>interval</i>、<i>dead-count</i>、<i>timeout</i> のデフォルト値は、それぞれ 3、60、3、1 です。</p>



(注)

プライマリからセカンダリ、またはその逆にスイッチオーバーする際は、アソシエートされているクライアントすべてが認証解除され、スイッチオーバー後に再アソシエートされます。プライマリとセカンダリの両方がダウンすると、トンネルに接続される SSID もダウンします。AP がプライマリ アドレスとセカンダリ アドレスのいずれかに到達可能になると、SSID が有効になり、クライアントへの対応を開始します。

例

```
ap(config)# dot11 tunnel sample
ap(config-dot11-tunnel)# backup destination 2.2.2.2
ap(config-dot11-tunnel)# backup timeout 60
ap(config-dot11-tunnel)# keepalive 3 60 3 3
ap(config-dot11-tunnel)# end
```

■ トンネル ゲートウェイ アドレスの冗長性の設定

翻訳について

このドキュメントは、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。