



インターフェイスおよびハードウェアコンポーネント コンフィギュレーション ガイド

Interface and Hardware Component Configuration Guide

Cisco IOS XE Release 3S

【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、米国シスコシステムズ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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

インターフェイスおよびハードウェア コンポーネント コンフィギュレーション ガイド
Copyright © 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010–2011, シスコシステムズ合同会社.
All rights reserved.



物理インターフェイス



物理インターフェイスの設定

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、ギガビット イーサネット、Packet over SONET (POS)、およびシリアル Shared Port Adapter (SPA; 共有ポート アダプタ) インターフェイスなどさまざまな種類の物理 (ハードウェア) インターフェイスをサポートします。ハードウェアの技術的説明およびインターフェイスの取り付けに関する情報については、ご使用の製品のハードウェアの取り付けおよび設定に関するマニュアルを参照してください。

設定情報

- ギガビット イーサネットの管理イーサネット インターフェイスの使い方については、次の URL で『Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide』の「Using the Management Ethernet Interface」の章を参照してください。
<http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/asrswcfg.html>
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでサポートされている SPA Interface Processors (SIP; SPA インターフェイス プロセッサ) および SPA の設定およびトラブルシューティングについては、次の URL の『Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide』を参照してください。
http://cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

コマンド リファレンス情報

- インターフェイスの設定に使用するコマンドの詳細については、次の URL の『Cisco IOS Interface and Hardware Component Command Reference』に記載されています。
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_book.html
- 他の Cisco IOS XE コマンドを参照する場合は、Command Lookup Tool (<http://tools.cisco.com/Support/CLILookup>) を使用するか、『Cisco IOS Master Command List, All Releases』 (http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html) を参照してください。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2009–2011, シスコシステムズ合同会社 .
All rights reserved.



仮想インターフェイス



仮想インターフェイスの設定

仮想インターフェイスは、Cisco IOS XE コマンドを使用してネットワーキング デバイスのメモリで作成するソフトウェアベースのインターフェイスです。仮想インターフェイスには、100BASE-T ファストイーサネット ネットワーク インターフェイス カードの RJ-45 メス型ポートなどのハードウェア コンポーネントがありません。このモジュールでは、Cisco IOS XE ソフトウェアを使用して設定できる 4 つの一般的な種類の仮想（論理）インターフェイスについて説明します。

- ループバック インターフェイス
- ヌル インターフェイス
- サブインターフェイス
- トンネル インターフェイス

目次

- 「仮想インターフェイスの設定の前提条件」(P.1)
- 「仮想インターフェイスの設定に関する情報」(P.2)
- 「仮想インターフェイスの設定方法」(P.6)
- 「仮想インターフェイスの設定例」(P.12)
- 「関連情報」(P.13)
- 「その他の参考資料」(P.13)

仮想インターフェイスの設定の前提条件

ネットワークで仮想インターフェイスを使用する前に、いくつかの物理（ハードウェア）インターフェイスを設定する必要があります。また、仮想インターフェイスを使用するネットワーキング デバイス間で通信できる必要があります。

仮想インターフェイスの設定に関する情報

仮想インターフェイスを設定するには、次の概念を理解しておく必要があります。

- 「仮想インターフェイス」 (P.2)
- 「仮想インターフェイスの利点」 (P.2)
- 「ループバック インターフェイス」 (P.3)
- 「ループバック インターフェイスとループバック モード」 (P.4)
- 「ヌル インターフェイス」 (P.5)
- 「サブインターフェイス」 (P.5)
- 「トンネル インターフェイス」 (P.6)

仮想インターフェイス

仮想インターフェイスは、物理インターフェイスに関連付けられていないネットワーク インターフェイスです。物理インターフェイスには、何らかの形式の物理的な要素（イーサネット ケーブルの RJ-45 オス型コネクタなど）が存在します。仮想インターフェイスはソフトウェアとしてだけ存在します。物理的な要素は存在しません。個々の仮想インターフェイスは、仮想インターフェイス名の後にある数値 ID を使用して識別します。たとえば、`loopback 0`、`tunnel 1`、`fastethernet 0/0/0.1` などです。この ID は名前文字列全体を一意にするために仮想インターフェイスの種類ごとに異なります。たとえば、`loopback 0` インターフェイスと `null 0` インターフェイスは共存できますが、単一のネットワーク キング デバイスで 2 つの `loopback 0` インターフェイスは共存できません。

Cisco IOS XE ソフトウェアは次の 4 つの種類の仮想インターフェイスをサポートします。

- ループバック
- ヌル
- サブインターフェイス
- トンネル

仮想インターフェイスの利点

ループバック インターフェイスは、IP アドレスや IPX アドレスなどのレイヤ 3 アドレスを割り当てることのできる安定したインターフェイスを提供できます。このアドレスは、ネットワーク キング デバイスが NetFlow や Cisco Discovery Protocol (CDP) などのプロトコルのデータをネットワークの別のデバイスに送信する必要があり、その受信側デバイスにネットワーク キング デバイスからの同じ送信元 IP アドレスを常に認識させたい場合に送信元アドレスとして設定できます。これは、複数の等コストパスが存在するネットワークで問題となります。これは、通常、ネットワーク キング デバイスで生成されたパケットはパケットの送信元アドレスとしてアウトバウンド インターフェイスの IP アドレスを使用したり、ネットワーク キング デバイスと受信側ホストの間に 2 つ以上の等コストパスが存在するネットワークでは、各パケットが異なるアウトバウンド インターフェイスを使用することがあるためです。

ヌル インターフェイスを使用すると、アクセス リストの使用に伴うオーバーヘッドを発生させない別の方法でフィルタリングを行えます。たとえば、宛先ネットワークへのトラフィックがインターフェイスから送信されるのを防ぐアウトバウンド アクセス リストを作成する代わりに、宛先ネットワークに対してヌル インターフェイスを示すスタティック ルートを設定できます。

サブインターフェイスは1つの物理インターフェイスを2つ以上のインターフェイスに仮想的に分割する方法として開発されました。サブインターフェイスは同じ物理インターフェイスを共有しますが、IPルーティングプロトコルは各リモート ネットワーキング デバイスへのネットワーク接続を別々の物理インターフェイスとして認識します。サブインターフェイスの最初の使用事例の1つは、フレーム リレー WAN のスプリット ホライズンに関する問題を解決することでした。

トンネリング（別のプロトコルでのトラフィックのカプセル化）が役に立つ状況は次のとおりです。

- 単一プロトコルのバックボーン上でマルチプロトコル ローカル ネットワークをイネーブルにする場合
- ホップ カウントが制限されたプロトコル（RIP バージョン 1 や AppleTalk など）を使用するネットワークに対して回避策を提供する場合
- 隣接していないサブネットワークを接続する場合
- WAN でバーチャル プライベート ネットワークを許可する場合

ループバック インターフェイス

ループバック インターフェイスと呼ばれるソフトウェアベースのインターフェイスを指定して、物理インターフェイスをエミュレートできます。ループバック インターフェイスはすべてのプラットフォームでサポートされます。ループバック インターフェイスは Cisco ルータ上の仮想インターフェイスであり、**no shutdown** コマンドを発行してから **shutdown** コマンドでディセーブルにするまで稼動（アクティブな状態）し続けます。サブインターフェイスとは異なり、ループバック インターフェイスは物理インターフェイスの状態に影響されません。

ループバック インターフェイスは、イネーブルにすると、シャット ダウンするまで稼動し続けるため、安定していると見なすことができます。このため、ループバック インターフェイスは、ネットワーク デバイスのいずれの物理インターフェイスの状態にも影響されない参照先として単一アドレスが必要なときに IP アドレスなどのレイヤ 3 アドレスを割り当てる場合に理想的です。この好例として、ループバック インターフェイスの IP アドレスをネットワーク デバイスの **Domain Name System (DNS; ドメイン ネーム システム)** ホスト アドレスの IP アドレスとして使用することが挙げられます。ループバック インターフェイスが使用できるようになる前は、ネットワーク管理者はルータ上の IP アドレスが割り当てられたすべてのインターフェイスに対し DNS ホスト エントリを設定する必要がありました。これは、ルータを管理する場合に任意の時点で使用可能となる可能性のあるインターフェイス IP アドレスがどれか分からないためです。次に示されたルータ A のインターフェイス設定と DNS エントリの例では、各インターフェイスに1つの DNS エントリが設定されています。

ループバック使用前のルータ A のインターフェイス設定

```
GigabitEthernet0 10.10.10.1 255.255.255.0
GigabitEthernet1 10.10.11.1 255.255.255.0
GigabitEthernet2 10.10.12.1 255.255.255.0
GigabitEthernet3 10.10.13.1 255.255.255.0
GigabitEthernet4 10.10.14.1 255.255.255.0
GigabitEthernet5 10.10.15.1 255.255.255.0
```

ループバック使用前のルータ A の DNS エントリ

```
RouterA    IN    A    10.10.10.1
           IN    A    10.10.11.1
           IN    A    10.10.12.1
           IN    A    10.10.13.1
           IN    A    10.10.14.1
           IN    A    10.10.15.1
```

ネットワーク デバイスのインターフェイスは、障害が発生したり、メンテナンスのために運転を停止する場合があります。ルータ A のいずれかのインターフェイスで障害が発生したり、これらのいずれかのインターフェイスが停止したりした場合、他のネットワーク デバイスは問題があるインターフェイスにアクセスできません。ループバック インターフェイスを使用してネットワーク デバイスを設定し、ネットワーク全体でアドバタイズされる IP アドレスをデバイスに割り当てる場合、ネットワーク デバイスに IP トラフィックを送受信できるネットワーク インターフェイスが少なくとも 1 つある限り、この IP アドレスを使用してネットワーク デバイスに到達できます。ループバック インターフェイス設定後のルータ A のインターフェイス設定と DNS エントリの例では、いずれかの物理インターフェイスを使用してルータに到達するために使用できる DNS エントリが 1 つだけ示されています。

ループバック使用後のルータ A のインターフェイス設定

```
Loopback 172.16.78.1 255.255.255.0
GigabitEthernet0 10.10.10.1 255.255.255.0
GigabitEthernet1 10.10.11.1 255.255.255.0
GigabitEthernet2 10.10.12.1 255.255.255.0
GigabitEthernet3 10.10.13.1 255.255.255.0
GigabitEthernet4 10.10.14.1 255.255.255.0
GigabitEthernet5 10.10.15.1 255.255.255.0
```

ループバック使用後のルータ A の DNS エントリ

```
RouterA IN A 172.16.78.1
```

ループバック インターフェイスの設定された IP アドレス (172.16.78.1) は、ルータで生成されたパケットの送信元アドレスとして使用し、ネットワーク管理アプリケーションとルーティングプロトコルに転送できます。このループバック インターフェイスは、明示的にシャットダウンされない限り、常に到達可能です。

ループバック インターフェイスは、Open Shortest Path First (OSPF) セッションまたは Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) セッションの終端アドレスとして使用できます。また、ループバック インターフェイスは、デバイスのコンソール ポートから補助ポートへの Telnet セッションを確立するためにも使用できます (他のすべてのインターフェイスがダウンしている場合)。他のルータやアクセスサーバがこのループバック インターフェイスに到達しようとするアプリケーションでは、ループバック アドレスに割り当てられたサブネットを配布するようルーティングプロトコルを設定する必要があります。

ループバック インターフェイスにルーティングされた IP パケットは、ルータまたはアクセス サーバに再びルーティングされ、ローカルで処理されます。ループバック インターフェイスからルーティングされ、宛先がループバック インターフェイスでない IP パケットは廃棄されます。これらの 2 つの状況では、ループバック インターフェイスがヌル インターフェイスのように動作することがあります。

ループバック インターフェイスとループバック モード

ループバック インターフェイスは安定した発信元インターフェイスを実現するもので、IP ルーティングプロトコルがループバック インターフェイスに割り当てられたサブネットをアドバタイズする限り、発信元インターフェイスに割り当てられた IP アドレスがいつでも到達可能になるようにします。ただし、ビット損失やデータ破損などの、WAN (シリアル) リンクに関する問題をテストおよび診断するには、ループバック モードが使用されます。ループバック モードでは、インターフェイスで受信されたデータ パケットをそのトラフィックの送信元であるデバイスに同じインターフェイスから送信し返すループを設定します。ループバック モードは、データ パケットが送信されたときと同じ状態で返信されていることを確認して問題のトラブルシューティングを行うために使用されます。データ パケットにエラーがあると、WAN インフラストラクチャに問題があることとなります。多くの種類のシリアル インターフェイスには、インターフェイスまたはコントローラ コンフィギュレーション モードで入力される独自の形式のループバック コマンド構文があります。

ヌル インターフェイス

ヌル インターフェイスはループバック インターフェイスに似た仮想ネットワーク インターフェイスです。ループバック インターフェイスへのトラフィックはルータ自体に送信されますが、ヌル インターフェイスに送信されたトラフィックは破棄されます。ヌル インターフェイスは常に稼働し、トラフィックを転送または受信できません。カプセル化は常に失敗します。ヌル インターフェイスは、ほとんどのオペレーティング システムで利用可能なヌル デバイスと同様に機能します。

ヌル インターフェイスは、不必要なネットワーク トラフィックを破棄する、オーバーヘッドが低い方法として使用されます。たとえば、ネットワーク ユーザが特定の IP サブネットに到達できないようにする場合は、そのサブネットに対してネットワーキング デバイスのヌル インターフェイスを指すスタティック IP ルートを作成できます。IP アクセス リストを使用するよりもスタティック IP ルートを使用した方が CPU 時間が短くなります。また、スタティックルート設定はインターフェイス コンフィギュレーション モードではなくグローバル コンフィギュレーション モードで行われるため、IP アクセス リストを使用した場合よりも簡単です。

ヌル インターフェイスにはアドレスを設定できないことがあります。トラフィックをヌル インターフェイスに送信するには、ネクスト ホップがヌル インターフェイス (Null 0 で表されます) であるスタティック ルートを設定する必要があります。ネクスト ホップをヌル インターフェイスとして設定する 1 つの例は、BGP を使用して発表できる集約ネットワークへのルートを作成する場合、または特定の範囲のアドレスへのトラフィックがルータを経由して伝播されないようにする場合 (多くの場合、セキュリティが目的) です。

ルータには常に単一のヌル インターフェイスが存在します。デフォルトでは、ヌル インターフェイスにパケットが送信されると、ルータは Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) 到達不能メッセージをパケットの送信元 IP アドレスに送信して応答します。これらの応答を送信するか、メッセージを表示せずにパケットを廃棄するようルータを設定できます。

サブインターフェイス

サブインターフェイスは物理インターフェイスに関連付けられます。サブインターフェイスが関連付けられた物理インターフェイスがイネーブルにされるとサブインターフェイスはイネーブルになり、物理インターフェイスがシャット ダウンされるとディセーブルになります。



(注)

サブインターフェイスは、関連付けられた物理ポートに関係なくイネーブルにしたり、シャット ダウンしたりできます。ただし、シャット ダウンされた物理インターフェイスのサブインターフェイスはイネーブルにできません。

サブインターフェイスは、物理インターフェイスを、IP サブネットなどの一意のレイヤ 3 ネットワーク アドレスを割り当てることができる 2 つ以上の仮想インターフェイスに分割することによって作成されます。サブインターフェイスの最初の使用事例の 1 つは、フレーム リレー WAN のスプリット ホライズンに関する問題を解決することでした。スプリット ホライズンは、IP サブネットが認識されたのと同じ物理インターフェイスからアドバタイズされない、RIP などの IP ルーティング プロトコルに関連付けられた動作です。スプリット ホライズンは、IP ネットワークでルーティング グループを防ぐために導入されました。ルーティング グループは、ネットワーク接続の両側のネットワーキング デバイスが同じ IP ルートをお互いにアドバタイズするときに作成されることがあります。スプリット ホライズンはフレーム リレー マルチポイント ネットワーク インターフェイス (単一の物理インターフェイスを使用して 2 つ以上のリモート ネットワーキング デバイスに接続するインターフェイス) の場合に問題でした。多くのネットワーキング デバイスのデフォルトの動作はスプリット ホライズンを導入することでした。つまり、ネットワーキング デバイスは、インターフェイスを使用して認識された IP ルートを同じ物理インターフェイス経由で到達可能な他のデバイスに同じインターフェイスからアドバタイズしませんでした。サブインターフェイスは 1 つの物理インターフェイスを 2 つ以上のインターフェイス

に仮想的に分割する方法として開発されました。サブインターフェイスは同じ物理インターフェイスを共有しますが、IP ルーティング プロトコルは各リモート ネットワーキング デバイスへのネットワーク接続を別々の物理インターフェイスとして認識します。TCP/IP ではデフォルトでスプリット ホライズンの制限がなくなりましたが、AppleTalk や IPX などのプロトコルはまだスプリット ホライズンの制限を受けています。

サブインターフェイスは、ハードウェアの Interface Descriptor (IDB) から構成されるプレフィクス、それに続くピリオドと、プレフィクスに対して一意の番号によって識別されます。フル サブインターフェイス番号は、ネットワーク デバイスに対して一意である必要があります。たとえば、GigabitEthernet インターフェイス 0/0/0 の最初のサブインターフェイスの名前は GigabitEthernet 0/0/0.1 となります。ここで .1 は最初のサブインターフェイスを示します。

トンネル インターフェイス

トンネリングを使用すると、トランスポート プロトコル内部の任意のパケットをカプセル化できます。トンネルは仮想インターフェイスとして実装され、簡単なインターフェイスを設定できるようになっています。トンネル インターフェイスは、特定の「パッセンジャ」プロトコルまたは「トランスポート」プロトコルに関連付けられていません。トンネル インターフェイスは、任意の標準的なポイントツーポイント カプセル化スキームを導入するのに必要なサービスを提供するよう設計されたアーキテクチャです。

提供する必要がある接続に応じて、複数の方法でトンネル インターフェイスを導入できます。トンネルの一般的な使用方法の 1 つは IPX などのネットワーク プロトコルのデータ トラフィックを IPX をサポートしないネットワークのデバイスを介して送信することです。たとえば、ネットワークのコアではなくネットワークの端にあるサイトで IPX を使用する場合は、IP で IPX をトンネリングすることにより、ネットワークの端にある IPX サイトをネットワークのコアを介して接続できます。

Cisco IOS XE ソフトウェアを使用して利用できるさまざまな種類のトンネリング技術の詳細については、『Cisco IOS XE Interface and Hardware Component Configuration Guide』の「[Implementing Tunnels](#)」モジュールを参照してください。

仮想インターフェイスの設定方法

ここでは、次の作業について説明します。

- 「[ループバック インターフェイスの設定](#)」(P.6) (必須)
- 「[ヌル インターフェイスの設定](#)」(P.8) (必須)
- 「[サブインターフェイスの設定](#)」(P.10) (任意)

ループバック インターフェイスの設定

この作業では、ループバック インターフェイスの設定方法について説明します。ループバック インターフェイスは、イネーブルにすると、シャット ダウンするまで稼動し続けるため、安定していると思えます。このため、ループバック インターフェイスはネットワーク デバイスのいずれの物理インターフェイスの状態にも影響を受けない参照先として使用する単一アドレスが必要となるときに IP アドレスなどのレイヤ 3 アドレスを割り当てる場合に理想的です。

前提条件

ループバック インターフェイスの IP アドレスは一意であり、他のインターフェイスによって使用されていない必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface loopback number**
4. **ip address ip-address mask [secondary]**
5. **end**
6. **show interfaces loopback number**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface loopback number 例： Router(config)# interface loopback 0	ループバック インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 • <i>number</i> 引数を使用し、作成または設定するループバック インターフェイスの数を指定します。 (注) 作成可能なループバック インターフェイスの数に制限はありません。
ステップ 4	ip address ip-address mask [secondary] 例： Router(config-if)# ip address 10.20.1.2 255.255.255.0	ループバック インターフェイスの IP アドレスを指定し、インターフェイスでの IP の処理をイネーブルにします。 • <i>ip-address</i> 引数および <i>mask</i> 引数を使用し、ループバック アドレスのサブネットを指定します。
ステップ 5	end 例： Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

コマンドまたはアクション	目的
<p>ステップ6 <code>show interfaces loopback number</code></p> <p>例： Router# show interfaces loopback 0</p>	<p>(任意) ループバック インターフェイスに関する情報を表示します。</p> <ul style="list-style-type: none"> <code>number</code> 引数を使用し、ある特定のループバック インターフェイスに関する情報を表示します。 <p>(注) この例では、この作業に適用される構文だけが使用されます。詳細については、『Cisco IOS Interface and Hardware Component Command Reference』を参照してください。</p>
<p>ステップ7 <code>exit</code></p> <p>例： Router# exit</p>	<p>特権 EXEC モードを終了します。</p>

例

次に、`show interfaces loopback` コマンドからの出力例を示します。

```
Router# show interfaces loopback

Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 10.20.1.2/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

ヌル インターフェイスの設定

この作業では、ヌル インターフェイスの設定方法について説明します。ヌル インターフェイスは、トラフィックをフィルタリングするアクセス コントロール リストに代わる方法を提供します。すべての不要なトラフィックをヌル インターフェイスに送信できます。ヌル インターフェイスはトラフィックを受信することも転送することもできません。または、トラフィックをカプセル化できます。

ヌル インターフェイスに指定できるインターフェイス コンフィギュレーション コマンドは、`no ip unreachable` コマンドだけです。

ヌル インターフェイスからの ICMP 到達不能メッセージ

デフォルトでは、ヌル インターフェイスにパケットが送信されると、ルータは Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) 到達不能メッセージをパケットの送信元 IP アドレスに送信して応答します。これらの応答を送信するか、メッセージを表示せずにパケットを廃棄するようルータを設定できます。

ヌル インターフェイスに送信されたパケットに対する応答で ICMP 到達不能メッセージの送信をディセーブルにするには、インターフェイス コンフィギュレーション モードで **no ip unreachable**s を使用します。ヌル インターフェイスに送信されたパケットに対する応答で ICMP 到達不能メッセージの送信を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip unreachable**s を使用します。

制約事項

各ネットワーク デバイスには 1 つのヌル インターフェイスしか設定できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface null *number***
4. **no ip unreachable**s
5. **end**
6. **show interfaces null [*number*] [*accounting*]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface null <i>number</i> 例： Router(config)# interface null 0	ヌル インターフェイスと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 • number 引数は常に 0 です。
ステップ 4	no ip unreachable s 例： Router(config-if)# no ip unreachable	インターフェイスで ICMP 到達不能メッセージが生成されないようにします。 • このコマンドは、すべての種類の ICMP 到達不能メッセージに影響を及ぼします。

	コマンドまたはアクション	目的
ステップ 5	end 例 : Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show interfaces null [number] [accounting] 例 : Router# show interfaces null 0	(任意) スル インターフェイスに関する情報を表示します。 <ul style="list-style-type: none"> スル インターフェイスの場合、<i>number</i> 引数は常に 0 になります。 (注) この例では、この作業に適用される構文だけが使用されます。詳細については、『 Cisco IOS Interface and Hardware Component Command Reference 』を参照してください。

例

次に、**show interfaces null** コマンドからの出力例を示します。

```
Router# show interfaces null

Null0 is up, line protocol is up
  Hardware is Unknown
  MTU 1500 bytes, BW 10000000 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets

    0 output buffer failures, 0 output buffers swapped out
```

サブインターフェイスの設定

この作業では、サブインターフェイスの設定方法について説明します。サブインターフェイスは、関連付けられた物理ポートに関係なくイネーブルにしたり、シャットダウンしたりできます。ただし、シャットダウンされた物理インターフェイスのサブインターフェイスはイネーブルにできません。

前提条件

サブインターフェイスの IP アドレスは一意であり、他のインターフェイスによって使用されていない必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number.subinterface-number**
4. **ip address ip-address mask [secondary]**
5. **end**
6. **show interfaces type number.subinterface-number**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number.subinterface-number 例： Router (config)# interface GigabitEthernet 2/3.5	インターフェイスの種類、インターフェイスの番号、およびサブインターフェイスの番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address ip-address mask [secondary] 例： Router (config-if)# ip address 209.165.200.225 255.255.255.224	インターフェイスの IP アドレスを指定し、インターフェイスでの IP の処理をイネーブルにします。
ステップ 5	end 例： Router (config-if) # end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show interfaces type number.subinterface-number 例： Router# show interfaces GigabitEthernet 2/3.5	(任意) インターフェイスに関する情報を表示します。
ステップ 7	exit 例： Router# exit	特権 EXEC モードを終了します。

例

次に、**show interfaces** コマンドからの出力例を示します。

```
Router# show interfaces GigabitEthernet 2/3.5

GigabitEthernet2/3.5432 is down, line protocol is down (notconnect)
  Hardware is c7600 1Gb 802.3, address is 001b.0de6.c100 (bia 001b.0de6.c100)
  Description: *sample*
  Internet address is 10.11.12.13/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 2339.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
```

仮想インターフェイスの設定例

ここでは、次の例について説明します。

- 「ループバック インターフェイスの設定：例」(P.12)
- 「ヌル インターフェイスの設定：例」(P.12)
- 「サブインターフェイスの設定：例」(P.12)

ループバック インターフェイスの設定：例

次に、ループバック インターフェイス loopback 0 の設定シーケンスの例を示します。

```
interface loopback 0
 ip address 209.165.200.225 255.255.255.0
end
```

ヌル インターフェイスの設定：例

次に、ヌル インターフェイスの設定シーケンスと ICMP 到達不能メッセージの廃棄方法の例を示します。ヌル インターフェイスに送信されたすべてのパケットは廃棄され、この例では、ヌル インターフェイスに送信されたパケットに対する応答で通常送信される ICMP メッセージが廃棄されます。

```
interface null 0
 no ip unreachable
end
```

サブインターフェイスの設定：例

次に、サブインターフェイスの設定シーケンスの例を示します。

```
interface GigabitEthernet 2/3.5
 description *sample*
 encapsulation dot1Q 2339
 ip address 209.165.200.225 255.255.255.224
end
```

関連情報

- ネットワークでトンネルを導入する場合は、『Cisco IOS XE Interface and Hardware Component Configuration Guide』の「[Implementing Tunnels](#)」モジュールを参照してください。
- ネットワークで物理（ハードウェア）インターフェイス（ギガビットイーサネットやシリアルインターフェイスなど）を導入する場合は、『Cisco IOS XE Interface and Hardware Component Configuration Guide』の「[Configuring Physical Interfaces](#)」モジュールを参照してください。

その他の参考資料

ここでは、仮想インターフェイスに関する関連資料について説明します。

関連資料

関連項目	参照先
インターフェイス コマンド：コマンド構文の詳細、コマンドモード、デフォルト値、コマンド履歴、使用上の注意事項、および例	『Cisco IOS Interface and Hardware Component Command Reference』
すべての Cisco IOS XE コマンド	<ul style="list-style-type: none"> • 『Cisco IOS Master Command List, All Releases』 • Command Lookup Tool
Cisco IOS XE Interface and Hardware Component コンフィギュレーション モジュール	『Cisco IOS XE Interface and Hardware Component Configuration Guide』
BGP でのループバック インターフェイスの使用方法を示す設定例	『Sample Configuration for iBGP and eBGP With or Without a Loopback Address』

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	<p>選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"> • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする <ul style="list-style-type: none"> – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する <p>この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/en/US/support/index.html</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2007–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2007–2011, シスコシステムズ合同会社.
All rights reserved.



トンネル



トンネルの実装

このモジュールでは、Cisco IOS XE ソフトウェアで使用可能な各種のトンネリング技術について説明します。物理インターフェイスまたは仮想インターフェイスを使用するトンネルタイプについては、設定の詳細および例が記載されています。多くのトンネリング技術は、テクノロジー固有のコマンドを使用して実装されており、該当するテクノロジー モジュールへのリンクが提供されます。

トンネリングを使用すると、トランスポート プロトコル内部の任意のパケットをカプセル化できます。トンネルは仮想インターフェイスとして実装され、簡単なインターフェイスを設定できるようになっています。トンネル インターフェイスは、特定の「パッセンジャ」プロトコルまたは「トランスポート」プロトコルに関連付けられるのではなく、任意の標準的なポイントツーポイント カプセル化スキームを実装するために必要なサービスを提供するアーキテクチャです。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「[トンネルの実装に関する機能情報](#)」(P.38) を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

目次

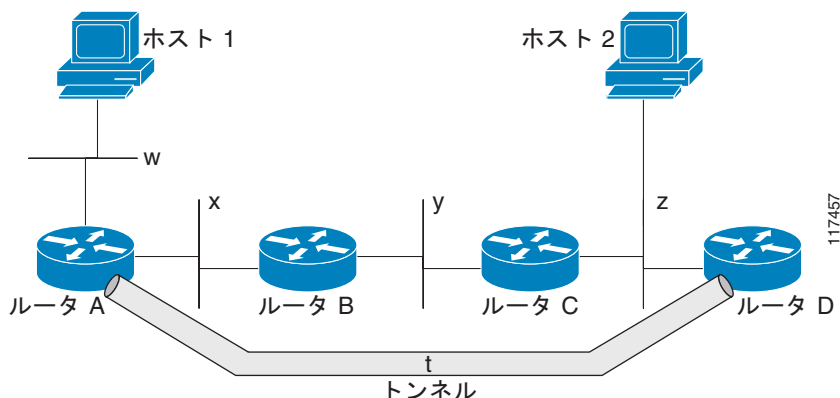
- 「トンネル実装の制約事項」(P.2)
- 「トンネルの実装に関する情報」(P.3)
- 「トンネルの実装方法」(P.12)
- 「トンネル実装の設定例」(P.29)
- 「その他の参考資料」(P.35)
- 「トンネルの実装に関する機能情報」(P.38)

トンネル実装の制約事項

- トンネルプロトコルがファイアウォールを通過でき、Access Control List (ACL; アクセスコントロールリスト) のチェックに合格できるようにすることが重要です。
- トンネルインターフェイスで帯域幅が正しく設定されていない場合、複数のポイントツーポイントトンネルがルーティング情報を使用して物理リンクを飽和させるおそれがあります。
- トンネルはシングルホップに似ているので、ルーティングプロトコルはマルチホップ物理パスよりもトンネルを優先することがあります。ただし、このことはトンネルがシングルホップに似ているとはいえ、マルチホップリンクよりもスピードの遅いパスを通過する場合がありますため、誤りを招くおそれがあります。トンネルは、実際に通過するリンクのように、堅牢で速いこともあれば、信頼性が低く遅いこともあります。ホップカウントのみに基づいて決定するルーティングプロトコルでは、一連の物理リンクよりもトンネルを優先することが多くなります。トンネルはワンホップのポイントツーポイントリンクであり、最もコストの低いパスのように思われますが、実際には、もう1つの選択肢である物理トポロジよりも遅延に関して高コストである可能性があります。

たとえば図 1 に示すトポロジでは、ホスト 1 からのパケットは、パス w、x、y、および z ではなく、トンネルホップカウントがより短いと思われるネットワーク w、t、および z を通ってホスト 2 に到達します。実際には、トンネルを通過するパケットは、ルータ A、B、および C を通って移動しますが、ルータ D まで移動してからルータ C に戻る必要があります。

図 1 トンネルに関する注意事項：ホップカウント



- ルーティングを慎重に設定しなければ、トンネルで再帰ルーティングの問題が発生する可能性があります。「トンネルの宛先」への最適なパスがトンネル自体を経由する場合、再帰ルーティングが原因でトンネルインターフェイスがフラップします。再帰ルーティングの問題を回避するには、次の方法を使用して、コントロールプレーンルーティングとトンネルルーティングを分離します。
 - 異なる自律システム番号またはタグを使用する。
 - 異なるルーティングプロトコルを使用する。
 - スタティックルートを使用して最初のホップを無効にする（ただし、ルーティングループには注意する）。

トンネルの宛先に対する再帰ルーティングが発生した場合は、次のエラーが表示されます。

```
%TUN-RECURDOWN Interface Tunnel 0
temporarily disabled due to recursive routing
```

トンネルの実装に関する情報

トンネルを設定するには、次の概念について理解しておく必要があります。

- 「トンネリングとカプセル化」(P.3)
- 「Tunnel ToS」(P.4)
- 「総称ルーティング カプセル化」(P.4)
- 「EoMPLS over GRE」(P.5)
- 「IPv6 向けオーバーレイ トンネル」(P.8)
- 「手動設定された IPv6 トンネル」(P.10)
- 「自動 6to4 トンネル」(P.10)
- 「ISATAP トンネル」(P.10)
- 「Path MTU Discovery (PMTUD)」(P.11)
- 「トンネル用 QoS オプション」(P.12)

トンネリングとカプセル化

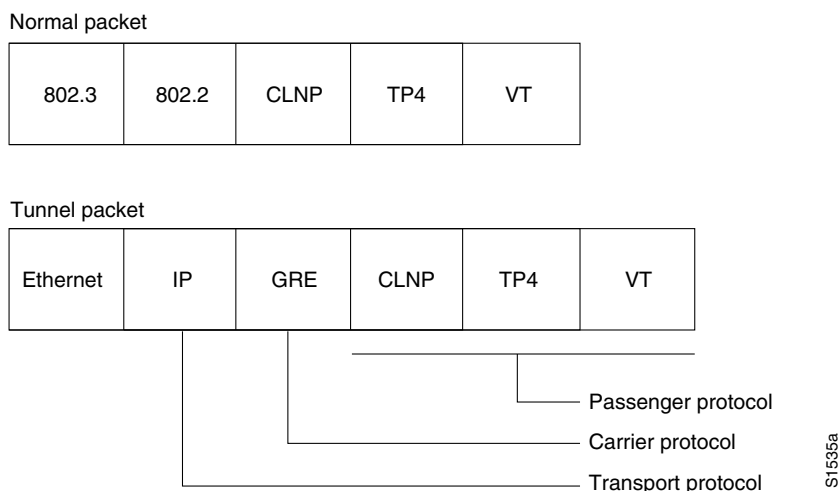
トンネルの動作のしくみを理解するためには、カプセル化とトンネリングの概念を区別することが重要です。カプセル化は、特定のプロトコルスタックの各レイヤでデータにヘッダーを追加するプロセスです。Open Systems Interconnection (OSI) リファレンスモデルは、それぞれのレイヤの上にレイヤが積み重なった7つのレイヤとしてネットワークの機能を説明しています。データがネットワーク上のホスト(たとえばPC)から別のホストに送信される場合、カプセル化のプロセスが使用されて、降順に並んでいる各プロトコルスタックレイヤのデータの先頭にヘッダーが追加されます。ヘッダーには、現在のレイヤのすぐ上のレイヤでカプセル化されているデータのタイプを示すデータフィールドが含まれている必要があります。パケットがネットワークの受信側のプロトコルスタックを上っていくにつれて、各カプセル化ヘッダーは逆の順番で削除されます。

トンネリングは、異なるプロトコル内の1つのプロトコルからデータパケットをカプセル化し、データパケットを変更することなく外部ネットワークを通じて送信します。トンネリングはカプセル化とは異なり、トンネルを経由してより低いレイヤのプロトコルまたは同じレイヤのプロトコルを送信できます。トンネルインターフェイスは、仮想(または論理)インターフェイスです。さまざまなネットワークの問題を解決するために多くのタイプのトンネルが作成されていますが、トンネリングは、次の3つの主要コンポーネントで構成されています。

- パッセンジャプロトコル: カプセル化の対象となるプロトコル。パッセンジャプロトコルの例は、IPv4 および IPv6 です。
- キャリアプロトコル: カプセル化を実行するプロトコル。キャリアプロトコルの例は、Generic Routing Encapsulation (GRE; 総称ルーティングカプセル化) および Multiprotocol Label Switching (MPLS; マルチプロトコルラベルスイッチング) です。
- トランスポートプロトコル: カプセル化されたプロトコルの送信に使用されるプロトコル。主なトランスポートプロトコルは、IP です。

図 2 に IP トンネリングの用語と概念を示します。

図 2 IP トンネリングの用語と概念



Tunnel ToS

Tunnel Type of Service (ToS; タイプ オブ サービス) では、ネットワーク トラフィックをトンネリングし、すべてのパケットを同一の特定の ToS バイト値にグループ化できます。ToS バイト値および Time-to-Live (TTL) ホップカウント値は、ルータ上の IP トンネル インターフェイス向けにトンネルパケットのカプセル化 IP ヘッダーで設定されます。Tunnel ToS 機能は、Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング)、ファスト スイッチング、およびプロセス スイッチングでサポートされています。

ToS バイト値および TTL バイト値は、RFC 791 で定義されています。RFC 791 で定義されているように、RFC 2474 および RFC 2780 では ToS バイト値の使用を廃止しました。RFC 791 では、ToS バイトのビット 6 および 7 (最初の 2 つの最下位ビット) は将来使用するために予約されており、0 に設定する必要がありますが指定されています。Cisco IOS XE Release 2.1 では、Tunnel ToS 機能はこの標準に準拠していません。ビット 6 および 7 を含むすべての ToS バイト値を設定し、パケットの ToS バイトが準拠する RFC 標準を決定できるようになっています。

総称ルーティング カプセル化

Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) は、RFC 2784 で定義されています。GRE はキャリア プロトコルです。さまざまな基盤となるトランスポート プロトコルと共に使用でき、各種のパッセンジャ プロトコルを伝送できます。RFC 2784 は、トランスポート プロトコルおよびパッセンジャ プロトコルとして、GRE と IPv4 の併用についても記述しています。Cisco IOS XE ソフトウェアは、次のようにさまざまな組み合わせのパッセンジャ プロトコルおよびトランスポート プロトコルと共に使用するキャリア プロトコルとして GRE をサポートしています。

- GRE を IPv4 ネットワーク上で使用 (GRE/IPv4) : GRE はキャリア プロトコル、IPv4 はトランスポート プロトコルです。これは、最も一般的なタイプの GRE トンネルです。設定の詳細については、「[GRE トンネルの設定](#)」(P.14) を参照してください。Cisco IOS XE ソフトウェアは、AppleTalk、IPX、IPv4、IPv6 など GRE/IPv4 向けの多くのパッセンジャ プロトコルをサポートしています。GRE/IPv4 で使用するパッセンジャ プロトコルとしての IPv6 の詳細については、「[IPv6 トラフィックに対する GRE/IPv4 トンネルのサポート](#)」(P.5) を参照してください。

- GRE を IPv6 ネットワーク上で使用 (GRE/IPv6) : GRE はキャリア プロトコル、IPv6 はトランスポート プロトコルです。Cisco IOS XE ソフトウェアは、GRE/IPv6 で使用するパッセンジャ プロトコルとして IPv4 および IPv6 をサポートしています。GRE/IPv6 で使用するパッセンジャ プロトコルとしての IPv4 および IPv6 の設定の詳細については、「GRE/IPv6 トンネルの設定」(P.18) を参照してください。

GRE トンネルについては、次の各項を参照してください。

- 「GRE トンネルの IP 送信元および宛先の VRF メンバーシップ」(P.5)
- 「IPv6 トラフィックに対する GRE/IPv4 トンネルのサポート」(P.5)

GRE トンネルの IP 送信元および宛先の VRF メンバーシップ

GRE トンネルの IP 送信元および宛先の VRF メンバーシップ機能では、トンネルの送信元および宛先が任意の Virtual Private Network (VPN; バーチャルプライベートネットワーク) Routing and Forwarding (VRF; VPN ルーティングおよび転送) テーブルに属するように設定できます。VRF テーブルは、各 VPN のルーティング データを保存します。VRF テーブルは、Network Access Server (NAS; ネットワーク アクセス サーバ) に接続されるカスタマー サイトの VPN メンバーシップを定義します。各 VRF テーブルは、IP ルーティング テーブル、生成された CEF テーブル、およびルーティング テーブルに含まれる情報を制御するガイドラインとプロトコル パラメータで構成されます。

Cisco IOS XE Release 2.2 よりも前の GRE IP トンネルでは、IP トンネルの宛先がグローバル ルーティング テーブルに含まれている必要がありました。この機能を実装することにより、トンネルの送信元および宛先が任意の VRF に属するように設定できます。トンネルの宛先へのルートが定義されていない場合、トンネルは、既存の GRE トンネルと同様にディセーブルになります。

IPv6 トラフィックに対する GRE/IPv4 トンネルのサポート

IPv6 トラフィックは、標準的なポイントツーポイントのカプセル化スキームの実装に必要なサービスを提供するように設計されている標準 GRE トンネリング技術を使用して、IPv4 GRE トンネルを介して伝送できます。IPv6 を手動設定したトンネルと同様、GRE トンネルは、各リンクに個別のトンネルを持つ 2 つのポイント間のリンクです。トンネルは、特定のパッセンジャ プロトコルまたはトランスポート プロトコルに関連付けられてはいませんが、この場合は IPv6 はパッセンジャ プロトコル、GRE はキャリア プロトコル、IPv4 はトランスポート プロトコルです。

GRE トンネルの主な用途は、2 つのエッジルータ間またはエッジルータとエンドシステムの間標準的でセキュアな通信を必要とする、安定した接続状態を確保することです。エッジルータとエンドシステムは、デュアル スタック実装にする必要があります。

GRE には、パッセンジャ プロトコルを識別するプロトコル フィールドがあります。GRE トンネルでは、Intermediate System to Intermediate System (IS-IS) または IPv6 をパッセンジャ プロトコルとして指定でき、IS-IS トラフィックと IPv6 トラフィックをともに同じトンネルを介して送出できます。GRE にプロトコル フィールドがない場合、トンネルが IS-IS または IPv6 のどちらの packets を伝送しているかを区別することはできません。つまり、GRE プロトコル フィールドを使用することで、GRE 内で IS-IS および IPv6 をトンネリングできるようになります。

EoMPLS over GRE

Ethernet over MPLS (EoMPLS) は、レイヤ 3 の MPLS ネットワークを経由したレイヤ 2 トラフィックのトンネリングを可能にするトンネリング メカニズムです。EoMPLS はレイヤ 2 トンネリングとしても知られています。

EoMPLS は、レイヤ 2 の長距離拡張を効果的に促進します。EoMPLS over GRE は、ハードウェアベースのスイッチドトンネルとして GRE トンネルを作成し、GRE トンネル内で EoMPLS をカプセル化できるようにします。GRE 接続が 2 つのコア ルータ間で確立され、MPLS Label Switched Path (LSP; ラベル スwitchドパス) がトンネリングされます。

GRE カプセル化は、転送前に追加されるヘッダー情報を持つパケットを定義するために使用されます。カプセル解除は、パケットが宛先トンネルのエンドポイントに到着したときに追加ヘッダー情報を削除するプロセスです。

パケットが GRE トンネルを経由して転送されると、パケットの先頭に 2 つの新しいヘッダーが追加されます。したがって、新しいペイロードの内容は変更されます。カプセル化が行われると、元のデータペイロードおよび独立した IP ヘッダーが GRE ペイロードとなります。GRE ヘッダーはパケットに追加されて、プロトコルタイプに関する情報を提供します。再計算されたチェックサムに関する情報も提供します。新しい IP ヘッダーは、GRE ヘッダーの先頭にも追加されます。この IP ヘッダーには、トンネルの宛先 IP アドレスが含まれます。

GRE ヘッダーは、ヘッダーがトンネルに入る前に IP、L2VPN、L3VPN などのパケットに追加されます。カプセル化されたパケットを受信する、パス沿いにあるすべてのルータは、新しい IP ヘッダーを使用してトンネル エンドポイントへのパケットの到達方法を決定します。

IP 転送では、新しい IP ヘッダーおよび GRE ヘッダーがトンネルの宛先エンドポイントに到着すると、これらのヘッダーはパケットから削除され、元の IP ヘッダーが使用されて最終の宛先にパケットが転送されるようになります。

EoMPLS over GRE 機能は、トンネルの宛先でパケットから新しい IP ヘッダーおよび GRE ヘッダーを削除し、MPLS ラベルを使用して適切なレイヤ 2 接続回線またはレイヤ 3 VRF へとパケットを転送します。

次の項のシナリオでは、Provider Edge (PE; プロバイダー エッジ) またはプロバイダー (P) ルータでの GRE 展開における L2VPN および L3VPN について説明します。

- [PE to PE GRE トンネル](#)
- [P to P GRE トンネル](#)
- [PE to P GRE トンネル](#)

PE to PE GRE トンネル

PE to PE GRE トンネルのシナリオでは、ユーザは、通常、コアのどの部分も MPLS に移行させてはいませんが、EoMPLS および基本的な MPLS VPN サービスの提供を希望しています。したがって、MPLS ラベル付きトラフィックの GRE トンネリングは、PE 間で実行されます。これは、ユーザのネットワークで使用される最も一般的なシナリオです。

P to P GRE トンネル

P to P GRE トンネルのシナリオは、MPLS が PE ルータと P ルータとの間でイネーブルになっているものの、ネットワーク コアに MPLS 対応ルータまたは IP 暗号化ボックスが存在しないというシナリオです。このシナリオでは、MPLS ラベル付きパケットの GRE トンネリングは IP ルータ間で実行されます。

PE to P GRE トンネル

PE to P GRE トンネルのシナリオでは、P to P ノードは MPLS 対応ですが、その一方で GRE トンネリングが PE to P 非 MPLS ネットワーク セグメントの間で実行されるネットワークです。

上記のシナリオを展開するには、次のリストに示される機能が必要です。

GRE に固有の機能

- トンネル エンドポイントは、ループバック インターフェイスまたは物理インターフェイス
- キープアライブ タイマーの期限が切れると、エンドポイント単位で設定可能なトンネルのキープアライブ タイマー パラメータおよび Syslog メッセージを生成
- トンネル障害およびトンネルを使用した Interior Gateway Protocol (IGP) に対する Bidirectional Forwarding Detection (BFD; 双方向フォワーディング検出) のサポート
- GRE トンネル全体における IGP ロード シェアリングのサポート
- GRE トンネル全体における IGP 冗長性のサポート
- GRE トンネル全体におけるフラグメンテーションのサポート
- ジャンボ フレーム通過機能のサポート
- すべての IGP コントロールプレーン トラフィックのサポート
- トンネル全体における IP ToS 保存のサポート
- トンネルは、ATM、Gig、Packet over SONET (POS)、TenGig などエンドポイントの物理インターフェイス タイプとは無関係
- 最大 100 の GRE トンネルのサポート

EoMPLS に固有の機能

- ポート モードの EoMPLS
- VLAN モードの EoMPLS
- 擬似配線の冗長性
- Any Transport over MPLS (AToM) シーケンス
- トンネル選択および特定の擬似配線を GRE トンネルにマップする機能
- IGP ロード シェアリングおよび冗長性
- 最大 200 の EoMPLS Virtual Circuit (VC; 仮想回線) のサポート

MPLS VPN に固有の機能

- IPv4 VRF での PE ロールのサポート
- すべての PE to Customer Edge (CE; カスタマー エッジ) プロトコルのサポート
- 複数のトンネルを経由したロード シェアリングおよび単一トンネルと等コストの IGP パス
- 単一トンネルと非等コストの IGP パスによる冗長性のサポート
- MPLS ラベルの expression (EXP) ビット フィールドにコピーされてから、GRE パケットの外部 IPv4 ToS フィールドの precedence ビットにコピーされる IP precedence 値のサポート

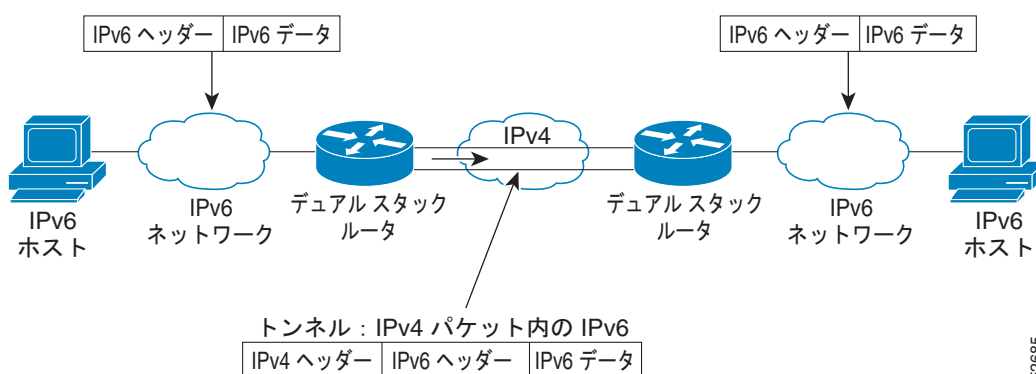
EoMPLS over GRE の設定シーケンスの例については、「[EoMPLS over GRE の設定 : 例](#)」(P.31) の項を参照してください。EoMPLS over GRE の詳細については、『[Deploying and Configuring MPLS Virtual Private Networks In IP Tunnel Environments](#)』を参照してください。

IPv6 向けオーバーレイ トンネル

オーバーレイ トンネリングでは、IPv4 パケット内で IPv6 パケットをカプセル化して、IPv4 インフラストラクチャ（コア ネットワークまたはインターネット）へ伝送します（図 3 を参照）。オーバーレイ トンネルを使用することで、独立した IPv6 ネットワークとの間で IPv4 インフラストラクチャをアップグレードしなくても、そのネットワークと通信できます。オーバーレイ トンネルは、境界ルータ間または境界ルータとホストの間で設定できますが、トンネルのエンドポイントがともに IPv4 プロトコルスタックおよび IPv6 プロトコルスタックを両方ともサポートしていることが必要となります。Cisco IOS XE IPv6 は現在、次のタイプのオーバーレイ トンネリング メカニズムをサポートしています。

- 6to4
- 総称ルーティング カプセル化
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- IPv4 互換
- 手動

図 3 オーバーレイ トンネル



(注)

オーバーレイ トンネルにより、インターフェイスの Maximum Transmission Unit (MTU; 最大伝送ユニット) が 20 オクテット減少します（ただし、基本 IPv4 パケット ヘッダーにオプション フィールドが含まれていないことを前提とします）。オーバーレイ トンネルを使用するネットワークは、トラブルシューティングが困難です。したがって、独立した IPv6 ネットワークに接続するオーバーレイ トンネルは、最終的な IPv6 ネットワーク アーキテクチャと見なしてはいけません。オーバーレイ トンネルの使用は、IPv4 プロトコルスタックおよび IPv6 プロトコルスタックの両方、または IPv6 プロトコルスタックだけをサポートするネットワークに対する過渡的な技術と考える必要があります。

表 1 を使用して、IPv4 ネットワークを介して IPv6 パケットを伝送するために設定するトンネルのタイプを決定します。

表 1 IPv4 ネットワークを介して IPv6 パケットを伝送する際の推奨されるトンネル タイプの使用方
法

トンネリング のタイプ	推奨される使用方法	使用方法に関する注釈
6to4	独立した IPv6 サイトへの接続に使用可能なポイントツーマルチポイント トンネル。	サイトは、プレフィクス 2002::/16 を使用します。
GRE/IPv4	サイト内またはサイト間で使用可能な単純なポイントツーポイント トンネル。	トンネルは、IPv6、CLNS、およびその他多数のパケット タイプを伝送可能です。
ISATAP	サイト内のシステム間の接続に使用可能なポイントツーマルチポイント トンネル。	サイトは任意の IPv6 ユニキャスト アドレスを使用できます。
手動	サイト内またはサイト間で使用可能な単純なポイントツーポイント トンネル。	トンネルは、IPv6 パケットのみ伝送可能です。

個々のトンネル タイプについては以降で詳しく説明します。シスコは、ユーザが実装を希望する特定のトンネル タイプについての情報を確認して理解することを推奨します。必要なトンネルのタイプについて十分理解できたら、表 2 のトンネル設定パラメータの概要を参照して役に立つ情報を確認してください。

表 2 トンネリング タイプ別オーバーレイ トンネルの設定パラメータ

オーバーレイ トンネリング タイプ	オーバーレイ トンネルの設定パラメータ			
	トンネル モード	トンネルの送信元	トンネルの宛先	インターフェイスのプレフィクス/アドレス
6to4	ipv6ip 6to4	IPv4 アドレスまたは IPv4 が設定されているインターフェイスのリファレンス	不要。これらは、すべてポイントツーマルチポイント トンネリング タイプです。IPv4 の宛先アドレスは、パケット単位で IPv6 の宛先から算出されます。	IPv6 アドレス。プレフィクスは、トンネル送信元の IPv4 アドレスを埋め込む必要があります。
GRE/IPv4	gre ip		IPv4 アドレス。	IPv6 アドレス。
ISATAP	ipv6ip isatap		不要。これらは、すべてポイントツーマルチポイント トンネリング タイプです。IPv4 の宛先アドレスは、パケット単位で IPv6 の宛先から算出されます。	eui-64 修正版 IPv6 形式のプレフィクス。IPv6 アドレスは、プレフィクスおよびトンネル送信元の IPv4 アドレスから生成されます。
手動	ipv6ip		IPv4 アドレス。	IPv6 アドレス。

手動設定された IPv6 トンネル

手動設定されたトンネルは、IPv4 バックボーン上の 2 つの IPv6 ドメイン間の固定リンクと同等です。主な用途は、2 つのエッジルータ間またはエンド システムとエッジルータの間に標準的でセキュアな通信を必要とする、安定した接続状態を確保したり、リモートの IPv6 ネットワークへ接続したりすることです。

IPv6 アドレスはトンネル インターフェイスで手動で設定します。また、手動設定された IPv4 アドレスはトンネルの送信元および宛先に割り当てられます。手動設定されたトンネルの両端のホストまたはルータは、IPv4 プロトコル スタックおよび IPv6 プロトコル スタックをサポートする必要があります。手動設定されたトンネルは、境界ルータ間または境界ルータとホストの間で設定できます。CEF スイッチングは、手動設定された IPv6 トンネルに使用できます。または、プロセス スイッチングが必要な場合は、CEF スイッチングをディセーブルにできます。

自動 6to4 トンネル

自動 6to4 トンネルにより、独立した IPv6 ドメインを IPv4 ネットワークを介してリモートの IPv6 ネットワークへ接続できます。自動 6to4 トンネルと手動設定されたトンネルとの主な違いは、トンネルがポイントツーポイントではなく、ポイントツーマルチポイントであることです。自動 6to4 トンネルでは、ルータは IPv4 インフラストラクチャを仮想 NonBroadcast MultiAccess (NBMA; 非ブロードキャスト マルチアクセス) リンクとして処理するため、ペアでは設定されません。IPv6 アドレスに埋め込まれている IPv4 アドレスは、自動トンネルのもう一端を検索するのに使用されます。

自動 6to4 トンネルは、独立した IPv6 ネットワーク内の境界ルータ上で設定できます。これにより、IPv4 インフラストラクチャ上の別の IPv6 ネットワーク内の境界ルータへのトンネルがパケット単位で作成されます。トンネルの宛先は、IPv6 アドレスから抽出された境界ルータの IPv4 アドレスによって決定され、プレフィクス 2002::/16 で始まる、2002:router-IPv4-address::/48 という形式になります。埋め込まれた IPv4 アドレスの後に 16 ビットが続き、サイト内のネットワークに番号付けするのに使用できます。6to4 トンネルの各終端の境界ルータは、IPv4 プロトコル スタックおよび IPv6 プロトコル スタックの両方をサポートする必要があります。6to4 トンネルは、境界ルータ間または境界ルータとホストの間で設定されます。

6to4 トンネルの最も単純な展開シナリオは、複数の IPv6 サイトに相互接続し、各サイトに共有 IPv4 ネットワークへの接続を少なくとも 1 つ設定することです。この IPv4 ネットワークは、グローバルインターネットまたは企業バックボーンである可能性があります。主な要件は、各サイトがグローバルに一意的な IPv4 アドレスを持つことです。Cisco IOS XE ソフトウェアはこのアドレスを使用して、グローバルに一意的な 6to4/48 IPv6 プレフィクスを作成します。他のトンネルメカニズムと同様に、IPv4 および IPv6 の両方に対してホスト名と IP アドレスとの間のマッピングを行う Domain Name System (DNS; ドメインネーム システム) 内の対応するエントリにより、アプリケーションは必要なアドレスを選択できます。

ISATAP トンネル

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) は、基盤となる IPv4 ネットワークを IPv6 に対する NBMA リンク層として使用する、自動オーバーレイ トンネリングメカニズムです。ISATAP は、ネイティブの IPv6 インフラストラクチャがまだ使用可能になっていない（希薄 IPv6 ホストがテスト用に展開されている場合などの）サイト内の IPv6 パケットを転送することを目的として設計されています。ISATAP トンネルにより、サイト内の個々の IPv4/IPv6 デュアルスタック ホストが同じ仮想リンク上の他のホストと通信でき、基本的に IPv4 インフラストラクチャを使用して IPv6 ネットワークを作成できます。

ISATAP ルータでは、ISATAP サイトに対して標準的なルータ アドバタイズメント ネットワーク設定がサポートされます。この機能により、クライアントは、イーサネットに接続した場合に行うと思われる設定をクライアント自身に自動的に実行できます。また、サイト外で接続を行えるよう設定することもできます。ISATAP は、任意のユニキャスト IPv6 プレフィクス (/64) で構成される明確な IPv6 アドレス形式を使用します。この形式は、リンクローカルまたはグローバル (6to4 プレフィクスを含む) にすることができ、IPv6 ルーティングをローカルまたはインターネットでイネーブルにできます。IPv4 アドレスは IPv6 アドレスの最後の 32 ビットで符号化され、自動 IPv6-in-IPv4 トンネリングをイネーブルにします。

ISATAP トンネリング メカニズムは他の自動トンネリング メカニズム (IPv6 6to4 トンネリングなど) と同様ですが、ISATAP はサイト間ではなく、サイト内の IPv6 パケットを転送するよう設計されています。

ISATAP は、64 ビットの IPv6 プレフィクスおよび 64 ビットのインターフェイス識別子を含むユニキャストアドレスを使用します。インターフェイス識別子は、修正版 EUI-64 形式で作成され、この形式では、最初の 32 ビットにはこのアドレスが IPv6 ISATAP アドレスであることを示す 000:5EFE という値が含まれます。表 3 に、ISATAP アドレスのレイアウトを示します。

表 3 ISATAP アドレスの例

64 ビット	32 ビット	32 ビット
リンク ローカルまたはグローバル IPv6 ユニキャストプレフィクス	0000:5EFE	ISATAP リンクの IPv4 アドレス

表 3 に示すとおり、ISATAP アドレスは IPv6 プレフィクスおよび ISATAP インターフェイス識別子で構成されます。このインターフェイス識別子には、基盤となる IPv4 リンクの IPv4 アドレスが含まれます。プレフィクスが 2001:0DB8:1234:5678::/64 で、埋め込まれた IPv4 アドレスが 10.173.129.8 の場合、実際の ISATAP アドレスがどのようなようになるかを次の例に示します。ISATAP アドレスでは、IPv4 アドレスは 0AAD:8108 のような 16 進数として表現されます。

2001:0DB8:1234:5678:0000:5EFE:0AAD:8108

Path MTU Discovery (PMTUD)

Path MTU Discovery (PMTUD) は、GRE または IP-in-IP トンネル インターフェイスでイネーブルにできます。トンネル インターフェイスで PMTUD (RFC 1191) がイネーブルの場合、ルータは GRE (または IP-in-IP) トンネル IP パケットに対して PMTUD 処理を実行します。ルータは、トンネルに入ってくる元のデータの IP パケットに対して常に PMTUD 処理を実行します。PMTUD がイネーブルの場合、Don't Fragment (DF) ビットがすべてのパケットに設定されるため、トンネルを通過するパケットに対してはパケットのフラグメンテーションは許可されません。トンネルに入ったパケットがそのパケットの MTU 値よりも小さい MTU 値を持つリンクを検出すると、パケットは廃棄され、パケットの送信元に Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) メッセージが返されます。このメッセージは、フラグメンテーションが要求されたこと (しかし許可されなかったこと) およびパケットが廃棄される原因となったリンクの MTU を示します。



(注)

トンネル インターフェイスの PMTUD は、トンネル エンドポイントがトンネルのパスでルータによって生成される ICMP メッセージを受信できることを要求します。ファイアウォール接続を通じて PMTUD を使用する前に、ICMP メッセージが受信できることを確認してください。

トンネルのパケットに対して PMTUD をイネーブルにするには、**tunnel path-mtu-discovery** コマンドを使用し、トンネルの PMTUD パラメータを確認するには、**show interfaces tunnel** コマンドを使用します。PMTUD が動作するトンネル インターフェイスは現在、GRE および IP-in-IP だけです。

トンネル用 QoS オプション

トンネル インターフェイスは、物理インターフェイスと同じ多数の Quality of Service (QoS) 機能をサポートします。QoS により、ミッションクリティカルなトラフィックのパフォーマンスを確実に受け入れ可能なレベルにする方法が提供されます。トンネル用 QoS オプションでサポートされる項目には、**Generic Traffic Shaping (GTS; ジェネリック トラフィック シェーピング)** のトンネル インターフェイスへの直接適用や、**Modular QoS Command-Line Interface (MQC; モジュラ QoS コマンドライン インターフェイス)** を使用したクラスベースのシェーピングなどが含まれます。またトンネル インターフェイスは、クラスベースのポリシングもサポートしますが、**Committed Access Rate (CAR; 専用アクセス レート)** はサポートしません。

GRE トンネルでは、ルータは、ToS バイトの IP precedence ビット値をトンネルまたは内部パケットをカプセル化している GRE IP ヘッダーにコピーできます。トンネルのエンドポイント間の中間ルータは、IP precedence 値を使用して、QoS 機能 (ポリシー ルーティング、**Weighted Fair Queuing (WFQ; 重み付け均等化キューイング)**、**Weighted Random Early Detection (WRED; 重み付けランダム早期検出)** など) 向けにパケットを分類できます。

トンネルまたは暗号化ヘッダーによってパケットがカプセル化されている場合、QoS 機能は元のパケットのヘッダーを調べてパケットを正しく分類することができません。同じトンネルを通過するパケットは、同じトンネルヘッダーを持つため、物理インターフェイスが輻輳している場合、パケットは同等に扱われます。ただしトンネルのパケットは、トンネリング前に分類でき、QoS の事前分類機能を使用することで、トンネル インターフェイス上またはクリプト マップ上で暗号化を行うことができます。



(注)

クラスベースのシェーピング内の **Class-based WFQ (CBWFQ; クラスベース WFQ)** は、マルチポイント インターフェイスではサポートされません。

トンネル インターフェイスでの一部の QoS 機能の実装方法の例については、「[トンネル インターフェイスにおける QoS オプションの設定 : 例](#)」(P.34) を参照してください。

トンネルの実装方法

ここでは、次の作業について説明します。

- 「[トンネル タイプの決定](#)」(P.13) (必須)
- 「[GRE トンネルの設定](#)」(P.14) (任意)
- 「[GRE/IPv6 トンネルの設定](#)」(P.18) (任意)
- 「[GRE トンネルの IP 送信元および宛先の VRF メンバーシップの設定](#)」(P.20) (任意)
- 「[IPv6 トンネルの手動設定](#)」(P.21) (任意)
- 「[6to4 トンネルの設定](#)」(P.23) (任意)
- 「[ISATAP トンネルの設定](#)」(P.25) (任意)
- 「[トンネルの設定と動作の確認](#)」(P.27) (任意)

トンネル タイプの決定

トンネルを設定する前に、作成するトンネルのタイプを決定する必要があります。

手順の概要

- パッセンジャ プロトコルを決定します。
- 必要に応じて、**tunnel mode** コマンド キーワードを決定します。

手順の詳細

1. パッセンジャ プロトコルを決定します。パッセンジャ プロトコルとは、カプセル化の対象となるプロトコルです。
2. 必要に応じて、**tunnel mode** コマンド キーワードを決定します。

表 4 に、**tunnel mode** コマンドで使用する適切なキーワードを決定する方法を示します。次の作業では、**tunnel mode** コマンドに関連するキーワードだけが示されます。

- GRE/IPv6 トンネルの設定
- 手動 IPv6 トンネルの設定
- 6to4 トンネルの設定
- ISATAP トンネルの設定

表 4 トンネル モードのコマンド キーワードの決定

キーワード	目的
dvmrp	ディスタンス ベクトル マルチキャストルーティング プロトコルのカプセル化の使用を指定するには、 dvmrp キーワードを使用します。
gre ip	IP での GRE カプセル化の使用を指定するには、 gre ip キーワードを使用します。
gre ipv6	IPv6 での GRE カプセル化の使用を指定するには、 gre ipv6 キーワードを使用します。
ipip [decapsulate-any]	IP-in-IP カプセル化の使用を指定するには、 ipip キーワードを指定します。オプションの decapsulate-any キーワードは、あるトンネル インターフェイスの任意の数の IP-in-IP トンネルを終了させます。このトンネルは発信トラフィックを伝送しませんが、任意の数のリモート トンネル エンドポイントは、このように設定されたトンネルを宛先として使用できることに注意してください。
ipv6	IPv6 での汎用パケット トンネリングの使用を指定するには、 ipv6 キーワードを使用します。

表 4 トンネル モードのコマンド キーワードの決定 (続き)

キーワード	目的
ipv6ip	IPv6 をパッセンジャ プロトコルとして使用し、IPv4 をキャリア (カプセル化) プロトコルおよびトランスポート プロトコルの両方として使用することを指定するには、 ipv6ip キーワードを使用します。追加のキーワードを使用しない場合は、手動 IPv6 トンネルが設定されます。追加のキーワードを使用して、IPv4 互換、6to4、または ISATAP の各トンネルを指定できます。
mpls	Traffic Engineering (TE; トラフィック エンジニアリング) トンネルの設定に MPLS の使用を指定するには、 mpls キーワードを使用します。

次の作業

- IP データ パケットを伝送するようにトンネルを設定するには、「GRE トンネルの設定」(P.14)に進みます。
- IPv6 データ パケットを伝送するようにトンネルを設定するには、「IPv6 向けオーバーレイ トンネル」(P.8)を確認し、次の作業のいずれかに進みます。
 - 「GRE/IPv6 トンネルの設定」(P.18)
 - 「IPv6 トンネルの手動設定」(P.21)
 - 「6to4 トンネルの設定」(P.23)
 - 「ISATAP トンネルの設定」(P.25)

GRE トンネルの設定

GRE トンネルを設定するには、次の作業を実行します。トンネル インターフェイスを使用して、通常プロトコルをサポートしないネットワークへプロトコル トラフィックを通過させます。トンネルを構築するには、トンネル インターフェイスを 2 つのルータそれぞれで定義し、そのトンネル インターフェイスが互いを参照する必要があります。各ルータでは、トンネル インターフェイスはレイヤ 3 アドレスを使用して設定する必要があります。トンネルのエンドポイント、トンネル送信元、およびトンネル宛先を定義して、トンネルのタイプを選択する必要があります。オプションの手順を実行して、トンネルをカスタマイズできます。

必ずトンネルの両側にルータを設定するようにしてください。トンネルの片側だけが設定されている場合、(キープアライブが設定されていない限り) トンネル インターフェイスはアップした状態になっていますが、トンネルに入ったパケットは廃棄されます。

GRE トンネル キープアライブ

キープアライブ パケットは、IP カプセル化された GRE トンネルを介して送信されるよう設定できます。キープアライブが送信されるレートと、インターフェイスが非アクティブになるまでデバイスが応答なしでキープアライブ パケットの送信を続行する回数を指定できます。GRE キープアライブ パケットは、トンネルの両側または片側のみのどちらからでも送信できます。

前提条件

この作業でトンネルの送信元として使用する物理インターフェイスがアップしており、適切な IP アドレスを使用して設定されていることを確認します。ハードウェアの技術的説明およびインターフェイスの取り付けに関する情報については、ご使用の製品のハードウェアの取り付けおよび設定に関するマニュアルを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **bandwidth kb/s**
5. **keepalive [period [retries]]**
6. **tunnel source {ip-address | interface-type interface-number}**
7. **tunnel destination {hostname | ip-address}**
8. **tunnel key key-number**
9. **tunnel mode {gre ip | gre multipoint}**
10. **ip mtu bytes**
11. **ip tcp mss mss-value**
12. **tunnel path-mtu-discovery [age-timer {aging-mins | infinite}]**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface tunnel 0	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 • トンネルを設定するには、 <i>type</i> 引数に tunnel を使用します。

コマンドまたはアクション	目的
<p>ステップ 4 <code>bandwidth kb/s</code></p> <p>例: Router(config-if)# bandwidth 1000</p>	<p>インターフェイスに対する現在の帯域幅を設定し、上位レベルプロトコルと通信します。パケットの送信に使用されるトンネル帯域幅を指定します。</p> <ul style="list-style-type: none"> 帯域幅をキロビット/秒単位 (kb/s) で設定するには、<i>kb/s</i> 引数を使用します。 <p>(注) これはルーティングパラメータのみのため、物理インターフェイスには影響を及ぼしません。トンネルインターフェイスのデフォルトの帯域幅設定は 9.6 kb/s です。トンネルの帯域幅を適切な値に設定する必要があります。</p>
<p>ステップ 5 <code>keepalive [period [retries]]</code></p> <p>例: Router(config-if)# keepalive 3 7</p>	<p>(任意) トンネルインターフェイスプロトコルがダウン状態になるまで、デバイスが応答なしでキープアライブパケットの送信を続行する回数を指定します。</p> <ul style="list-style-type: none"> GRE キープアライブパケットは、トンネルの片側または両側のどちらでも設定できます。 GRE キープアライブをトンネルの両側で設定した場合、リンクの各側の <i>period</i> 引数および <i>retries</i> 引数は異なる値に設定できます。 <p>(注) このコマンドがサポートされるのは、GRE ポイントツーポイントトンネルだけです。</p> <p>(注) GRE トンネルのキープアライブ機能は、VRF トンネルでは設定しないでください。この組み合わせの機能はサポートされていません。</p>
<p>ステップ 6 <code>tunnel source {ip-address interface-type interface-number}</code></p> <p>例: Router(config-if)# tunnel source GigabitEthernet 0/0/0</p>	<p>トンネルの送信元を設定します。</p> <ul style="list-style-type: none"> 送信元 IP アドレスを指定するには、<i>ip-address</i> 引数を使用します。 使用するインターフェイスを指定するには、<i>interface-type</i> 引数および <i>interface-number</i> 引数を使用します。 <p>(注) トンネルの送信元と宛先の IP アドレスは、2つの個別のデバイス上で定義する必要があります。</p>
<p>ステップ 7 <code>tunnel destination {hostname ip-address}</code></p> <p>例: Router(config-if)# tunnel destination 172.17.2.1</p>	<p>トンネルの宛先を設定します。</p> <ul style="list-style-type: none"> ホストの宛先の名前を指定するには、<i>hostname</i> 引数を指定します。 ホストの宛先の IP アドレスを指定するには、<i>ip-address</i> 引数を指定します。 <p>(注) トンネルの送信元と宛先の IP アドレスは、2つの個別のデバイス上で定義する必要があります。</p>

コマンドまたはアクション	目的
<p>ステップ 8 <code>tunnel key key-number</code></p> <p>例: Router(config-if)# tunnel key 1000</p>	<p>(オプション) トンネルインターフェイスの ID キーをイネーブルにします。</p> <ul style="list-style-type: none"> 各パケットで運ばれるトンネル キーを識別するには、key-number 引数を使用します。 トンネルの ID キーは、強度の劣るセキュリティ形式として使用して、外部ソースからのパケットの不適切な設定や挿入を防止できます。 <p>(注) このコマンドがサポートされるのは、GRE トンネルインターフェイスだけです。セキュリティ目的でこのキーに依存することは推奨しません。</p>
<p>ステップ 9 <code>tunnel mode {gre ip gre multipoint}</code></p> <p>例: Router(config-if)# tunnel mode gre ip</p>	<p>トンネルで使用されるカプセル化プロトコルを指定します。</p> <ul style="list-style-type: none"> IP カプセル化での GRE の使用を指定するには、gre ip キーワードを使用します。 Multipoint GRE (mGRE; マルチポイント GRE) の使用を指定するには、gre multipoint キーワードを使用します。
<p>ステップ 10 <code>ip mtu bytes</code></p> <p>例: Router(config-if)# ip mtu 1400</p>	<p>(任意) 各インターフェイスで送信される IP パケットの MTU サイズを設定します。</p> <ul style="list-style-type: none"> インターフェイスに設定されている MTU を IP パケットが超過した場合、DF ビットが設定されていない場合は、Cisco IOS XE ソフトウェアは IP パケットをフラグメント化します。 物理メディアのすべてのデバイスが動作するには、同じプロトコル MTU が設定されている必要があります。 IPv6 パケットに対しては、ipv6 mtu コマンドを使用します。 <p>(注) ステップ 12 で tunnel path-mtu-discovery コマンドがイネーブルになっている場合は、このコマンドを設定しないでください。</p>
<p>ステップ 11 <code>ip tcp mss mss-value</code></p> <p>例: Router(config-if)# ip tcp mss 250</p>	<p>(任意) ルータ上で開始または終了する TCP 接続に対して、Maximum Segment Size (MSS; 最大セグメントサイズ) を指定します。</p> <ul style="list-style-type: none"> TCP 接続に対する最大セグメントサイズをバイト単位で指定するには、mss-value 引数を使用します。
<p>ステップ 12 <code>tunnel path-mtu-discovery [age-timer {aging-mins infinite}]</code></p> <p>例: Router(config-if)# tunnel path-mtu-discovery</p>	<p>(任意) GRE または IP-in-IP トンネルインターフェイスで Path MTU Discovery (PMTUD) をイネーブルにします。</p> <ul style="list-style-type: none"> トンネルインターフェイスで PMTUD をイネーブルにした場合、PMTUD は GRE IP トンネル パケット用に動作し、トンネル エンドポイント間のパス内のフラグメンテーションを最低限に抑えます。
<p>ステップ 13 <code>end</code></p> <p>例: Router(config-if)# end</p>	<p>インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。</p>

次の作業

「トンネルの設定と動作の確認」(P.27)に進みます。

GRE/IPv6 トンネルの設定

この作業では、IPv6 ネットワーク上での GRE トンネルの設定方法について説明します。GRE トンネルを設定して、IPv6 ネットワーク層を介して実行し、IPv6 トンネルに IPv6 パケットを転送して、IPv6 トンネルに IPv4 パケットを転送できます。

前提条件

GRE/IPv6 トンネルが設定されている場合、IPv6 アドレスはトンネルの送信元および宛先に割り当てられます。トンネル インターフェイスには、IPv4 アドレスまたは IPv6 アドレスのいずれかを割り当てることができます（このことは、以降の作業では示されていません）。手動設定されたトンネルの両端のホストまたはルータは、IPv4 プロトコル スタックおよび IPv6 プロトコル スタックをサポートする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel *tunnel-number***
4. **tunnel source {*ipv6-address* | *interface-type interface-number*}**
5. **tunnel destination *ipv6-address***
6. **tunnel mode gre ipv6**
7. **ipv6 mtu *bytes***
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ2	<code>configure terminal</code> 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>interface tunnel tunnel-number</code> 例： Router(config)# interface tunnel 0	トンネルのインターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	<code>tunnel source {ipv6-address interface-type interface-number}</code> 例： Router(config-if)# tunnel source GigabitEthernet 0/0/0	送信元 IPv6 アドレスまたは送信元のインターフェイス タイプおよびトンネルインターフェイスの番号を指定します。 • インターフェイスのタイプおよび番号が指定されている場合、そのインターフェイスは IPv6 アドレスを使用して設定する必要があります。 (注) このコンテキストで使用される構文だけが表示されます。詳細については、『 Cisco IOS IPv6 Command Reference 』を参照してください。
ステップ5	<code>tunnel destination ipv6-address</code> 例： Router(config-if)# tunnel destination 2001:0DB8:0C18:2::300	トンネル インターフェイスの宛先の IPv6 アドレスを指定します。 (注) このコンテキストで使用される構文だけが表示されます。詳細については、『 Cisco IOS IPv6 Command Reference 』を参照してください。
ステップ6	<code>tunnel mode gre ipv6</code> 例： Router(config-if)# tunnel mode gre ipv6	GRE IPv6 トンネルを指定します。 (注) <code>tunnel mode gre ipv6</code> コマンドは、トンネルのカプセル化プロトコルとして GRE を指定します。
ステップ7	<code>ipv6 mtu bytes</code> 例： Router(config-if)# ipv6 mtu 1400	(任意) 各インターフェイスで送信される IPv6 パケットの MTU サイズを設定します。
ステップ8	<code>end</code> 例： Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

「トンネルの設定と動作の確認」(P.27) に進みます。

GRE トンネルの IP 送信元および宛先の VRF メンバーシップの設定

この作業では、トンネルの送信元および宛先を任意の VRF テーブルに属するように設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel slot**
4. **ip vrf forwarding vrf-name**
5. **ip address ip-address subnet-mask**
6. **tunnel source {ip-address | type number}**
7. **tunnel destination ip-address {hostname | ip-address}**
8. **tunnel vrf vrf-name**

手順の詳細

ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface tunnel slot 例： Router(config)# interface tunnel 0	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip vrf forwarding vrf-name 例： Router(config-if)# ip vrf forwarding vrf1	トンネル インターフェイスに関連付けられる VRF を定義します。
ステップ 5	ip address ip-address subnet-mask 例： Router(config-if)# ip address 10.7.7.7 255.255.255.255	IP アドレスおよびサブネット マスクを指定します。
ステップ 6	tunnel source {ip-address type number} 例： Router(config-if)# tunnel source loopback 0	トンネルの送信元を指定します。

	コマンドまたはアクション	目的
ステップ7	tunnel destination {hostname ip-address} 例： Router(config-if)# tunnel destination 10.5.5.5	トンネルの宛先を定義します。
ステップ8	tunnel vrf vrf-name 例： Router(config-if)# tunnel vrf financel	トンネル パケットの送信元である物理インターフェイスに関連付けられる VRF を定義します。

次の作業

「トンネルの設定と動作の確認」(P.27) に進みます。

IPv6 トンネルの手動設定

この作業では、IPv6 オーバーレイ トンネルの手動設定方法について説明します。

前提条件

IPv6 トンネルを手動で設定した場合、IPv6 アドレスはトンネル インターフェイスで設定されます。また、手動設定された IPv4 アドレスはトンネルの送信元および宛先に割り当てられます。手動設定されたトンネルの両端のホストまたはルータは、IPv4 プロトコル スタックおよび IPv6 プロトコル スタックをサポートする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel tunnel-number**
4. **ipv6 address ipv6-prefix/prefix-length [eui-64]**
5. **tunnel source {ip-address | interface-type interface-number}**
6. **tunnel destination ip-address**
7. **tunnel mode ipv6ip**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	interface tunnel tunnel-number 例： Router(config)# interface tunnel 0	トンネルのインターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	ipv6 address ipv6-prefix/prefix-length [eui-64] 例： Router(config-if)# ipv6 address 2001:0DB8:1234:5678::3/126	インターフェイスに割り当てられる IPv6 ネットワークを指定し、インターフェイスでの IPv6 処理をイネーブルにします。 (注) IPv6 アドレスの設定の詳細は、「 Configuring Basic Connectivity for IPv6 」モジュールを参照してください。
ステップ5	tunnel source {ip-address interface-type interface-number} 例： Router(config-if)# tunnel source GigabitEthernet 0/0/0	送信元 IPv4 アドレスまたは送信元インターフェイス タイプおよびトンネルインターフェイスの番号を指定します。 • インターフェイスが指定されている場合、そのインターフェイスは IPv4 アドレスを使用して設定する必要があります。
ステップ6	tunnel destination ip-address 例： Router(config-if)# tunnel destination 192.168.30.1	トンネルインターフェイスの宛先の IPv4 アドレスを指定します。
ステップ7	tunnel mode ipv6ip 例： Router(config-if)# tunnel mode ipv6ip	手動設定した IPv6 トンネルを指定します。 (注) tunnel mode ipv6ip コマンドは、手動 IPv6 トンネル向けに IPv6 をパッセンジャ プロトコルとして指定し、IPv4 をキャリア (カプセル化) プロトコル およびトランスポート プロトコルの両方として指定します。
ステップ8	end 例： Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

「トンネルの設定と動作の確認」(P.27) に進みます。

6to4 トンネルの設定

この作業では、6to4 オーバーレイ トンネルの設定方法について説明します。

前提条件

6to4 トンネルでは、トンネルの宛先は、境界ルータの IPv4 アドレスによって決定されます。このアドレスは、プレフィクス 2002::/16 と連結されて 2002:border-router-IPv4-address::/48 という形式になります。6to4 トンネルの各終端の境界ルータは、IPv4 プロトコル スタックおよび IPv6 プロトコル スタックの両方をサポートする必要があります。

制約事項

ルータでサポートされる設定は、IPv4 互換トンネルおよび 6to4 IPv6 トンネルそれぞれ 1 つだけです。同じルータで両方のトンネル タイプの設定を選択する場合は、これらが同じ送信元を共有しないようにすることを強く推奨します。

6to4 トンネルと IPv4 互換トンネルが同じインターフェイスを共有できない理由は、これらがともに NBMA「ポイントツーマルチポイント」アクセス リンクであり、多重化されたパケット ストリームを着信インターフェイスの単一パケット ストリームに再度配列するには、トンネルの送信元しか使用できないためです。したがって、IPv4 プロトコル タイプが 41 のパケットがインターフェイスに到着すると、このパケットは IPv4 アドレスに基づいて、IPv6 トンネル インターフェイスにマッピングされます。ただし、6to4 トンネルと IPv4 互換トンネルが同じ送信元インターフェイスを共有している場合、ルータは、着信パケットを割り当てるべき IPv6 トンネル インターフェイスを区別できません。

手動トンネルは「ポイントツーポイント」リンクであり、トンネルの IPv4 送信元と IPv4 宛先がともに定義されているので、IPv6 の手動設定トンネルは同じ送信元インターフェイスを共有できます。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface tunnel tunnel-number`
4. `ipv6 address ipv6-prefix/prefix-length [eui-64]`
5. `tunnel source {ip-address | interface-type interface-number}`
6. `tunnel mode ipv6ip 6to4`
7. `exit`
8. `ipv6 route ipv6-prefix/prefix-length tunnel tunnel-number`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code> 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>interface tunnel tunnel-number</code> 例： Router(config)# interface tunnel 0	トンネルのインターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>ipv6 address ipv6-prefix/prefix-length [eui-64]</code> 例： Router(config-if)# ipv6 address 2002:c0a8:6301:1::1/64	インターフェイスに割り当てられる IPv6 アドレスを指定し、インターフェイスでの IPv6 処理をイネーブルにします。 • 最初のプレフィクス 2002::/16 に続く 32 ビットは、トンネル送信元に割り当てられている IPv4 アドレスに相当します。 (注) IPv6 アドレスの設定の詳細は、「 Configuring Basic Connectivity for IPv6 」モジュールを参照してください。
ステップ 5	<code>tunnel source {ip-address interface-type interface-number}</code> 例： Router(config-if)# tunnel source GigabitEthernet 0/0/0	送信元 IPv4 アドレスまたは送信元インターフェイス タイプおよびトンネル インターフェイスの番号を指定します。 (注) <code>tunnel source</code> コマンドで指定されているインターフェイスのタイプおよび番号は、IPv4 アドレスを使用して設定することが必要です。
ステップ 6	<code>tunnel mode ipv6ip 6to4</code> 例： Router(config-if)# tunnel mode ipv6ip 6to4	6to4 アドレスを使用して、IPv6 オーバーレイ トンネルを指定します。

	コマンドまたはアクション	目的
ステップ7	<code>exit</code> 例： Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ8	<code>ipv6 route ipv6-prefix/prefix-length tunnel tunnel-number</code> 例： Router(config)# ipv6 route 2002::/16 tunnel 0	指定されているトンネル インターフェイスへの IPv6 6to4 プレフィクス 2002::/16 のスタティック ルートを設定します。 (注) 6to4 オーバーレイ トンネルを設定する際、6to4 トンネル インターフェイスへの IPv6 6to4 プレフィクス 2002::/16 のスタティック ルートを設定する必要があります。 • <code>ipv6 route</code> コマンドで指定されるトンネル番号は、 <code>interface tunnel</code> コマンドで指定されているトンネル番号と同じであることが必要です。

次の作業

「トンネルの設定と動作の確認」(P.27)に進みます。

ISATAP トンネルの設定

この作業では、ISATAP オーバーレイ トンネルの設定方法について説明します。

前提条件

ISATAP トンネルの設定で使用される `tunnel source` コマンドは、IPv4 アドレスを使用して設定されたインターフェイスをポイントする必要があります。ISATAP IPv6 アドレスおよびアドバタイズされたプレフィクス (1 つまたは複数) は、ネイティブ IPv6 インターフェイス向けに設定されます。IPv6 トンネル インターフェイスは、修正された EUI-64 アドレスを使用して設定する必要があります。これは、インターフェイス識別子の最後の 32 ビットが IPv4 トンネル送信元アドレスを使用して作成されているためです。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface tunnel tunnel-number`
4. `ipv6 address ipv6-prefix/prefix-length [eui-64]`
5. `no ipv6 nd suppress-ra`
6. `tunnel source {ip-address | interface-type interface-number}`
7. `tunnel mode ipv6ip isatap`
8. `end`

手順の詳細

ステップ1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	interface tunnel tunnel-number 例： Router(config)# interface tunnel 1	トンネルのインターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
コマンドまたはアクション		目的
ステップ4	ipv6 address ipv6-prefix/prefix-length [eui-64] 例： Router(config-if)# ipv6 address 2001:0DB8:6301::/64 eui-64	インターフェイスに割り当てられる IPv6 アドレスを指定し、インターフェイスでの IPv6 処理をイネーブルにします。 (注) IPv6 アドレスの設定の詳細は、「 Configuring Basic Connectivity for IPv6 」モジュールを参照してください。
ステップ5	no ipv6 nd suppress-ra 例： Router(config-if)# no ipv6 nd suppress-ra	IPv6 ルータ アドバタイズメントの送信をイネーブルにして、クライアントによる自動設定を可能にします。 • デフォルトでは、トンネルインターフェイスでの IPv6 ルータ アドバタイズメントはディセーブルになります。
ステップ6	tunnel source {ip-address interface-type interface-number} 例： Router(config-if)# tunnel source GigabitEthernet 0/0/1	送信元 IPv4 アドレスまたは送信元インターフェイス タイプおよびトンネルインターフェイスの番号を指定します。 (注) tunnel source コマンドで指定されているインターフェイスのタイプおよび番号は、IPv4 アドレスを使用して設定することが必要です。
ステップ7	tunnel mode ipv6ip isatap 例： Router(config-if)# tunnel mode ipv6ip isatap	ISATAP アドレスを使用して、IPv6 オーバーレイ トンネルを指定します。
ステップ8	end 例： Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

「[トンネルの設定と動作の確認](#)」(P.27) に進みます。

トンネルの設定と動作の確認

この任意の作業では、トンネルの設定と動作の確認方法について説明します。この手順に含まれる **show** コマンドおよび **ping** コマンドは、任意の順序で実行でき、繰り返し実行する必要がある場合があります。次のコマンドは、GRE トンネル、IPv6 手動設定トンネル、および IPv4 GRE トンネルを介する IPv6 に使用できます。

手順の概要

1. **enable**
2. **show interfaces tunnel number [accounting]**
3. **ping [protocol] destination**
4. **show ip route [address [mask]]**
5. **ping [protocol] destination**

手順の詳細

ステップ 1 enable

特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。

```
Router> enable
```

ステップ 2 show interfaces tunnel number [accounting]

IPv6 手動設定トンネルおよび IPv4 GRE トンネルを介する IPv6 の両方に適した汎用例を想定して、2 つのルータがトンネルのエンドポイントとして設定されているとします。ルータ A では、IPv4 アドレスが 10.0.0.1、IPv6 プレフィクスが 2001:0DB8:1111:2222::1/64 のトンネル インターフェイス 0 に対する送信元として、GigabitEthernet インターフェイス 0/0/0 が設定されています。ルータ B では、IPv4 アドレスが 10.0.0.2、IPv6 プレフィクスが 2001:0DB8:1111:2222::2/64 のトンネル インターフェイス 1 に対する送信元として、ギガビットイーサネット インターフェイス 0/0/0 が設定されています。

トンネルの送信元および宛先アドレスが設定されていることを確認するには、ルータ A で **show interfaces tunnel** コマンドを使用します。

```
RouterA# show interfaces tunnel 0
```

```
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.0.1 (GigabitEthernet0/0/0), destination 10.0.0.2, fastswitch TTL 255
Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
Tunnel TTL 255
Checksumming of packets disabled, fast tunneling enabled
Last input 00:00:14, output 00:00:04, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  4 packets input, 352 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```

8 packets output, 704 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

```

ステップ 3 ping [protocol] destination

ローカルエンドポイントが設定され、動作していることを確認するには、ルータ A で **ping** コマンドを使用します。

```

RouterA# ping 2001:0DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0DB8:1111:2222::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

```

ステップ 4 show ip route [address [mask]]

リモートエンドポイントアドレスに対するルートが存在するかどうかを確認するには、**show ip route** コマンドを使用します。

```

RouterA# show ip route 10.0.0.2

Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet0/0/0
    Route metric is 0, traffic share count is 1

```

ステップ 5 ping [protocol] destination

リモートエンドポイントアドレスが到達可能かどうかを確認するには、ルータ A で **ping** コマンドを使用します。



(注)

フィルタリングが原因で、**ping** コマンドを使用してもリモートエンドポイントアドレスが到達可能でない場合がありますが、トンネルトラフィックは宛先に到達可能です。

```

RouterA# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/28 ms

```

リモート IPv6 トンネルエンドポイントが到達可能かどうかを確認するには、ルータ A でもう一度 **ping** コマンドを使用します。この例にも、フィルタリングに関する同じ注釈が適用されます。

```

RouterA# ping 1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

```

これらの手順は、トンネルのもう一方のエンドポイントでも繰り返します。

トンネル実装の設定例

ここでは、次の例について説明します。

- 「GRE/IPv4 トンネルの設定：例」(P.29)
- 「GRE/IPv6 トンネルの設定：例」(P.30)
- 「GRE トンネルの IP 送信元および宛先の VRF メンバーシップの設定：例」(P.30)
- 「EoMPLS over GRE の設定：例」(P.31)
- 「IPv6 トンネルの手動設定：例」(P.33)
- 「6to4 トンネルの設定：例」(P.34)
- 「ISATAP トンネルの設定：例」(P.34)
- 「トンネルインターフェイスにおける QoS オプションの設定：例」(P.34)

GRE/IPv4 トンネルの設定：例

次に、GRE トンネリングの単純な設定例を示します。ギガビットイーサネットインターフェイス 0/0/1 はルータ A のトンネル送信元であり、ルータ B のトンネル宛先です。ファストイーサネットインターフェイス 0/0/1 はルータ B のトンネル送信元であり、ルータ A のトンネル宛先です。

ルータ A

```
interface Tunnel 0
 ip address 10.1.1.2 255.255.255.0
 tunnel source GigabitEthernet 0/0/1
 tunnel destination 192.168.3.2
 tunnel mode gre ip
!
interface GigabitEthernet 0/0/1
 ip address 192.168.4.2 255.255.255.0
```

ルータ B

```
interface Tunnel 0
 ip address 10.1.1.1 255.255.255.0
 tunnel source FastEthernet 0/0/1
 tunnel destination 192.168.4.2
 tunnel mode gre ip
!
interface FastEthernet 0/0/1
 ip address 192.168.3.2 255.255.255.0
```

次に、ルータ A とルータ B との間で IS-IS および IPv6 トラフィックをともに送出する GRE トンネルを設定する例を示します。

ルータ A

```
ipv6 unicast-routing
clns routing
!
interface Tunnel 0
 no ip address
 ipv6 address 2001:0DB8:1111:2222::1/64
 ipv6 router isis
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 10.0.0.2
```

```

tunnel mode gre ip
!
interface GigabitEthernet 0/0/0
 ip address 10.0.0.1 255.255.255.0
!
router isis
 network 49.0000.0000.000a.00

```

ルータ B

```

ipv6 unicast-routing
clns routing
!
interface Tunnel 0
 no ip address
 ipv6 address 2001:0DB8:1111:2222::2/64
 ipv6 router isis
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 10.0.0.1
 tunnel mode gre ip
!
interface GigabitEthernet 0/0/0
 ip address 10.0.0.2 255.255.255.0
!
router isis
 network 49.0000.0000.000b.00
 address-family ipv6
 redistribute static
 exit-address-family

```

GRE/IPv6 トンネルの設定 : 例

次に、IPv6 トランスポートで GRE トンネルを設定する方法の例を示します。ギガビットイーサネット インターフェイス 0/0/0 には IPv6 アドレスが設定されており、これがトンネル インターフェイスが使用する送信元アドレスとなります。トンネルの宛先 IPv6 アドレスは、直接指定されます。この例では、トンネルは IPv4 トラフィックおよび IS-IS トラックの両方を伝送します。

```

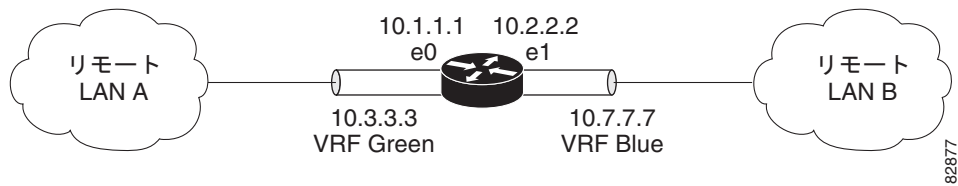
interface Tunnel 0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 2001:DB8:1111:2222::1
 tunnel mode gre ipv6
!
interface FastEthernet 0/0
 no ip address
 ipv6 address 2001:DB8:1111:1111::1/64
!
router isis
 net 49.0001.0000.0000.000a.00

```

GRE トンネルの IP 送信元および宛先の VRF メンバーシップの設定 : 例

この例では、VRF green を使用してファストイーサネット インターフェイス 0 で受信されたパケットが、VRF blue を使用してファストイーサネット インターフェイス 1 を使用してトンネルから外部へ転送されます。図 4 に、単純なトンネルのシナリオを示します。

図 4 GRE トンネルの図



次に、図 4 に示したトンネルの設定例を示します。

```
ip vrf blue
 rd 1:1

ip vrf green
 rd 1:2

interface loopback 0
 ip vrf forwarding vrf blue
 ip address 10.7.7.7 255.255.255.255

interface tunnel 0
 ip vrf forwarding vrf green
 ip address 10.3.3.3 255.255.255.0
 tunnel source loopback 0
 tunnel destination 10.5.5.5
 tunnel vrf blue

interface GigabitEthernet 0/0/0
 ip vrf forwarding vrf green
 ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet 0/0/1
 ip vrf forwarding vrf blue
 ip address 10.2.2.2 255.255.255.0

ip route vrf blue 10.5.5.5 255.255.255.0 GigabitEthernet 0/0/1
```

EoMPLS over GRE の設定 : 例

次に、EoMPLS over GRE の設定シーケンスの例を示します。

ルータ A の設定

```
vrf definition VPN1
 rd 100:1
 address-family ipv4
 route-target both 100:1
 exit-address-family
!
mpls label protocol ldp
mpls ldp neighbor 209.165.200.224 targeted
mpls ldp router-id Loopback0 force
!
interface Tunnel 0
 ip address 209.165.200.225 255.255.255.224
 mpls label protocol ldp
 mpls ip
 keepalive 10 3
 tunnel source TenGigabitEthernet 2/1/0
```

```

    tunnel destination 209.165.200.226
    !
interface Loopback 0
  ip address 209.165.200.230 255.255.255.224
  !
interface TenGigabitEthernet 2/1/0
  mtu 9216
  ip address 209.165.200.235 255.255.255.224
  !
interface TenGigabitEthernet 9/1
  no ip address
  !
interface TenGigabitEthernet 9/1.11
  vrf forwarding VPN1
  encapsulation dot1Q 300
  ip address 209.165.200.237 255.255.255.224
  !
interface TenGigabitEthernet 9/2
  mtu 9216
  no ip address
xconnect 209.165.200.239 200 encapsulation mpls
  !
router bgp 65000
  bgp log-neighbor-changes
  neighbor 209.165.200.240 remote-as 65000
  neighbor 209.165.200.240 update-source Loopback0
  neighbor 209.165.200.245 remote-as 100
  !
address-family vpnv4
  neighbor 209.165.200.240 activate
  neighbor 209.165.200.240 send-community extended
  !
address-family ipv4 vrf VPN1
  no synchronization
  neighbor 209.165.200.247 remote-as 100
  neighbor 209.165.200.248 activate
  neighbor 209.165.200.249 send-community extended
  !
ip route 209.165.200.251 255.255.255.224 Tunnel 0
ip route 209.165.200.254 255.255.255.224 209.165.200.256

```

ルータ B の設定

```

vrf definition VPN1
  rd 100:1
  address-family ipv4
  route-target both 100:1
exit-address-family
  !
mpls ldp neighbor 209.165.200.229 targeted
mpls label protocol ldp
mpls ldp router-id Loopback0 force
  !
interface Tunnel 0
  ip address 209.165.200.230 255.255.255.224
  mpls label protocol ldp
  mpls ip
  keepalive 10 3
  tunnel source TenGigabitEthernet 3/3/0
  tunnel destination 209.165.200.232
  !
interface Loopback 0
  ip address 209.165.200.234 255.255.255.224
  !

```



```
interface TenGigabitEthernet 2/1
  mtu 9216
  no ip address
  xconnect 209.165.200.237 200 encapsulation mpls
!
interface TenGigabitEthernet 2/3
  mtu 9216
  no ip address
!
interface TenGigabitEthernet 2/3.11
  vrf forwarding VPN1
  encapsulation dot1Q 300
  ip address 209.165.200.239 255.255.255.224
!
interface TenGigabitEthernet 3/3/0
  mtu 9216
  ip address 209.165.200.240 255.255.255.224
!
router bgp 65000
  bgp log-neighbor-changes
  neighbor 209.165.200.241 remote-as 65000
  neighbor 209.165.200.241 update-source Loopback0
  neighbor 209.165.200.244 remote-as 200
!
  address-family vpnv4
    neighbor 209.165.200.241 activate
    neighbor 209.165.200.241 send-community extended
  exit-address-family
!
  address-family ipv4 vrf VPN1
    no synchronization
    neighbor 209.165.200.246 remote-as 200
    neighbor 209.165.200.246 activate
    neighbor 209.165.200.246 send-community extended
  exit-address-family
!
ip route 209.165.200.226 255.255.255.224 Tunnel 0
ip route 209.165.200.229 255.255.255.224 209.165.200.235
```

IPv6 トンネルの手動設定：例

次に、ルータ A とルータ B の間に IPv6 トンネルを手動で設定する例を示します。例では、ルータ A とルータ B の両方のトンネル インターフェイス 0 は、グローバル IPv6 アドレスを使用して手動で設定されています。トンネルの送信元および宛先のアドレスも手動設定されています。

ルータ A

```
interface GigabitEthernet 0/0/0
  ip address 192.168.99.1 255.255.255.0

interface tunnel 0
  ipv6 address 2001:0db8:c18:1::3/126
  tunnel source GigabitEthernet 0/0/0
  tunnel destination 192.168.30.1
  tunnel mode ipv6ip
```

ルータ B

```
interface GigabitEthernet 0/0/0
  ip address 192.168.30.1 255.255.255.0
```

```
interface tunnel 0
  ipv6 address 2001:0db8:c18:1::2/126
  tunnel source GigabitEthernet 0/0/0
  tunnel destination 192.168.99.1
  tunnel mode ipv6ip
```

6to4 トンネルの設定 : 例

次に、独立した IPv6 ネットワーク内の境界ルータで 6to4 トンネルを設定する例を示します。IPv4 アドレスは 192.168.99.1 で、IPv6 プレフィクス 2002:c0a8:6301::/48 に変換されます。IPv6 プレフィクスは、トンネルインターフェイス用に 2002:c0a8:6301::/64、1 番目の IPv6 ネットワーク用に 2002:c0a8:6301:1::/64、2 番目の IPv6 ネットワーク用に 2002:c0a8:6301:2::/64 というようにサブネット化されます。スタティック ルートにより、IPv6 プレフィクス 2002::/16 はトンネルインターフェイス 0 に送信され自動的にトンネリングが行われます。

```
interface GigabitEthernet 0/0/0
  description IPv4 uplink
  ip address 192.168.99.1 255.255.255.0
!
interface GigabitEthernet 0/0/1
  description IPv6 local network 1
  ipv6 address 2002:c0a8:6301:1::1/64
!
interface GigabitEthernet 0/0/2
  description IPv6 local network 2
  ipv6 address 2002:c0a8:6301:2::1/64
!
interface Tunnel 0
  description IPv6 uplink
  no ip address
  ipv6 address 2002:c0a8:6301::1/64
  tunnel source GigabitEthernet 0/0/0
  tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 Tunnel0
```

ISATAP トンネルの設定 : 例

次に、ギガビットイーサネット インターフェイス 0/0/0 で定義されるトンネル送信元および ISATAP トンネルの設定に使用される **tunnel mode** コマンドの例を示します。ルータ アドバタイズメントをイネーブルにして、クライアントによる自動設定を可能にします。

```
interface Tunnel 1
  tunnel source GigabitEthernet 0/0/0
  tunnel mode ipv6ip isatap
  ipv6 address 2001:0DB8::/64 eui-64
  no ipv6 nd suppress-ra
```

トンネル インターフェイスにおける QoS オプションの設定 : 例

次の設定例は、トンネル インターフェイスの GTS に直接適用されます。この例では、設定によりトンネル インターフェイスが総出力レート 500 kb/s にシェーピングされます。

```
interface Tunnel 0
  ip address 10.1.2.1 255.255.255.0
```

```
traffic-shape rate 500000 125000 125000 1000
tunnel source 10.1.1.1
tunnel destination 10.2.2.2
```

次の設定例では、**Modular QoS CLI (MQC)** コマンドを備えたトンネル インターフェイスに同じシェーピング ポリシーを適用する方法を示します。

```
policy-map tunnel
  class class-default
  shape average 500000 125000 125000
!
interface Tunnel 0
  ip address 10.1.2.1 255.255.255.0
  service-policy output tunnel
  tunnel source 10.1.35.1
  tunnel destination 10.1.35.2
```

ポリシングの例

インターフェイスが混雑しており、パケットのキューイングを開始した場合、送信待ちのパケットにキューイング方式を適用できます。この例に挙げているトンネル インターフェイスである **Cisco IOS XE** 論理インターフェイスは、混雑した状況を本質的にサポートしておらず、キューイング方式を適用するサービス ポリシーの直接適用もサポートしていません。その代わりに、階層型ポリシーを適用する必要があります。**priority** コマンドを使用した低遅延キューイングや、**bandwidth** コマンドを使用したキューイング メカニズムを設定する「子」ポリシー、つまり下位ポリシーを作成します。

```
policy-map child
  class voice
  priority 512
```

クラスベースのシェーピングに適用する「親」ポリシー、つまり上位ポリシーを作成します。子クラスのアドミッション制御は親クラスのシェーピング レートに従って実行されるので、親ポリシー下で子ポリシーをコマンドとして適用します。

```
policy-map tunnel
  class class-default
  shape average 2000000
  service-policy child
```

親ポリシーをトンネル インターフェイスに適用します。

```
interface tunnel 0
  service-policy tunnel
```

次の例では、トンネル インターフェイスは、シェーピングを行わないキューイングを適用するサービス ポリシーを使用して設定されます。この設定がサポートされないことを通知するログ メッセージが表示されます。

```
Router(config)# interface tunnel1
Router(config-if)# service-policy output child
```

```
Class Based Weighted Fair Queueing not supported on this interface
```

その他の参考資料

ここでは、トンネルの実装に関する関連資料について説明します。

関連資料

関連項目	参照先
トンネル コマンド：コマンド構文の詳細、コマンドモード、デフォルト、コマンド履歴、使用上の注意事項、および例	『Cisco IOS Interface and Hardware Component Command Reference』
IPv6 コマンド：コマンド構文の詳細、コマンドモード、デフォルト、コマンド履歴、使用上の注意事項、および例	『Cisco IOS IPv6 Command Reference』
すべての Cisco IOS XE コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS XE Interface and Hardware Component コンフィギュレーション モジュール	『Cisco IOS XE Interface and Hardware Component Configuration Guide, Release 2』
Cisco IOS XE IPv6 コンフィギュレーション モジュール	『Cisco IOS XE IPv6 Configuration Guide, Release 2』
Cisco IOS XE Quality of Service Solutions コンフィギュレーション モジュール	『Cisco IOS XE Quality of Service Solutions Configuration Guide, Release 2』
Cisco IOS XE Multiprotocol Label Switching コンフィギュレーション モジュール	『Cisco IOS XE Multiprotocol Label Switching Configuration Guide, Release 2』
VRF 対応 Dynamic Multipoint VPN (DMVPN; ダイナミック マルチポイント VPN) の設定例	『Cisco IOS XE Security Configuration Guide: Secure Connectivity, Release 2』の「Dynamic Multipoint VPN (DMVPN)」コンフィギュレーション モジュール

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 791	『Internet Protocol』
RFC 1191	『Path MTU Discovery (PMTUD)』
RFC 1323	『TCP Extensions for High Performance』

RFC	タイトル
RFC 1483	「 <i>Multiprotocol Encapsulation over ATM Adaptation Layer 5</i> 」
RFC 2003	「 <i>IP Encapsulation Within IP</i> 」
RFC 2018	「 <i>TCP Selective Acknowledgment Options</i> 」
RFC 2460	「 <i>Internet Protocol, Version 6 (IPv6)</i> 」
RFC 2473	「 <i>Generic Packet Tunneling in IPv6 Specification</i> 」
RFC 2474	「 <i>Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers</i> 」
RFC 2516	「 <i>A Method for Transmitting PPP over Ethernet (PPPoE)</i> 」
RFC 2547	「 <i>BGP/MPLS VPNs</i> 」
RFC 2780	「 <i>IANA Allocation Guidelines for Values in the Internet Protocol and Related Headers</i> 」
RFC 2784	「 <i>Generic Routing Encapsulation (GRE)</i> 」
RFC 2890	「 <i>Key and Sequence Number Extensions to GRE</i> 」
RFC 2893	「 <i>Transition Mechanisms for IPv6 Hosts and Routers</i> 」
RFC 3056	「 <i>Connection of IPv6 Domains via IPv4 Clouds</i> 」
RFC 3147	「 <i>Generic Routing Encapsulation over CLNS Networks</i> 」

シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"> • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする <ul style="list-style-type: none"> – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する <p>この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	http://www.cisco.com/en/US/support/index.html

トンネルの実装に関する機能情報

表 5 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS XE ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。



(注) 表 5 には、一連の Cisco IOS XE ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS XE ソフトウェア リリースだけを示します。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS XE ソフトウェア リリースでもサポートされます。

表 5 トンネルの実装に関する機能情報

機能名	リリース	機能の設定情報
GRE トンネルの IP 送信元および宛先の VRF メンバーシップ	Cisco IOS XE Release 2.2	<p>この機能では、トンネルの送信元および宛先が任意の VPN VRF テーブルに属するように設定できます。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「GRE トンネルの IP 送信元および宛先の VRF メンバーシップ」(P.5) 「GRE トンネルの IP 送信元および宛先の VRF メンバーシップの設定」(P.20) 「GRE トンネルの IP 送信元および宛先の VRF メンバーシップの設定：例」(P.30) <p>この機能をサポートするために tunnel vrf コマンドが導入されました。</p>
GRE トンネル キープアライブ	Cisco IOS XE Release 2.1	<p>GRE トンネル キープアライブ機能により、IP カプセル化された GRE トンネルを介してキープアライブ パケットが送信されるように設定できるようになります。キープアライブが送信されるレートと、インターフェイスが非アクティブになるまでデバイスが応答なしでキープアライブ パケットの送信を続行する回数を指定できます。GRE キープアライブ パケットは、トンネルの両側または片側のみのどちらからでも送信できます。</p> <p>この機能については、次の項に説明があります。</p> <ul style="list-style-type: none"> 「GRE トンネルの設定」(P.14) <p>この機能により、keepalive コマンド（トンネル インターフェイス）が導入されました。</p>

表 5 トンネルの実装に関する機能情報 (続き)

機能名	リリース	機能の設定情報
IPv6 IP トンネルを介する IP	Cisco IOS XE Release 2.4	<p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「GRE/IPv6 トンネルの設定」(P.18) 「GRE/IPv6 トンネルの設定：例」(P.30) <p>この機能により、tunnel destination、tunnel mode、および tunnel source の各コマンドが導入されました。</p>
GRE トンネル向け IP Precedence	Cisco IOS XE Release 2.1	<p>この機能は、Cisco ASR 1000 アグリゲーション サービス ルータに導入されました。</p>
Tunnel ToS	Cisco IOS XE Release 2.1	<p>Tunnel ToS 機能を使用して、ルータの IP トンネル インターフェイス向けのトンネル パケットの IP カプセル化 ヘッダーに、ToS および Time-to-Live (TTL) バイト値を設定できます。Tunnel ToS 機能は、シスコ エクスプレス フォワーディング、ファスト スイッチング、および プロセス スイッチング フォワーディングの各モードでサポートされます。</p> <p>この機能については、次の項に説明があります。</p> <ul style="list-style-type: none"> 「Tunnel ToS」(P.4) <p>この機能によって、show interfaces tunnel、tunnel tos、および tunnel ttl の各コマンドが導入されました。</p>
EoMPLS over GRE	Cisco IOS XE Release 2.5	<p>EoMPLS over GRE 機能により、レイヤ 3 MPLS ネットワークを経由してレイヤ 2 トラフィックをトンネリングできます。またこの機能では、GRE トンネル内で EoMPLS フレームをカプセル化する高性能のハードウェアベースのスイッチド トンネルとして GRE トンネルを作成できます。</p> <p>この機能については、次の項に説明があります。</p> <ul style="list-style-type: none"> 「EoMPLS over GRE」(P.5) <p>この機能によって導入または変更された新しいコマンドはありません。</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2005–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2005–2011, シスコシステムズ合同会社.
All rights reserved.



MPLS VPN over mGRE



MPLS VPN over mGRE

MPLS VPN over mGRE 機能は、IP 専用ネットワークで接続されているネットワーク間に Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) 接続を提供できるようにすることによって、MPLS をサポートするという通信事業者の要件を克服します。これにより、MPLS の Label Switched Path (LSP; ラベル スイッチドパス) では Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) トンネルを使用してルーティング エリア、自律システム、および Internet Service Provider (ISP; インターネット サービス プロバイダー) を横断することが可能になります。multipoint GRE (mGRE) による MPLS VPN を設定すると、標準ベースの IP コアを使用して Layer-3 (L3; レイヤ 3) Provider Edge (PE; プロバイダー エッジ) ベースの Virtual Private Network (VPN; バーチャル プライベート ネットワーク) を展開できます。これにより、オーバーレイ方式を使用しないで VPN サービスを提供することができます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「[MPLS VPN over mGRE の機能情報 \(P.16\)](#)」を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム サポートおよび Cisco ソフトウェア イメージ サポートに関する情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

- 「[MPLS VPN over mGRE の前提条件](#)」 (P.2)
- 「[MPLS VPN over mGRE の制約事項](#)」 (P.2)
- 「[MPLS VPN over mGRE に関する情報](#)」 (P.2)
- 「[MPLS VPN over mGRE の設定方法](#)」 (P.5)
- 「[MPLS VPN over mGRE の設定例](#)」 (P.11)
- 「[その他の参考資料](#)」 (P.14)

- 「MPLS VPN over mGRE の機能情報」(P.16)

MPLS VPN over mGRE の前提条件

mGRE トンネルを使用して MPLS VPN を設定する前に、MPLS VPN が設定され、正しく動作していることを確認してください。MPLS VPN の設定については、「[Configuring MPLS Layer 3 VPNs](#)」モジュールを参照してください。

MPLS VPN over mGRE の制約事項

- トンネル タグ トラフィックは、MPLS VPN over mGRE をサポートするライン カード経由でルータに入る必要があります。
- 各 PE ルータでサポートされるトンネル コンフィギュレーションは 1 つだけです。
- MPLS VPN over mGRE では、VPN 間のマルチキャスト トラフィックの転送はサポートされません。
- GRE トンネルの宛先アドレスおよび送信元アドレスが mGRE と同じである場合は、トンネルでルートキャッシュが切り替えられます。
- フラグメンテーションが必要なパケットではルートキャッシュが切り替えられます。
- L3VPN プロファイルが削除され、再び追加された場合は、**clear ip bgp soft** コマンドを使用して Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) をクリアする必要があります。
- mGRE が作成されると、ダミー トンネルも作成されます。
- BGP コンフィギュレーションのアップデート元で使用されるループバックまたは IP アドレスは、L3VPN プロファイルの送信元と同じである必要があります。
- mGRE は Stateful Switchover (SSO; ステートフル スイッチオーバー) には対応していません。ただし、mGRE と SSO は共存します。
- mGRE と Multicast Distribution Tree (MDT; マルチキャスト分散ツリー) トンネルに同じループバック アドレスを設定しないでください。

MPLS VPN over mGRE 機能の制限事項は、次のとおりです。

- ハードウェアで、すべての GRE オプションがサポートされるわけではありません (GRE 拡張ヘッダーや GRE キーなど)。
- トンネルでは、同一 VLAN (Internet Control Message Protocol(ICMP; インターネット制御メッセージ プロトコル)リダイレクト) のチェックはサポートされていません。
- トンネルでは、unicast Reverse Path Forwarding (uRPF; ユニキャスト リバース パス転送) や BGP ポリシー アカウンティングなどの機能はサポートされていません。

MPLS VPN over mGRE に関する情報

mGRE トンネルを設定して、IP バックボーンをオーバーレイするマルチポイント トンネル ネットワークを作成できます。このオーバーレイによって、VPN トラフィックを転送するための PE ルータが接続されます。

さらに、mGRE による MPLS VPN を設定すると、標準ベースの IP コアを使用して、L3 PE ベースの VPN サービスを展開できます。これにより、オーバーレイ方式を使用しないで VPN サービスを提供することができます。MPLS VPN over mGRE を設定すると、システムは IPv4 ベースの mGRE トンネルを使用して、PE 間で VPN ラベル付きの IPv4 および IPv6 パケットをカプセル化します。

MPLS VPN over mGRE 機能を設定するには、次の概念を理解しておく必要があります。

- 「MPLS VPN over mGRE」(P.3)

MPLS VPN over mGRE

GRE は、2 つのピアがトンネルのエンドポイントを構成するポイントツーポイント トンネリング プロトコルです。GRE はネットワークレイヤのパケットを IP トンネリング パケットにカプセル化するように設計されています。mGRE は同様のプロトコルですが、トンネルの一方は単一のエンドポイントで、それがトンネルの他方にある複数のエンドポイントに接続されています。mGRE トンネルによって、同じ VPN に接続された支社間に共通のリンクが提供されます。mGRE はポイントツーマルチポイントモデルなので、MPLS VPN の PE デバイスを相互接続するためにフル メッシュ構造の GRE トンネルは必要ありません。

MPLS は広く採用されている VPN インターネット アーキテクチャです。MPLS では、ネットワーク内のすべてのコア ルータが MPLS をサポートしている必要があります。この機能は、サービス プロバイダーがバックボーン事業者を使用して接続を提供しているネットワークで有用です。

MPLS VPN over mGRE 機能は、IP 専用ネットワークで接続されているネットワーク間に MPLS 接続を提供できるようにすることによって、MPLS をサポートするという通信事業者の要件を克服します。これにより、MPLS の LSP では GRE トンネルを使用してルーティング エリア、自律システム、および ISP を横断することが可能になります。

mGRE による MPLS VPN を設定すると、標準ベースの IP コアを使用して、L3 PE ベースの VPN サービスを展開できます。これにより、LSP や Label Distribution Protocol (LDP; ラベル配布プロトコル) を使用しないで VPN サービスを提供することができます。システムは IPv4 ベースの mGRE トンネルを使用して、PE 間で VPN ラベル付きの IPv4 および IPv6 パケットをカプセル化します。

また、MPLS VPN over mGRE 機能により、既存の MPLS VPN LSP カプセル化テクノロジーを MPLS VPN over mGRE と同時に導入し、特定トラフィックのルーティングに使用されるカプセル化方式をシステムが決定できるようにすることも可能です。入力 PE ルータによって、パケットがリモート PE ルータに送信されるときに使用するカプセル化テクノロジーが決定されます。

ここでは、MPLS VPN over mGRE 機能に関する次の項目について説明します。

- 「ルート マップ」(P.4)
- 「トンネル エンドポイントの検出および転送」(P.4)
- 「トンネルの非カプセル化」(P.4)
- 「トンネルの送信元」(P.5)
- 「IPv6 VPN」(P.5)

ルート マップ

デフォルトでは、VPN トラフィックは LSP を使用して送信されます。MPLS VPN over mGRE 機能では、ユーザ定義のルート マップを使用して、mGRE トンネルで到達可能な VPN プレフィクスと LSP を使用して到達可能な VPN プレフィクスを決定します。ルート マップは、VPNv4 および VPNv6 アドレス ファミリのアドバタイズメントに適用されます。ルート マップでは、ネクスト ホップ トンネル テーブルを使用して VPN トラフィックのカプセル化方式を決定します。

mGRE トンネルを使用してトラフィックをルーティングするために、システムは mGRE トンネルでトラフィックをカプセル化することによってすべてのネクスト ホップに到達可能であることを示す代替アドレス空間を作成します。特定のルートが mGRE トンネルを使用するように設定するには、ユーザがそのルート用のエントリをルート マップに追加します。その新しいエントリによって、代替アドレス空間へのルートの Network Layer Reachability Information (NLRI; ネットワーク レイヤ到着可能性情報) が再マッピングされます。あるルートの再マッピング エントリがルート マップに存在しない場合、そのルート上のトラフィックは LSP を使用して転送されます。

ユーザが MPLS VPN over mGRE を設定すると、代替アドレス空間が自動的にプロビジョニングされ、通常の場合、トンネル カプセル化 Virtual Routing and Forwarding (VRF; 仮想ルーティング/転送) インスタンスに保持されます。このアドレス空間経由で到達可能なすべてのトラフィックが mGRE トンネルで確実にカプセル化されるように、システムにはトンネル外への単一のデフォルト ルートがインストールされます。また、ルート マップ上にデフォルトのトンネルも作成されます。ユーザは、このデフォルト ルート マップを適切な BGP アップデートに対応付けることができます。

トンネル エンドポイントの検出および転送

MPLS VPN over mGRE 機能が正常に機能するためには、システムがシステム内のリモート PE を検出し、これらのリモート PE のトンネル転送情報を作成できる必要があります。また、リモート PE が有効でなくなったときを検出し、その PE のトンネル転送情報を削除することも必要です。

入力 PE は、BGP による VPN アドバタイズメントを受信すると、ルート ターゲット属性 (入力 PE が VRF に挿入) とアドバタイズメントの MPLS VPN ラベルを使用して、プレフィクスを適切なカスタマーに関連付けます。挿入されたルートのネクスト ホップは、アドバタイズメントの NLRI に設定されます。

アドバタイズされたプレフィクスには、システム内のリモート PE に関する情報が (NLRI の形式で) 含まれます。PE はこの情報を使用して、NLRI がアクティブまたは非アクティブになったときにシステムに通知します。システムは、この通知を使用して PE 転送情報をアップデートします。

システムは新しいリモート PE の通知を受信すると、その情報をトンネル エンドポイント データベースに追加します。これによって、システムはトンネル インターフェイスに関連付けられた隣接関係を作成します。この隣接関係の説明には、カプセル化に関する情報と、カプセル化パケットを新しいリモート PE に送信するためにシステムで実行する必要があるその他の処理に関する情報が含まれます。

この隣接情報は、トンネル カプセル化 VRF に挿入されます。ユーザが (ルート マップを使用して) VPN の NLRI を VRF 内のルートに再マッピングすると、システムはその NLRI を隣接関係にリンクさせます。その結果、VPN がトンネルにリンクされます。

トンネルの非カプセル化

出力 PE は、MPLS VPN over mGRE 機能を使用するトンネル インターフェイスからパケットを受信すると、そのパケットを非カプセル化して VPN ラベル タグ付きのパケットを作成し、MPLS Forwarding (MFI) コードに送信します。

トンネルの送信元

MPLS VPN over mGRE 機能では、mGRE トンネルとして設定された単一のトンネルを使用して、多数のエンドポイント（リモート PE）を持つシステムを設定します。トンネルカプセル化パケットの送信元を識別するために、システムではトンネル送信元情報が使用されます。

送信側（入力）PE では、VPN パケットがトンネルに送信される時、トンネル宛先は NLRI です。受信側（出力）PE では、トンネル送信元は mGRE トンネルでカプセル化されたパケットが受信されるアドレスです。したがって、出力 PE では、パケットの宛先がローカル PE からの NLRI と一致している必要があります。

IPv6 VPN

アドバタイジング PE ルータのアドレスが IPv6 である場合、（PE 間のネットワークに関係なく）NLRI のアドレスも IPv6 である必要があります。各 PE 間のネットワークが IPv4 ベースである場合、システムは ::FFFF:IPv4-PE-address という形式の IPv4 射影アドレスを使用してアドバタイジング PE の IPv6 アドレスを作成します。受信側 PE は、VPN タグの IPv6 プレフィクス用のネクスト ホップを、IPv6 の NLRI に埋め込まれた IPv4 アドレスに設定します。これにより、PE は VPNv4 トラフィックをマッピングするのと同じように、VPNv6 トラフィックを LSP または mGRE トンネルにリンクすることが可能になります。

PE が VPNv6 アップデートを受信すると、そのアップデートは IPv6 ルート マップに適用されます。MPLS VPN over mGRE 機能では、IPv6 ルート マップを使用して、Tunnel_Encap VRF にネクスト ホップ情報を設定します。

MPLS VPN over mGRE の設定方法

mGRE トンネルによる MPLS VPN を展開するには、VRF インスタンスを作成し、L3 VPN カプセル化をイネーブルにして設定し、ルート マップをアプリケーション テンプレートにリンクし、BGP VPNv4 と VPNv6 の交換を設定してアップデートがルート マップでフィルタリングされるようにします。

MPLS VPN over mGRE を展開するための設定手順は、次の各項で説明します。

- 「L3VPN カプセル化プロファイルの設定」(P.5) (必須)
- 「BGP およびルート マップの設定」(P.7) (必須)

L3VPN カプセル化プロファイルの設定

ここでは、L3VPN カプセル化プロファイルを設定する方法について説明します。



(注)

この設定では、IPv6、MPLS、IP、および Layer 2 Tunneling Protocol version 3 (L2TPv3) などのトランスポート プロトコルも使用できます。

手順の概要

1. `enable`
2. `configure terminal`
3. `l3vpn encapsulation ip profile-name`

4. `transport ipv4 [source interface-type interface-number]`
5. `protocol gre [key gre-key]`
6. `end`
7. `show l3vpn encapsulation ip profile-name`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ2	<code>configure terminal</code> 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>l3vpn encapsulation ip profile-name</code> 例： Router(config)# l3vpn encapsulation ip tunnel encap	L3 VPN カプセル化コンフィギュレーション モードを開始してトンネルを作成します。
ステップ4	<code>transport ipv4 [source interface-type interface-number]</code> 例： Router(config-l3vpn-encap-ip)# transport ipv4 source loopback 0	(任意) IPv4 トランスポートの送信元モードを指定し、トランスポートの送信元インターフェイスを定義します。 • transport ipv4 source interface-type interface-number コマンドを使用する場合は、指定した送信元アドレスが、PE によってアドバタイズされた BGP アップデートのネクスト ホップとして使用されていることを確認します。 • このコマンドを使用しない場合は、 bgp update source または bgp next-hop コマンドがトンネル送信元として自動的に使用されます。
ステップ5	<code>protocol gre [key gre-key]</code> 例： Router(config-l3vpn-encap-ip)# protocol gre key 1234	GRE をトンネル モードとして指定し、GRE キーを設定します。
ステップ6	<code>end</code> 例： Router(config-l3vpn-encap-ip)# end	L3 VPN カプセル化コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ7	<code>show l3vpn encapsulation ip profile-name</code> 例： Router# show l3vpn encapsulation ip tunnel encap	(任意) プロファイルの状態と基盤となるトンネル インターフェイスを表示します。

BGP およびルート マップの設定

BGP およびルート マップを設定するには、次の作業を実行します。次の手順では、ルート マップをアプリケーション テンプレートにリンクし、BGP VPNv4 と VPNv6 の交換を設定してアップデートがルート マップでフィルタリングされるようにすることもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp *as-number***
4. **bgp log-neighbor-changes**
5. **neighbor *ip-address* remote-as *as-number***
6. **neighbor *ip-address* update-source *interface-name* *interface-number***
7. **address-family ipv4**
8. **no synchronization**
9. **redistribute connected**
10. **neighbor *ip-address* activate**
11. **no auto-summary**
12. **exit**
13. **address-family vpnv4**
14. **neighbor *ip-address* activate**
15. **neighbor *ip-address* send-community both**
16. **neighbor *ip-address* route-map *map-name* in**
17. **exit**
18. **address-family vpnv6**
19. **neighbor *ip-address* activate**
20. **neighbor *ip-address* send-community both**
21. **neighbor *ip-address* route-map *map-name* in**
22. **exit**
23. **route-map *map-tag* permit *position***
24. **set ip next-hop encapsulate l3vpn *profile-name***
25. **set ipv6 next-hop encapsulate l3vpn *profile-name***
26. **exit**
27. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp as-number 例： Router(config)# router bgp 100	他の BGP ルータに対してルータを識別する自律システムの番号を指定し、渡されるルーティング情報にタグ付けし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	bgp log-neighbor-changes 例： Router(config-router)# bgp log-neighbor-changes	BGP ネイバー リセットのロギングをイネーブルにします。
ステップ 5	neighbor ip-address remote-as as-number 例： Router(config-router)# neighbor 209.165.200.225 remote-as 100	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 6	neighbor ip-address update-source interface name 例： Router(config-router)# neighbor 209.165.200.225 update-source loopback 0	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。
ステップ 7	address-family ipv4 例： Router(config-router)# address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始して、IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 8	no synchronization 例： Router(config-router-af)# no synchronization	Cisco IOS ソフトウェアが IGP を待たずにネットワーク ルートをアドバタイズできるようにします。
ステップ 9	redistribute connected 例： Router(config-router-af)# redistribute connected	あるルーティング ドメインから別のルーティング ドメインにルートを再配布し、ターゲット プロトコルが、ソース プロトコルによって認識されたルートおよびソース プロトコルが実行されている各インターフェイス上の接続プレフィクスを再配布できるようにします。

	コマンドまたはアクション	目的
ステップ 10	neighbor ip-address activate 例： Router(config-router-af)# neighbor 209.165.200.225 activate	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 11	no auto-summary 例： Router(config-router-af)# no auto-summary	自動サマライズをディセーブルにし、サブプレフィクスルーティング情報をクラスフル ネットワーク境界間で送信します。
ステップ 12	exit 例： Router(config-router-af)# exit	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 13	address-family vpnv4 例： Router(config-router)# address-family vpnv4	アドレス ファミリ コンフィギュレーション モードを開始して、標準の VPNv4 アドレス プレフィクスを使用するルーティングセッション (BGP など) を設定します。
ステップ 14	neighbor ip-address activate 例： Router(config-router-af)# neighbor 209.165.200.225 activate	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 15	neighbor ip-address send-community both 例： Router(config-router-af)# neighbor 209.165.200.225 send-community both	標準コミュニティと拡張コミュニティの両方のコミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 16	neighbor ip-address route-map map-name in 例： Router(config-router-af)# neighbor 209.165.200.225 route-map SELECT_UPDATE_FOR_L3VPN in	指定されたルート マップを受信ルートに適用します。
ステップ 17	exit 例： Router(config-router-af)# exit	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 18	address-family vpnv6 例： Router(config-router)# address-family vpnv6	アドレス ファミリ コンフィギュレーション モードを開始して、VPNv6 アドレス プレフィクスを使用するルーティングセッション (BGP など) を設定します。
ステップ 19	neighbor ip-address activate 例： Router(config-router-af)# neighbor 209.165.200.252 activate	BGP ネイバーとの情報交換をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 20	<pre>neighbor ip-address send-community both</pre> <p>例:</p> <pre>Router(config-router-af)# neighbor 209.165.200.252 send-community both</pre>	標準コミュニティと拡張コミュニティの両方のコミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 21	<pre>neighbor ip-address route-map map-name in</pre> <p>例:</p> <pre>Router(config-router-af)# neighbor 209.165.200.252 route-map SELECT_UPDATE_FOR_L3VPN in</pre>	指定されたルート マップを受信ルートに適用します。
ステップ 22	<pre>exit</pre> <p>例:</p> <pre>Router(config-router-af)# exit</pre>	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 23	<pre>route-map map-tag permit position</pre> <p>例:</p> <pre>Router(config-router)# route-map SELECT_UPDATE_FOR_L3VPN permit 10</pre>	<p>ルート マップ コンフィギュレーション モードを開始し、あるルーティング プロトコルから別のルーティング プロトコルにルートを再分配するための条件を定義します。</p> <ul style="list-style-type: none"> • redistribute ルータ コンフィギュレーション コマンドは、指定されたマップ タグを使用して、このルート マップを参照します。複数のルート マップが同じマップ タグ名を共有する場合があります。 • このルート マップの一致基準が満たされた場合、ルートは設定アクションによる制御に応じて再分配されます。 • 一致基準が満たされない場合、同じマップ タグを持つ次のルート マップがテストされます。あるルートが同じ名前を共有する一連のルート マップの一致基準のいずれも満たさなかった場合、ルートはその設定で再分配されません。 • position 引数は、すでに同じ名前を設定されているルート マップのリスト内に新しいルート マップが入る位置を示します。
ステップ 24	<pre>set ip next-hop encapsulate l3vpn profile-name</pre> <p>例:</p> <pre>Router(config-route-map)# set ip next-hop encapsulate l3vpn my profile</pre>	ルート マップの match 句を渡す出力 IPv4 パケットが、トンネル カプセル化のために VRF に送信されることを示します。
ステップ 25	<pre>set ipv6 next-hop encapsulate l3vpn profile-name</pre> <p>例:</p> <pre>Router(config-route-map)# set ip next-hop encapsulate l3vpn tunnel encap</pre>	ルート マップの match 句を渡す出力 IPv6 パケットが、トンネル カプセル化のために VRF に送信されることを示します。

	コマンドまたはアクション	目的
ステップ 26	exit 例： Router(config-route-map)# exit	ルート マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 27	exit 例： Router(config)# exit	グローバル コンフィギュレーション モードを終了します。

MPLS VPN over mGRE の設定例

- 「例：MPLS VPN over mGRE 設定の確認」(P.11)
- 「例：MPLS VPN over mGRE の設定シーケンス」(P.12)

例：MPLS VPN over mGRE 設定の確認

設定が正しく動作していることを確認するには、次の例を使用します。

シスコ エクスプレス フォワーディング (CEF) スイッチング

CEF スイッチングが予想どおりに動作していることを確認できます。

```
Router# show ip cef vrf Customer_A tunnel 0
```

```
209.165.200.250/24
  nexthop 209.165.200.251 Tunnel0 label 16
```

エンドポイントの作成

作成されたトンネル エンドポイントを確認できます。

```
Router# show tunnel endpoints tunnel 0
```

```
Tunnel0 running in multi-GRE/IP mode

Endpoint transport 209.165.200.251 Refcount 3 Base 0x2AE93F0 Create Time 00:00:42
overlay 209.165.200.254 Refcount 2 Parent 0x2AE93F0 Create Time 00:00:42
```

隣接関係

対応する隣接関係が作成されていることを確認できます。

```
Router# show adjacency tunnel 0
```

```
Protocol Interface Address
IP Tunnel0 209.165.200.251(4)
TAG Tunnel0 209.165.200.251(3)
```

プロファイルの状態

show l3vpn encapsulation profile-name コマンドを使用して、アプリケーションの基本的な状態に関する情報を取得できます。このコマンドの出力には、基盤となるトンネルの詳細が表示されます。

```
Router# show l3vpn encapsulation ip tunnel encap
```

```

Profile: tunnel encap
transport ipv4 source Auto: Loopback0
protocol gre
Tunnel Tunnel0 Created [OK]
Tunnel Linestate [OK]
Tunnel Transport Source (Auto) Loopback0 [OK]

```

例 : MPLS VPN over mGRE の設定シーケンス

この例では、MPLS VPN over mGRE の設定シーケンスを示します。

```

vrf definition Customer A
rd 100:110
route-target export 100:1000
route-target import 100:1000
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
!
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
!
l3vpn encapsulation ip sample profile name
transport source loopback 0
protocol gre key 1234
!
!
interface Loopback0
ip address 209.165.200.252 255.255.255.224
ip router isis
!
interface Serial2/0
vrf forwarding Customer A
ip address 209.165.200.253 255.255.255.224
ipv6 address 3FFE:1001::/64 eui-64
no fair-queue
serial restart-delay 0
!
router bgp 100
bgp log-neighbor-changes
neighbor 209.165.200.254 remote-as 100
neighbor 209.165.200.254 update-source Loopback0
!
address-family ipv4
no synchronization
redistribute connected
neighbor 209.165.200.254 activate
no auto-summary
exit-address-family
!
address-family vpnv4
neighbor 209.165.200.254 activate
neighbor 209.165.200.254 send-community both
neighbor 209.165.200.254 route-map SELECT_UPDATE_FOR_L3VPN in
exit-address-family

```

```
!  
address-family vpnv6  
  neighbor 209.165.200.254 activate  
  neighbor 209.165.200.254 send-community both  
  neighbor 209.165.200.254 route-map SELECT_UPDATE_FOR_L3VPN in  
exit-address-family  
!  
address-family ipv4 vrf Customer A  
  no synchronization  
  redistribute connected  
exit-address-family  
!  
address-family ipv6 vrf Customer A  
  redistribute connected  
  no synchronization  
exit-address-family  
!  
!  
route-map SELECT_UPDATE_FOR_L3VPN permit 10  
set ip next-hop encapsulate sample profile name  
set ipv6 next-hop encapsulate sample profile name
```

その他の参考資料

関連資料

関連項目	参照先
MPLS レイヤ 3 VPN の設定	『Cisco IOS XE Multiprotocol Label Switching Configuration Guide』
シスコ エクスプレス フォワーディング	『Cisco IOS XE IP Switching Configuration Guide』
総称ルーティング カプセル化	『Cisco IOS XE Interface and Hardware Component Configuration Guide』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
IETF-PPVPN-MPLS-VPN-MIB	<p>選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
RFC 2547	『BGP/MPLS VPNs』
RFC 2784	『Generic Routing Encapsulation (GRE)』
RFC 2890	『Key Sequence Number Extensions to GRE』
RFC 4023	『Encapsulating MPLS in IP or Generic Routing Encapsulation』
RFC 4364	『BGP/MPLS IP Virtual Private Networks (VPNs)』

シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none">• テクニカル サポートを受ける• ソフトウェアをダウンロードする• セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける• ツールおよびリソースへアクセスする<ul style="list-style-type: none">– Product Alert の受信登録– Field Notice の受信登録– Bug Toolkit を使用した既知の問題の検索• Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する• トレーニング リソースへアクセスする• TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する <p>この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

MPLS VPN over mGRE の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。



(注)

表 1 には、一連のソフトウェア リリースのうち、特定の機能のサポートが初めて導入されたソフトウェア リリースだけを示します。その機能は、特に明記されていない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1 MPLS VPN over mGRE の機能情報

機能名	リリース	機能情報
MPLS VPN over mGRE	Cisco IOS XE リリース 3.1S	<p>この機能では、mGRE による MPLS レイヤ 3 VPN トラフィックの伝送のサポートが提供されます。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「L3VPN カプセル化プロファイルの設定」(P.5) 「BGP およびルート マップの設定」(P.7) <p>この機能によって、コマンド l3vpn encapsulation ip、protocol gre、show l3vpn encapsulation ip、transport ipv4、set ip next-hop、set ipv6 next-hop が導入または変更されています。</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Copyright © 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010–2011, シスコシステムズ合同会社.
All rights reserved.



1+1 SR-APS Without Bridging



1+1 SR-APS Without Bridging

Automatic Protection Switching (APS; 自動保護スイッチング) 機能は、リンクの冗長性を提供し、回線障害の発生時に Packet over SONET (POS) 回線のスイッチオーバーを可能にします。この機能は多くの場合、Synchronous Optical Networking (SONET) 装置を通信装置に接続する際に必要となります。Single Router (SR) APS 機能では、保護インターフェイスと現用インターフェイスの両方が同じルータ上にある必要があります。

APS は、現用 POS インターフェイスのバックアップとして、SONET ネットワーク内の保護 POS インターフェイスを使用するメカニズムです。現用インターフェイスに障害が発生した場合、保護インターフェイスが即座にそのトラフィック負荷を引き継ぎます。設定に基づいて、2つの回線は同じルータで終端できます。保護メカニズムには、双方向接続による 1+1 アーキテクチャが含まれています。ブリッジングとは、ユーザデータを現用インターフェイスと保護インターフェイスの両方に送信することを意味します。非ブリッジングの場合は、現用インターフェイスだけにユーザデータが送信されません。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「[1+1 SR-APS Without Bridging の機能情報](#)」(P.14) を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム サポートおよび Cisco ソフトウェア イメージ サポートに関する情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「[1+1 SR-APS Without Bridging の前提条件](#)」(P.2)
- 「[1+1 SR-APS Without Bridging の制約事項](#)」(P.2)
- 「[1+1 SR-APS Without Bridging に関する情報](#)」(P.2)
- 「[1+1 SR-APS Without Bridging の設定方法](#)」(P.3)

- 「1+1 SR-APS Without Bridging の設定例」 (P.10)
- 「その他の参考資料」 (P.12)
- 「1+1 SR-APS Without Bridging の機能情報」 (P.14)

1+1 SR-APS Without Bridging の前提条件

インターフェイスの IP アドレスとともに、最初に現用インターフェイスを設定します。この設定により、APS の設定中に保護インターフェイスがアクティブ回線になるのを防止します。保護インターフェイスが誤って最初に設定され、アクティブになった場合は、**shut** または **no shut** コマンドを使用して現用インターフェイスをアクティブにすることができます。

1+1 SR-APS Without Bridging の制約事項

- 保護インターフェイスと現用インターフェイスは、まったく同じに設定する必要があります。2 つのインターフェイスの設定が異なっても、警告メッセージは表示されません。
- 保護インターフェイスと現用インターフェイスの設定が同じでない場合、APS ペア（保護インターフェイスと現用インターフェイス）の動作は予測できません。
- Online Insertion and Removal (OIR; 活性挿抜) 時、または Shared Port Adapter (SPA; 共有ポートアダプタ) や Carrier Card (CC; キャリアカード) の破損時には、50 ミリ秒以内の APS スイッチオーバーはサポートされません。
- APS の切り替えが Route Processor (RP; ルート プロセッサ) または Forwarding Plane (FP; フォワーディングプレーン) の High Availability (HA; ハイ アベイラビリティ) と同時に行われる場合は、50 ミリ秒以内である必要はありません。

1+1 SR-APS Without Bridging に関する情報

1+1 SR-APS Without Bridging 機能を設定するには、次の概念を理解しておく必要があります。

- 「1+1 SR-APS Without Bridging」 (P.2)

1+1 SR-APS Without Bridging

APS 機能は、リンクの冗長性を提供し、回線障害の発生時に POS 回線のスイッチオーバーを可能にします。この機能は多くの場合、SONET 装置を通信装置に接続する際に必要となります。SR-APS 機能では、保護インターフェイスと現用インターフェイスの両方が同じルータ上にある必要があります。

APS は、現用 POS インターフェイスのバックアップとして、SONET ネットワーク内の保護 POS インターフェイスを使用するメカニズムです。現用インターフェイスに障害が発生した場合、保護インターフェイスが即座にそのトラフィック負荷を引き継ぎます。設定に基づいて、2 つの回線は同じルータで終端できます。保護メカニズムには、双方向接続による 1+1 アーキテクチャが含まれています。

1+1 アーキテクチャでは、1 つの現用インターフェイス（回線）と 1 つの保護インターフェイスが存在し、送信側からのペイロードと同じペイロードが両方の受信側に送信されます。受信側は、使用する必要があるインターフェイスを決定します。SONET フレームの Line OverHead (LOH; ライン オーバー

ヘッド) のバイト (K1 および K2) は、ステータスとアクションを示します。あるインターフェイスがダウンした場合、または K1/K2 バイトが変化した場合、APS は通常のインターフェイス設定メッセージを使用して保護インターフェイスを起動します。

ブリッジングとは、ユーザ データを現用インターフェイスと保護インターフェイスの両方に送信することを意味します。非ブリッジングの場合は、現用インターフェイスにのみユーザ データが送信されます。現用インターフェイスがアクティブ インターフェイスになるように設定する必要があります。Cisco ASR 1000 シリーズ ルータ (ASR1000) は、非ブリッジングだけをサポートしています。

非ブリッジングでは、ASR1000 (APS をイネーブルに設定) はリモート エンドに信号を送信します。ASR1000 は (K1/K2 バイト以外の) 信号を現用インターフェイスにのみ送信し、保護インターフェイスには送信しません。K1/K2 バイトは保護インターフェイスにのみ送信されます。一方、ASR1000 をブリッジング APS 対応のデバイスに接続することは可能です。つまり、デバイスは ASR1000 の現用インターフェイスと保護インターフェイスの両方に同じ信号を送信します。ただし ASR1000 は (K1/K2 バイト以外の) ユーザ データをデバイスの現用インターフェイスにのみ送信します。K1/K2 バイトは保護インターフェイスに送信されます。

SR-APS では、現用インターフェイスと保護インターフェイスの間で Protect Group Protocol (PGP) が使用されます。保護インターフェイスの APS 設定には、PGP を使用して現用インターフェイスと通信するために、同一ルータ上のループバック インターフェイスの IP アドレスを含める必要があります。PGP を使用することで、チャネル信号の劣化または損失、または手動介入が発生した場合に、POS インターフェイスを切り替えることができます。双方向モードでは、受信チャネルと送信チャネルがペアとして切り替えられます。

双方向 APS では、ローカル接続とリモート接続が、データ パス用に選択される入力インターフェイスをネゴシエートします。出力インターフェイスのトラフィックは、現用インターフェイスと保護インターフェイスのいずれにも送信されません。

1+1 SR-APS Without Bridging の設定方法

ここでは、次の手順について説明します。

- 「APS 現用および保護インターフェイスの設定」(P.3) (必須)
- 「その他の APS オプションの設定」(P.5) (任意)
- 「APS のモニタリングと保守」(P.6) (任意)
- 「SONET アラーム レポートの設定」(P.7) (任意)
- 「APS スイッチオーバー トリガーとしての LAIS の設定」(P.8) (任意)

APS 現用および保護インターフェイスの設定

APS 現用および保護インターフェイスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface pos slot/sub-slot/port**
4. **aps working circuit-number**
5. **aps protect circuit-number ip-address**

6. end
7. show controllers pos
8. show interfaces pos
9. show aps

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface pos slot/sub-slot/port 例： Router(config)# interface pos 2/0/0	現用インターフェイスとして設定される POS インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	aps working circuit-number 例： Router(config-if)# aps working 1	インターフェイスを現用インターフェイスとして設定します。
ステップ 5	aps protect circuit-number ip-address 例： Router(config-if)# aps protect 1 209.165.200.224	インターフェイスを保護インターフェイスとして設定します。現用インターフェイスを含む同一ルータ上のループバック インターフェイスの IP アドレスを指定します。
ステップ 6	end 例： Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	show controllers pos 例： Router(config)# show controllers pos	インターフェイスが正しく設定されていることを確認できるように、POS コントローラに関する情報を表示します。
ステップ 8	show interfaces pos 例： Router(config)# show interfaces pos	設定されたインターフェイスに関する情報を表示します。
ステップ 9	show aps 例： Router(config)# show aps	設定されたルータの APS に関する情報を表示します。

その他の APS オプションの設定

その他の APS オプションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface pos slot/sub-slot/port**
4. **aps force circuit-number**
5. **aps group group-number**
6. **aps lockout circuit-number**
7. **aps manual circuit-number**
8. **aps revert minutes**
9. **end**

手順の詳細

	コマンド	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface pos slot/sub-slot/port 例： Router(config)# interface pos 2/0/0	現用インターフェイスとして設定される POS インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	aps force circuit-number 例： Router(config-if)# aps force 1	(任意) 同等またはより高いプライオリティの要求が有効である場合を除いて、指定した回線を手動で保護インターフェイスに切り替えます。
ステップ 5	aps group group-number 例： Router(config-if)# aps group 20	(任意) ルータ上で複数の保護インターフェイスまたは現用インターフェイス グループをサポートできるようにします。
ステップ 6	aps lockout circuit-number 例： Router(config-if)# aps lockout 1	(任意) 現用インターフェイスが保護インターフェイスに切り替わるのを防止します。

	コマンド	目的
ステップ7	<code>aps manual circuit-number</code> 例： Router(config-if)# <code>aps manual 1</code>	(任意) 同等またはより高いプライオリティの要求が有効である場合を除いて、回線を手動で保護インターフェイスに切り替えます。
ステップ8	<code>aps revert minutes</code> 例： Router(config-if)# <code>aps revert 3</code>	(任意) 現用インターフェイスが使用可能になったあと、保護インターフェイスから現用インターフェイスへの自動スイッチオーバーをイネーブルにします。
ステップ9	<code>end</code> 例： Router(config-if)# <code>end</code>	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

APS のモニタリングと保守

APS のモニタおよび保守を行うには、次の作業を実行します。

手順の概要

1. `enable`
2. `configure terminal`
3. `show controllers pos`
4. `show interfaces pos`
5. `show aps`

手順の詳細

	コマンド	目的
ステップ1	<code>enable</code> 例： Router> <code>enable</code>	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ2	<code>configure terminal</code> 例： Router# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>show controllers pos</code> 例： Router(config)# <code>show controllers pos</code>	インターフェイスが正しく設定されていることを確認できるように、POS コントローラに関する情報を表示します。

コマンド	目的
ステップ4 <code>show interfaces pos</code> 例： <code>Router(config)# show interfaces pos</code>	設定されたインターフェイスに関する情報を表示します。
ステップ5 <code>show aps</code> 例： <code>Router(config)# show aps</code>	設定されたルータの APS に関する情報を表示します。

SONET アラーム レポートの設定

レポートされる SONET アラームのしきい値およびタイプを設定するには、次のコマンドのいずれかを使用します。ここに挙げるコマンドは必須ではありません。現在の Bit Error Rate (BER; ビットエラー レート) しきい値の設定を表示、または SONET アラームのレポートを表示するには、**show controllers pos** コマンドを使用します。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface pos slot/sub-slot/port`
4. `pos threshold {b1-tca | b2-tca | b3-tca | sd-ber | sf-ber} rate`
5. `pos report {b1-tca | b2-tca | b3-tca | lais | lrdi | pais | plop | prdi | rdool | sd-ber | sf-ber | slof | slos}`
6. `end`

手順の詳細

コマンド	目的
ステップ1 <code>enable</code> 例： <code>Router> enable</code>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • プロンプトが表示されたら、パスワードを入力します。
ステップ2 <code>configure terminal</code> 例： <code>Router# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ3 <code>interface pos slot/sub-slot/port</code> 例： <code>Router(config)# interface pos 2/0/0</code>	現用インターフェイスとして設定される POS インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ4	<pre>pos threshold {b1-tca b2-tca b3-tca sd-ber sf-ber} rate</pre> <p>例： Router(config-if)# pos threshold b1-tca 4</p>	(任意) Signal Failure (SF; 信号障害)、Signal Degrade (SD; 信号劣化)、または Threshold Crossing Alarm (TCA; しきい値超過アラーム) の BER しきい値を設定します。
ステップ5	<pre>pos report {b1-tca b2-tca b3-tca lais lrldi pais plop prdi rdool sd-ber sf-ber slof slo}</pre> <p>例： Router(config-if)# pos report b2-tca</p>	(任意) 選択した SONET アラームのレポートをイネーブルにします。
ステップ6	<pre>end</pre> <p>例： Router(config-if)# end</p>	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

APS スイッチオーバー トリガーとしての LAIS の設定

現用インターフェイスを管理シャットダウン状態にすると、**pos ais-shut** の有無にかかわらずスイッチオーバーが発生します。インターフェイスで **pos ais-shut** をイネーブルにすると、インターフェイスは管理シャットダウンのリモート エンドに Line Alarm Indicate Signal (LAIS; 回線アラーム検出信号) アラームを送信します。LAIS アラームにより、スイッチオーバーが少し速くなります。**carrier-delay msec milliseconds** コマンドおよび **ppp timeout retry seconds [milliseconds]** コマンドも、APS スイッチオーバーの発生を高速化するために使用されます。

carrier-delay msec milliseconds コマンドは、POS インターフェイスのリンク ダウン イベント処理を遅らせます。たとえば、キャリア遅延を 50 ミリ秒 (ms) に設定した場合、ルータは 50 ミリ秒以内にクリアされるすべてのリンク ダウン イベントを無視します。リンクがダウンした場合、50 ミリ秒間は APS スイッチオーバーが発生しません。デフォルトのキャリア遅延は 2 秒で、APS スイッチオーバーはリンクのダウン後 2 秒間発生しません。したがって、スイッチオーバーを高速化するためにキャリア遅延が 50 ミリ秒に設定されます。

ppp timeout retry seconds [milliseconds] コマンドは、指定した時間に PPP リトライ タイムアウトを設定します。たとえば、タイムアウト リトライを 200 ミリ秒に設定した場合、ルータは APS スイッチオーバーによる信号停止を検出後、200 ミリ秒で PPP リンクを確立しようと試みます。デフォルトのリトライ タイムアウトである 2 秒を使用した場合は、APS スイッチオーバーの 2 秒後に PPP リンクが確立されます。したがって、スイッチオーバーを高速化するために PPP タイムアウト リトライが 50 ミリ秒に設定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface pos slot/sub-slot/port**
4. **pos ais-shut**
5. **carrier-delay msec milliseconds**
6. **ppp timeout retry seconds [milliseconds]**
7. **end**

手順の詳細

コマンド	目的
ステップ1 <code>enable</code> 例: <code>Router> enable</code>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • プロンプトが表示されたら、パスワードを入力します。
ステップ2 <code>configure terminal</code> 例: <code>Router# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ3 <code>interface pos slot/sub-slot/port</code> 例: <code>Router(config)# interface pos 2/0/0</code>	現用インターフェイスとして設定される POS インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4 <code>pos ais-shut</code> 例: <code>Router(config-if)# pos ais-shut</code>	インターフェイスの管理シャットダウン時に Line Alarm Indicate Signal (LAIS; 回線アラーム検出信号) アラームを送信します。
ステップ5 <code>carrier-delay msec milliseconds</code> 例: <code>Router(config-if)# carrier-delay msec 50</code>	POS インターフェイスのリンク ダウン イベント処理を遅らせて、APS スイッチオーバーを高速化します。
ステップ6 <code>ppp timeout retry seconds [milliseconds]</code> 例: <code>Router(config-if)# ppp timeout retry 0 200</code>	PPP ネゴシエーション時の応答に対する最大待ち時間を設定して、APS スイッチオーバーを高速化します。
ステップ7 <code>end</code> 例: <code>Router(config-if)# end</code>	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

1+1 SR-APS Without Bridging の設定例

ここでは、次の設定例について説明します。

- 「例：1+1 SR-APS Without Bridging の設定」(P.10)

例：1+1 SR-APS Without Bridging の設定

次の例では、1+1 SR-APS の設定シーケンスを示します。

```
interface loopback 1
ip address 1.1.1.1 255.255.255.0
interface pos 2/0/0
  aps group 1
  aps working 1
  pos ais-shut
end

interface pos 3/0/0
  aps group 1
  aps protect 1 1.1.1.1
  pos ais-shut
end
```

次の例では、現用インターフェイスを持つルータに設定された APS の出力例を示します。

Router# **show aps**

```
POS2/1/1 APS Group 0: protect channel 0 (Inactive)
  Working channel 1 at 10.0.1.1 (Enabled)
  bidirectional, revertive (60 seconds)
  PGP timers (default): hello time=1; hold time=3
    hello fail revert time=120
  SONET framing; SONET APS signalling by default
  Received K1K2: 0x00 0x05
    No Request (Null)
  Transmitted K1K2: 0x00 0x05
    No Request (Null)
  Remote APS configuration: (null)

POS2/1/0 APS Group 0: working channel 1 (Active)
  Protect at 10.0.1.1
  PGP timers (from protect): hello time=1; hold time=3
  SONET framing
  Remote APS configuration: (null)
```

次の例では、POS コントローラの表示を示します。

Router# **show controller pos 2/1/0**

```
POS2/1/0
SECTION
  LOF = 0          LOS   = 1          BIP (B1) = 0
LINE
  AIS = 2          RDI   = 2          FEBE = 14          BIP (B2) = 0
PATH
  AIS = 2          RDI   = 2          FEBE = 4          BIP (B3) = 6
  PLM = 0          UNEQ  = 0          TIM  = 0          TIU   = 0
  LOP = 1          NEWPTR = 2        PSE  = 0          NSE   = 0

Active Defects: None
```

```

Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

Framing: SONET
APS
  working (active)
    COAPS = 13          PSBF = 0
    State: PSBF_state = False
    Rx(K1/K2): 00/00   Tx(K1/K2): 00/00
    Rx Synchronization Status S1 = 00
    S1S0 = 00, C2 = CF
    Remote aps status (none); Reflected local aps status (none)
CLOCK RECOVERY
  RDOOL = 0
  State: RDOOL_state = False
PATH TRACE BUFFER: STABLE
  Remote hostname : SPA-APS2
  Remote interface: POS2/2/0
  Remote IP addr  : 10.1.1.1
  Remote Rx(K1/K2): 00/00   Tx(K1/K2): 00/00

BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Clock source: internal

```

次の例では、POS インターフェイスの設定情報および統計情報を示します。

```

Router# show interface pos 2/1/0

POS2/1/0 is up, line protocol is up (APS working - active)
  Hardware is SPA-4XOC12-POS
  Internet address is 10.1.1.2/24
  MTU 4470 bytes, BW 155000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Scramble disabled
  Last input 00:00:02, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    102477 packets input, 2459448 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 4 giants, 0 throttles 0 parity
    4 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    102486 packets output, 2459934 bytes, 0 underruns
    0 output errors, 0 applique, 2 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    10 carrier transitions

```

その他の参考資料

関連資料

関連項目	参照先
APS コマンド	『 Cisco IOS Interface and Hardware Component Command Reference 』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	<p>選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
なし	

シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none">• テクニカル サポートを受ける• ソフトウェアをダウンロードする• セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける• ツールおよびリソースへアクセスする<ul style="list-style-type: none">– Product Alert の受信登録– Field Notice の受信登録– Bug Toolkit を使用した既知の問題の検索• Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する• トレーニング リソースへアクセスする• TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する <p>この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

1+1 SR-APS Without Bridging の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。



(注)

表 1 には、一連のソフトウェア リリースのうち、特定の機能のサポートが初めて導入されたソフトウェア リリースだけを示します。その機能は、特に明記されていない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1 1+1 SR-APS Without Bridging の機能情報

機能名	リリース	機能情報
1+1 SR-APS Without Bridging	Cisco IOS XE Release 3.1S	この機能では、1+1 Single Router APS Without Bridging のサポートが提供されます。 この機能で導入または変更されたコマンドはありません。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Copyright © 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010–2011, シスコシステムズ合同会社.
All rights reserved.